

**UNCLASSIFIED**

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

**Office of Audits**

**Audit of the Process To Request and Prioritize  
Physical Security-Related Activities at Overseas Posts**

**AUD-FM-14-17  
March 2014**

**~~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.~~

**UNCLASSIFIED**

**UNCLASSIFIED**



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

PREFACE

This report is being transmitted 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 as part of the Office of Inspector General's (OIG) responsibility to promote effective management, accountability, and positive change in the Department of State and the Broadcasting Board of Governors.

This report addresses the Department of State's process for requesting and prioritizing physical security-related activities at overseas posts. The report is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and a review of applicable documents.

OIG contracted with the independent public accountant Kearney & Company, P.C. (Kearney), to perform this audit. The contract required that Kearney perform its audit in accordance with guidance contained in the *Government Auditing Standards*, issued by the Comptroller General of the United States. Kearney's report is included.

Kearney identified four areas in which improvements could be made: developing and implementing standard policies and procedures for requesting funds and responding to posts' requests; collecting and maintaining a comprehensive list of all posts' physical security deficiencies; developing and implementing formal, standardized processes to prioritize physical security deficiencies; and better defining the roles of Department bureaus in these processes.

OIG evaluated the nature, extent, and timing of Kearney's work; monitored progress throughout the audit; reviewed Kearney's supporting documentation; evaluated key judgments; and performed other procedures as appropriate. The recommendations contained in the report were developed on the basis of the best knowledge available and were discussed in draft form with those individuals responsible for implementation. OIG's analysis of management's response to the recommendations has been incorporated into the report. OIG trusts that this report will result in more effective, efficient, and/or economical operations.

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

A handwritten signature in blue ink, appearing to read "Norman P. Brown".

Norman P. Brown  
Assistant Inspector General for Audits

**UNCLASSIFIED**



---

1701 Duke Street, Suite 500, Alexandria, VA 22314  
PH: 703.931.5600, FX: 703.931.3655, www.kearneyco.com

**Audit of the Process to Request and Prioritize Physical Security-Related Activities  
at Overseas Posts**

Office of Inspector General  
U.S. Department of State  
Washington, D.C.

Kearney & Company, P.C. (referred to as “we” in this letter), has performed an audit of the Department of State’s process to request and prioritize physical security-related activities at overseas posts. This performance audit, performed under Contract No. SAQMMA09D0002, was designed to meet the objective identified in the report section titled “Objective” and further defined in Appendix A, “Scope and Methodology,” of the report.

We conducted this performance audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. We communicated the results of our performance audit and the related findings and recommendations to the U.S. Department of State Office of Inspector General.

We appreciate the cooperation provided by personnel in Department offices during the audit.

A handwritten signature in blue ink that reads "Kearney &amp; Company". The signature is written in a cursive, flowing style.

Kearney & Company, P.C.  
Alexandria, Virginia  
March 6, 2014

---

**Acronyms**

BMIS	Buildings Management Integrated System
D&CP	Diplomatic and Consular Programs
DS	Bureau of Diplomatic Security
ESCM	Embassy, Security, Construction, and Maintenance
FE/BR	forced-entry/ballistic-resistant
FAH	<i>Foreign Affairs Handbook</i>
FAM	<i>Foreign Affairs Manual</i>
GAO	Government Accountability Office
GFMS	Global Financial Management System
NEC	new embassy compound
OBO	Bureau of Overseas Buildings Operations
OSPB	Overseas Security Policy Board
R&I	Repair and Improvement
RSO	Regional Security Officer
SECCA	Secure Embassy Construction and Counterterrorism Act of 1999
SERM	Security Equipment Responsibilities Matrix
SETL	Security Environment Threat List

**Table of Contents**

Executive Summary .....1

Background .....2

Objectives .....7

Audit Results.....8

    Finding A. Not All FY 2012 Physical Security Funding and Expenditures  
        Could Be Identified.....8

    Finding B. Processes To Request Funds for Physical Security Needs Could Be  
        Improved .....14

    Finding C. Department Did Not Have Information To Ensure Highest Priority  
        Physical Security Needs Were Funded .....23

List of Recommendations.....39

Appendices

    A. Scope and Methodology .....41

    B. Office of Inspector General – Physical-Security Funding Questionnaire .....45

    C. Bureau of Diplomatic Security Response .....53

    D. Bureau of Overseas Buildings Operations Response.....59

## **Executive Summary**

Overseas embassies have long been a target of attacks against the United States. The Department of State (Department) has more than 4,500 Government-owned or long-term leased residential and non-residential buildings in more than 280 overseas locations. Over 86,000 U.S. Government employees from more than 30 agencies work or live in these facilities. The protection of these employees is the responsibility of the Secretary of State. A fundamental component of protecting U.S. Government employees is maintaining sufficient physical security at overseas facilities. The Department's Bureau of Diplomatic Security (DS) and Bureau of Overseas Buildings Operations (OBO) share responsibility for ensuring that overseas facilities are safe and secure.

The objectives of this audit were to identify the FY 2012 funding mechanisms and amounts expended for physical security-related activities at Department-owned or Department-operated buildings overseas, determine whether the process for posts to request funds for physical security needs was easy to use and was understood by post security officials, and determine to what extent the Department used physical security funds for high-priority physical security needs at overseas posts during FY 2012. An external audit firm, Kearney & Company, P.C. (Kearney), acting on behalf of the Office of Inspector General (OIG), performed this audit.

Kearney found that the Department funded its FY 2012 physical security-related activities at overseas Department facilities primarily with funds received for Worldwide Security Upgrades, which amounted to \$775 million in FY 2012. The Department also received \$511.4 million from other agencies at overseas posts through cost-sharing agreements. In addition, the Department can use other appropriated funds for physical security needs, including funds received for Repair and Construction, Overseas Contingency Operations, and Worldwide Security Protection. Kearney identified physical security-related expenditures amounting to \$76.1 million for Worldwide Security Upgrades and \$48 million for Worldwide Security Protection. However, Kearney could not identify all FY 2012 Department expenditures for physical security-related activities overseas because the Department did not, and was not required to, discretely track all physical security expenditures.

Kearney found that the majority of post security officials responding to an OIG questionnaire believed that the processes to request funds for physical security-related needs were clear and easy to use. However, a significant number of post security officials believed the processes were unclear and difficult and expressed dissatisfaction with the timeliness or sufficiency of the responses received to their formal requests for physical security funding. The lack of understanding, perceived complexity of the processes, and dissatisfaction with responses to requests occurred because the Department had not developed standardized and documented policies and procedures for the processes to request funds for the majority of physical security-related needs. In addition, some post security officials indicated that the training provided for requesting funds was inadequate. The lack of standard documented policies and

## **UNCLASSIFIED**

procedures may result in post physical security needs not being addressed adequately or promptly.

Kearney could not determine the extent to which the Department used physical security funds for high-priority physical security needs at overseas posts during FY 2012 because the Department did not have complete information to prioritize post physical security needs. Specifically, DS did not have a comprehensive list of physical security deficiencies at all overseas posts, and neither DS nor OBO maintained a list of posts' FY 2012 requests for physical security funding and the disposition of those requests. In addition, neither DS nor OBO had formal processes to prioritize physical security needs; funding decisions were often made by one individual without documented standards and guidance. Further, DS and OBO did not have sufficient formal processes for coordinating the establishment of standards to help determine priorities and facilitate agreement on funding decisions. Nor had DS and OBO prepared a comprehensive long-range physical security plan that would help focus attention on critical needs. As a result, the Department could not ensure that the highest priority physical security-related needs at overseas posts were corrected and that posts' vulnerability to threats had been sufficiently reduced.

OIG made 10 recommendations to the Department related to developing and implementing standard policies and procedures for requesting funds and responding to posts' requests; collecting and maintaining a comprehensive list of all posts' physical security deficiencies; developing and implementing formal, standardized processes to prioritize physical security deficiencies; and better defining the roles and responsibilities of DS and OBO in these processes.

In its February 21, 2014, response (see Appendix C) to the draft report, DS concurred with the six recommendations addressed to it. In its February 19, 2014, response (see Appendix D) to the draft report, OBO concurred with three recommendations and did not concur with one recommendation addressed to it. Based on the comments received, OIG considers six of the 10 recommendations resolved, pending further action, and four recommendations unresolved. Management's responses and OIG's replies to those responses are included after each recommendation.

## **Background**

Embassies have long been the target of terrorist attacks against the United States overseas. Since 1993, there have been more than 20 attacks on U.S. diplomatic facilities, including the deadly car bombings in Tanzania and Kenya and the assault on the U.S. Mission in Benghazi, Libya. In August 2013, the threat of violence closed embassies in more than 10 countries for several days.

The Department has more than 4,500 Government-owned or long-term leased residential and non-residential buildings in more than 280 overseas locations. Over 86,000 U.S. Government employees from more than 30 agencies, including the Department, the U.S. Agency for International Development, the U.S. Department of Agriculture, and the Department of Commerce, work or live in these facilities. The protection of these employees is the

## **UNCLASSIFIED**

responsibility of the Secretary of State, as designated under the Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended.

A fundamental component of protecting U.S. Government employees is maintaining sufficient physical security<sup>1</sup> at overseas facilities. Physical security relates to physical measures—such as locked doors, perimeter fences, and other barriers—designed to protect facilities against access by unauthorized personnel (including attacks or intruders) and to safeguard personnel working in those facilities.

The average age of the Department’s overseas buildings exceeds 40 years. After the bombings of the U.S. embassies in 1998, the Department determined that “195 (80 percent) of its overseas facilities did not meet security standards and should be replaced.”<sup>2</sup> The Department reported that as of February 2012, it had completed 98 new facilities and was continuing to manage the ongoing construction or design of 43 facilities.

### **Physical Security-Related Legislation and Directives**

Over the past several decades, legislation and Presidential Directives have been implemented to help ensure the security of U.S. diplomatic facilities and U.S. personnel on official duty abroad. Those addressing physical security include the Omnibus Diplomatic Security and Antiterrorism Act of 1986, the Secure Embassy Construction and Counterterrorism Act of 1999 (SECCA), and Presidential Decision Directive/NSC-29.<sup>3</sup>

### **Omnibus Diplomatic Security and Antiterrorism Act of 1986**

Under Section 103(a) of the Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended, the Secretary of State must develop and implement, in consultation with the heads of other Federal agencies having personnel or missions abroad, policies and programs to provide for the security of U.S. Government operations of a diplomatic nature. These policies and programs must include, among other things, protection of all U.S. Government personnel on official duty abroad and their accompanying dependents, and establishment and operation of security functions at all U.S. Government missions abroad.<sup>4</sup> In addition, Section 301 of the Act requires the Secretary of State to convene an Accountability Review Board whenever there is serious injury, loss of life, or significant destruction of property at or related to a U.S. mission abroad.

---

<sup>1</sup> Closely related to physical security are the technical security safeguards required to protect certain facilities against intelligence collection or observation and procedural security to monitor and control physical access to facilities. Technical security involves measures such as metal detectors, x-ray machines, alarm systems, and bomb detection devices. Procedural security includes functions such as guard services, including marine guards.

<sup>2</sup> Congressional Budget Justification, Volume 1: Department of State Operations, Fiscal Year 2014, p. 393.

<sup>3</sup> *Security Policy Coordination*, Sept. 1994.

<sup>4</sup> The Secretary of State’s security responsibilities under this act do not apply to personnel or facilities under the command or control of a U.S. area military commander.

## UNCLASSIFIED

### **Secure Embassy Construction and Counterterrorism Act**

As a result of the 1998 attacks on the U.S. Embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, and the findings of the Accountability Review Boards convened as a result of those attacks, Congress passed SECCA. SECCA established certain statutory security requirements for U.S. diplomatic facilities. Specifically, SECCA required that the Department implement an emergency action plan for overseas posts and provide crisis management and other security-related training to Department personnel. In addition, SECCA required the Department, when it selected a site for any new U.S. diplomatic facility abroad, to collocate all U.S. Government personnel (except for those under the command of an area military commander) on the site and to ensure the buildings would be located at least 100 feet from the perimeter of the property.

### **Presidential Decision Directive/NSC-29**

In September 1994, the President transferred the functions of the Department's Overseas Security Policy Group to the Overseas Security Policy Board (OSPB) under the Assistant to the President for National Security Affairs. Chaired by the Assistant Secretary for DS, OSPB's members include directors of the foreign affairs and intelligence agencies represented at U.S. missions abroad. The OSPB is responsible for implementing requirements from the Omnibus Diplomatic Security and Antiterrorism Act and SECCA. The OSPB considers, develops, coordinates, and promotes policies, standards, and agreements on overseas security operations, programs, and projects that affect all U.S. Government agencies under the authority of a Chief of Mission.<sup>5</sup>

### **Department Bureaus and Offices With Security-Related Responsibilities**

Two Department bureaus share the responsibility for ensuring that the Department's overseas facilities are safe and secure: DS and OBO. The *Foreign Affairs Manual (FAM)* assigns DS the responsibility for ensuring that all new construction and major renovation design plans for buildings occupied by U.S. Government personnel comply with physical security standards established by SECCA and OSPB. The FAM assigns OBO the responsibility for incorporating physical security standards into the Department's building projects.<sup>6</sup>

### **Bureau of Diplomatic Security**

DS is responsible for providing a safe and secure environment for the conduct of U.S. foreign policy. DS also protects people, property, and information at the Department's missions worldwide. Every diplomatic mission in the world operates under a security program designed and maintained by DS.

---

<sup>5</sup> In each embassy, the Chief of Mission (usually an Ambassador) is responsible for executing U.S. foreign policy goals and for coordinating and managing all U.S. Government functions in the host country.

<sup>6</sup> 12 FAM 312, "Program Management Responsibilities."

## UNCLASSIFIED

Several offices within DS have responsibilities relating to physical security. Three offices with a significant level of involvement in physical security-related issues are the International Programs Directorate, the Office of Physical Security Programs, and the Threat Investigations and Analysis Directorate.

**International Programs Directorate/High Threat Programs Directorate.** The mission of these directorates is to provide leadership, support, and oversight of overseas security and law enforcement programs and related policy for the benefit of U.S. Government interests and the international community. The Directorate's Office of Regional Directors works to provide a safe and secure environment for the conduct of U.S. foreign policy through the oversight and support of Regional Security Offices worldwide. The Office of Regional Directors oversees the work of over 700 Regional Security Officers (RSO) at over 250 posts worldwide. RSOs serve as personal security advisors to the Chiefs of Mission on all security issues. RSOs are responsible for implementing and managing the Department's security and law enforcement programs abroad, and they identify security needs at posts and request funds for those needs. RSOs are residents at a particular post, but they may be responsible for other constituent posts within their respective region.

**Office of Physical Security Programs.** The Office of Physical Security Programs, which is under the purview of DS' Countermeasures Directorate, directs and develops worldwide physical security standards, policies, procedures, and guidelines. The Office's Physical Security Division provides oversight for new construction and major renovation projects abroad by ensuring conformance with OSPB-approved security standards.

Within the Physical Security Division, the Project Coordination Branch evaluates projects to ensure the proper application of physical security standards in the selection, design, construction, and modification of facilities abroad. The goal of the physical security program is to provide a safe and secure physical security environment at overseas diplomatic posts for the protection of U.S. Government personnel, facilities, and classified information under the authority of the Chief of Mission. The Project Coordination Branch uses OSPB-approved physical security standards and the statutory requirements contained in SECCA to achieve this goal. In addition, the New Office Building Branch provides project oversight to ensure that OSPB standards and SECCA requirements are implemented for new office buildings abroad.

Desk Officers in the Project Coordination Branch provide post management and RSOs with subject matter guidance and assistance. Desk Officers serve as the RSOs' points of contact for all physical security matters. Specifically, Desk Officers work closely with RSOs to ensure that RSOs' requests for physical security upgrades, waivers to SECCA, or exceptions to OSPB standards have merit, are accurate, are complete, are coordinated with OBO, and are tracked to conclusion.

**Threat Investigations and Analysis Directorate.** The Threat Investigations and Analysis Directorate is the primary DS organization that gathers, analyzes, investigates, and disseminates threat information to protect American interests worldwide. The Directorate's Office of Intelligence and Threat Analysis ensures that timely intelligence information is made available to DS officers, both domestically and overseas. The Office of Intelligence and Threat

## UNCLASSIFIED

Analysis also prepares annually the Security Environment Threat List (SETL), which categorizes threats at posts overseas into five threat categories with four levels—critical, high, medium, or low. The OSPB physical security standards applied to an overseas facility<sup>7</sup> correspond with the SETL threat level identified for that post.

### **Bureau of Overseas Buildings Operations**

OBO is responsible for incorporating physical security standards, including SECCA and OSPB requirements, into building projects. OBO formulates and directs the implementation of building policies to provide safe, secure, and functional facilities overseas. Additionally, OBO determines priorities for the design, construction, acquisition, maintenance, utilization, and sale of real properties.

OBO offices primarily involved with physical security-related issues include the Offices of Security Management, Operations, and Design and Engineering.

**Office of Security Management.** The Office of Security Management, within OBO's Construction, Facilities and Security Management Directorate, allocates the majority of the funding for physical security activities overseas. The Office of Security Management's mission is to ensure that all appropriate physical, technical, and procedural security measures are incorporated into every OBO project design for U.S. diplomatic facilities and to manage construction security programs that prevent physical and technical penetration and safeguard against mob violence and terrorist attacks. The Office of Security Management directs and monitors adherence to physical and technical security policies and standards for new office buildings, major renovations, and other upgrade projects for facilities abroad to protect against physical or technical compromise during construction.

