

~~**SENSITIVE BUT UNCLASSIFIED**~~

**United States Department of State
and the Broadcasting Board of Governors
Office of Inspector General**

Report of Inspection

Inspection of Bureau of Diplomatic Security/ Countermeasures Directorate

Report Number ISP-I-11-06, November 2010

~~**IMPORTANT NOTICE**~~

~~This report is intended solely for the official use of the Department of State or the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies or organizations, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code, 5 U.S.C. 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.~~

~~**SENSITIVE BUT UNCLASSIFIED**~~

PURPOSE, SCOPE AND METHODOLOGY OF THE INSPECTION

This inspection was conducted in accordance with the Quality Standards for Inspections, as issued by the President's Council on Integrity and Efficiency, and the Inspector's Handbook, as issued by the Office of Inspector General for the U.S. Department of State (Department) and the Broadcasting Board of Governors (BBG).

PURPOSE

The Office of Inspections provides the Secretary of State, the Chairman of the BBG, and Congress with systematic and independent evaluations of the operations of the Department and the BBG. Inspections cover three broad areas, consistent with Section 209 of the Foreign Service Act of 1980:

- **Policy Implementation:** whether policy goals and objectives are being effectively achieved; whether U.S. interests are being accurately and effectively represented; and whether all elements of an office or mission are being adequately coordinated.
- **Resource Management:** whether resources are being used and managed with maximum efficiency, effectiveness, and economy and whether financial transactions and accounts are properly conducted, maintained, and reported.
- **Management Controls:** whether the administration of activities and operations meets the requirements of applicable laws and regulations; whether internal management controls have been instituted to ensure quality of performance and reduce the likelihood of mismanagement; whether instance of fraud, waste, or abuse exist; and whether adequate steps for detection, correction, and prevention have been taken.

METHODOLOGY

In conducting this inspection, the inspectors: reviewed pertinent records; as appropriate, circulated, reviewed, and compiled the results of survey instruments; conducted on-site interviews; and reviewed the substance of the report and its findings and recommendations with offices, individuals, organizations, and activities affected by this review.



**United States Department of State
and the Broadcasting Board of Governors**

Office of Inspector General

PREFACE

This report was prepared by the Office of Inspector General (OIG) pursuant to the Inspector General Act of 1978, as amended, and Section 209 of the Foreign Service Act of 1980, as amended. It is one of a series of audit, inspection, investigative, and special reports prepared by OIG periodically as part of its responsibility to promote effective management, accountability and positive change in the Department of State and the Broadcasting Board of Governors.

This report is the result of an assessment of the strengths and weaknesses of the office, post, or function under review. It is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and a review of applicable documents.

The recommendations therein have been developed on the basis of the best knowledge available to the OIG and, as appropriate, have been discussed in draft with those responsible for implementation. It is my hope that these recommendations will result in more effective, efficient, and/or economical operations.

I express my appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in black ink, appearing to read "H. W. Geisel".

Harold W. Geisel
Deputy Inspector General

TABLE OF CONTENTS

| | |
|--|----|
| KEY JUDGMENTS | 1 |
| CONTEXT | 3 |
| EXECUTIVE DIRECTION | 5 |
| PROGRAM IMPLEMENTATION | 7 |
| Office of Security Technology Program Property | 7 |
| Office of Physical Security Programs | 11 |
| Office of Diplomatic Courier Services | 18 |
| Information Resource Management | 22 |
| RESOURCE MANAGEMENT | 25 |
| Human Resources | 25 |
| LIST OF RECOMMENDATIONS | 29 |
| INFORMAL RECOMMENDATIONS | 31 |
| PRINCIPAL OFFICIALS | 33 |
| ABBREVIATIONS | 35 |

CONTEXT

The multifaceted mission of DS/C is to oversee the development and implementation of Overseas Security Policy Board security standards and Department of State (Department) policies associated with the physical and technical security of U.S. diplomatic missions worldwide; to ensure construction and transit security at construction projects; to provide defensive equipment to protect American lives and property from acts of violence; and to provide secure, expeditious delivery of classified, sensitive, and other approved material among diplomatic missions, the Department, and other customers.

The Office of Security Technology (DS/C/ST) provides technical security countermeasures. Its divisions are facility security engineering (DS/ST/FSE), security technology operations (DS/ST/STO), and countermeasures programs (DS/ST/CMP). The branches in each of these divisions assess emerging technologies; define security requirements; develop, implement, and maintain technical security policies; and work with the Director of National Intelligence's Center for Security Evaluation to implement risk management techniques and manage programs and resources. DS/ST/FSE works with OBO on cross-cutting issues and the Capital Security Construction Program's Top 80 list.

The Office of Physical Security Programs (DS/C/PSP) oversees the development and implementation of Overseas Security Policy Board standards and serves as a member of the board. It is responsible for accrediting and certifying that new construction and major renovations are adequate and appropriate. It also oversees construction at domestic Department facilities. Further, it provides defensive equipment and armored vehicles.

The U.S. Diplomatic Courier Service (DS/C/DC) provides safe, secure, and expeditious delivery of classified, sensitive, and other approved material to and between U.S. diplomatic missions, the Department, and other customers it serves. The work is primarily dedicated to supporting overseas requirements for classified mail and equipment. DS/C/DC has regional divisions in Frankfurt, Miami, and Bangkok, and courier hub offices in Dakar, Manama, Pretoria, Sao Paulo, Seoul, and Sydney.

With more than 1,200 employees in domestic locations and overseas, DS/C represents a significant portion of the Bureau of Diplomatic Security. Domestically, it has more than 280 full-time equivalent positions, including Foreign Service and Civil Service employees; about 100 personal services contract employees and 335 third party contract employees; and 15 when-actually-employed staff members. Overseas, according to staffing data provided by the DS/C front office, there are about 265 full-time equivalent positions, 135 locally employed staff, and 114 U. S. Navy Seabees. The FY 2010 funding, exclusive of salaries, was \$214 million, including \$53,000 for the front office, \$136 million for security technology programs, \$65 million for physical security programs, and \$12 million for couriers.

