United States Government Accountability Office

Report to Congressional Addressees

September 2017

DIPLOMATIC SECURITY

Key Oversight Issues

Accessible Version

GAO-17-681SP

Contents

Tables

Figures

Abbreviations

ARB	Accountability Review Board
CISO	Chief Information Security Officer
Diplomatic Security	Bureau of Diplomatic Security
DOD	Department of Defense
EAC	Emergency Action Committee
EAP	Emergency Action Plan
FACT	Foreign Affairs Counter Threat training
FAH	*Foreign Affairs Handbooks*
FISMA	Federal Information Security Modernization Act of 2014
HTSOS	High Threat Security Overseas Seminar
LES	locally employed staff
LDP	language-designated position
M/PRI	Office of Management Policy, Rightsizing, and Innovation
MSG	Marine Security Guard
IRM	Bureau of Information Resource Management
OBO	Bureau of Overseas Buildings Operations
OCO	Overseas Contingency Operations
OMB	Office of Management and Budget
OSPB	Overseas Security Policy Board
RSO	Regional Security Officer
SED	standard embassy design
SPMAGTF-CR	Special Purpose Marine Air-Ground Task Force for Crisis Response
State	Department of State

USAID	U.S. Agency for International Development

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

September 7, 2017

Congressional Addressees:

On August 7, 1998, terrorists bombed the U.S. embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, killing over 220 people and injuring 4,000 others. The 1998 bombings marked a pivotal moment in the conduct of U.S. diplomacy, as it became clear that terrorist networks had the ability and intent to exploit security vulnerabilities at American diplomatic missions.[1] Since 1998, U.S. personnel working in diplomatic facilities overseas have faced increasing threats to their safety and security, including numerous attacks in high-risk locations. On September 11, 2012, U.S. facilities in Benghazi, Libya, came under attack, and four U.S. officials—including the Ambassador—were killed. In the same month, a car bomb hit U.S. government vehicles in Pakistan, injuring two Americans, and protesters in Egypt, Yemen, Sudan, and Tunisia overran the U.S. embassies' security defenses and broke into the embassy compounds. These attacks resulted in close scrutiny of the Department of State's (State) security practices overseas. In response to these security incidents over the years, and in light of its policy to maintain diplomatic missions in Iraq, Afghanistan, and other increasingly dangerous environments, State has taken a number of steps to enhance its risk management and security efforts aimed at protecting U.S. personnel and facilities at its overseas diplomatic posts.

State's Bureau of Diplomatic Security (Diplomatic Security) is responsible for the protection of people, property, and information at State's 275 overseas posts[2] and 152 domestic locations.[3] In addition to guarding against threats from terrorism, Diplomatic Security must also counter a range of other threats, such as crime, espionage, visa and passport fraud, technological intrusions, political violence, and weapons of mass destruction. To fulfill its mission, Diplomatic Security collaborates with

[1]All U.S. embassies, consulates, and other diplomatic posts in foreign countries are known collectively as *missions* and they all share the common goal of carrying out the foreign policy of the U.S. government.

[2]State operates 183 foreign missions. A mission might be comprised of more than one post.

[3]Domestic locations refers to domestic facilities that Diplomatic Security is responsible for protecting such as State's headquarters, Diplomatic Security field offices, and passport agency offices, among others.

other State entities—such as the Bureaus of Overseas Buildings Operations (OBO) and Information Resource Management—and other U.S. government agencies, including the Department of Defense (DOD).

Given the ongoing threats facing U.S. personnel overseas who carry out U.S. foreign policy and the amount of resources needed to counter those threats, we prepared this special publication to identify a number of key issues for Congress to consider in its oversight of U.S. diplomatic security. We believe these issues warrant significant oversight because of their cost and impact and the need to ensure progress. This report contains 11 enclosures, each including information based largely on prior GAO work in the following specific areas:

- *Diplomatic Security Funding:* Since 1998, Diplomatic Security funding has increased considerably in reaction to a number of security incidents overseas and domestically. In fiscal year 2016, total funding for Diplomatic Security operations—which includes its bureau managed funds as well as other funding, such as personnel salaries, managed by other bureaus and offices—was almost $4.8 billion.
- *Diplomatic Security Staffing Challenges:* Diplomatic Security's workforce—including 3,488 direct-hire, 1,989 other U.S. government, and 45,870 contract personnel—continues to grow. However, potential challenges exist regarding the distribution of domestic and overseas positions, posting fully-qualified individuals in the assignments with the greatest needs, and ongoing efforts to fill language-designated positions.
- *Physical Security of U.S. Diplomatic Facilities:* Diplomatic Security and OBO collaborate to ensure that safety standards are met when constructing new embassies and mitigating risks at existing facilities. However, we found weaknesses in their process to address some security vulnerabilities, among other things. In addition, State does not have guidelines in place for security at temporary facilities, which they use in dangerous posts, such as Kabul, Afghanistan.
- *Physical Security of Diplomatic Residences and Other Soft Targets:* State has taken steps to address residential security vulnerabilities and manage risks at schools and other soft targets overseas. However, we found weaknesses in State's process to address residential security vulnerabilities.
- *Security Training Compliance:* While State has robust security training requirements, it lacks consistent monitoring and enforcement processes, particularly for its Foreign Affairs Counter Threat training and for security refresher briefings at posts.