Within the Office of Security Management's Security Operations Division, the Program Security Operations Branch is responsible for the compound security program. This branch controls the funding for physical security upgrades of existing facilities. The Program Security Operations Branch manages major upgrades, which are large-scale, multimillion-dollar projects. Minor projects, such as installing bollards and window grills, are usually managed by posts, with the Program Security Operations Branch providing design expertise and some assistance.

**Office of Operations.** The Office of Operations mission is to serve as overseas posts' point of contact within OBO. Within the Office of Operations, the Area Management Division provides customer service support to posts and acts as a liaison between posts and OBO, explaining posts' needs and limitations to OBO and OBO's policies and procedures to posts. Posts' Repair and Improvement (R&I) projects are managed by the Area Management Division.

**Office of Design and Engineering.** The Office of Design and Engineering, under OBO's Program Development, Coordination and Support Directorate, provides design, research, and technical assistance bureau-wide for all Department facilities overseas. The Office of Design and Engineering's Mechanical Engineering Division is responsible for establishing

---

<sup>7</sup> The OSPB standards provide requirements for eight types of facilities.

## UNCLASSIFIED

U.S. Government requirements for environmental security for overseas buildings, including chanceries, office annexes, consulates, residences, Marine Security Guard quarters, warehouses, and compound access control facilities. The Mechanical Engineering Division establishes criteria for plans, designs, specifications, and analysis in new construction and in retrofits and upgrades of existing overseas buildings.

### **Overseas Security Policy Board**

OSPB working groups develop security standards for threat categories. These standards cover topics that include Construction Security, Construction Materials and Transit Security Design and Construction of Controlled Access Areas, Physical Security of Unclassified Warehouses, and Physical Security.<sup>8</sup> For physical security, OSPB develops standards on items such as the height of perimeter walls, the number of minutes of protection for forced-entry/ballistic-resistant (FE/BR) doors, and the distance for building setbacks.

### **Prior OIG Reports**

OIG issued a number of audit and inspection reports related to physical security issues at overseas posts. For example, in its reports *Audit of Department of State Compliance With Physical/Procedures Security Standards at Selected High Threat Level Posts*<sup>9</sup> and *Audit of Department of State Compliance With Physical Security Standards at Selected Posts Within the Bureau of African Affairs*,<sup>10</sup> OIG's Office of Audits found that posts were not always in compliance with current physical security standards and that common physical and procedural security deficiencies occurred among the posts included in the audits. In addition, in the report *Review of Overseas Security Policy Board Exceptions and Security Embassy Construction and Counterterrorism Act of 1999 Waivers*,<sup>11</sup> the Office of Inspections reported that DS had not adequately tracked exceptions granted to the OSPB physical security standards or SECCA waivers of collocation and setback.

## **Objectives**

The objectives of this audit were the following:

- To identify the FY 2012 funding mechanisms and amounts expended for physical security-related activities at Department-owned or -operated buildings overseas.
- To determine whether the process for posts to request funds for physical security needs at Department-owned or -operated buildings was easy to use and was understood by post security officials.
- To determine to what extent the Department used physical security funds for high-priority physical security needs at overseas posts during FY 2012.

---

<sup>8</sup> 12 FAM 314, "OSPB Security Standards."

<sup>9</sup> AUD-SI-13-32, Jun. 2013.

<sup>10</sup> AUD-HCI-13-40, Sept. 2013.

<sup>11</sup> ISP-I-13-06, Jan. 2013.

**Audit Results**

**Finding A. Not All FY 2012 Physical Security Funding and Expenditures Could Be Identified**

The Department funded its FY 2012 physical security-related activities at Department-owned or -operated buildings overseas primarily with funds received for Worldwide Security Upgrades in the Department's Embassy, Security, Construction, and Maintenance (ESCM) appropriation. These funds, amounting to \$775 million in FY 2012, supported OBO's Compound Security Program, Capital Security Construction Program, and Maintenance Cost Sharing Program. The Department also received \$511.4 million for the Capital Security Construction and Maintenance Cost Sharing Programs from other agencies at overseas posts through cost-sharing agreements. In addition, although not provided specifically for physical security, other funds may have been used for physical security needs in FY 2012, including funds received by OBO for Repair and Construction and Overseas Contingency Operations, as well as funds received by DS for Worldwide Security Protection.

Kearney could not identify all Department expenditures for physical security-related activities overseas because the Department did not, and was not required to, discretely track all physical security expenditures. The Department used various accounting codes to classify and account for its financial transactions. For example, function codes<sup>12</sup> were used to show the purpose of and to account for expenditures and program costs. The Department had established specific physical security-related function codes for Compound Security Program expenditures and other function codes for non-residential and residential physical security expenditures. However, not all physical security-related activities had discrete function codes. For example, OBO expended approximately \$938 million of Worldwide Security Upgrades funds in FY 2012, but only \$76.1 million of that amount, which was expended through the Compound Security Program, was recorded with physical security-related function codes and could be directly attributed to physical security activities.<sup>13</sup> (The methodology used to identify physical security-related transactions is described in Appendix A.) OBO expenditures from other Worldwide Security Upgrades programs, as well as expenditures from Repair and Construction and Overseas Contingency Operations funds, were recorded with non-physical security-related function codes and could not be directly attributed to physical security activities. In addition to the Compound Security Program expenditures of \$76.1 million, Kearney identified DS expenditures amounting to approximately \$48 million from Worldwide Security Protection funds for non-residential physical security.

---

<sup>12</sup> 4 FAH-1 H-500, "Function Classification Structure."

<sup>13</sup> Kearney did not test expenditures as part of this audit. Although Kearney could not directly attribute all Worldwide Security Upgrades expenditures to physical security activities based on the accounting codes used, nothing came to Kearney's attention within the limited scope of its analysis of expenditures that would indicate the expenditures were not appropriate.

## **Worldwide Security Upgrades**

The Department's FY 2012 ESCM appropriation contained \$775 million in funding for worldwide security upgrades, acquisition, and construction. This funding supported three OBO Programs: Compound Security, Capital Security Construction, and Maintenance Cost Sharing. In addition, other agencies provided a total of \$511.4 million for the Capital Security Construction and Maintenance Cost Sharing Programs.

OBO expended approximately \$938 million of Worldwide Security Upgrades funds in FY 2012. However, only \$76.1 million of that amount, which was expended for the Compound Security Program, could be directly attributed to physical security activities. Kearney could not identify the physical security expenditures for the Capital Security Construction and Maintenance Cost Sharing Programs by the function codes used.

### **Compound Security Program**

The Department received \$85 million in FY 2012 for the Compound Security Program. This program funded physical security upgrades at long-term leased and Government-owned facilities, including comprehensive security upgrade projects, major FE/BR resistant door and window replacement projects, chemical/biological projects, emergency egress projects, and security upgrades for soft targets. The program also funded the design and construction of compound access controls, replacement of shatter-resistant window film, replacement of active and passive vehicle barriers, and other physical security measures.

During FY 2012, OBO expended approximately \$76.1 million of Compound Security Program funds specifically for physical security-related projects. Approximately 44 percent, or \$33.3 million, of the expenditures were associated with comprehensive major compound security upgrades. For example, OBO expended funds for newly initiated comprehensive physical security upgrade projects at four posts and for over 20 projects that had been initiated in prior years. An additional 19 percent of the funds, or \$14.5 million, were spent for the installation or lifecycle replacement of major FE/BR doors and windows, including new projects at 10 posts, nearly a dozen projects that were initiated in prior years, and the planning and design of future projects for five posts.

In addition to the major compound physical security upgrades and FE/BR projects, OBO expended approximately \$2.4 million for physical security-related projects, including one major emergency egress project, in response to riots and attacks that occurred at some posts. OBO also expended about \$7.3 million for minor physical security upgrade projects, primarily related to the improvement of perimeter security, such as the construction of mantraps and gates and upgrades to perimeter walls and fences, at dozens of posts. Further, expenditures of approximately \$7.1 million for environmental security included the installation of off-compound mail screening facilities at 26 posts. All FY 2012 Compound Security Program expenditures by function code are summarized in Table 1.

**UNCLASSIFIED**

**Table 1. FY 2012 Compound Security Program Expenditures**

<b>Function Code</b>	<b>Description</b>	<b>Amount</b>
7941	Minor Physical Security Upgrades	\$7,269,196
7943	Major FE/BR Doors and Windows	14,514,437
7944	Environmental Security	7,054,265
7945	Major Compound Physical Security Upgrades	33,301,229
7946	Minor FE/BR Doors and Windows	4,669,274
7947	Emergency Fire and Egress	2,389,973
794X	Other	6,890,508
<b>Total</b>		<b>\$76,088,882</b>

Source: Prepared by Kearney based on its analysis of FY 2012 expense transactions in the Department's financial accounting system.

**Capital Security Construction Program**

The Department received \$579.2 million in FY 2012 to fund the Capital Security Construction Program. In addition, other agencies with overseas staff under Chief of Mission authority contributed \$429.1 million to the Capital Security Construction Program through the Capital Security Cost Sharing Program.<sup>14</sup> This funding, totaling \$1 billion in FY 2012, supported the planning, design, and construction of new embassy compounds (NEC) and other capital projects to replace existing facilities.

During FY 2012, OBO expended \$820 million of Capital Security Construction Program funds. These funds were used to complete projects at nine overseas posts, including Kyiv, Ukraine; Monrovia, Liberia; and Mumbai, India. The funds were also used to manage the ongoing design and construction of 43 facilities, including NECs and other capital projects at Cotonou, Benin; Jakarta, Indonesia; Jeddah, Saudi Arabia; Taipei, Taiwan; and Mbabane, Swaziland.

Construction expenditures amounted to approximately \$616 million and accounted for 75 percent of the total expenditures. Other significant expenditures were for project supervision (about \$42.7 million, or 5 percent), the acquisition of unimproved land (about \$39.3 million, or 5 percent), and onsite security at construction projects (about \$30.6 million, or 4 percent). FY 2012 program expenditures by function code are summarized in Table 2.

---

<sup>14</sup> The Capital Security Cost Sharing Program requires that all affected agencies at overseas posts pay a proportionate share toward the construction of secure facilities. Other agencies' shares are based upon their total number of existing and projected authorized positions overseas.

**UNCLASSIFIED**

**Table 2. FY 2012 Capital Security Construction Program Expenditures**

<b>Function Code</b>	<b>Description</b>	<b>Amount</b>
7110	Unimproved Land	\$39,293,476
7111	Design/Development	16,528,185
7112	Construction	616,249,866
7113	Site Maintenance and Development Plan	8,885,265
713X	Furnishings	18,002,215
7141	Project Supervision Capital Projects	42,661,309
7142	Construction Security Site Operations	30,621,695
7143	Construction Surveillance/Guards	18,596,348
7144	Other Construction Security Program	3,257,902
7531	Planning & Development Program Support	24,602,703
7541	Real Estate Program Costs	1,337,708
<b>Total</b>		<b>\$820,036,672</b>

Source: Prepared by Kearney based on its analysis of FY 2012 expense transactions in the Department's financial accounting system.

Kearney was unable to determine the amount of Capital Security Construction Program funds spent specifically for physical security-related items by the function codes used. However, the Department considers all Capital Security Construction Program expenditures to be related to physical security because these funds were used only if the requirement for new construction was driven primarily by security concerns<sup>15</sup> and the facilities are built to meet SECCA standards.

### **Maintenance Cost Sharing Program**

The Department received \$110.8 million in FY 2012 for the Maintenance Cost Sharing Program. In addition, other agencies contributed \$82.2 million to the Maintenance Cost Sharing Program through the Capital Security Cost Sharing Program.<sup>16</sup> Although provided for worldwide security upgrades, the use of these funds is not limited to physical security-related items. This funding, totaling \$193 million in FY 2012, was used for the maintenance and rehabilitation of non-residential properties that were shared by multiple agencies at post. The Maintenance Cost Sharing Program funds major rehabilitation projects as well as routine facility maintenance and repair and preventive maintenance contracts. Major rehabilitation projects include upgrades to fire and life safety systems, heating and air conditioning systems, electrical systems, and physical and technical security items. Routine maintenance and repair includes repairs of a minor nature, such as fixing broken pipes, painting, and purchasing supplies in bulk.

OBO expended approximately \$15.7 million of Maintenance Cost Sharing Program funds in FY 2012, which was the first year of the Maintenance Cost Sharing Program. The majority of expenditures for FY 2012, \$10.7 million, were for routine maintenance and repair. OBO also expended Maintenance Cost Sharing Program funds for four major rehabilitation projects at

---

<sup>15</sup> The Department receives separate funding for the construction of new overseas facilities if the requirement is primarily for other than security reasons.

<sup>16</sup> The Capital Security Cost Sharing Program was expanded in FY 2012 to include the Maintenance Cost Sharing Program.

**UNCLASSIFIED**

Budapest, Hungary; Frankfurt, Germany; Vilnius, Lithuania; and Wellington, New Zealand. FY 2012 Maintenance Cost Sharing Program expenditures by function code are summarized in Table 3.

**Table 3. FY 2012 Maintenance Cost Sharing Program Expenditures**

Function Code	Description	Amount
7901	Post Routine Maintenance and Repair	\$10,708,100
7904	Facility Rehabilitation and Support Systems	2,077,835
7905	Environmental Security Protection Systems Program	1,728,012
791X	Major Rehabilitation Design/Construction/ Supervision/Security	1,162,578
<b>Total</b>		<b>\$15,676,525</b>

Source: Prepared by Kearney based on its analysis of FY 2012 expense transactions in the Department's financial accounting system.

Kearney was unable to determine the amount of Maintenance Cost Sharing Program expenditures for physical security because the physical security-related expenditures were not discretely tracked by the Department. All post routine maintenance and repairs are recorded to the same function code. In addition, when a major rehabilitation project is scheduled at a post that is also scheduled to receive a physical security upgrade, the physical security upgrade is performed as part of the major rehabilitation project to avoid developing two separate plans for the projects. Because the physical security component was included as part of the overall project, the physical security expenditures could not be identified separately.

**Miscellaneous Worldwide Security Upgrades Expenditures**

In addition to the expenditures for the three Worldwide Security Upgrades programs, Kearney identified expenditures of approximately \$26.9 million for other items. Kearney was unable to determine whether any of these expenditures were for physical security-related items based on the function codes used.<sup>17</sup> These additional expenditures by function code are summarized in Table 4.

**Table 4. FY 2012 Other Expenditures**

Function Code	Description	Amount
6134	Procurement Services - ICASS	\$20,542,097
7663	Maintenance Tech Support Program	6,279,567
768X/Blank	Miscellaneous	66,437
<b>Total</b>		<b>\$26,888,101</b>

Source: Prepared by Kearney based on its analysis of FY 2012 expense transactions in the Department's financial accounting system.

---

<sup>17</sup> According to OBO management, the "Procurement Services – ICASS" expenditures amounting to \$20.5 million may have been related to NEC and rehabilitation projects.

## **Other Funding Used for Physical Security**

While the majority of the Department's physical security projects were funded from OBO's Worldwide Security Upgrades programs, funds from other sources were used for physical security. For example, funds provided to OBO for Repair and Construction and Overseas Contingency Operations can be used for some physical security needs. In addition, funds provided to DS for Worldwide Security Protection can also be used for physical security.

### **Repair and Construction**

The Department's FY 2012 ESCM appropriation contained \$63 million for repair and construction. This funding supported two OBO programs: R&I and Major Rehabilitation. Some funds from these programs were used for physical security needs.

**Repair and Improvement Program.** The Department received \$51 million in FY 2012 for OBO's R&I Program. This program funds repairs and upgrades at Department facilities and is a core component of the OBO maintenance program. Although the use of R&I Program funds for physical security is fairly limited, posts may fund certain repairs relating to physical security using these funds. For example, walls, FE/BR doors, and non-FE/BR doors can be repaired using R&I funds. In FY 2012, OBO expended \$22.8 million for R&I. Because R&I expenditures were recorded using the R&I function codes, the physical security expenditures could not be identified separately.

**Major Rehabilitation Program.** The Department received \$12 million in FY 2012 for OBO's Major Rehabilitation Program. The Major Rehabilitation Program funds major comprehensive renovations of existing facilities that are occupied only by Department personnel. In FY 2012, OBO expended \$65.6 million for major rehabilitation projects. These projects may include physical security components. However, because the physical security components are included as part of the overall project, the physical security expenditures cannot be identified separately by function code in the Department's accounting system. The types and costs of physical security-related items may be identifiable in the construction contract for each major rehabilitation project; however, Kearney did not review the construction contracts as part of this audit.

### **Overseas Contingency Operations**

In FY 2012, the Department received Overseas Contingency Operations funds amounting to \$115.7 million under the ESCM appropriation. This funding, which began in FY 2012, provides for the extraordinary and temporary costs for operations and assistance in Iraq, Afghanistan, and Pakistan.

In FY 2012, OBO expended Overseas Contingency Operations funds amounting to \$9.7 million from the ESCM appropriation. Of the \$9.7 million, \$9 million was for rent expenses and approximately \$0.7 million was related to a major rehabilitation project in Tripoli, Libya. Kearney could not determine whether the major rehabilitation project included a physical security component based on the function codes used for these expenditures.