EXECUTIVE DIRECTION

At the time of the inspection, the deputy assistant secretary (DAS) had been in place for about 8 months. He had been acting DAS for a short period and was director of PSP before that. Working in close collaboration with the Assistant Secretary and principal DAS of the Bureau of Diplomatic Security (DS), he is a hands-on, collegial manager. He holds weekly meetings with his divisions' senior staff, a weekly meeting with the Center for Security Evaluations, and one-on-one meetings with each of his divisions' leaders. The tone of these meetings is open and collaborative. Members of the DAS's front office and the DS/C staff ensure that he is made aware of pertinent and critical issues; thus, decisions are made expeditiously.

DS/C staff credit the DAS for the directorate's success and ongoing achievements. Other agencies' representatives and Department leaders gave the directorate high marks, noting that the present working relationship is very good. For example, OBO stated that DS/C is extremely cooperative in its role of overseeing and expediting construction and accrediting new or upgraded diplomatic facilities abroad. In New York City, the DAS helped to resolve the final issues regarding physical and technical security requirements for the new U.S. Mission to the United Nations building. The customers of DS/C/DC also praise the service they receive. The armored vehicles program is so effective that other agencies regularly use its services to meet their armored vehicle needs. The Department's regional executive officers unanimously expressed satisfaction with DS/C's service and cooperation in meeting their embassies' needs.

DS/C focuses appropriately on the most dangerous areas where there are diplomatic facilities. The April 2010 attack on Consulate General Peshawar, Pakistan, resulted in no deaths and only minimal damage—in good part because DS/C had researched, tested, and implemented up-to-date countermeasures technology.

The DAS and his staff travel frequently to Pakistan and Afghanistan to assess the facilities under construction there. Looking forward, DS/C is devoting focused effort to prepare for the time when the U.S. military will withdraw from Iraq, leaving the security burden to the Department, with particular emphasis on DS/C's role. Many

of the Department's overseas facilities were designed for temporary or short-time use, but they now have been occupied for longer periods, without replacement; the DAS has instructed the directorate to make sure that the next generation of temporary offices adheres more closely to security standards.

The DAS worked to extend the security management system enterprise to cover about 240 posts. The network has been upgraded and allows for improved situational awareness and data collection. According to the unclassified information on the DS/C Web site, the program provides information to the DS command center provides advanced communications and information technology, and tracks and reports threats and security incidents directed against U.S. interests. The program also feeds video, alarm, and sensor information from overseas facilities to the command center and elsewhere.

PROGRAM IMPLEMENTATION

OFFICE OF SECURITY TECHNOLOGY PROGRAM PROPERTY

Currently, DS/C/ST's primary management control tool is DS's computerized maintenance management system and a corollary software system known as Maximo, which works to provide lifecycle management information by listing equipment location, inventory number, and creation or accession date. This information yields a lifecycle (replacement) date, which facilitates budgeting for and timely replacement of equipment.

DS/C/ST uses a lifecycle documentation framework that starts with a technology needs assessment, then a technology decision memorandum, followed by evaluation, testing, and integration. All of these steps precede an equipment deployment decision and associated training plan.

For the past three years, DS/C/ST has been integrating the two computerized management systems mentioned above into everyday office operations. Now, with the integration almost completed, the computerized maintenance management system provides management with a number of reports that provide status information for DS/C/ST activities.

DS/C/ST gets high marks from its customers. The OIG team has been assured that the equipment it provides to posts has been successful in providing countermeasures, thwarting potential assaults, and responding well to actual attacks. The directorate points with pride to Sanaá, Yemen, and Peshawar, Pakistan, where its countermeasures programs successfully thwarted attacks.

A 2009 OIG report¹ stated that there were serious deficiencies in the management and oversight of property stored at a contractor-operated warehouse, and the OIG inspectors had recommended that the Bureau of Diplomatic Security convert its various inventory systems to the Department's Integrated Logistics Management

¹Report of Inspection, The Executive Office, Bureau of Diplomatic Security, Report Number ISP-I-09-16, April 2009

System. The current OIG team was assured that the shortcomings have been thoroughly addressed and resolved. The goal of getting equipment to posts quickly and in a timely fashion has been reasonably successful as the new inventory systems are providing better controls.

Priorities guide that process, with the focus on new equipment and high risk posts. According to some DS/C/ST budget figures, if more lifecycle funding had been made available, vehicles at engineering service facilities might have been replaced; additional technical surveillance countermeasures monitoring equipment could have been replaced, etc. DS/C/ST estimated the total cost for equipment that had reached the end of its lifecycle and had not been replaced at about \$6 million. However, the effect of not replacing the equipment at the end of its lifecycle was not significant, because the equipment was still functional. Given that DS/C decides the priorities for its entire budget, lifecycle funding could be a priority if DS/C management felt it was important in certain instances.

Countermeasures Program

DS/C/ST's director told the OIG team that the countermeasures program is unique, because most of its work is not directed exclusively at counterterrorism; therefore, it does not get the same attention as the other divisions. Many people believe that the countermeasures program is a Cold War spy-era holdover and therefore not so important. Although the director believes this perception and the lack of previous management support may have diminished morale and lessened funding, the OIG inspectors found high morale and no indications that funding was not adequate.

The countermeasures program manages the Department's domestic and overseas technical countermeasures programs. It integrates other federal agencies' countermeasures programs and serves as the Department's point of contact for technical countermeasures operations in the intelligence community. The division has four branches: emanations countermeasures; technical analysis; technology evaluation; and technical surveillance and countermeasures. Some of the branches' responsibilities include:

- developing, implementing, and maintaining technical security countermeasure policies; assessing the vulnerabilities of emerging technologies; defining security requirements and specifications for major security systems and equipment, as required by federal law and regulations;

- working with the Center for Security Evaluation to evaluate and implement a risk management program designed to identify locations where cost effective countermeasures can be used to protect classified and sensitive information;
- performing TEMPEST² countermeasures reviews to determine TEMPEST countermeasures requirements; performing TEMPEST inspections worldwide to ensure compliance with national emanations standards;
- managing certified shielded enclosures, built-in conference rooms, and secure conference room programs; providing preventative maintenance for and certifying shielded enclosures and conference rooms worldwide;
- managing the security risk evaluation and approval process responsible for introducing new technology and equipment into overseas facilities; and
- providing centralized support for technical surveillance countermeasures equipment, including procurement, inventory, development, and certification of all technical surveillance countermeasures components.

The director indicated that technical surveillance countermeasures equipment is continually evolving in sophistication; therefore, the countermeasures program is always attempting to implement new technology and provide training. The life span for the more sophisticated technical security equipment is often shorter than the life span for older equipment, but the sophisticated equipment is well maintained. Further, vendors provide maintenance manuals and help desk support. The vendors also provide the training on new equipment at domestic facilities. Given that security engineering staff is widely dispersed around the world, some staff do not get the opportunity to take vendor-provided training, however, they are given extensive on-the-job training from their vendor-trained colleagues.

Facilities Security Engineering

The facilities security engineering division (DS/ST/FSE) enhances posts' technical security capability by recognizing and reducing security risks through perimeter security technical equipment and technical security upgrades. The division has technical security responsibilities for about 200 domestic facilities. The division tracks its success and failures through customer surveys. A new FAM, under review at the present time, provides standards and requirements that will receive additional review.

² TEMPEST equipment (or TEMPEST-approved equipment): Equipment designed or modified to suppress compromising signals. It is approved at the national level for U.S. classified applications after undergoing testing.

The division's branches are: domestic management and engineering; field support; project management and engineering; and technology development. DS/ST/FSE is also responsible for the global identification program, the personal identity verification program, and the security technology assistance center. It accomplishes its missions by:

- planning and implementing DS-funded overseas technical security upgrade projects;
- furnishing logistics management and maintenance of technical security equipment for overseas operations;
- delivering technical assistance to field personnel;
- providing liaison services across DS/C/PSP and DS/C/ST, and OBO; and
- providing staff to the DS command center for oversight of the security management system enterprise, in support of the command center's watch officers.

This division is the directorate's "meat and potatoes." DS/ST/FSE is responsible for technical security hardware from beginning to end, with lifecycle management responsibility for over \$25 million worth of equipment. Supply and logistics were outsourced four years ago. Posts order directly from the vendor, and the company is paid when the items are received at the overseas location. Posts have commented that logistics operations are running more smoothly than in the past. The supply distribution system uses classified and unclassified pouches. The director of the courier service meets frequently with DS/ST/FSE leadership to ensure prompt delivery of technical security equipment. (See reference to OIG report cited above.)

DS/ST/FSE has been working very hard to respond to the wars in Iraq and Afghanistan. New technologies are being considered for those zones and others to ensure that adequate security is implemented.

Security Technology Operations

The mission of the security technology operations division (DS/ST/STO) is to enhance security worldwide, by reducing exposure to threats and fostering a safe working environment. To meet present and future security challenges, it provides the most advanced equipment that meets budget and funding limits. In the past several years, DS/C/ST's budget had been enhanced by supplemental funding related to efforts in Iraq and Afghanistan. DS/C has been making decisions based on its prioritization of the programs it wishes to fund.

The division is broken down into the U.S. Navy Support Unit (Seabees) and three branches: overseas support, quality assurance liaison, and security engineering services.

The Seabees unit, with its diverse set of skills that are different from those of the security engineering officers, is called upon to respond to various technical problems. There are 114 Seabees now working with the Department, each of whom serves 2- to 3-year tours. The Department reimburses the U.S. Navy for their services. The Seabees are deployed at a Department annex and at engineering service centers overseas.

The overseas support branch is DS/ST/STO's largest branch. The Department reduced DS/ST/STO's domestic staffing to support requirements and needs in Iraq and Afghanistan based on the full-time equivalent positions that are available. The overseas support branch oversees the security engineering officers, security technical specialists, and regional security technicians who are assigned directly to posts or to overseas security engineering centers or security engineering offices. To provide additional overseas support, the overseas branch has established technical security offices in a number of countries and regions.

DS/ST/STO's quality assurance liaison branch provides quality assurance for the technical security systems that are designed and deployed for overseas operations. This branch provides contract oversight, conducts onsite reviews, and develops and compiles the Department's technical security systems standards in 1 FAM, which defines all security technology positions, and 12 FAM 700, and in the uncompleted Technical Security Handbook, which contains guidance for field-based personnel responsible for technical security programs and systems.

The security engineering services branch is responsible for providing a technically secure environment for the Secretary of State. It also administers the operational countermeasures program for the Department's nearly 200 domestic facilities.

OFFICE OF PHYSICAL SECURITY PROGRAMS

The Office of Physical Security Programs (DS/C/PSP) oversees the development and implementation of Overseas Security Policy Board standards associated with physical security, construction security, transit security, secure procurement, defensive equipment, and armored vehicles. DS/C/PSP is also responsible for designing and implementing security standards for the Department's domestic facilities.

The office has a well motivated work force and communications are excellent. The majority of responses to OIG's personal and workplace and quality of life questionnaires were above average. Complaints were few, and most of those related to reportedly subpar services from DS's executive office and the Bureau of Information Resource Management (IRM).

DS/C/PSP encompasses three divisions: facilities security (DS/PSP/FSD), physical security (DS/PSP/PSD), and defensive equipment and armored vehicles (DS/PSP/DEAV).