## **Worldwide Security Protection**

The Department's FY 2012 Diplomatic & Consular Programs (D&CP) appropriations contained \$1.35 billion in funding for Worldwide Security Protection and an additional \$236.2 million in Overseas Contingency Operations funds. This funding supports primarily security staffing to ensure the safety of American diplomats, to protect the integrity of the data and systems on which these personnel rely, and to secure the facilities in which these personnel work and reside. Specifically, the funding supports the worldwide local guard program, high-threat protection, security technology, armored vehicles, cyber security, information security, facility protection, and diplomatic couriers. It also supports emergency preparedness programs, internal and interagency collaborations and information sharing, and medical emergencies planning in the event of mass casualties from a biological or chemical attack.

Although the majority of physical security needs are funded by OBO, DS has used Worldwide Security Protection funds for physical security-related projects. Kearney identified FY 2012 expenditures amounting to approximately \$48 million for non-residential physical security that were recorded to function code 5831—Perimeter and Internal Security. A DS official stated that DS used this function code for physical security-related activities. For example, DS had provided Worldwide Security Protection funds totaling \$259,920 in FY 2012 for six physical security projects relating to perimeter and internal security in Libya, Saudi Arabia, and Yemen. A summary of FY 2012 expenditures recorded to function code 5831—Perimeter and Internal Security by appropriation, or expenditure account, is provided in Table 5.

**Table 5. FY 2012 Function Code 5831 Expenditures by Expenditure Account**

<b>Expenditure Account</b>	<b>Amount</b>
D&CP Afghanistan Operations – Overseas Contingency Operations	\$27,645,000
D&CP Afghanistan Operations	1,791,224
D&CP Emergency Supplemental	17,605,430
D&CP Iraq Embassy Operations	1,218,002
D&CP Machine Readable Visa Processing Fee	6,038
<b>Total</b>	<b>\$48,265,694</b>

Source: Prepared by Kearney based on its analysis of FY 2012 expense transactions in the Department's financial accounting system.

## **Finding B. Processes To Request Funds for Physical Security Needs Could Be Improved**

The majority of the post security officials responding to an OIG questionnaire indicated that the processes to request funds for physical security-related needs at Department-owned or Department-operated buildings were clear and easy to use. (The process used for the questionnaire is explained in Appendix A, and the questionnaire is in Appendix B.) However, a significant number of post security officials responded that the processes were unclear and difficult to use. In addition, a significant number of respondents expressed dissatisfaction with

**UNCLASSIFIED**

the timeliness or sufficiency of the responses OBO provided to the respondents' formal requests for physical security funding.

The lack of understanding, the perceived complexity of the processes, and dissatisfaction with responses to formal requests occurred because neither DS nor OBO had developed standardized and documented policies and procedures for the processes to request funds for the majority of physical security-related needs. In addition, many post security officials indicated that the training provided for requesting funds was inadequate. As of September 2013, DS was developing a tool to help identify and document post physical security-related needs, which may clarify and simplify the request processes. However, this tool was not expected to be fully implemented until 2016. The lack of standard, documented policies and procedures may result in post physical security needs not being addressed adequately or promptly.

**Many Posts Indicated Physical Security-Related Needs Existed During FY 2012**

In response to the OIG questionnaire, 83 (63 percent) of 132 post security officials indicated that their posts had physical security-related needs in FY 2012. The types of needs identified by these post officials included minor physical security upgrades, major physical security upgrades, other security issues, and R&I, as shown in Table 6.

**Table 6. Physical Security-Related Needs During FY 2012 Reported in Response to OIG Questionnaire**

Type of Need	Definition	Number of Needs
Minor Physical Security Upgrade	Post-managed projects, generally less than \$250,000, with upgrades to perimeter protection, facility protection, and interior protection to bring deficient facilities into compliance with OSPB standards.	136
Major Physical Security Upgrade	OBO-managed projects, generally \$250,000 or more, with upgrades to perimeter protection, facility protection, and interior protection to bring deficient facilities into compliance with OSPB standards.	62
Other Security Issues	Any projects relating to physical security that are not encompassed by the other categories, such as upgrades that are not related to OSPB standards but may be warranted given special circumstances at an overseas post.	13
Repair and Improvement	Projects to restore deteriorated or damaged property to its original condition or increase a property's value or change its use.	60
<b>Total</b>		<b>271</b>

Source: Prepared by Kearney based on its analysis of questionnaire responses.

The majority of the post needs were identified as having been existing deficiencies (71, or 46 percent), with the second largest number identified as occurring because of normal deterioration of the facilities (38, or 24 percent).

## UNCLASSIFIED

Although 83 respondents said that their posts had physical security-related needs in FY 2012, only 59 (71 percent) of the 83 indicated that they had formally requested funding for those needs. The reasons provided for not formally requesting funding for physical security needs included that post did not believe the need would be funded, post used its own funds to fill the need, a post was scheduled for a NEC, and physical security needs were incorporated into a major rehabilitation project for which funding was provided through a different process.

### **Processes Existed for Requesting Physical Security Funds Depending on Need**

The processes for requesting funding for minor and major physical security upgrades were similar. Generally, when RSOs identify a physical security need or deficiency, they first contact their respective Desk Officers informing them of the need via email. The Desk Officer reviews the informal request to determine whether the need is required to meet OSPB standards. If it is required, the Desk Officer communicates the request to OBO's Program Security Operations Branch. If OBO agrees with the request, the RSO prepares, with the Desk Officer's assistance if needed, a formal request cable for submission to OBO. Once OBO approves the formal request, OBO enters the request into the Buildings Management Integrated System,<sup>18</sup> which generates a project number. OBO officials stated that OBO will approve funds for minor physical security upgrades when it receives the formal request. Approved major physical security upgrades are added to an "out-year" schedule and are completed in order of priority.

Other processes existed to request funding for specific physical security-related items. For example, when posts need FE/BR products, such as doors or windows, the RSO informs OBO's Program Security Operations Branch directly via email. If the request is minor, which includes the maintenance and repair of existing FE/BR doors and windows, OBO funds the request in the year in which it is requested. Major FE/BR requests, which include large and significant projects to install new or perform lifecycle replacement of FE/BR doors, windows, and glazing panels, are added to an "out-year" schedule.

In addition, posts may request security-related items, such as repairs of walls, roofs, and non-FE/BR windows and doors, through OBO's process for funding R&I projects. Posts submit requests for R&I projects, both security and non-security related, to OBO electronically through a Web-based system that interfaces with the Buildings Management Integrated System on a nightly basis. Area Managers in the Area Management Division review and approve each request in the system.

### **Processes To Request Funding Were Clear and Easy but Needed Improvement**

Many of the post security officials who responded to the OIG questionnaire found the processes to request funding for physical security-related needs clear and easy to use. But some post security officials believed the processes were unclear or difficult. Overall, in response to a question regarding whether the processes were clear or unclear,<sup>19</sup> more than twice the responses

---

<sup>18</sup> The Buildings Management Integrated System is the database that OBO uses to track and prioritize OBO-funded facility maintenance requirements, capital construction projects, and noncapital repair and rehabilitation projects.

<sup>19</sup> For this report, clear is defined as "easily understood or free from doubt or confusion."

**UNCLASSIFIED**

were “very clear” or “somewhat clear” (206 [56 percent] of 370) than were “very unclear” or “somewhat unclear” (101 [27 percent] of 370). Similarly, in response to a question regarding whether the processes were easy<sup>20</sup> or difficult, more responses were “very easy” or “somewhat easy” (148 [41 percent] of 360) than were “very difficult” or “somewhat difficult” (96 [27 percent] of 360). The number of responses for each category of physical security need is provided in Table 7.

**Table 7. Understanding of the Process To Request Funding for Physical Security Needs**

Category	Clarity		Ease of Use	
	Clear	Unclear	Easy	Difficult
Minor Physical Security Upgrades	(65) 65%	(20) 20%	(48) 48%	(24) 24%
Major Physical Security Upgrades	(47) 50%	(32) 34%	(29) 33%	(29) 33%
Repair and Improvement	(51) 56%	(25) 27%	(38) 43%	(22) 25%
Other Security Issues	(43) 51%	(24) 28%	(33) 40%	(21) 25%
<b>Total</b>	<b>(206) 56%</b>	<b>(101) 27%</b>	<b>(148) 41%</b>	<b>(96) 27%</b>

Source: Prepared by Kearney based on its analysis of responses to OIG’s questionnaire.

One factor that likely contributed to post security officials’ positive perception of the processes was the adequacy of assistance provided to posts during the request processes by DS and OBO. A large majority, 93 (84 percent) of 111 respondents, found DS assistance to be either “very adequate” or “somewhat adequate,” and 81 (74 percent) of 110 respondents deemed DS assistance to be either “very timely” or “timely.” Almost half of the respondents, 49 (47 percent) of 105, also found OBO assistance to be either “very adequate” or “somewhat adequate.” One post security official commented that the points of contact “at both bureaus have generally been helpful in providing appropriate guidance on how to request funding.” Another post security official commented “[i]n my experience I have been serviced well by OBO and DS concerning needs for physical security upgrades and RSO inquiries.” A third post security official stated that their post had been “well supported in the area of physical security upgrades. Both DS and OBO have for the most part been very helpful during the process.”

Although there were many positive responses to the questionnaire relating to the clarity and ease of the processes to request funding for physical security needs, there were a significant number of responses that the request processes were unclear (27 percent) or difficult (27 percent). The perception that the processes were unclear or difficult did not appear to be the result of less experience with the processes. In fact, officials with greater experience generally found the processes for requesting funds for minor physical security upgrades, major physical security upgrades, and other security issues to be more difficult than officials who had less experience.

---

<sup>20</sup> For this report, easy is defined as “not hard to do or requiring little effort.”

## UNCLASSIFIED

### **Some Questionnaire Respondents Believed Responses to Posts' Funding Requests Were Insufficient**

Many post security officials who responded to the OIG questionnaire also indicated that the assistance provided to post was untimely and that information provided to posts by OBO related to the denial of formal requests was inadequate.

Specifically, 31 (30 percent) of 103 respondents indicated that OBO's assistance during the process of requesting funds was "untimely" or "very untimely." For example, one respondent stated that their post's FY 2012 requests "have still not been approved or denied" in August 2013, or 10 months later. Another respondent stated, "I requested funds for a project, 6 months later [OBO] responded and requested more info [information] before [close of business]. Then [OBO] did not respond for about 2 months before another short fuse request." An additional respondent stated that "cables and emails went unanswered and were it not for the intervention by the Ambassador direct to the Director of OBO, we do not believe we would have received a response."

Respondents were also dissatisfied with the responses received when their requests for funding were denied. Specifically, 14 (41 percent) of 34 respondents indicated that the responses received were either "somewhat inadequate" or "very inadequate." Respondents to the questionnaire who stated that some of their FY 2012 requests were not funded reported on average that only 44 percent of their denied requests included an explanation of the denial of funding.

OBO officials stated that OBO had an informal goal of responding to all official requests for physical security funding within 2 weeks of receiving the request but that this goal was not always met. One OBO official explained that workload backlogs and competing priorities resulted in some responses being delayed. OBO officials further explained that they were confident that OBO had informed posts about decisions related to requests but that the respondent may not have been aware of the response. For example, an OBO official stated that OBO might have informed and provided information to a different representative at a post, such as the post's Facilities Manager, rather than to the post security official. In these cases, OBO's response might not have been shared with all relevant parties at the post. In addition, posts sometimes submitted a request for funding to an incorrect program within OBO, which increased response time while the request was transferred to the correct program.

Although there are circumstances in which OBO responses may be delayed or when communications with posts are not relayed to all interested parties, the significant rate of dissatisfied customers indicates that OBO should take action to better communicate with posts on formal requests for physical security funding.

### **Processes Were Not Standardized and Documented, and Training Was Not Sufficient**

The negative perceptions expressed by post security officials can be attributed, in part, to the lack of formal policies and procedures for the processes to request funds for physical security-related needs, including the roles of DS and OBO in those processes. In addition, some

## UNCLASSIFIED

post security officials commented that they had not received sufficient training on how to request funding.

### **Some Processes Were Not Standardized and Documented**

According to the Government Accountability Office's (GAO) document "Standards for Internal Control in the Federal Government,"<sup>21</sup> "[M]anagement is responsible for developing the detailed policies, procedures, and practices to fit their agency's operations and to ensure that they are built into and an integral part of operations." However, Kearney found that neither DS nor OBO had developed or documented standard policies and procedures for requesting funding for most physical security-related needs at posts. Many questionnaire respondents, 57 of 96 (59 percent), indicated that the written policies and procedures for requesting funds were "very adequate" or "somewhat adequate." However, Kearney did not identify, either in the Department's FAM or the *Foreign Affairs Handbook* (FAH) or other available information from DS or OBO in any documented format, formal policies and procedures for requesting funding for minor physical security upgrades, major physical security upgrades, or other security issues such as FE/BR products.<sup>22</sup> In addition, there were no standard formats or templates for post to use to make their requests.

The process to request funding for physical security needs is initially conducted informally, primarily through emails, until a preliminary decision is made to approve the request. Although initial discussions are normally between the post security official and the Desk Officer, both DS and OBO officials stated that posts sometimes bypassed the Desk Officer and contacted OBO officials directly. One post security official commented, "There seems to be no formal process other than trading emails with [points of contact] in various DS and OBO offices – if there is, it's not clear to the [people in the] field."

In addition to the initial requests, there were no standard policies and procedures for responding to the requests. Responses to the OIG questionnaire indicated that posts received notifications that their formal requests were not funded in different manners, including cables, emails from OBO or DS, and telephone calls from OBO or DS, or they were not notified at all. One respondent indicated that there needs to be "a better process to new [Assistant] RSOs and RSOs on whom to contact in their region and what the entire process from request to receiving funds looks like."

Some post security officials expressed confusion about the roles and responsibilities of DS and OBO in the request process. In discussions with both DS and OBO regarding each bureau's responsibilities for physical security-related requests, officials referred Kearney to the Security Equipment Responsibilities Matrix (SERM). The SERM is a guide that identifies the offices responsible and funding sources for the installation, maintenance, and repair of security equipment. However, the SERM does not describe the processes for requesting funds, and it does not include all physical security-related items. For example, although the SERM contains

---

<sup>21</sup> GAO/AIMD-00-21.3.1, Nov. 1999, p. 7.

<sup>22</sup> OBO has developed and documented policies and procedures for requesting R&I funds in the "Repair and Improvement Program Cookbook," which is available on OBO's SharePoint site.

## UNCLASSIFIED

information relating to the installation and maintenance of FE/BR doors, it does not provide similar information for perimeter walls. DS officials stated that the SERM was designed to address technical, rather than physical, security requirements. If physical security-related items do not have a technical security aspect, the items are not included in the SERM. One respondent commented, “While the security funding matrix is very helpful, it is not all-inclusive and still leaves wiggle room as to where responsibility falls on some things.” Another respondent commented that there “seems to be little coordination between DS and OBO at the [Washington, DC] level on security upgrade projects, and it’s unclear who is in charge of these for both funding and execution as many of these projects do not fit into the security equipment matrix.”

DS and OBO officials agreed that the process for requesting funds for physical security-related needs was complicated but stated that it was very difficult to develop a standard process for posts to use because each physical security-related need was unique. The officials further stated that post security officials should contact the Desk Officers, who will guide the post officials through the process to request funds. Although responses to the OIG questionnaire indicated that Desk Officer assistance had been beneficial, it was clear that post security officials believed that DS and OBO needed to develop a better method to instruct posts in how to request funding. In addition, DS and OBO need to develop a standardized, timely method to respond to posts about the decisions made on each request.

As of September 2013, DS was taking action to improve the process for posts to request funding for physical security needs by developing a SharePoint<sup>23</sup> tool to be used for documenting and tracking posts’ physical security needs. This tool is planned to allow RSOs to directly enter into SharePoint specific physical security-related information for different types of facilities. The tool could eliminate or decrease the need for and reliance on individual requests. However, DS officials stated that they did not expect the tool to be fully populated with post data until FY 2016.

### **Some Questionnaire Respondents Believed Training Was Not Sufficient**

GAO’s “Standards for Internal Control in the Federal Government” states that “management needs to identify appropriate knowledge and skills needed for various jobs and provide needed training.” According to the results of the questionnaire, however, 41 (51 percent) of 81 respondents indicated that the training for requesting funds for physical security needs was either “somewhat inadequate” or “very inadequate,” while only 23 (28 percent) of 81 respondents selected “somewhat adequate” or “very adequate.” Additional written comments by some respondents to the questionnaire provided detail as to the deficiencies of the training to request funding. For example, one respondent commented that they had “never received any instruction as to the proper way to request money for funding of physical security upgrades. I know nothing about the process by which this happens or how these decisions are made.” Another respondent stated that the “RSO training related to the physical security funding process is wholly inadequate.” A third respondent stated that they did not “think many people ever receive training in the Department of State on how to request assistance. It is more a matter of

---

<sup>23</sup> SharePoint is a Microsoft Web application platform that provides Intranet portals, document and file management collaboration, system migration, process integration, and workflow capabilities.

## UNCLASSIFIED

personal motivation—if you want to achieve something, you look up the contact name in the [global address list] or on the intranet for the section which makes most sense.”

According to DS officials, RSOs receive training on how to request funding for physical security-related needs during Basic Regional Security Officer training, which all RSOs attend before they leave for their overseas assignments. Kearney noted that the training curriculum and related training materials for physical security contained some information indicating that funding requests for minor and major physical security upgrades were covered on a limited basis during the training. Although post security officials could contact Desk Officers for assistance, the responses to the questionnaires indicate that post security officials would prefer additional training on the process to request funding.

### **Lack of Adequate Process Could Discourage Posts from Requesting Funding or Lead to Posts Funding Projects Directly**

The lack of standard documented policies and procedures for requesting physical security funds and the resulting lack of understanding of those processes may dissuade post security officials from submitting requests for funding. In fact, two respondents to the OIG questionnaire indicated that they did not formally request funding for all of their physical security needs because their posts considered the process to be confusing or difficult. If even one post does not request funds for a significant security need, that post may become more vulnerable to an attack that could result in destruction of property, injury, or loss of life.

In addition, post security officials who do not clearly understand the request process may submit requests that have insufficient information or support or to the incorrect individuals. If requests are not submitted correctly, they must be resubmitted, which requires additional time and may delay the process for obtaining needed physical security items.

Further, 22 respondents (17 percent) stated that their physical security needs in FY 2012 resulted from the establishment of new physical security requirements, and 18 (14 percent) stated that their needs resulted from an increase in physical security-related risks. Although, in general, most post security officials understood the processes to request physical security funding and found the processes easy to use, an increase in the number of requests because of increased requirements or risks may make the existing informal system less able to accommodate the requests in a manner that ensures that critical physical security needs are addressed effectively and in a timely manner.

**Recommendation 1.** OIG recommends that the Bureau of Diplomatic Security, in coordination with the Bureau of Overseas Buildings Operations, develop and implement standard policies and procedures for requesting funds for physical security-related needs and document the policies and procedures in a manner that is easily accessible by post security officials (for example, in a “physical security funding handbook”). Consideration should be given to how the SharePoint tool currently in development can be used to simplify the request processes.

**UNCLASSIFIED**

**DS Response:** DS stated that it “currently has a process for posts that require additional funding” and that the “process will be clearly articulated as part of an annual operating cable sent to RSOs.” DS noted that posts are instructed “to send a front channel cable outlining the security requirement and include funding implications.” DS further stated that “a formal front channel cable funding request with direct response from the appropriate DS program office” and funding validation are more appropriate than using SharePoint.

**OBO Response:** OBO suggested that OIG change the recommendation from “physical security-related needs” to “physical security upgrades.” According to OBO, the “distinction is needed since funding is near the end of the process.”

**OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that DS, in conjunction with OBO, has developed and implemented standardized policies and procedures for requesting funds for physical security-related needs. OIG does not believe it is necessary to change “physical security needs” to “physical security upgrades” in the recommendation. OIG expects that the policies and procedures will provide guidance for requesting funds for all types of physical security deficiencies and should not be limited to upgrades.

**Recommendation 2.** OIG recommends that the Bureau of Overseas Buildings Operations develop and implement a process to respond to posts’ formal requests for physical security-related funding, which should include commitments to respond within certain timeframes.

**OBO Response:** OBO concurred with the recommendation, noting that “funding will be part of the overall process developed” for Recommendation 1.

**OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that OBO has developed and implemented a process and timeframes for responding to requests for physical security-related funding.

**Recommendation 3.** OIG recommends that the Bureau of Diplomatic Security develop and implement a methodology to periodically communicate the processes to request funds for physical security-related needs to all post security officials.

**DS Response:** DS concurred with the recommendation, stating that it will “explore the possibility of integrating funding guidance and/or a funding request process” within its new Physical Security Survey site or Project Management Solution, as well as include “language about requesting funds for physical security upgrades in its annual operating cable.”

**OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that DS has developed

**UNCLASSIFIED**

and implemented a methodology to periodically communicate the processes to request funds to all post security officials.

**Finding C. Department Did Not Have Information To Ensure Highest Priority Security Needs Were Funded**

Kearney could not determine the extent to which the Department used physical security funds for the highest priority physical security needs at overseas posts during FY 2012. During that fiscal year, the Department funded four major physical security upgrades, 85 minor physical security upgrades, and 10 major FE/BR projects. However, Kearney could not determine whether the highest priority security needs were funded for the following reasons:

- DS did not have a comprehensive list of all post physical security deficiencies.
- Neither DS nor OBO maintained a list of posts' FY 2012 requests for physical security funding and the disposition of those requests.
- Neither DS nor OBO had formal processes to prioritize physical security needs. Instead, decisions on which project to fund were often made by one individual without documented standards and guidance for prioritizing physical security needs.
- DS and OBO did not have sufficient formal processes for coordinating with each other to establish standards for determining priority and to agree on funding decisions.
- Neither DS nor OBO had developed a comprehensive long-range physical security plan that would help focus attention on critical needs.

For the reasons cited, the Department could not ensure that the highest priority physical security needs at overseas posts were corrected and that the posts' vulnerability to threats had therefore been reduced sufficiently.

**Complete Information Needed To Prioritize Post Physical Security Needs Was Not Maintained**

GAO's "Standards for Internal Control in the Federal Government" states that "[i]nternal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination." However, the Department did not have the information needed to prioritize post physical security needs. Specifically, DS did not have a comprehensive list of physical security deficiencies at all overseas posts, and neither DS nor OBO maintained a list of posts' FY 2012 requests for physical security funding or the disposition of those requests.

## **Comprehensive List of Physical Security Deficiencies Was Not Available**

DS did not have a comprehensive list of physical security deficiencies at all overseas posts. When Kearney requested such a list, DS officials stated that a comprehensive list did not exist.

Kearney found that a comprehensive list was not available because DS did not have sufficient processes in place for collecting the information and developing such a list. The FAM<sup>24</sup> requires that RSOs at each post conduct a physical security survey of their post facilities at least once every 3 years to determine whether the facilities meet OSPB security standards and to identify physical security deficiencies requiring correction. RSOs provide the completed physical security survey to DS' International Programs Directorate.<sup>25</sup> The directorate maintains the surveys in a centralized DS repository. In addition, RSOs provide a copy of the survey to their respective Desk Officer and inform the Desk Officer of the physical security deficiencies that arise between survey reporting periods. However, the physical security deficiencies identified during the surveys and reported by posts were not compiled and tracked aggregately by DS. Instead, each of the Desk Officers determined how they would track and monitor the physical security deficiencies at the posts for which they were responsible.

**OBO Maintains  
Comprehensive List of R&I Needs**

Although the Department does not maintain a list of physical security-related needs, it has other programs that it could use as a basis for developing a comprehensive tracking process for physical security-related deficiencies. For example, for R&I, OBO obtains requests from posts through a formal process, normally once a year; has a formal process for prioritizing the requests; and maintains a complete prioritized list of R&I requirements in the Buildings Management Integrated System.

Although the physical security survey results could provide a basis for compiling a comprehensive list of all physical security deficiencies worldwide, the survey as structured may not provide all of the information necessary. Specifically, the survey form was not constructed in a manner that enables the RSO to complete it efficiently or the DS Desk Officer to interpret the results easily. For example, OSPB standards provide physical security requirements for eight different types of facilities.<sup>26</sup> However, the same survey form is used for all types of facilities and for all threat categories, and the form does not include information on the requirements for each type of facility being assessed and does not include the specific standards that apply to a post based on its threat category. This format requires that RSOs spend additional time looking up the standards for each facility.

In addition, the survey consists of many open-ended questions that require the RSO to describe an aspect of physical security rather than simply identify whether or not the facility meets that aspect of the applicable standards. For example, one question instructs RSOs to "describe perimeter fence/wall" rather than stating that the perimeter wall should be a certain

---

<sup>24</sup> 12 FAM 315.2c, "OSPB Security Standards – Exception Authority."

<sup>25</sup> 12 FAM 425a, "Regional Security Officer (RSO) Reporting Requirements."

<sup>26</sup> The eight types of facilities are a Chancery or Consulate, Sole Occupant of Building or Compound, Tenant in a Commercial Office Space, New On-Compound Housing; Public Office Facility, Voice of America Relay Stations, Unclassified Warehouse, and Public Diplomacy Facility.

**UNCLASSIFIED**

height based on the threat level of the post and asking the RSO to report on whether the perimeter wall meets this requirement. Because the RSOs simply give a description of the wall without explicitly pointing out whether a standard was met or a deficiency existed, the responsible Desk Officer had to make that determination based on the description.

Before the beginning of this audit, DS recognized the need to track physical security deficiencies and maintain a comprehensive list of physical security needs for all posts in one, easily-accessible location. As discussed in Finding B, as of September 2013, DS' Physical Security Division had been developing a new physical security survey, using SharePoint, that would track all areas of non-compliance with physical security standards in a comprehensive and uniform manner. The SharePoint survey addresses the flaws in the current survey process. For example, the SharePoint tool will include separate survey forms for each of the eight types of facilities, and each form will include the specific standards for that type of facility. RSOs will use drop-down menus and other tools to indicate whether or not the facility being assessed is in compliance with the standards. In addition, RSOs will be able to provide additional descriptive information for non-compliant facilities, which will make it easier for DS to capture all identified physical security deficiencies at all posts. A DS official stated that RSOs will be able to update the information in SharePoint to include new physical security deficiencies as they are identified. DS officials stated that DS also plans to develop the functionality necessary to consolidate all physical security deficiencies in SharePoint into one report.

If implemented successfully, the SharePoint tool could provide DS and OBO with information on physical security needs at overseas posts that could be used to make informed funding decisions. However, DS had not developed a full implementation plan for the new survey tool. Certain aspects of the tool's use after it was fully populated were still unclear, such as whether OBO would have access to view the completed surveys and generate reports to obtain specific information. A complete implementation plan, which includes details of how the tool will be used across DS offices as well as by OBO, would be key to the successful completion of this project.

Additionally, the new physical security survey specifically tracks only areas of non-compliance with OSPB standards, not other physical security deficiencies such as issues with the condition of physical security items that may render the items incapable of performing as intended. For example, if the RSO is assessing the perimeter wall, the survey asks if the wall was built in accordance with the appropriate standard(s), not whether there are cracks or other signs of deterioration in the structure that could indicate a deficiency in the facility's physical security. The survey form has a text box at the end of each section (for example, perimeter walls) where RSOs can note these types of physical security deficiencies as well as provide additional information about the areas of non-compliance identified. Although DS should be able to generate a report that lists all facilities that are not compliant with the OSPB standards and the areas of non-compliance, capturing the information on other physical security deficiencies in the report will be more difficult.

DS officials stated that they anticipated having the SharePoint survey tool available during 2014. However, the database will not be populated with complete information for at least 3 years. DS plans to have posts input information during the physical security survey process

## **UNCLASSIFIED**

performed once every 3 years. The security survey process is normally performed on a rolling basis; that is, approximately one-third of overseas posts perform the survey each year. DS officials stated that a phased-in approach was necessary because of the large number of facilities, over 2,000, that must be surveyed and the limited number of staff available to analyze survey results. Therefore, complete information on all overseas physical security deficiencies may not be available until 2016.

### **Complete List of Post FY 2012 Requests for Physical Security Funding Was Not Available**

Neither DS nor OBO had a complete list of all funding requests for physical security-related items made by posts during FY 2012. Kearney requested a complete list of all informal requests made by RSOs in FY 2012 to DS officials, but DS officials explained that such a list did not exist. The Desk Officers review and screen post requests and inform the RSOs about which requests should be formally submitted to OBO. Although the Desk Officers had records, such as emails, of the requests that they had received from their posts, DS did not compile and maintain a complete list of posts' FY 2012 requests, including the requests that posts were advised not to submit formally.

Kearney also requested a comprehensive list of all formal requests for funding to OBO, but OBO officials explained that OBO did not track all incoming requests and that such a list did not exist. OBO officials stated that requests were tracked informally through ongoing discussions between OBO staff, DS Desk Officers, and the requesting RSO. OBO maintained and provided Kearney copies of spreadsheets that listed the major physical security upgrade and FE/BR projects that OBO had approved and scheduled. OBO officials stated that OBO's policy is to fund all requests for projects that are needed to bring the posts into compliance with OSPB standards. OBO officials stated that they did not believe it was necessary to track post requests that were not funded because denials were issued very infrequently. However, without a complete list of the formal requests, Kearney could not determine whether or how many formal requests were made and how many of those requests were denied.

### **Formal Processes To Prioritize Physical Security Requests Were Not in Place**

As part of any successful program, an organization should prioritize needs so that funds can be used in the most efficient and effective manner. In order to prioritize activities, program managers should implement a systematic process to select projects and allocate resources to these projects in order to maximize value added. However, neither DS nor OBO had formal processes in place to prioritize posts' physical security needs. The processes used by DS to review posts' initial informal requests and by OBO to determine which formal requests for major and minor physical security upgrades and FE/BR projects were funded, were often performed by one individual without documented standards and guidance.

#### **DS Review Process**

DS used an informal process to review RSO requests before the RSO could submit a formal request for funding to OBO. As reported in Finding B, when RSOs identify a need, they

## UNCLASSIFIED

discuss the need with the post's Desk Officer. In some cases, the Desk Officer may inform the RSO not to submit a formal request for funding to OBO because the Desk Officer believes that the request will not be funded. For example, if an RSO identifies a physical security deficiency that exceeds OSPB minimum standards, the Desk Officer may discourage the RSO from requesting funds to correct the deficiency. In response to the OIG questionnaire, security officials at four posts indicated that they were advised by Washington-based officials not to request funds for their physical security needs. Desk Officers generally based their determinations on information provided by the posts, such as information in emails and photographs if available. There was no standard template for posts to make requests, and there were no formal standards or guidance for the Desk Officers to use to make their determinations. Instead, each Desk Officer used his or her own experience and knowledge about the funding process to determine whether to encourage posts to submit a formal request for funding.

### **OBO Processes To Prioritize Physical Security Needs**

OBO had several processes to determine which physical security projects were funded depending on the type of project. Specifically, OBO had separate processes for major physical security upgrades, minor upgrades, and FE/BR projects.

**Major Physical Security Upgrades.** There were no documented standards or guidance for prioritizing major physical security upgrade projects. One individual, an OBO program manager, received all formal requests for funding and determined the priority of the projects. The manager determined whether to fund a post request based primarily on the post's ranking on the DS Risk Matrix. The DS Risk Matrix lists posts in the order of priority. The post ranked number one on the Matrix receives a vulnerability score of "1," with the remaining posts' scores calculated as a percentage of how vulnerable each post is in relation to the first post. The scores on the DS Risk Matrix are generally based on the condition of the facility; its SETL threat levels; and, to a small degree, other factors related to the host country. In addition to the DS Risk Matrix ranking, the program manager considers other factors, including the overall condition of physical security at the post and whether the post is scheduled for other major projects, such as the construction of a NEC or a major rehabilitation.

When requests are received for major physical security upgrades that cannot be funded immediately, OBO places them on out-year project schedules. As of April 2013, 55 major physical security upgrade projects were scheduled to be funded from FY 2012 through FY 2019. Kearney evaluated the project schedules provided by OBO to determine whether higher threat posts were prioritized before lower threat posts. Kearney concluded that generally, posts with higher scores on the DS Risk Matrix were scheduled before posts with lower scores. However, Kearney identified some instances in which posts with higher DS Risk Matrix scores were scheduled after posts with lower scores. OBO officials stated that in some cases, projects for higher threat posts could not always be given higher priority because of physical, logistical, or host government constraints. For example, a project for one post that was ranked highly on the DS Risk Matrix was scheduled for FY 2014, but the project was pushed back to FY 2015 because of the lack of host government cooperation. Kearney also identified an instance where a post that was ranked in the top 15 percent of the most vulnerable posts on the DS Risk Matrix was not scheduled for an upgrade until FY 2017, while 25 of the 29 posts scheduled for upgrades

**UNCLASSIFIED**

between FY 2012 and FY 2016 were ranked lower. An OBO official explained that this project had been pushed back on the schedule because of a reduction in funding from the initial budget requests that OBO had submitted. Although the funds available for physical security-related projects may not be sufficient to cover the costs of a large project at a vulnerable post, the funds may cover several smaller, needed projects at less vulnerable posts.

**Minor Physical Security Upgrades.** There were no formal standards or guidance for prioritizing minor physical security upgrade projects. OBO officials explained that OBO generally funds all minor physical security upgrade projects. When requests are received, an OBO manager determines whether the request is for a valid minor project. If it is a valid project, OBO either funds it immediately or delays the project until it is feasible. For example, if a post requests multiple minor projects, OBO may fund a few of the projects initially and fund the remaining projects after the post completes the initial projects. OBO does not track the minor projects that have been postponed. OBO officials stated that OBO ensures that pending minor projects do not get overlooked by having ongoing conversation with RSOs and Desk Officers regarding the statuses of their minor projects. However, according to the responses to the OIG questionnaire, of 117 requests for minor physical security needs, only 85 were funded, meaning that 32 were not funded.

**FE/BR Projects.** There were no documented standards or guidance for prioritizing FE/BR projects. Requests for FE/BR projects are reviewed by one individual, an OBO program manager. The manager makes prioritization decisions based upon several factors. Specifically, the manager considers the information provided by the requesting post, such as photographs of faulty equipment; the post's SETL threat ratings; and whether a major rehabilitation project, major upgrade project, or construction of a NEC is scheduled for that post in the near future.

When requests are received for FE/BR upgrades that cannot be funded immediately, OBO places the requests on out-year project schedules. Kearney reviewed the out-year project schedules for FY 2011 through FY 2013 and found that 31 FE/BR projects were scheduled to begin during that period. Kearney evaluated the FE/BR project schedule provided by OBO to determine whether posts with a higher SETL threat rating were scheduled before posts with a lower rating. Kearney concluded that in general, posts with a high SETL threat rating were scheduled before posts with a lower rating.