Facilities Security Division

The facilities security division (DS/PSP/FSD) provides oversight for the physical security protection of the Department's approximately 200 domestic facilities. These include annexes, passport agencies, DS field and resident agent offices, the DS Office of Foreign Missions, and dispatch offices. Morale within FSD is very high, with highly qualified personnel serving as branch chiefs and desk officers. The division develops security standards that are derived from the *Foreign Affairs Manual* and *Foreign Affairs Handbook*, the U.S. Department of Justice vulnerability assessments, and the Interagency Security Committee. This division maintains an extensive spreadsheet that tracks physical security problems and fixes, including inoperable turnstiles and badges that do not work, etc.

DS/C has implemented a domestic security monitoring system called Alarm Net, which is similar to the overseas monitoring system, the security management system enterprise network. Alarm Net provides DS's domestic command center, at the Harry S Truman building, with domestic alarm monitoring capability. This system also indicates where security systems at various domestic locations are not working, where doors are open, and where expired badges are being used.

DS/PSP/FSD is comprised of three branches: security standards and compliance, domestic buildings, and projects coordination.

The Department downplayed domestic security until terrorist events and security breaches within U.S. borders increased concerns about domestic security. The work of past office directors dramatically increased DS/PSP/FSD's profile and funding. There are currently 80 to 100 ongoing domestic security projects; the renovation of the Harry S Truman building and the new U.S. Mission to the United Nations building are the largest. FSD is also the Department's point of contact with the Interagency Security Committee, an organization that develops domestic security standards for U.S. Government-owned buildings and leased office space.

For many years, security for domestic facilities was published as guidance only. There was no compliance enforcement, and Department bureaus could ignore or reject recommended security upgrades, at their discretion. However, with domestic standards due to become formal policy in the *Foreign Affairs Manual*, compliance will soon be mandatory. The cost estimate for domestic building projects must include the cost for integrating required security upgrades.

Physical Security Division

The physical security division (DS/PSP/PSD) provides physical security oversight for new diplomatic facilities that meet OBO's standard embassy designs. DS/PSP/PSD also ensures that major renovation projects are also implemented in conformance to Overseas Security Policy Board standards. DS/PSP/PSD conducts the Accreditation Inspection and the Construction Security Certification Programs in compliance with the Foreign Relations Authorization Act for FY 1988 and 1989 (PL 100-204) and 12 FAM 360. This mandate requires security for new construction and major renovations of overseas diplomatic facilities, for the protection of classified information, national security related activities, and personnel. DS/PSP/PSD tests and certifies new forced-entry, ballistic-resistant, and antiram equipment that the Department acquires for the protection of embassies and consulates.

DS/PSP/PSD consists of the research and development section and three branches: new office buildings; project coordination; and certification, accreditation, and transit security.

The new office building group provides oversight for facilities that are designed to meet standard embassy designs and ensures that renovations meet standards. The project and coordination branch acts as intermediary between posts and OBO in physical security project development. It ensures compliance to standards, and if compliance is not possible, the office informs the post that a waiver or exception will be needed. The office processes all requests for exceptions to the physical security standards that the Secretary or Assistant Secretary for Diplomatic Security must sign. The transit security group ensures that security materials for new buildings are properly and securely transported via the courier service. Desk officers also inspect design plans for upgrade projects for proper application of physical security standards in the selection, design, construction, and modification of diplomatic facilities.

To educate regional security officers and post security officers about current physical security applications for diplomatic facilities, the project coordination branch presents a training module in the DS Training Center's basic regional security officer course, in-service refresher course, and post security officer course. The curriculum is continuously revised. The program teaches:

- how to find information regarding required physical security standards for projects;
- how posts obtain security funding for projects; and
- how posts obtain waivers and exceptions to physical security standards that cannot be met.

The project coordination branch also provides instructors to the Foreign Service Institute and the DS Antiterrorism Assistance program, as needed.

The research and development section was created as a result of the East Africa bombings in 1998. Structural engineers proficient in blast mitigation develop cost effective countermeasures aimed at countering the effects of violent acts of terrorism. Through the International Physical Security Forum, for which DS/PSP/PSD is the lead office, research is shared with other federal agencies and friendly foreign governments, regarding antiram, forced-entry/ballistic-resistant equipment, and blast mitigation techniques. The 15-member group, made up of Austria, Australia, Belgium, Canada, Denmark, France, Germany, Israel, Netherlands, Norway, Singapore, Spain, Switzerland, United Kingdom and the United States, shares technology information.

Capital Security Construction Program

One of the division's primary responsibilities is to provide OBO with an annual security risk and vulnerability matrix for all overseas locations. OBO uses this matrix and other vital information to determine the priority for constructing new embassy and other diplomatic facilities. This compilation for the Capital Security Construction Program is also known as the Top 80. To standardize the procedures and to eliminate subjective input, in 2004, DS and OBO adopted a software decision tool called Expert Choice. The software ranks embassies and consulates according to threat levels of political violence and terrorism. It is weighted with other risk/vulnerability considerations that include chemical/biological attack, seismic and blast construction, building construction and façade type (concrete, masonry/block, wood frame and glass), and setback. Once the ranking order is established and posts are removed from the Top 80 list as construction contracts are awarded, the list is amended. Priorities may change, based on management decisions regarding possible alternatives to new embassy construction at a particular post.

Defensive Equipment Armored Vehicles Division

The defensive equipment armored vehicles division (DS/PSP/DEAV) has two branches: the armored vehicle branch, and the defensive equipment branch. DS/PSP/DEAV's mission is to provide armored vehicles and special protective equipment to protect chiefs of mission, principal officers, and other mission personnel from threats of terrorism, war, and civil disturbances. The director and branch chiefs are DS federal agents; the staff, made up of Civil Service and contract personnel, is extremely knowledgeable and have years of experience in armored vehicle procurement and logistics. Morale is high, and communications within and outside of the division are excellent. DS/PSP/DEAV personnel operate in a close-knit, cohesive atmosphere.