**Repair and Improvement Projects.** OBO documented standards and guidance for prioritizing R&I projects. OBO's "Repair and Improvement Program Cookbook" provides detailed instructions and operational guidance for the R&I process, including how R&I requests are prioritized. When R&I requests are received, Area Management Officers within OBO's Office of Area Management score the requests by assigning weighted factors to 14 specific criteria to define the level of importance of the requests. The "BMIS Scoring Guide" defines the scoring factors and provides recommended scores for various facility and building system conditions. Scored requests are reviewed and approved by OBO management. Approved requests become R&I requirements, which are ordered by the priority score. The higher the priority score, the more likely the project will be funded.

## **Coordination Between DS and OBO Was Not Sufficient**

GAO's "Standards for Internal Control in the Federal Government" states, "Effective communication should occur in a broad sense with information flowing down, across, and up the organization. In addition to internal communication, management should ensure there are adequate means of communicating with, and obtaining information from, external stakeholders that may have a significant impact on the agency achieving its goals." Although DS and OBO share responsibility for ensuring that posts' physical security needs are addressed, coordination between the bureaus to establish prioritization standards was not sufficient.

Although DS is responsible for protecting Americans overseas and establishing physical security standards, DS had not been sufficiently involved in the decision-making process to prioritize and fund physical security projects. DS Desk Officers are in regular communication with RSOs to understand posts' physical security needs and the importance of funding those needs. However, a DS official stated that once a post submits a formal request for physical security funding to OBO, DS' Project Coordination Branch does not play a role in the prioritization of the major physical security upgrade projects. Because OBO is appropriated the funds for addressing physical security deficiencies, OBO takes the lead in determining which physical security projects will be funded and when. DS and OBO officials meet on a weekly basis to discuss the requests for physical security projects that have not been funded and to gain an understanding as to why the requests were not funded. This meeting provides DS officials an opportunity to have input into the decision-making process. For example, during these meetings, DS may emphasize the importance of a project to OBO and explain the physical security deficiencies that need to be corrected. However, there is no formal process in place for DS to object to OBO's decisions.

Post security officials identified concerns with the lack of coordination between DS and OBO. For example, one respondent to OIG's questionnaire stated, "The [l]argest problem with physical security funding is that OBO . . . considers it a DS thing and DS . . . does not control funding. . . . This confuses the whole process, introduces delays and makes it cumbersome." It is essential that OBO and DS improve their process for sharing information to assist in the decision-making process and work together to ensure that the best funding decisions are being made.

Kearney identified several significant instances in which the lack of coordination between OBO and DS created the potential for disagreements in determining which physical security needs should be funded. For example, OBO and DS had differing interpretations of how OSPB standards should be applied, the bureaus did not agree on the factors to prioritize major physical security upgrade projects, and the bureaus had not established specific criteria for funding physical security projects at posts scheduled to receive a NEC or undergo major rehabilitation.

## UNCLASSIFIED

### **Inconsistent Interpretation of Security Standards**

DS and OBO had differing interpretations of the OSPB standards. OBO officials stated that OBO makes decisions on which projects to fund based on the OSPB standards in the FAH.<sup>27</sup> OBO officials stated that OBO's priority is to bring posts that are not in compliance with OSPB standards into compliance. They considered the OSPB standards to be the **maximum** physical security standards required for a post and believe that projects that are not related to standards, or that go "above and beyond" the standards are difficult to prioritize. For example, OBO would not normally fund physical security projects that are outside the perimeter of a compound. DS officials stated that there are no policies in place to determine who has funding responsibility for items outside perimeter walls. Kearney reviewed the standards and the SERM and determined that, except for vehicle barriers, there were no policies requiring physical security measures outside the perimeter wall.

DS officials stated that they consider the OSPB standards to be the **minimum** requirements for physical security that posts must meet and believe that there are circumstances in which it is necessary to go above the minimum standards. According to DS officials, high-threat posts may have security needs that are above and beyond the standards listed in the FAH. For example, in response to a bombing that occurred at a building near the U.S. embassy at one post, DS officials requested that OBO fund barriers to block off the road leading to the chancery entrance. However, OBO initially did not fund the request because the barriers would be placed outside the perimeter of the compound and were therefore not required by OSPB standards.<sup>28</sup> In another example, in FY 2012 a post requested funding to replace or repair the "tire killers" located outside the compound perimeter because some of the spikes were not functional. However, OBO did not fund the request because funding items outside of the perimeter was not specified in the standards.

Nevertheless, OBO has, in some cases, funded requests for projects that go beyond OSPB standards. For example, in FY 2012 OBO funded a post's request to install barbed wire. Generally in these cases, DS officials work with OBO officials to provide OBO a better understanding of the need for the projects. However, when OBO does decline to fund physical security needs that DS considers essential, the DS Desk Officers attempt to identify available funding that can be used. For instance, in FY 2012, the Office of Physical Security Programs funded six physical security projects, totaling \$259,820, that were related to perimeter security.

Of the six DS-funded physical security projects in FY 2012, four projects were for Mission Benghazi, which received the DS-funds for minor projects in December 2011 and in February, March, and June 2012. Communications between the requesting RSO, DS, and OBO, and as reported by the Benghazi Accountability Review Board, indicated that OBO did not fund the requests because Benghazi was a short-term leased facility. According to the FAH,<sup>29</sup> OBO's primary program to fund physical security needs, the Compound Security Program, provides funding only for Government-owned and long-term leased facilities. Because the standards did

---

<sup>27</sup> 12 FAH-5 and 12 FAH-6.

<sup>28</sup> According to OBO management, this project was funded in November 2012.

<sup>29</sup> 4 FAH-1 H-520, "Function Codes, Titles, and Definitions."

not require the funding of upgrades at short-term leased facilities, OBO did not fund the requests for physical security upgrades at Benghazi.<sup>30</sup>

On June 11, 2013, the FAH<sup>31</sup> was updated to state that “[s]tandards and measurements in this handbook are the required minimum acceptable standards.” Clarifying the intent of OSPB standards is a useful step in improving the decision-making process for physical security funding. However, until DS and OBO develop a mutual understanding about the needs at posts, there could be additional issues with funding of projects to correct high-risk physical security deficiencies at overseas posts. In addition, to successfully prioritize physical security needs, objective criteria for ranking the needs, including needs that are not required by OSPB standards, would be needed.

### **Lack of Agreement on Prioritization Factors for Major Physical Security Upgrade Projects**

DS and OBO also did not agree on the factors used to prioritize major physical security upgrade projects. OBO primarily used the DS Risk Matrix to prioritize the projects. DS officials stated that the DS Risk Matrix was not an appropriate tool for prioritizing physical security upgrades because it was not developed for that purpose. DS developed the DS Risk Matrix to support the prioritization of posts that were scheduled to receive a new embassy under the Capital Security Construction Program. One DS official stated that DS’ official position is that OBO’s prioritization using the DS Risk Matrix does not align with how DS would prioritize upgrade projects because certain posts had physical security needs that were not reflected in the DS Risk Matrix. DS officials stated that they believed a different matrix should be used for prioritizing major physical security upgrade projects. The new matrix could include many of the same factors as the DS Risk Matrix, but these factors would be weighted differently to prioritize physical security upgrades. DS officials stated that they offered to create such a matrix. An OBO official stated that using the DS Risk Matrix to prioritize major physical upgrade projects was appropriate because the matrix lists and prioritizes the posts that are not scheduled to receive a NEC as well as the posts that are scheduled to receive a NEC. Additionally, the OBO official believed that the use of the DS Risk Matrix was reasonable because OBO does not prioritize the projects solely based on the threat rankings in the DS Risk Matrix but merely uses the matrix as a consideration. Nevertheless, OBO officials expressed their willingness to collaborate with DS on developing a different tool for prioritizing major physical security upgrades.

### **Physical Security Projects at Posts Receiving a NEC or Undergoing Major Rehabilitation**

To make the most efficient use of a limited budget, OBO may defer funding physical security needs at posts that are scheduled to receive a NEC or undergo a major rehabilitation project in the near future. Although this can result in funding efficiencies, it can also leave posts vulnerable to threats when the planned NEC or major rehabilitation projects are delayed. Delays

---

<sup>30</sup> In January 2013, the Department issued guidance indicating that OSPB standards apply to all permanent, interim, and temporary diplomatic facilities.

<sup>31</sup> 12 FAH-5 H-411.1, “Minimum Standards.”

**UNCLASSIFIED**

can result from changes to the list of posts scheduled to receive a NEC<sup>32</sup> and the inherent complexities involved with planning and executing a large-scale construction project in a high-risk overseas environment. For example, the 2010 out-year schedule for major physical security upgrades included one post that was scheduled to receive a major upgrade in FY 2015. This post was in the top 20 of the DS Risk Matrix. However, that project was deleted from the schedule in FY 2011 because it was added to the list of posts scheduled to receive a NEC in FY 2017; thus security improvements would be delayed by an additional 2 years.

In response to the OIG questionnaire, some post security officials expressed concerns about such delays. For example, one post security official stated, “We’re supposed to move into a new facility, but the date keeps changing. We’re over 2 years behind the move. Hard to get funding when you’re supposed to keep moving to a new post.” Another security official stated that the “Embassy was slated for an entire rehab in 2014 – since put off to 2017.”

An OBO official explained that there are instances in which OBO will fund minor projects to temporarily address physical security needs at a post that is scheduled for a NEC or a major rehabilitation project. In addition, OBO officials stated that OBO monitors the NEC project schedule and will consider funding a major upgrade project for a post with physical security deficiencies if the NEC project is scheduled several years into the future. For example, one post security official stated that their post “was scheduled for a new embassy project in FY 2016, but then it got pushed out to FY 2023 at which time OBO conducted a survey for a physical security upgrade project now scheduled for FY 2016.” Kearney verified that this post was added to the out-year schedule in FY 2012 for a major upgrade project in FY 2016.

OBO was also reluctant to fund physical security deficiencies at posts that had recently received a NEC. DS officials explained that physical security standards change constantly and that posts can be non-compliant with security standards immediately following a major project. DS officials referred to this situation as the “moving target principle,” where standards change between the time a project is planned and the time the project is completed. For example, in June 2013, OIG reported<sup>33</sup> that multiple embassies and consulates that had received new embassy compounds had physical security deficiencies attributable to changes in physical security standards since the construction of the compounds was completed. DS officials stated that once a post receives a NEC, major rehabilitation project, or major security upgrade project, that post would be far less likely to receive Compound Security Program funding. Although NECs may need physical security upgrades, OBO believes that funding has to be focused on older buildings that have more OSPB deficiencies than the NECs unless there is a specific threat or need at a NEC.

---

<sup>32</sup> DS publishes a Vulnerability List, which ranks facilities according to their vulnerability across a wide variety of security threats on an annual basis, as mandated by SECCA. This list is then used to establish the Top 80 list of posts in which NECs are needed to reduce security vulnerabilities. The Top 80 list shows which posts are scheduled to receive a NEC.

<sup>33</sup> *Audit of Department of State Compliance With Physical/Procedural Security Standards at Selected High Threat Level Posts* (AUD-SI-13-21, Jun. 2013).

## **Long-Range Plan to Address Physical Security Deficiencies Was Lacking**

The Department did not have a comprehensive long-range physical security plan. A long-range plan helps an organization focus on critical needs and provides a sense of direction and purpose. Long-range plans also make day-to-day operations more effective and can be used as the vehicle to guide decision-making for spending.

Although the Department did not have a long-range plan to address physical security deficiencies, OBO developed and issued a Long-Range Plan that provided detailed information, post by post on new construction projects and needed repairs and improvements.<sup>34</sup> According to OBO, the Long-Range Plan is needed to communicate and coordinate maintenance and operations needs to stakeholders—specifically, it helps stakeholders better understand how OBO is addressing challenges and identifying long-term needs. The Long-Range Plan also collocates projects and maintenance needs in one document, serves as a budget tool, and supports long-term strategic efforts.

Kearney reviewed the Long-Range Overseas Maintenance Plan issued in 2010 and found that it included some compound security upgrade projects for posts; however, almost all of these projects were for the installation of mantraps and compound access controls and for FE/BR upgrades. The security standards for these three areas were upgraded, thus OBO included the new requirements in the long-range plan. However, existing physical security needs were not included in the long-range plan.

Although OBO maintained various informal lists detailing when certain physical security projects would be funded, it did not have a plan that illustrated physical security deficiencies, the priority of the deficiencies, and the cost of addressing those deficiencies. Physical security deficiencies are a high-priority issue that should have equal or greater focus than construction or maintenance projects. Having a Long-Range Physical Security Plan would be beneficial to OBO, DS, and all other stakeholders interested in the Department's physical security needs, and it would increase the transparency of the funding process.

## **Important Physical Security Needs Might Not Have Been Funded, and Accountability Was Lacking**

Without complete information on all physical security needs at overseas posts, the Department cannot ensure that it funds the highest priority needs. The Department cannot objectively make a determination about which projects are high priority without a comprehensive list of all physical security needs. Significant physical security deficiencies at all posts, or less significant deficiencies that may create a greater risk at higher threat posts, may not be funded and corrected, leaving some posts more vulnerable to threats. The lack of formal prioritization processes and standards may also result in inconsistent funding decisions on similar physical security deficiencies at posts.

---

<sup>34</sup> Prior to 2012, OBO issued two separate plans—the Long-Range Overseas Buildings Plan and the Long-Range Overseas Maintenance Plan.

**UNCLASSIFIED**

In addition, accountability cannot be established without documentation supporting all post requests, both informal and formal, and the disposition, including the denial, of those requests. Some RSOs expressed concerns that they might be held accountable if they did not make a formal request and an adverse event happened at their post. For example, one post security official stated that because the Department did not always send formal denials for requests for physical security funding, the posts ended up “stuck holding the responsibility if something happens.” This official stated that they believed that DS or OBO should be “forced to send a formal denial” rather than the post being put in “the position of . . . I talked to DS/OBO and they said no.” Another respondent stated, “RSOs have no real mechanism to force OBO . . . to take appropriate action.” The lack of documentation of all decisions made during the request and prioritization processes will also make it difficult to identify breakdowns in the processes and correct them before attacks occur.

Further, if RSOs are discouraged from requesting funding for a physical security need or do not understand the prioritization processes and why their requests are denied, RSOs may not inform or communicate all physical security needs and deficiencies to their respective Desk Officers. This could create an environment in which RSOs feel that they can report only certain types of physical security needs, thereby leaving posts, especially high-threat posts, more vulnerable to threats.

The lack of coordination between DS and OBO may also create confusion about which bureau is responsible for addressing physical security deficiencies outside of OSPB standards, what risk factors should be considered when determining which projects to fund, and how to handle physical security deficiencies at posts where future work is planned. Both DS and OBO are ultimately responsible for ensuring that U.S. Government employees are safe and secure at overseas facilities. Therefore, it is essential that decisionmakers have the most up-to-date information from both DS and OBO on the current environment at the 280 overseas locations to ensure that informed physical security funding decisions are made.

**Recommendation 4.** OIG recommends that the Bureau of Diplomatic Security (DS), in coordination with the Bureau of Overseas Buildings Operations (OBO), develop and implement a process to collect and maintain a comprehensive list of all posts’ physical security-related deficiencies. The list of physical security deficiencies should include all needs, not just those that have been approved or instances of non-compliance with standards. The process should also require that the list be updated when new physical security deficiencies are identified. If DS and OBO elect to use the DS SharePoint Tool as the basis for maintaining a list of physical security needs, DS should ensure that OBO’s requirements are integrated into the development of the tool and that OBO has sufficient access to the information.

**DS Response:** DS concurred with the recommendation, stating that it had deployed a Physical Security Survey site, which, in addition to its Project Management Solution, “will provide a comprehensive list of physical security deficiencies.” However, DS noted that the “physical security requirements are based upon standards set forth by” OSPB. DS further stated that the recommendation is “very inclusive” and “does not take into account the difference between ‘needs’ and ‘wants,’” which “would add an un-vetted

**UNCLASSIFIED**

request and label it as a security deficiency.” DS added that it planned to “meet with OBO to determine OBO requirements to be considered for integration into the new” SharePoint Tool.

**OBO Response:** OBO stated that “the list of physical security deficiencies should consist of valid deficiencies vetted by DS against the appropriate” standards. OBO stated that this would “provide a validated universe of requirements to be addressed, with new valid requirements added as they are identified.”

**OIG Analysis:** OIG considers the recommendation unresolved. OIG agrees that the list of physical security deficiencies to be maintained by the Department should include only “valid” deficiencies. However, there seems to be a discrepancy between what DS, OBO, and OIG consider to be “valid” physical security deficiencies. The list of deficiencies maintained by the Department should include any instance when the physical security at a post is not in accordance with OSPB standards, as suggested by DS and OBO. However, OIG believes the list should also include instances where the condition of the physical security-related equipment or structure no longer allows the item to function properly, which is not always considered a deficiency by the Department. For example, during the exit conference, one DS official suggested that if a FE/BR door had a broken lock, it should not be considered a physical security deficiency, because the existence of a FE/BR door meant that OSPB standards were met. The DS official considered the broken lock to be a maintenance issue, not a physical security deficiency, and did not believe that it was necessary to track this item as a physical security deficiency. In addition, as explained in the report, posts may have physical security deficiencies that are not addressed by OSPB standards.

The Department should maintain a comprehensive list of all physical security-related deficiencies. The list could identify those that have not been approved, are maintenance related, or are not required by standards. However, these deficiencies should be included in a comprehensive and transparent list, and these items should be considered when making decisions on which deficiencies have the highest priority for funding. OIG will resolve this recommendation once DS, in coordination with OBO, agrees to develop and implement a process to collect and maintain a comprehensive list of all posts physical security-related deficiencies, not just one type of deficiency.

**Recommendation 5.** OIG recommends that the Bureau of Diplomatic Security develop an implementation plan for the new SharePoint physical security survey tool. This implementation plan should establish a reasonable deadline for all posts to populate the tool with information on physical security deficiencies and should ensure that the tool has the functionality needed to generate sufficient reports in order to more easily determine posts’ physical security needs.

**DS Response:** DS concurred with the recommendation, stating that it “has established an implementation timeline.” DS further stated that it had “deployed the physical security survey site four months ago” and that its goal was to survey all Chief of Mission facilities “within three years.”

**UNCLASSIFIED**

**OIG Analysis:** OIG considers the recommendation unresolved. The recommendation required DS to develop an implementation plan for the SharePoint physical security survey tool. One component of an implementation plan would be timeframes for implementation, but there are many other items that should be a part of an effective implementation plan. For example, the plan would include details of how the tool would be used across DS offices as well as by OBO. The plan would also ensure that the SharePoint tool had the functionality to generate sufficient reports related to physical security deficiencies. OIG will resolve this recommendation once DS agrees to develop a comprehensive implementation plan for the SharePoint physical security survey tool.

**Recommendation 6.** OIG recommends that the Bureau of Overseas Buildings Operations develop and implement a formal process to document all formal requests made by posts for physical security funding, not just the requests that have been funded or approved, and the disposition of those requests.

**OBO Response:** OBO concurred with the recommendation, noting that “funding will be part of the overall process developed” for Recommendation 1.

**OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that OBO has developed and implemented a process to document all formal requests for funding and the disposition of those requests.

**Recommendation 7.** OIG recommends that the Bureau of Diplomatic Security develop and implement a formal standardized process to vet informal physical security-related funding requests made by posts, which would include documenting all informal requests made by posts for physical security funding, not just the requests that have been approved, and the disposition of those requests.

**DS Response:** DS concurred with the intent of the recommendation but suggested that the recommendation be reworded “to state that DS does not have “informal” requests and all formal requests” are reviewed as outlined in its response to Recommendation 1.

**OIG Analysis:** OIG considers the recommendation unresolved. DS did have an informal process in place to vet posts’ requests before the RSO could submit a formal request for funding. RSOs and Desk Officers discuss a post’s physical security needs. In some cases, the Desk Officer tells the post not to submit a formal request because the Desk Officer believes that it will not be funded. Because this is an informal process, there is no assurance of consistency in decisions being made about what should be submitted for funding. In addition, the Department does not have a comprehensive list of what posts have identified as deficiencies or an accurate report of the disposition of the deficiencies, which makes accountability for decisions made on funding more difficult to determine. OIG will resolve this recommendation once DS agrees to develop and implement a formal standardized process to vet informal physical security-related funding requests made by posts.

**UNCLASSIFIED**

**Recommendation 8.** OIG recommends that the Bureau of Overseas Buildings Operations, in coordination with the Bureau of Diplomatic Security, develop and implement formal standardized processes to prioritize physical security-related deficiencies at posts by category, such as major physical security upgrades, forced-entry/ballistic-resistant projects, and minor physical security upgrades. The prioritizations should be performed based on a comprehensive list of all physical security needs and should be periodically updated based on changes in risk factors or posts' needs. The processes used to perform the prioritizations should be documented and repeatable. In addition, in developing the processes, consideration should be given to how the Overseas Security Policy Board standards will be utilized, what risk factors will be considered, and what impact upcoming major rehabilitation projects or new construction would have on the prioritized rankings.

**OBO Response:** OBO concurred with the recommendation. However, OBO stated that “the prioritization should be performed on a comprehensive list of DS validated deficiencies.”

**OIG Analysis:** OIG considers the recommendation resolved based on OBO's concurrence. This recommendation can be closed when OIG reviews and accepts documentation showing that OBO, in coordination with DS, has developed and implemented formal standardized processes to prioritize physical security-related deficiencies. OIG agrees that OBO should not prioritize physical security-related deficiencies that DS has determined are not valid deficiencies. However, OIG again emphasizes that the list of physical security-related deficiencies should be comprehensive and should note the disposition of the deficiencies, including those determined by DS to not be valid and which OBO will not include in its prioritization process.

**Recommendation 9.** OIG recommends that the Bureau of Diplomatic Security (DS), in coordination with the Bureau of Overseas Buildings Operations (OBO), better define the roles and responsibilities of each bureau to ensure that both bureaus are fully involved in the process to prioritize and fund physical security needs at posts. As part of developing these roles and responsibilities, a process should be established to have a neutral party review and make decisions when disagreements arise about funding decisions between OBO and DS.

**DS Response:** DS concurred with the intent of the recommendation but stated that “DS and OBO work collaboratively” to ensure that the “proper State Operations appropriation is used to fund physical security upgrades.”

**OBO Response:** OBO concurred with the recommendation “with the exception of the neutral party.” OBO stated that it did not think there were “funding decisions” that could not be resolved between OBO and DS; however, if there were, the Under Secretary for Management would make the decision.

**UNCLASSIFIED**

**OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that DS and OBO have better defined roles and responsibilities to ensure that both bureaus are fully involved in the process to prioritize and fund physical security needs at posts. DS and OBO should include a description of the Under Secretary for Management's role in the process.

**Recommendation 10.** OIG recommends that the Bureau of Overseas Buildings Operations, in coordination with the Bureau of Diplomatic Security, develop and issue a Long-Range Physical Security Plan.

**OBO Response:** OBO did not concur with the recommendation, stating that its existing Long-Range Plan "includes Compound Security Program project details and funding totals post by post, where applicable."

**OIG Analysis:** OIG considers the recommendation unresolved. As OIG noted in the report, OBO's Long-Range Plan included some compound security program projects. However, the Plan did not include all physical security-related deficiencies. An acceptable alternative to developing a separate long-range physical security plan would be to expand the existing Long-Range Plan to include all physical security-related deficiencies. OIG will resolve this recommendation when OBO, in coordination with DS, agrees to develop and issue a Long-Range Physical Security Plan.

## **List of Recommendations**

**Recommendation 1.** OIG recommends that the Bureau of Diplomatic Security, in coordination with the Bureau of Overseas Buildings Operations, develop and implement standard policies and procedures for requesting funds for physical security-related needs and document the policies and procedures in a manner that is easily accessible by post security officials (for example, in a “physical security funding handbook”). Consideration should be given to how the SharePoint tool currently in development can be used to simplify the request processes.

**Recommendation 2.** OIG recommends that the Bureau of Overseas Buildings Operations develop and implement a process to respond to posts’ formal requests for physical security-related funding, which should include commitments to respond within certain timeframes.

**Recommendation 3.** OIG recommends that the Bureau of Diplomatic Security develop and implement a methodology to periodically communicate the processes to request funds for physical security-related needs to all post security officials.

**Recommendation 4.** OIG recommends that the Bureau of Diplomatic Security (DS), in coordination with the Bureau of Overseas Buildings Operations (OBO), develop and implement a process to collect and maintain a comprehensive list of all posts’ physical security-related deficiencies. The list of physical security deficiencies should include all needs, not just those that have been approved or instances of non-compliance with standards. The process should also require that the list be updated when new physical security deficiencies are identified. If DS and OBO elect to use the DS SharePoint Tool as the basis for maintaining a list of physical security needs, DS should ensure that OBO’s requirements are integrated into the development of the tool and that OBO has sufficient access to the information.

**Recommendation 5.** OIG recommends that the Bureau of Diplomatic Security develop an implementation plan for the new SharePoint physical security survey tool. This implementation plan should establish a reasonable deadline for all posts to populate the tool with information on physical security deficiencies and should ensure that the tool has the functionality needed to generate sufficient reports in order to more easily determine posts’ physical security needs.

**Recommendation 6.** OIG recommends that the Bureau of Overseas Buildings Operations develop and implement a formal process to document all formal requests made by posts for physical security funding, not just the requests that have been funded or approved, and the disposition of those requests.

**Recommendation 7.** OIG recommends that the Bureau of Diplomatic Security develop and implement a formal standardized process to vet informal physical security-related funding requests made by posts, which would include documenting all informal requests made by posts for physical security funding, not just the requests that have been approved, and the disposition of those requests.

**Recommendation 8.** OIG recommends that the Bureau of Overseas Buildings Operations, in coordination with the Bureau of Diplomatic Security, develop and implement formal

**UNCLASSIFIED**

standardized processes to prioritize physical security-related deficiencies at posts by category, such as major physical security upgrades, forced-entry/ballistic-resistant projects, and minor physical security upgrades. The prioritizations should be performed based on a comprehensive list of all physical security needs and should be periodically updated based on changes in risk factors or posts' needs. The processes used to perform the prioritizations should be documented and repeatable. In addition, in developing the processes, consideration should be given to how the Overseas Security Policy Board standards will be utilized, what risk factors will be considered, and what impact upcoming major rehabilitation projects or new construction would have on the prioritized rankings.

**Recommendation 9.** OIG recommends that the Bureau of Diplomatic Security (DS) and the Bureau of Overseas Buildings Operations (OBO) better define the roles and responsibilities of each bureau to ensure that both bureaus are fully involved in the process to prioritize and fund physical security needs at posts. As part of developing these roles and responsibilities, a process should be established to have a neutral party review and make decisions when disagreements arise about funding decisions between OBO and DS.

**Recommendation 10.** OIG recommends that the Bureau of Overseas Buildings Operations, in coordination with the Bureau of Diplomatic Security, develop and issue a Long-Range Physical Security Plan.

## **Scope and Methodology**

The Office of Inspector General (OIG) contracted with Kearney & Company, P.C., to conduct a performance audit of the processes used by overseas posts to request funds for physical security-related activities and the processes used by the Department of State (Department) to determine which requests for physical security-related activities to fund. Specifically, the objectives of this audit were to identify the FY 2012 funding mechanisms and amounts expended for physical security-related activities at Department-owned or -operated buildings overseas, determine whether the process for posts to request funds for physical security needs at Department-owned or -operated buildings was easy to use and was understood by post security officials, and determine to what extent the Department used physical security funds for high-priority physical security needs at overseas posts during FY 2012.

Kearney conducted fieldwork for this audit from March to August 2013 at the Bureaus of Diplomatic Security (DS), Overseas Buildings Operations (OBO), and Budget and Planning. Kearney planned and performed this audit in accordance with requirements in the Government Accountability Office's *Government Auditing Standards*. Those standards require that Kearney plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. Kearney believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

To obtain background information for this audit, Kearney researched and reviewed the U.S. Code; the Department's *Foreign Affairs Manual* and *Foreign Affairs Handbook*, including the Overseas Security Policy Board standards; the Security Environment Threat List; the Long Range Overseas Maintenance Plan; prior OIG and Government Accountability Office reports; and information available on the Department's Intranet. Kearney reviewed OBO's Repair and Improvement Program Cookbook and the Buildings Management Integrated System (BMIS) overview of the Repair and Improvement program to gain an understanding of the process used to request funds. Kearney obtained the Basic Regional Security Officer course curriculum and materials to gain an understanding of the degree to which Regional Security Officers (RSO) are trained on the process to request funds for physical security needs.

Kearney met with officials from the Bureau of Budget and Planning and OBO to obtain an understanding of the sources of funds the bureaus used to address physical security needs at Department-owned or -operated buildings overseas and the fiscal codes used to record overseas physical security transactions in the Department's accounting system. Based on the information obtained, Kearney identified the fund codes that the Department used for physical security needs. Kearney also identified the function codes<sup>1</sup> that were specific to physical security-related activities. Kearney used this information to identify the amounts expended for physical security-related activities overseas. Specifically, Kearney obtained a detailed transaction listing of

---

<sup>1</sup> Function codes are codes used to identify and report on the type of expenses related to the Department's programs and activities.

**UNCLASSIFIED**

FY 2012 expense activity from the Department's domestic accounting system, the Global Financial Management System (GFMS). Using the security-related fund codes, Kearney summarized the expense activity by program to identify security-related expenditures. Kearney then determined the expenses specifically related to physical security using the identified function codes.

Kearney met with DS and OBO officials to obtain an understanding of the processes for requesting and prioritizing physical security-related activities at overseas posts. Specifically, Kearney met with officials in OBO's Program Security Operations Branch, OBO's Office of Area Management, DS' Project Coordination Branch, and DS' Office of Overseas Protective Operations to gain an understanding of their roles and responsibilities in the physical security funding process. Kearney also obtained an understanding of the Compound Security Program and the types of physical security requests funded from officials in OBO's Program Security Operations Branch, as well as this branch's process for receiving and prioritizing requests.

Kearney met with various officials from OBO's Office of Area Management to determine whether they fund any aspects of physical security as part of the Repair and Construction Program, as well as to learn more about BMIS and how it is used. Kearney met with officials from both the Forced-Entry/Ballistic-Resistant and Mechanical Engineering Divisions, each of which manage subprograms within the Compound Security Program, to determine the specific aspects of compound security upgrades they fund and their process for receiving and prioritizing requests. Kearney met with officials overseeing OBO's Value Engineering programs to obtain information on the value engineering review of all OBO projects and on whether the review has had any significant impact on physical security projects.

Kearney also met with DS Desk Officers from the Project Coordination Branch to obtain an understanding of their role in facilitating and funding physical security requests. Kearney met with officials from DS' Overseas Support Branch to learn if that branch, which is responsible for funding most technical security needs at overseas posts, also funded any aspects of physical security. Kearney met with DS' Office of Regional Directors to learn more about their role in collecting and reviewing security surveys conducted by post security officials. Kearney met with DS' Office of Overseas Protective Operations to gain an understanding of whether that office funds physical security other than through the Residential Security Program. Kearney met with officials from DS' Physical Security Division to learn about the new SharePoint site that DS was creating that will host and retain physical security surveys conducted by post security officials.

To determine whether the process for posts to request funds for physical security-related needs was easy to use and was understood, Kearney, in conjunction with OIG, distributed a questionnaire to post security officials. Information on the methodology used to develop and distribute the questionnaire is included in the section "Detailed Questionnaire Methodology" in this appendix.

To determine the extent to which the Department used physical security funds for high-priority physical security needs, Kearney requested a comprehensive list of all posts' physical security-related deficiencies and a list of posts' FY 2012 requests. However, these lists were not maintained by the Department. In addition, Kearney requested, but was unable to obtain,

## **UNCLASSIFIED**

standard documented criteria for prioritizing the physical security deficiencies and requests. Without this information, Kearney was not able to select a sample of post physical security deficiencies and requests and duplicate the prioritization process. As a result, Kearney could not determine the extent to which high-priority physical needs were funded.

### **Use of Computer-Processed Data**

The audit team used computer-processed data obtained from the Department during this audit. Kearney obtained the FY 2012 trial balance for the Department and details of expenditures made by the Department during FY 2012 from the Department's domestic financial management system, GFMS. The objectives of this audit were not to ensure the accuracy of expenditures made. The information was instead used to try to determine the amount spent during FY 2012 on physical security-related activities. Therefore, Kearney did not perform tests of controls or substantive testing of the expenditure information obtained from GFMS to assess data reliability. However, GFMS is used to prepare the annual financial statements, which are audited. Based on how the information was used in this report, Kearney determined that the data was sufficiently reliable for its needs.

Kearney obtained reports from BMIS to determine whether requests from high-priority posts existed for FY 2012 that had not been addressed, scheduled, or funded by the Department. However, Kearney noted that BMIS was not used to its maximum extent for tracking physical security needs, and the information in the reports did not reflect the current status of potential projects. Therefore, Kearney did not validate the information provided and did not use data from BMIS to draw conclusions.

### **Work Related to Internal Controls**

Kearney performed steps to assess the adequacy of internal controls related to the areas audited. For example, Kearney identified control deficiencies that led to its findings related to the Department's processes to request funding for and prioritize physical security needs. Work performed on internal controls during the audit is detailed in the section "Audit Results" of the report.

### **Detailed Questionnaire Methodology**

The primary objective of the questionnaire was to obtain feedback from post security officials as to whether the process to request funds for physical security needs at overseas buildings was clear and easy to use. OIG requested that responses be limited to funding for physical security-related needs. OIG's SharePoint<sup>2</sup> specialist developed and placed the questionnaire on SharePoint. As post security officials completed and submitted their responses, Kearney viewed and collected those responses via SharePoint.

---

<sup>2</sup> SharePoint is a Microsoft web application platform that provides intranet portals, document and file management collaboration, system migration, process integration, and workflow capabilities.

### **Identification of Regional Security Officers**

OIG obtained a DS Telephone List, dated July 19, 2013, from the DS Intranet site to identify RSOs. If the RSO position for a post was vacant on the DS Telephone List, OIG used the Department's Telephone Directory of Key Officers List, dated July 22, 2013, which was obtained from the Department's Intranet site, to identify the RSO at that location. If there was no RSO listed on either of these lists, OIG identified the next security officer listed for that post, such as the Deputy RSO or the Security Analyst.

OIG emailed the questionnaire with instructions for completion to the 218 security officials identified. In some cases, OIG received a response to the email with an auto-reply message that the individual either had transferred from the post or would be out of the office past the date of the questionnaire's deadline. In these cases, OIG replaced the original addressee by emailing the questionnaire to the next security official on the DS Telephone list or to the alternate person identified in the auto-reply message.