Armored vehicles are built under strict, classified design standards to protect against different categories of ballistics fire and (to a degree) blasts from improvised explosive devices. DS/PSP/DEAV has witnessed a rapid expansion of its mission and responsibilities, with the catalyst being the East Africa embassy bombings in 1998 and U.S. engagement in Iraq and Afghanistan. Worldwide inventory grew from 115 armored vehicles assigned to chiefs of mission at high and critical threat posts, to more than 3,000 armored vehicles. Today, there are more than 900 armored vehicles in Iraq alone. The DS/PSP/DEAV budget has increased to \$40 million for base worldwide procurement, with a \$200 million supplemental for Iraq and Afghanistan.

The Department of State, U.S. Secret Service, Defense Intelligence Agency, and Central Intelligence Agency are the only four federal agencies that have a formal armored vehicle procurement program. Other federal law enforcement, intelligence, and security agencies use DS/PSP/DEAV to acquire their armored vehicles. The Department receives one percent of the cost of each vehicle for providing this service.

The Bureau of Administration, Office of Logistics Management is responsible for procuring the initial vehicles, identified as base units, which include sedans, vans, sport utility vehicles, and Mine Resistant Ambush Protected vehicles for combat zones. After the initial procurement, DS/PSP/DEAV is responsible for armoring the vehicles and transporting them to their embarkation port at Baltimore, Maryland. Base units are sent to one of seven approved manufacturers for armoring. Under certain circumstances, DS/PSP/DEAV also provides BMW and Mercedes sedans that are built fully-armored at their respective plants.

The receiving embassy or other diplomatic facility is responsible for shipping costs, maintenance and repair, and disposal. An exception is that DS will pay for repair and replacement of the vehicle's armor components, including windshields and windows that delaminate or crack.

The OIG team notes two areas of concern: the proper disposal of armored vehicles and the Buy American Act, which hinders operations.

Armored Vehicle Disposal

Through previous onsite embassy inspections, OIG has determined that, in many instances, armored vehicles that exceeded their five-year life span (two years for vehicles in Iraq and Afghanistan) and that embassies determined could not be repaired, have not been destroyed per 12 FAM 388 requirements. DS/PSP/DEAV agrees that this is an ongoing problem.

Approved disposal methods include burial at sea, explosive demolition, burning, crushing, or burial on U.S. Government-controlled land. However, burial at sea will no longer be an approved method for vehicle disposal, because environmental groups object to this procedure. Proper disposal has not been accomplished due to a lack of embassy funds, lack of means for destruction, a post's apathy or indifference, or any combination of these reasons. Keeping idle, out-of-service armored vehicles warehoused at embassies can lead to inventory discrepancies among the Office of Logistics Management, DS, and the embassy. These differences affect the security and integrity of the armored vehicle program.

Before 2003, this situation was not a problem. Older armored vehicles could be sold if the armor was stripped from the vehicle. This is no longer an option because the newer generation of armored vehicles' armor is an integral part of the vehicle and cannot be detached.

DS/PSP/DEAV's direct involvement in the disposal process of armored vehicles at embassies will ensure that 12 FAM 388 requirements are met, and there will be fewer inconsistencies in vehicle inventories including embassies' International Cooperative Administrative Support Services inventories; more accurate projections for future armored vehicle replacement budgets; and better oversight of the security features of armored vehicles, by precluding posts' unauthorized disposal of vehicles.

Recommendation 1: The Bureau of Diplomatic Security, in coordination with the Bureau of Administration, Office of Logistics Management, should establish a system whereby posts shall dispose of armored vehicles in accordance with prescribed disposal requirements. (Action: DS, in coordination with A)

Buy America Act

Under the Buy American Act, 41 U.S.C. § 10a, DS/PSP/DEAV is generally required to purchase American-manufactured vehicles, whenever possible, or the Office of Logistics Management must register an exception. The exceptions that the Office of Logistics Management has sought include obtaining right-hand drive vehicles, where required, and diesel fuel-fired vehicles for locations where that is the only fuel available.

Although DS/PSP/DEAV works within the law to meet the spirit and word of the Buy America Act, its requirements can create difficulties with regard to maintenance and operational security. For instance, General Motors (GM) products (Chevrolet Suburban and Cadillac) are sent to third world countries that do not have GM repair parts or local mechanics trained in servicing GM vehicles. Some embassies have experienced significant downtime when GM parts must be ordered and shipped from the United States. With regard to suburban utility vehicles, Toyota Land Cruisers are better suited for these areas, because Toyota has a worldwide distribution network and can, thus, be easily serviced.

American-made vehicles also can pose an operational security threat because they are conspicuous. For example, embassy-owned, white Chevrolet Suburban armored vehicles have been shot at in Colombia. Also, in areas of high or critical terrorist or political violence threat, armored Cadillacs are a concern to some regional security officers because these vehicles clearly transport American diplomats and have visible American labels and markings.

Best Practice: Regional Maintenance Technician Program

Issue: Armored vehicles require additional and specialized maintenance because of their weight and short life cycle.

Response: DS/PSP/DEAV created a Regional Maintenance Technician Training Program.

Results: U.S. Embassy Cairo first adopted the training program. GM-certified mechanics trained embassy mechanics, in Cairo and at DS/PSP/DEAV, on the complex maintenance requirements for GM's armored vehicles. Embassy Cairo's mechanics, in turn, have trained locally employed mechanics at embassies in the Bureau of Near Eastern Affairs and the Bureau of African Affairs regions. As a result, the GM vehicles are better maintained.

OFFICE OF DIPLOMATIC COURIER SERVICES

The U.S. Diplomatic Courier Service (DS/C/DC) provides secure and expeditious delivery of classified, sensitive, and other approved material to and among U.S. diplomatic missions, their customers, and the Department. Couriers ensure the inviolability of diplomatic pouches delivered across international borders, in accordance with the Omnibus Diplomatic Security and Anti-Terrorism Act (1986), the Vienna Convention on Diplomatic Relations (1972), the Vienna Convention on Consular Relations (1969), and 12 FAM 100.

DS/C/DC supports Department components and numerous federal agencies. The goal is to escort classified materials in a rapid, reliable, and cost effective manner, while meeting security requirements. DS/C/DC couriers are located around the globe to facilitate expeditious service. Sites of DS/C/DC posts and support routes are adjusted, as required, to ensure the best outcomes related to diplomatic requirements, world events, airline and other transportation schedules, etc. At present, DS/C/DC's front office is in Rosslyn, Virginia (SA-20). The classified pouching facility, the domestic focal point for classified shipments, is colocated with the Washington regional diplomatic courier division. Regional courier divisions also are located in Miami, Florida; Frankfurt, Germany; and Bangkok, Thailand. Courier hub offices are located in Dakar, Senegal; Manama, Bahrain; Pretoria, South Africa; Sao Paulo, Brazil; Seoul, South Korea; and Sydney, Australia.

Regular courier pouch delivery service is provided on a weekly, biweekly, or monthly schedule. The frequency of service is determined primarily by the supported diplomatic post's needs. A regularly updated schedule shows the frequency of deliveries, but does not show the specific days that deliveries are scheduled. For example, the schedule shows that deliveries from Washington to Abidjan are made every two weeks, but it does not indicate precisely what week in any given month the delivery will occur. According to the schedule, deliveries are made twice a week to Frankfurt and every four weeks to Baku, but the actual weeks of the deliveries are not specified. Courier pouch customers have asked for more specific information on when deliveries will occur. The OIG team made an informal recommendation that more specific information be included in the delivery schedules.

In conjunction with other federal agencies, couriers regularly use military support flights to augment other transportation. These flights are arduous, sometimes lasting 20 days and visiting 14 or 15 countries. Couriers might use sleeping bags and eat microwaveable food during these flights, and spend few nights in hotels. One courier told the OIG team, "You do what you got to do." This corps of professional messengers is an innovative, security-centric logistics organization.

Some couriers take a "jump seat" flight on a commercial cargo delivery plane and spend 30 hours en route. In another scenario, based on the pouch or the cargo, a courier will sit in a commercial aircraft's business class seat, because of the requirement to get off the plane quickly to secure the cargo. (Note: couriers do not travel business class when returning to the division or hub office, unless they are returning with classified material.) Couriers are met at the airport by an embassy representative, who will escort the courier and the pouch or cargo to a classified storage facility.

There is also a category of service called Specials. If a customer requires an urgent or special delivery, the courier service provides the special accommodation, but the customer must pay for couriers' expenses, fares, per diem, etc., and \$7.70 per pound for the freight. Staff at the Washington Regional Courier Division ensures that reimbursement is collected.

Clearly the couriers' travel is demanding and often conducted with little advance notice. Getting Department and other customers' classified information and materials where they need to be (even the next day) has become very difficult. Given the couriers' attitude and work ethic, the team found it easy to understand why, to date, there have been no reported failures to deliver. Delays are rare, but may occur under unusual circumstances—for example, the recent ash plume resulting from volcano activity in Iceland.

Electronic Government Travel

In keeping with the E-Government Act of 2002, 44 U.S.C. § 101, the Department uses the E2 Solutions electronic travel application. E2 Solutions provides online access for travel reservations, for a fee, and online assistance, for an additional fee. There also are additional fees for telephone assistance, which is commonly needed for overseas travel. Despite the Department's requirement to use E2 Solutions, the U.S. General Services Administration's Office of Inspector General issued a report indicating that customers do not consider E2 Solutions to be user-friendly or intuitive.

Until recently, the couriers were using the travel system (whether E2 Solutions or the Department's earlier travel system, Travel Manager) in use at their respective posts; however, DS/C now requires all overseas and domestic couriers to use the domestic E2 Solutions. DS/C also requires that business class authorizations be signed at the DAS level, in Washington, DC. Both these decisions have put timely courier travel in a precarious state.

The OIG team conducted a survey of the ten courier divisions and hub offices. Some divisions have hired administrative assistants to process the couriers' E2 Solutions travel authorizations. However, doing so does not save money. As noted above, couriers sometimes must travel business class to oversee cargo and pouches and meet an embassy escort. Division and hub office courier directors noted that getting business class authorizations into E2 Solutions to authorize a ticket could take more than a week, given time differences and work days in Washington.

The decision to require all couriers to use the domestic E2 Solutions application stems from a concern that embassy financial management offices might erroneously use the courier travel budget. The OIG team heard of one instance some time ago, when a post had used the DS travel budget for lease payments, but the error was corrected. Moreover, the Department has developed and deployed financial management systems (for example, the Consolidated Overseas Accountability Support Toolkit) that would allow DS headquarters and division and hub managers to track funds.

For travel originating in Washington, DC, to ensure compliance with 41 C.F.R. 301-10, 41 C.F.R. 301-50, and 41 C.F.R. 301-73 all employees in the Washington metropolitan area must use the current Travel Management Center in Washington per 14 FAM 542 a. For travel originating outside the continental United States, all employees must use the current Travel Management Center under contract with the Department of State or other Foreign Affairs Agency, 14 FAM 542 b. (1), at that location.

DS has a mailbox for business class authorization requests. The logistics management section monitors the mailbox and routes the requests and itineraries to the DAS for signature. In an emergency or when the mailbox is not monitored, the courier requesting business class authorization must instead contact Carlson-Wagonlit's and the Department's travel director. Such authorizations take two to three days, at least, and in some cases obtaining them is impossible—for instance, when a courier must change his or her itinerary while on the tarmac in a distant location.

There are alternatives that could alleviate these difficulties, but they are not currently available. One courier budget officer suggested having the regional office sign the business class authorization and enter it into the E2 Solutions system. This process would be helpful for distant offices that do not have direct access to the domestic E2 Solutions system and also would address the concern about controlling the budget. It also shows the logic for having the division and hub officials sign the business class authorizations instead of sending them back to Washington for the DAS's signature as currently required by DS/C.