### **Completed Questionnaires**

Of 218 questionnaires distributed to post security officials, OIG received 133 completed questionnaires, for a response rate of 61 percent. Kearney collected the completed questionnaires via SharePoint and exported the data to an Excel spreadsheet for analysis. Of 133 questionnaires received, Kearney excluded one from its aggregate analysis because a response to one question contradicted another, along with the fact that the most of the questionnaire had not been completed. As a result, Kearney analyzed 132 completed questionnaires. The survey and the survey results are provided in Appendix B.



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

*Office of Inspector General*

**Physical-Security Funding Questionnaire**

The Office of Inspector General (OIG), Office of Audits, is conducting an audit of the process used by posts to request funding for physical security-related needs. OIG is requesting that you complete a questionnaire on this subject.

RSOs at Critical/High Threat posts previously received an OIG questionnaire in January 2013, related to **improving security** at critical and high threat posts. That OIG questionnaire included a few questions related to funding needs. After it received the responses to the preliminary questionnaire, OIG made a decision to significantly expand its work related to funding to include an assessment of the process used by all posts to request funding for any physical security need.

The purpose of the current questionnaire is to obtain feedback from post officials as to whether the process for posts to request **funds** for physical security needs at overseas buildings is understandable and easy to use. Although OIG is sending this questionnaire to RSOs, we encourage RSOs to obtain additional information from other post officials, such as the Facilities Maintenance Officer, in order to provide complete information on the **process** used by posts to request funding for physical security needs. If an RSO is responsible for more than one post, OIG requests the responses address funding issues solely at the primary post for which the RSO is responsible.

OIG is requesting that responses be limited to funding for physical security-related needs. For purposes of this questionnaire, OIG defines “physical security” as measures designed to deny access to unauthorized personnel (including attacks or intruders) from facilities and to safeguard personnel working in those facilities. Physical security includes concrete, tangible measures to deter access, such as locked doors, perimeter fences, or other barriers. Technical or Procedural Security needs are not being covered by this audit. In addition, short-term leased, residential property is not included in this audit.

This questionnaire is intended as an initial data-gathering tool. OIG will not issue recommendations based solely on the responses to this questionnaire. This questionnaire should take approximately 15 minutes to complete. However, some requested information may need to be obtained from other sources within the Embassy. Please complete the questionnaire by marking the desired choice or typing in a response when required. Space has been provided at the end of the questionnaire for any additional comments you might want to make.

**UNCLASSIFIED**

*Kearney Notes:*

- 1. Responses are first expressed in raw totals enclosed by parenthesis followed by percentages, unless specified otherwise.*
- 2. The number of responses to each question is not identical because respondents did not answer all questions and some questions allowed multiple answers.*
- 3. Percentages may not add to 100 due to rounding.*
- 4. For Questions 8, 9, and 11-19, asterisks indicate that “Not applicable” responses were filtered from the data for clarity of the analysis and presentation. Only respondents actually providing assessments were included in calculating the percentages reported.*

**UNCLASSIFIED**

1. What is your position at post? *(Please select one.)*
  1. [(104) 79%] Regional Security Officer
  2. [(3) 2%] Deputy Regional Security Officer
  3. [(21) 16%] Assistant Regional Security Officer
  4. [(0) 0%] Post Security Officer
  5. [(4) 3%] Other
  
2. Approximately how many years of experience do you have in Department of State security matters?  years

**Responses averaged 13 years of experience.**

3. Did your post have any physical security-related needs in FY 2012?
  1. [(83) 63%] Yes
  2. [(49) 37%] No
  
4. What was the reason(s) for the physical security-related need(s) of your post in FY 2012? *(Please select all that apply.)*
  1. [(71)] Existing deficiencies
  2. [(38)] Normal deterioration of the facility
  3. [(22)] New physical security requirements established
  4. [(18)] Increase in physical security-related risks at post
  5. [(7)] Other
  
5. Did your post formally request funding for **any** of these physical security-related needs during FY 2012?
  1. [(59) 71%] Yes
  2. [(24) 29%] No
  
6. Please provide the reason(s) for **not** formally requesting funding for **all** needs. *(Please select all that apply; only select "Not applicable" if your post formally requested funds for all of its FY 2012 physical security-related needs.)*
  1. [(8)] Post chose to fund need using post funds
  2. [(8)] Post did not believe that the need would be funded
  3. [(4)] Post was advised by Department officials in Washington not to request funds
  4. [(3)] Funds for same need were requested previously and denied
  5. [(4)] Post received waiver/exception for physical security-related need
  6. [(2)] Post considered process to request funds confusing or difficult
  7. [(30)] Other
  8. [(37)] Not applicable.

**UNCLASSIFIED**

7. Please complete the table below regarding the physical security-related needs of your post in FY 2012. (Please provide the “Number of Needs” for each type of security need; insert “NA” for “Not applicable” in the columns only if you post did **not** make any formal requests to the Department for funds.)

For purposes of this questionnaire, OIG is using the following definitions:

- Minor Physical Security Upgrade – Post-managed projects with upgrades to perimeter protection, facility protection, and interior protection to bring deficient facilities into compliance with OSPB standards. Generally less than \$250,000.
- Major Physical Security Upgrade – OBO-managed projects with upgrades to perimeter protection, facility protection, and interior protection to bring deficient facilities into compliance with OSPB standards. Generally more than \$250,000.
- Repair and Improvement – Projects to restore deteriorated or damaged property to its original condition or increase a property’s value or change its use.
- Other Security Issues – Any projects relating to physical security that are not encompassed by the previous categories, such as upgrades that are not related to OSPB standards but may be warranted given special circumstances at an overseas post.

Type of Security-Related Need	Number of Needs	Number of Requests to Fund Needs	Number of Requests Funded by the Department
Minor Physical Security Upgrades	[Range: 0–12]	[Range: 0–10]	[Range: 0–10]
Major Physical Security Upgrades	[Range: 0–6]	[Range: 0–5]	[Range: 0–5]
Repair and Improvement	[Range: 0–20]	[Range: 0–10]	[Range: 0–10]
Other Security Issues Please Specify in the box provided, which will expand. <input type="text"/>	[Range: 0–5]	[Range: 0–2]	[Range: 0–2]

8. For approximately what **percentage** of formal requests that were **not** funded did the post receive an explanation from Department officials in Washington? (Please insert the percent in the box below; only select “Not applicable” if your post’s formal requests were always funded or your post did not make any formal requests.)

[Responses averaged 44%]  percent

[\*]  Not applicable

**UNCLASSIFIED**

9. Generally, how adequate or inadequate were the responses from Department officials in Washington as to why formal requests were **not** funded? *(Please select one; only select “Not applicable” if your post never received a response or your post did not make any formal requests.)*

1. **[(8) 24%]** Very adequate
2. **[(5) 15%]** Somewhat adequate
3. **[(7) 21%]** Neither adequate nor inadequate
4. **[(5) 15%]** Somewhat inadequate
5. **[(9) 26%]** Very inadequate
6. **[\*]** Not applicable

10. For formal requests for physical security funding made by the post that were **not** funded, in what manner was post notified that the request was denied? *(Please select all that apply; only select “Not applicable” if your post’s requests were always funded or your post did not make any formal requests.)*

1. **[7]** Cable
2. **[9]** E-mail from OBO
3. **[4]** E-mail from DS
4. **[4]** Phone call from OBO
5. **[1]** Phone call from DS
6. **[6]** Post was not informed that a formal request was denied
7. **[12]** Other
8. **[50]** Not applicable

11. Irrespective of whether your post formally requested funding for any physical security-related needs, please provide the approximate total dollar amount of post funds spent in FY 2012 to address physical security-related needs. *(Please insert the amount in the box below; only select “Not applicable” if your post did not spend any of its funds for physical security-related needs.)*

**[Responses ranged between \$1,000-\$2,500,000 and averaged \$198,410]** \$  of post funds  
**[\*]**  Not applicable

**UNCLASSIFIED**

12. Irrespective of whether your post formally requested funding for any physical security-related needs, please provide the approximate total dollar amount spent in FY 2012 from funds received from other agencies to address physical security-related needs. *(Please insert the amount in the box below; only select “Not applicable” if your post did not formally request and did not receive any funds from other agencies.)*

**[Responses ranged between \$15,000-\$6,000,000 and averaged \$1,086,421]** \$  from other agencies  
[\*]  Not applicable

13. How adequate or inadequate are the written policies and procedures requesting funds for physical security-related needs? *(Please select one; only select “Not applicable” if you never formally requested funds for security-related needs in FY 2012 or any other time.)*

1. **[(19) 20%]** Very adequate
2. **[(38) 40%]** Somewhat adequate
3. **[(19) 20%]** Neither adequate nor inadequate
4. **[(14) 15%]** Somewhat inadequate
5. **[(6) 6%]** Very inadequate
6. [\*] Not applicable

14. To what extent, if at all, do you find the Security Equipment Responsibilities Matrix useful to request funding for security-related needs? *(Please select one; only select “Not applicable” if you never used the matrix.)*

1. **[(21) 23%]** Very great use
2. **[(24) 26%]** Great use
3. **[(27) 29%]** Moderate use
4. **[(12) 13%]** Some use
5. **[(9) 10%]** Little or no use
6. [\*] Not applicable

15. How adequate or inadequate is the training for requesting funds for physical security-related needs? *(Please select one; only select “Not applicable” if you never received training.)*

1. **[(3) 4%]** Very adequate
2. **[(20) 25%]** Somewhat adequate
3. **[(17) 21%]** Neither adequate nor inadequate
4. **[(17) 21%]** Somewhat inadequate
5. **[(24) 30%]** Very inadequate
6. [\*] Not applicable

**UNCLASSIFIED**

16. How adequate or inadequate is the assistance for requesting funds for physical security-related needs provided by the following sources of assistance. (Please select one box in each row; only select “NA” for “Not applicable” if you **never** availed yourself of any assistance from DS and/or OBO.)

Source of Assistance	Very Adequate	Somewhat Adequate	Neither Adequate nor Inadequate	Somewhat Inadequate	Very Inadequate	Not Applicable
DS assistance	[(44) 40%]	[(49) 44%]	[(11) 10%]	[(6) 5%]	[(1) 1%]	*
OBO assistance	[(18) 17%]	[(31) 30%]	[(23) 22%]	[(19) 18%]	[(14) 13%]	*

17. How timely or untimely is the assistance provided by the following sources during the process of requesting funds for physical security-related needs? (Please select one box in each row; only select “NA” for “Not applicable” if you **never** availed yourself of any assistance from DS and/or OBO.)

Source of Assistance	Very Timely	Timely	Neither Timely nor Untimely	Untimely	Very Untimely	Not Applicable
DS assistance	[(33) 30%]	[(48) 44%]	[(21) 19%]	[(8) 7%]	[(0) 0%]	*
OBO assistance	[(14) 14%]	[(27) 26%]	[(31) 30%]	[(20) 19%]	[(11) 11%]	*

18. How clear or unclear do you find the processes to request funding for security-related needs in the following categories? (Please select one box in each row; only select “NA” for “Not applicable” if you **never** requested funds for security-related needs in FY 2012 or any other time.)

Type of Need	Very Clear	Somewhat Clear	Neither Clear Nor Unclear	Somewhat Unclear	Very Unclear	Not Applicable
Minor Physical Security Upgrades	[(21) 21%]	[(44) 44%]	[(15) 15%]	[(17) 17%]	[(3) 3%]	*
Major Physical Security Upgrades	[(17) 18%]	[(30) 32%]	[(15) 16%]	[(21) 22%]	[(11) 12%]	*
Repair and Improvement	[(18) 20%]	[(33) 36%]	[(15) 16%]	[(21) 23%]	[(4) 4%]	*
Other Security Issues	[(14) 16%]	[(29) 34%]	[(18) 21%]	[(22) 26%]	[(2) 2%]	*

**UNCLASSIFIED**

19. How easy or difficult to use do you find the process to request funding for security-related needs in the following categories? *(Please select one box in each row; only select “NA” for “Not applicable” if you **never** requested any funds for security-related needs in FY 2012 or any other time.)*

Type of Need	Very Easy	Somewhat Easy	Neither Easy nor Difficult	Somewhat Difficult	Very Difficult	Not Applicable
Minor Physical Security Upgrades	[(13) 13%]	[(35) 35%]	[(28) 28%]	[(20) 20%]	[(4) 4%]	*
Major Physical Security Upgrades	[(5) 6%]	[(24) 27%]	[(31) 35%]	[(18) 20%]	[(11) 12%]	*
Repair and Improvement	[(11) 13%]	[(27) 31%]	[(28) 32%]	[(18) 20%]	[(4) 5%]	*
Other Security Issues	[(7) 8%]	[(26) 31%]	[(29) 35%]	[(16) 19%]	[(5) 6%]	*

20. Please provide any comments concerning the overall process for requesting funds for physical security-related needs as well as any other information that you think is important or pertinent. *(If you choose to respond, please type in the box provided, which will expand to accommodate the size of your response.)*

**69 responses were provided to this optional question.**

**Bureau of Diplomatic Security Response**



United States Department of State

Washington, D.C. 20520

[www.state.gov](http://www.state.gov)

**UNCLASSIFIED**

February 21, 2014

**INFORMATION MEMO TO INSPECTOR GENERAL LINICK – OIG**

FROM: DS– Gregory B. Starr

A handwritten signature in black ink, appearing to read "Gregory B. Starr".

FEB 21 2014

SUBJECT: DS Comments and Responses to the OIG Audit of the Process to Request and Prioritize Physical Security-Related Activities at Overseas Posts (AUD-FM-14-XX, January 2014)

Attached is the Bureau of Diplomatic Security's response to the draft report.

**Attachment:**

As stated.

**UNCLASSIFIED**

UNCLASSIFIED

**DS Comments to OIG Audit Draft Report  
Audit of the Process to Request and Prioritize  
Physical Security-Related Activities at Overseas Posts  
(January 2014)**

DS appreciates the opportunity to comment on the Office of Inspector General's (OIG), (Draft) Report of the Audit of the Process to Request and Prioritize Physical Security Activities at Overseas Posts. DS believes the independent audits and analysis undertaken by OIG are valuable tools in improving the performance of our programs. DS also appreciates that OIG recognized the Bureau's efforts to incorporate recommendations and strengthen our programs.

On February 3, 2014, DS requested OIG send a copy of this draft report to each Regional Bureau Executive (EX) office for their comments. The Regional Bureau EX offices had lease issues that are entwined with physical security recommendations. The Post Management Officers (PMOs) need to have some visibility on facility recommendations. However, DS was informed that OIG would not allow the draft report to be sent to the regional EX offices. OIG would only share the draft reports with the action bureau at this time. DS believes it is necessary for the regional EX offices to provide input and would like it noted that we requested action be taken.

UNCLASSIFIED

## UNCLASSIFIED

UNCLASSIFIED

DS provides the following edits to the attached OIG draft audit:

**International Programs Directorate/High Threat Programs Directorate.** The ~~International Programs Directorate's~~ mission of these directorates is to provide leadership, support, and oversight of overseas security and law enforcement programs and related policy for the benefit of U.S. Government interests and the international community. The Directorate's Office of Regional Directors works to provide a safe and secure environment for the conduct of U.S. foreign policy through the oversight and support of Regional Security Offices worldwide. The Office of Regional Directors oversees the work of over 700 regional security officers (RSO) at over 250 posts worldwide. RSOs serve as personal security advisors to the Chiefs of Mission on all security issues. RSOs are responsible for implementing and managing the Department's security and law enforcement programs abroad, and identify security needs at posts and request funds for those needs. RSOs are residents at a particular post, but may be responsible for other constituent posts within their respective region.

**Recommendation 1:** OIG recommends that the Bureau of Diplomatic Security, in coordination with the Bureau of Overseas Buildings Operations, develop and implement standard policies and procedures for requesting funds for physical security-related needs and document the policies and procedures in a manner that is easily accessible by post security officials (for example, in a "physical security funding handbook"). Consideration should be given to how the SharePoint tool currently in development can be used to simplify the request processes.

**DS Comment:** DS currently has a process for posts that require additional funding, whether it is related to physical security, residential security, the local guard program, etc. The process will be clearly articulated as part of an annual operating cable sent to RSOs, which is in draft. Posts, RSOs in particular, are instructed through operational cables and also through regular communications from program offices via cable, email, or telephone to send a front channel cable outlining the security requirement and include funding implications. The security requirement is vetted by the appropriate DS program office and, if approved as a security requirement, the DS office determines whether the requirement should be funded by DS or the Bureau of Overseas Buildings Operations (OBO). If funding is not available, the DS office coordinates with the Office of the Chief Financial Officer (DS/EX/CFO) to identify funding. DS/EX/CFO also validates the requests to ensure the correct State Operations appropriation is used. If DS believes that OBO, not DS, should fund, then DS/EX/CFO works with the appropriate offices within the Office of the Legal Adviser and OBO's Office of Financial

UNCLASSIFIED

## UNCLASSIFIED

UNCLASSIFIED

Management (OBO/RM/FM) to make a determination. DS will ensure this procedure is clearly articulated to posts, including through the use of an annual operating cable.

Regarding SharePoint, DS uses this program for many tasks; however, for requesting funding, a formal front channel cable funding request with direct response from the appropriate DS program office and DS/CFO funding validation are more appropriate.

**Recommendation 3:** OIG recommends that the Bureau of Diplomatic Security develop and implement a methodology to periodically communicate the processes to request funds for physical security-related needs to all post security officials.