Another alternative for alleviating the lengthy process and budget concerns of authorizing business class travel might be the use of blanket authorizations. According to 14 FAM 567.2-2 (B), blanket or open authorization is prohibited for first or business class travel. Each premium travel trip must be authorized separately. Guidance in 14 FAM 520 outlines the requirements for travel authorizations and 14 FAM 523.2-2(D) a. and b. states that authorizing officials designated in 14 FAM 523.2-2 (A) and (B) may be authorized to approve first- and business-class air accommodations. Here again, blanket authorizations may obviate budget concerns—another reason that they are prohibited for business authorization. The OIG team notes that no business class authorization for a courier has ever been denied.

The clear solution to alleviating the lengthy process and budget concerns of authorizing business class travel is to return the funds to the missions where the couriers are posted, and have the supervisors who are knowledgeable about the couriers' travel sign the business class authorization.

Recommendation 2: The Bureau of Diplomatic Security should allocate funding for couriers' travel to the financial management systems at the missions where the couriers are posted and authorize these missions to initiate and complete travel authorizations and vouchers. (Action: DS)

Recommendation 3: The Bureau of Diplomatic Security should authorize courier division and hub office directors to sign premium class travel authorizations for couriers' travel, when needed. (Action: DS)

INFORMATION RESOURCE MANAGEMENT

Information management operations are a relatively fluid concept within DS/C; they are constantly evolving and innovating. Elements of the office of the chief technology officer (CTO) and IRM all have a hand in managing information technology (IT) assets operating in support of DS/C. They are simultaneously pushing towards greater consolidation of desktop support services and server hardware management under IRM, while individual offices are realizing greater specialization and functionality of their applications. This change is partly a natural evolution, and partly due to IRM's program to consolidate desktop services. Some fairly complicated relationships have arisen among DS/C, CTO, and IRM that are not adequately captured in the Department's Information Technology Asset Baseline (ITAB) systems inventory or associated documentation. Inadequately defined roles and responsibilities, coupled with an adjustment period after IT consolidation, have had some attendant negative effects on customer service.

IT functions supporting DS/C range from providing basic desktop connectivity for end users to installing a distributed network that spans the globe, to bringing real-time camera footage and other security information from posts overseas to the DS command center in Rosslyn, VA. IRM took over system administrator and helpdesk duties for OpenNet connectivity to the desktop in January 2009, when the IT consolidation program completed DS's transition from managing their own networks to being managed by IRM. However, DS retained considerable resources to manage specialized applications that support DS's mission. The majority of these resources reside within CTO under the office of the executive director. There is still further IT specialization within DS/C.

The Department's official inventory of IT applications, ITAB, identifies 24 active applications for DS/C; seven of them are major applications. However, the actual ownership and management of these applications is more complicated than ITAB would indicate. CTO actually manages many of these applications: the courier travel system, the technical security countermeasures system, and the visitor access control system. CTO had a role in the development of the identity management system, and its servers reside in CTO's data center, but DS/C personnel support the servers.

RESOURCE MANAGEMENT

HUMAN RESOURCES

Facilities Security Engineering

DS/ST/FSE's four branches employ about 300 staff members, including more than 200 third-party contractors. The division believes converting the third-party contractors to personal services contractors would provide better oversight and continuity. The OIG team did not analyze the implications of this assertion.

Security Technology Staffing Shortfalls

DS/C/ST is working to preclude staffing shortfalls through an aggressive recruiting and hiring campaign this year. It plans to hire 40 new security engineering officers, adding to its current level of nearly 180. This goal will provide more than enough staff for the jobs that open up through normal attrition and authorized new positions; it will allow DS/C/ST to staff to the authorized ceiling for the security engineering officer skill code. Likewise, DS/C/ST plans to recruit and hire 30 security technical specialists.

Facilities Security Division

The DS/PSP/FSD desk officers claim that the division's new emphasis on domestic security requirements has changed their positions and added new responsibilities. DS/PSP/FSD is currently rewriting the position description for its desk officers, to include the new domestic security responsibilities and requirements. Once it is rewritten, DS/PSP/FSD will send the job description to the DS human resource office, to determine whether the position description should be reclassified to a higher grade.

There has been a retention problem within DS/PSP/FSD, because the Civil Service desk officers are classified at the GS-12 level. Most employees are hesitant to leave DS/PSP/FSD and its cohesive working environment, but some have left to seek career advancement and increased pay. Desk officers in DS/PSP/FSD's sister divisions are graded at the GS-13 level. The DS/PSP/FSD desk officers believe that similar positions in other federal agencies are also at the GS-13 level. The division's efforts to rewrite the position description and submit for possible reclassification are appropriate steps.

Couriers

The courier service has 101 positions; approximately 93 are filled. The couriers' personnel deficit results from excursion tours to Iraq and Afghanistan and normal attrition. The director's new policy will limit the number of excursion tours to a maximum of five at any one time. Given the specialized nature of courier work, the Department has had a courier serving in a career development officer role within DS/C; however, this position will relocate to Bureau of Human Resources when the current incumbent is reassigned.

During the inspection, the OIG inspectors observed courier managers' efforts to interview potential candidates whose attributes would lead to successful careers. Courier managers structure the interviews to allow candidates to display creativity, commitment, and responsibility: key characteristics needed for this work. This year's recruiting goal is to hire nine new couriers. A rule of thumb is that about 10 percent of prospective candidates will be successful. Courier positions have been added to the hard-to-fill list. General schedule, Civil Service employees are invited and encouraged to bid on the hard-to-fill positions.

Courier Time in Class Limits

A courier reaching the time in class or "tic" limit (15 years of service, without promotion) is a problem for DS/C and the couriers. The OIG team notes that an individual may stay in the Foreign Service until the "tic" limit is reached. An experienced courier will likely have a proven track record and will have learned how to build networks of contacts with airport and airline officials and customs officers around the world. In early 2010, DS/C asked the Bureau of Human Resources to waive the "tic" limit. The Director General declined the request. DS/C has decided not to send a reclama in this regard. The OIG team found the Director General's reasoning based on sound logic and precedent.