**DS Comment:** DS concurs with the OIG recommendation. DS will explore the possibility of integrating funding guidance and/or a funding request process within our new Physical Security Survey site or Project Management Solution. DS will also include language about requesting funds for physical security upgrades in its annual operating cable.

**Recommendation 4:** OIG recommends that the Bureau of Diplomatic Security (DS), in coordination with the Bureau of Overseas Buildings Operations (OBO), develop and implement a process to collect and maintain a comprehensive list of all posts' physical security-related deficiencies. The list of physical security deficiencies should include all needs, not just those that have been approved or instances of noncompliance with standards. The process should also require that the list be updated when new physical security deficiencies are identified. If DS and OBO elect to use the DS SharePoint Tool as the basis for maintaining a list of physical-security needs, DS should ensure that OBO's requirements are integrated into the development of the tool and that OBO has sufficient access to the information.

**DS Comment:** DS concurs with the OIG recommendation. On September 16, 2013, DS deployed the Physical Security Survey site, which provides RSOs with re-designed survey templates, a set of tools, and guidance to conduct accurate and comprehensive physical security surveys. This survey site, in addition to our Project Management Solution, will provide a comprehensive list of physical security deficiencies. However, it should be noted the physical security requirements are based upon standards set forth by the Overseas Security Policy Board (OSPB). In circumstances where extraordinary measures are recommended,

UNCLASSIFIED

**UNCLASSIFIED**

UNCLASSIFIED

these recommendations must be vetted at the appropriate Assistant Secretary or Under Secretary level within the Department.

DS believes the recommendation is very inclusive and does not take into account the difference between “needs” and “wants.” This would add an un-vetted request and label it as a security deficiency under a master list.

DS will meet with OBO to determine OBO requirements to be considered for integration into the new Physical Security Survey Site and business process. DS cannot provide a timeframe for integration until OBO requirements are defined.

**Recommendation 5:** OIG recommends that the Bureau of Diplomatic Security develop an implementation plan for the new SharePoint physical security survey tool. This implementation plan should establish a reasonable deadline for all posts to populate the tool with information on physical security deficiencies and should ensure that the tool has the functionality needed to generate sufficient reports in order to more easily determine posts’ physical security needs.

**DS Comment:** DS concurs with the OIG recommendation and has established an implementation timeline. DS deployed the physical security survey site four months ago. A message was sent on the RSO console to posts worldwide explaining the new tool (refer to the details in the attached document). In addition, training was offered during the Bureau of Western Hemisphere Affairs (WHA) and High Threat Programs (DS/HTP) RSO conferences held in Washington.

The DS goal is to survey all COM facilities (2,000 +) within three years. The three-year time frame is aligned with the existing survey update cycle.

**Recommendation 7:** OIG recommends that the Bureau of Diplomatic Security develop and implement a formal standardized process to vet informal physical security-related funding requests made by posts, which would include documenting all informal requests made by posts for physical security funding, not just the requests that have been approved, and the disposition of those requests.

**DS Comment:** DS concurs with the intent of this OIG recommendation but recommends rewording the language. DS clearly states that if a post has a requirement, post must send a cable. If an RSO sends an email and the program office agrees with the need, the RSO should be instructed to send a cable, per guidance. DS believes the language should be changed to state that DS does not

UNCLASSIFIED

**UNCLASSIFIED**

UNCLASSIFIED

have “informal” requests and all formal requests, i.e., those sent via cable, are reviewed as outlined in Recommendation 1.

**Recommendation 9:** OIG recommends that the Bureau of Diplomatic Security (DS) and the Bureau of Overseas Buildings Operations (OBO) better define the roles and responsibilities of each bureau to ensure that both bureaus are fully involved in the process to prioritize and fund physical security needs at posts. As part of developing these roles and responsibilities, a process should be established to have a neutral party review and make decisions when disagreements arise about funding decisions between OBO and DS.

**DS Comment:** DS concurs with the intent of this recommendation. As described in the response to Recommendation 1, DS and OBO work collaboratively and in close coordination with the Office of the Legal Adviser to ensure the proper State Operations appropriation is used to fund physical security upgrades. Moreover, DS and OBO strictly adhere to the “pick-and-stick” rule that appropriated funding for a specific activity must adhere to that specified purpose, as well as to the regulations as codified in the FAM and FAH.

UNCLASSIFIED

**UNCLASSIFIED**

**Appendix D**

**Bureau of Overseas Buildings Operations Response**



United States Department of State

Washington, D.C. 20520

**UNCLASSIFIED**  
**MEMORANDUM**

FEB 19 2014

TO: OIG/AUD – Mr. Norman Brown

FROM: OBO/RM – Jürg Hochuli *jh*

SUBJECT: Draft Report on *Audit of the Process to Request and Prioritize Physical Security Related Activities at Overseas Posts*

The Bureau of Overseas Buildings Operations (OBO) appreciates the opportunity to provide comments on the subject draft report.

Attached are OBO's comments on the draft report. Our comments have been coordinated with the Bureau of Diplomatic Security.

Attachment:

As stated

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

**OBO Comments on the OIG Draft Report on  
Audit of the Process to Request and Prioritize Physical  
Security Related Activities at Overseas Posts**

The OIG requested OBO comments on the subject draft report. OBO appreciates the opportunity to provide the following comments.

**OBO's Comments:** The draft report contains several misleading statements concerning the auditor's inability to determine how much was expended for physical security in FY 2012. The report indicates that the Department expended approximately \$938 million of Worldwide Security Upgrade funds, but could only attribute \$76.1 million directly to physical security-related activities. The Department strongly disagrees with this mischaracterization of the facts. Funding in the Worldwide Security Upgrade account is appropriated by Congress specifically and solely for the purpose of making physical security upgrades to existing facilities or for the acquisition or construction of new facilities to improve the security of the most vulnerable overseas posts. The Department is prohibited by law from using those funds for a purpose other than for security upgrades so by definition, all expenditures of these funds are for physical security. Therefore, the report should be corrected to recognize the fact that the Department expended approximately \$938 million of Worldwide Security Upgrade funds for physical security-related activities, including the acquisition and construction of new facilities.

The report makes several references to spending for security upgrades from accounts such as R&I and Major Rehabilitation and includes statements such as "Because R&I expenditures were recorded using R&I function code, the physical security expenditures could not be accounted for separately" or "...because physical security components are included as part of the overall project, the physical security expenditures cannot be identified separately by function code..." Such statements can be interpreted to imply that OBO did not properly account for the physical security costs or that there is a deficiency in the Department's account structure. In fact, those costs were accounted for appropriately.

The Compound Security Program exists specifically to fund physical security upgrade projects, but it is not the only account from which security work may be funded. As the report mentions, repairs to building systems or structures are funded from the R&I account and it is a legitimate use of R&I funds to apply them

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

to a repair of a wall, door, or window. Similarly, the Major Rehabilitation Program funds comprehensive renovation projects that may include physical security enhancements. All expenditures for these projects are correctly charged to the R&I or Major Rehab function codes, regardless of the specific scopes of work or what building systems are being worked on. The security components are not accounted for separately, and neither is the electrical, plumbing, or structural work. For management and reporting purposes, the tracking of spending is done at the project and function code level and the Department has no need or ability to track costs for every type of work that may be included in a project.

OIG Statement on Page 12: The OIG states on page 12 that “In addition to the expenditures for the three Worldwide Security Upgrade Programs, Kearney identified expenditures of approximately \$26.9 million for other items.”

**OBO’s Comments**: **The \$26.9 million figure includes \$20.5 million of ICASS charges, likely from ICASS services on NEC and rehab projects.**

OIG Statement on Page 13: The OIG states on page 13 “Because R&I expenditures were recorded using the R&I function *code*, the physical security expenditures could be identified separately.”

**OBO’s Comments**: ***Code* should be *codes* as there is more than one R&I function code. Secondly, as noted above, the security components are not accounted for separately. For management and reporting purposes, the tracking of spending is done at the project and function code level and the Department has no need or ability to track costs for every type of work that may be included in a project.**

OIG Statement on Page 14: OIG states on page 14 that ... “DS has used Worldwide Security Protection funds for physical security related projects when the projects were not funded by OBO... For example, DS had provided Worldwide Security Protection funds totaling \$259,920 in FY 2012 for six physical security projects relating to perimeter and internal security in Libya, Saudi Arabia, and Yemen.”

**OBO’s Comments**: **This implies that the costs should have been OBO costs. While we do not have the specific details, DS provided funding in FY 2012 for the Sanaa residential security upgrade, as well as upgrades at temporary mission facilities, using the correct DS funding. Same comment on page 30,**

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

**the funding was for the temporary mission facilities, again using the correct (DS) funding.**

OIG Statement on Page 21: OIG states on page 21 that, “Further, 40 respondents (30 percent) stated that their posts used post funds ranging from \$1,000 to \$2.5 million for physical security needs in FY 2012 rather than submitting a formal request for funding.”

**OBO’s Comments**: The report notes that OBO and DS stated this would be in violation of appropriation law. It is speculation without knowing the posts in question, but a more likely answer (since the survey went only to security officers and not finance officers) is that the survey responses were in error. Finance is not something RSOs specialize in, nor should they. They often refer to funding sent by OBO as “DS funding”. The wording of the question could also have contributed to the responses (see OBO Comments to Questionnaire Question 11 below, see page 5).

OIG Statement on Page 23: OIG states on page 23 that ... “Instead funding decisions were often made by one individual without documented standards and guidance.”

**OBO’s Comments**: Funding decisions (determining the appropriate funding source for proposed security upgrades) are based on the funding responsibilities outlined in 15 FAM 165. In addition, OBO would like to note that there is an OBO-DS Physical Security Responsibility Matrix that was approved by U/S Kennedy. This document describes which office/Bureau is responsible for funding and undertaking repairs and/or maintenance of physical security equipment at posts thereby guiding funding decisions.

OIG Statement on Page 23: OIG states on page 23 that “Neither DS nor OBO had developed a comprehensive long-range physical security plan that would help focus attention on critical needs.”

**OBO’s Comments**: OBO would like to note that OBO’s Long-Range Plan which is made available to all posts includes Compound Security Program project details and funding totals for each post, where applicable.

OIG Statement on Page 27: The OIG states on page 27 “Kearney also identified an instance where a post that was ranked in the top 15 percent of the most vulnerable

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

posts on the DS Risk Matrix was not scheduled for an upgrade until FY 2017, while 25 of the 29 posts scheduled ... were ranked lower.”

**OBO’s Comments:** The post at issue is a low risk post which is considered in our assessment of the vulnerabilities. The main facilities have very little setback, and there has been a succession of projects to improve the security situation as much as possible, given the location. There was a PAC project in 2005, and there were barriers, booths, and knee wall projects around 2009. As was noted specifically on this post and projects in the interviews, we are currently working with post on safe area projects in the main and leased office space, but most of what can be done with the existing facility has already been done. It is not being ignored, but there is little more that can be done.

OIG Statement on Page 28: The OIG states on page 28 that ...“Area Management Officers within OBO’s Office of Area Management score the requests by assigning weighted factors to 12 specific criteria...”

**OBO’s Comments:** OBO uses 14 specific criteria, not 12.

OIG Statement on Page 30: The OIG states on page 30...“DS officials requested that OBO fund barriers to block off the road leading to the chancery entrance. However, OBO did not fund the request because the barriers would be placed outside the perimeter of the compound and were therefore not required by OSPB standards.”

**OBO’s Comments:** The post in question is a fully OSPB-compliant NEC, and the initial plan was to construct a diplomatic enclave by installing barriers on public roads approaching our compound and enclosing numerous missions in the area. Nonetheless, once the details of the project were worked out, it was funded in November 2012.

OIG Statement on Page 30: The OIG also states on page 30, “However, when OBO does decline to fund physical security needs that DS considers essential, it can be difficult for DS to address the deficiency. If DS considers the deficiency significant, the Desk Officers attempt to identify available funding that can be used. For instance, in FY 2012, the Office of Physical Security Programs funded six physical security projects, totaling \$259,820, that were related to perimeter security.”

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

and received. The independent clause – “please provide the approximate total dollar amount of post funds spent in FY 2012 to address physical security-related needs” likely included physical security funding provided to posts.

**OBO Comments on the Recommendations:**

Recommendation 1: OIG recommends that DS in coordination with OBO, develop standard policies and procedures for requesting funds for physical security related needs and document the policies and procedures.

**OBO’s Comments:** The recommendation should be changed slightly to “... policies and procedure for requesting physical security upgrades and document the policies and procedures ...” The distinction is needed since funding is near the end of the process – first the need has to be identified, scoped, possibly designed, etc. before a funding action is needed.

Recommendation 2: OIG recommends that the OBO develop and implement a process to respond to posts’ formal requests for physical security-related funding, which should include commitments to respond within certain timeframes.

**OBO’s Comments:** OBO concurs, noting that funding will be part of the overall process developed in Recommendation 1.

Recommendation 4: OIG recommends that the Bureau of Diplomatic Security (DS), in coordination with the Bureau of Overseas Buildings Operations (OBO), develop and implement a process to collect and maintain a comprehensive list of all posts’ physical security-related deficiencies. The list of physical security deficiencies should include all needs, not just those that have been approved or instances of noncompliance with standards. The process should also require that the list be updated when new physical security deficiencies are identified. If DS and OBO elect to use the DS SharePoint Tool as the basis for maintaining a list of physical-security needs, DS should ensure that OBO’s requirements are integrated into the development of the tool and that OBO has sufficient access to the information.

**OBO’s Comments:** The list of physical security deficiencies should consist of valid deficiencies vetted by DS against the appropriate OSPB physical security standards. This will provide a validated universe of requirements to be addressed, with new valid requirements added as they are identified.

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

**OBO's Comments:** The six projects were properly funded by DS with DS funds. Sanaa was residential security upgrades to a STL property.

OIG Statement on Page 32: The OIG also states on page 32 that ... "OBO developed and issued a Long-Range Plan that provided detailed information post by post on new construction projects and needed repairs and improvements."

**OBO's Comments:** As noted previously, the Long-Range Plan which is made available to all posts also includes Compound Security Program project details and funding totals post by post, where applicable.

**OBO Comments on Questionnaire:**

It is difficult to address the conclusions from the questionnaire data without knowing the specific posts and issues. For example, "formal requests" would typically be via cable. Absent more specific information, we cannot determine whether the "denial" was by DS or OBO, or the reason for the denial of specific individual items.

Since the posts that responded to the questionnaire stated that they have pending security upgrade needs, the specific posts should be identified to OBO and DS for immediate follow-up to help identify and address existing vulnerabilities.

OIG Questionnaire Question 4: What was the reason for physical security related needs for your post?

**OBO's Comments:** The second most common answer was "normal deterioration of the facility". It is unclear how this is physical security related – absent more specific information.

OIG Questionnaire Question 11: Irrespective of whether your post formally requested funding for any physical security-related needs, please provide the approximate total dollar amount of post funds spent in FY 2012 to address physical security-related needs.

**OBO's Comments:** Given the large dollar amounts reported, it is likely that the reported totals include security upgrade funding that post had requested

**UNCLASSIFIED**

5

**UNCLASSIFIED**

**UNCLASSIFIED**

**Recommendation 6:** OIG recommends that the Bureau of Overseas Buildings Operations develop and implement a formal process to document all formal requests made by posts for physical security funding, not just the requests that have been funded or approved, and the disposition of those requests.

**OBO's Comments:** OBO concurs, noting that funding will be part of the overall process developed in Recommendation 1.

**Recommendation 8:** OIG recommends that the Bureau of Overseas Buildings Operations, in coordination with the Bureau of Diplomatic Security, develop and implement formal standardized processes to prioritize physical security-related deficiencies at posts by category, such as major physical security upgrades, forced-entry/ballistic-resistant projects, and minor physical security upgrades. The prioritizations should be performed based on a comprehensive list of all physical security needs and should be periodically updated based on changes in risk factors or posts' needs. The processes used to perform the prioritizations should be documented and repeatable. In addition, in developing the processes, consideration should be given to how the Overseas Security Policy Board standards will be utilized, what risk factors will be considered, and what impact upcoming major rehabilitation projects or new construction would have on the prioritized rankings.

**OBO's Comments:** OBO concurs, with the same comment as Recommendation 4 – the prioritization should be performed on a comprehensive list of DS validated deficiencies.

**Recommendation 9:** OIG recommends that the Bureau of Diplomatic Security (DS) and the Bureau of Overseas Buildings Operations (OBO) better define the roles and responsibilities of each bureau to ensure that both bureaus are fully involved in the process to prioritize and fund physical security needs at posts. As part of developing these roles and responsibilities, a process should be established to have a neutral party review and make decisions when disagreements arise about funding decisions between OBO and DS.

**OBO's Comments:** OBO concurs with the exception of the neutral party. We do not think there are, or have been, "funding decisions" that could not be resolved within and between OBO and DS. If it really reached that level, M would decide.

**UNCLASSIFIED**

7

**UNCLASSIFIED**

**UNCLASSIFIED**

Recommendation 10: OIG recommends that the Bureau of Overseas Buildings Operations, in coordination with the Bureau of Diplomatic Security, develop and issue a Long-Range Physical Security Plan.

**OBO's Comments**: OBO does not concur. OBO's Long-Range Plan which is made available to all posts includes Compound Security Program project details and funding totals post by post, where applicable.

**UNCLASSIFIED**

8

**UNCLASSIFIED**