Most couriers enjoy the challenges of courier life and understand that they may remain at the FS-04 level for their entire careers. Some couriers, however, aspire to be promoted. Others take excursion tours outside of the diplomatic security umbrella and work in public diplomacy, consular affairs, management, etc. These excursions allow them to increase their salaries and gain within-grade step increases. The courier service's management pyramid is steep, with most couriers at grades FS-04 and FS-03, numerous FS-02s, a few FS-01s and two Senior Foreign Service positions. Competition for the higher grades and more responsible positions is intense.

Contrary to 3 FAM 2638.2 a., which requires that each bureau's position descriptions shall undergo a formal maintenance review on a periodic basis, the position descriptions for the courier job series 2580 at the FS-04 and FS-03 levels have not been updated since 1987, nor have they been subject to reclassification criteria. Many things in the courier service have changed in the past 23 years. Air travel itself has changed, and the couriers now report to DS and not IRM. Further, the position descriptions do not reflect the need for an associate's degree or 60 hours of college level courses. These position descriptions must be reviewed and updated.

In its comments on the OIG draft report, the Director General's office noted that the position descriptions that require updating are identical to the FS-02 overseas courier positions that were updated in 2002. The Bureau of Human Resources stated that it will develop an up-to-date, standardized courier position description for worldwide use, using the standards in the FS-02 overseas position description discussed here.

Recommendation 5: The Bureau of Diplomatic Security, in coordination with the Bureau of Human Resources, should review and update position descriptions for the U.S. Diplomatic Courier Service and reclassify them, if indicated. (Action: DS, in coordination with DGHR)

Courier Quality Manual

The courier service is developing a standard operating procedures manual. It is applying some ISO 9000³ quality system techniques for this project. The process has involved bringing couriers to Washington to participate in drafting the procedures and reviewing the outcomes. This is a laudable method for involving staff in the development and approval of standards. A few couriers told the OIG team that, although they would have preferred to work on their scheduled courier runs, they did find the process useful overall.

³ International Organization for Standardization 9000, a global quality management standard with a family of standards for quality management systems.

LIST OF RECOMMENDATIONS

- Recommendation 1:** The Bureau of Diplomatic Security, in coordination with the Bureau of Administration, Office of Logistics Management, should establish a system whereby posts shall dispose of armored vehicles in accordance with prescribed disposal requirements. (Action: DS, in coordination with A)
- Recommendation 2:** The Bureau of Diplomatic Security should allocate funding for couriers' travel to the financial management systems at the missions where the couriers are posted and authorize these missions to initiate and complete travel authorizations and vouchers. (Action: DS)
- Recommendation 3:** The Bureau of Diplomatic Security should authorize courier division and hub office directors to sign premium class travel authorizations for couriers' travel, when needed. (Action: DS)
- Recommendation 4:** The Bureau of Diplomatic Security should clearly define roles and responsibilities for managing software applications which the Diplomatic Security/Countermeasures directorate owns, and document those definitions as well as other required items in updates to the applications' entries in the Information Technology Asset Baseline. (Action: DS)
- Recommendation 5:** The Bureau of Diplomatic Security, in coordination with the Bureau of Human Resources, should review and update position descriptions for the U.S. Diplomatic Courier Service and reclassify them, if indicated. (Action: DS, in coordination with DGHR)

INFORMAL RECOMMENDATIONS

Informal recommendations cover operational matters not requiring action by organizations outside the inspected unit and/or the parent regional bureau. Informal recommendations will not be subject to the OIG compliance process. However, any subsequent OIG inspection or on-site compliance review will assess the mission's progress in implementing the informal recommendations.

DS/C/DC's customers would like more specific information regarding which days of the week or which weeks of the month classified mail and material will be shipped or delivered.

Informal Recommendation 1: The Bureau of Diplomatic Security should require that the U.S. Diplomatic Courier Service include specific information regarding which days of the week and which weeks of the month classified mail and material will be shipped or delivered.

PRINCIPAL OFFICIALS

| | Title | Arrival on Duty |
|-------------------------|---|------------------------|
| Gentry O. Smith | Deputy Assistant Secretary | October 2009 |
| Office Directors | | |
| Debra Glass | U.S. Diplomatic Courier Service | July 2008 |
| Wayne B. Ashbery | Office of Security Technology | August 2008 |
| Nancy C. Rolph | Office of Physical Security Programs | May 2010 |

ABBREVIATIONS

| | |
|-------------|--|
| A/LM | Bureau of Administration/Logistics Management |
| CTO | Chief technology officer |
| DAS | Deputy assistant secretary |
| DS/C | Bureau of Diplomatic Security/Countermeasures Directorate |
| DS/C/ST | Office of security technology |
| DS/ST/FSE | Facilities security engineering division |
| DS/ST/STO | Security technology operations |
| DS/ST/CMP | Countermeasures program division |
| DS/C/PSP | Office of physical security programs |
| DS/PSP/DEAV | Defensive equipment and armored vehicles |
| DS/PSP/FSD | Facility security division |
| DS/C/DC | U.S. diplomatic courier service |
| FAM | Foreign Affairs Manual |
| GSA | U.S. General Services Administration |
| ITAB | Information technology asset baseline |
| IRM | Bureau of Information Resource Management |
| IT | Information technology |
| OBO | Bureau of Overseas Buildings Operations |
| OIG | Office of Inspector General |
| Seabees | U.S. Navy Support Unit |

FRAUD, WASTE, ABUSE, OR MISMANAGEMENT
of Federal programs
and resources hurts everyone.

Call the Office of Inspector General
HOTLINE
202-647-3320
or 1-800-409-9926
or e-mail oighotline@state.gov
to report illegal or wasteful activities.

You may also write to
Office of Inspector General
U.S. Department of State
Post Office Box 9778
Arlington, VA 22219
Please visit our Web site at:
<http://oig.state.gov>

Cables to the Inspector General
should be slugged "OIG Channel"
to ensure confidentiality.