- *Embassy Crisis and Evacuation Preparedness:* Gaps in State's implementation and monitoring of crisis and evacuation preparedness could endanger staff assigned to overseas posts and the family members accompanying them.
- *Department of Defense Support to U.S. Diplomatic Missions:* Following the Benghazi attacks, DOD increased its support to U.S. diplomatic missions by creating dedicated military forces to respond to crises in Africa and the Middle East and expanding the Marine Security Guard program at overseas missions. However, State and DOD reported that they have experienced some logistical and other challenges in implementing this increased support. State and DOD continue to update their plans and policies for coordination in times of crisis.
- *Dissemination of Threat Information:* State has processes for communicating threat information to post personnel and U.S. citizens in country. However, post personnel—including locally employed staff—have not always received important information in a timely manner. In addition, infrequent drills to test that the system used to alert other U.S. citizens in the country to potential threats may increase the risk to their security.
- *Countering Human Intelligence Threats:* Foreign intelligence entities from host nations and third parties are motivated to collect information on U.S. operations and intentions. State has established measures to counter the human intelligence threats—which are tailored to the threat level of the post—and works with other U.S. government agencies to identify and assess the human intelligence threats to overseas posts.
- *Ensuring Information Security:* GAO has designated federal information security as a government-wide, high-risk area. State faces evolving threats and challenges to maintaining obsolete technology, defining clear roles and responsibilities for information security, and overseeing technology contractors.
- *Status of Recommendations Made in Reports following the Benghazi Attack:* State has addressed many recommendations stemming from the reports generated by a group of Interagency Security Assessment Teams and the Accountability Review Board, both of which were convened subsequent to the 2012 attacks in Benghazi.

This report also includes six appendixes with additional supporting information, comprising the following:

- Appendix I contains additional details about our scope and methodology.
- Appendix II provides a time line of selected attacks against U.S. diplomatic missions and subsequent legal and policy changes.
- Appendix III provides information on Diplomatic Security responsibilities, components, and collaboration with other U.S. government agencies.
- Appendix IV provides a comparison of Diplomatic Security staffing levels in fiscal years 2008, 2011, and 2017.
- Appendix V contains a list of open GAO recommendations regarding Diplomatic Security and made to State that should be given high priority for implementation.
- Appendix VI contains a list of GAO products directly related to this report and each of the enclosures.

To identify key issues affecting Diplomatic Security, we reviewed GAO's body of work related to this issue and reports issued by State and other entities. We also interviewed U.S. officials in Washington, D.C., and Arlington, Virginia, from State, DOD, and the U.S. Agency for International Development (USAID) to obtain their views on key issues, obtain updated information and data, and follow up on actions State and its partner agencies have taken on past GAO and other oversight report recommendations. We undertook steps to ensure that the updated data were sufficiently reliable for our purposes, as described in appendix I.

We conducted this performance audit from January 2017 to September 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Agency Comments

We provided a draft of this report to State, DOD, and USAID for review. None of the agencies provided formal comments. However, State provided technical comments, which we have incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretaries of State and Defense, and to the USAID Administrator. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff members have any questions about this report, please contact me at (202) 512-8980 or courtsm@gao.gov, or the individual(s) listed at the end of each enclosure. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff members who made key contributions to this report are listed in appendix VII.

Michael J. Courts
Director
International Affairs and Trade

List of Addressees

The Honorable John McCain
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Bob Corker
Chairman
The Honorable Ben Cardin
Ranking Member
Committee on Foreign Relations
United States Senate

The Honorable Claire McCaskill
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Lindsey Graham
Chairman
The Honorable Patrick Leahy
Ranking Member
Subcommittee on State, Foreign Operations, and Related Programs
Committee on Appropriations
United States Senate

The Honorable Mac Thornberry
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Ed Royce
Chairman
The Honorable Eliot Engel
Ranking Member
Committee on Foreign Affairs
House of Representatives

The Honorable Trey Gowdy
Chairman
The Honorable Elijah Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Devin Nunes
Chairman
Permanent Select Committee on Intelligence
House of Representatives

The Honorable Hal Rogers
Chairman
The Honorable Nita Lowey
Ranking Member
Subcommittee on State, Foreign Operations, and Related Programs
Committee on Appropriations
House of Representatives

Enclosure I: Diplomatic Security Funding

Enclosure I: Diplomatic Security Funding

Background

The Department of State's (State) Bureau of Diplomatic Security (Diplomatic Security) manages much of the security-related funding within State's Diplomatic and Consular Programs budget, the largest category of which comes from the Worldwide Security Protection account. Salaries for Diplomatic Security personnel are managed separately by State's Bureau of Budget and Planning.

Issue

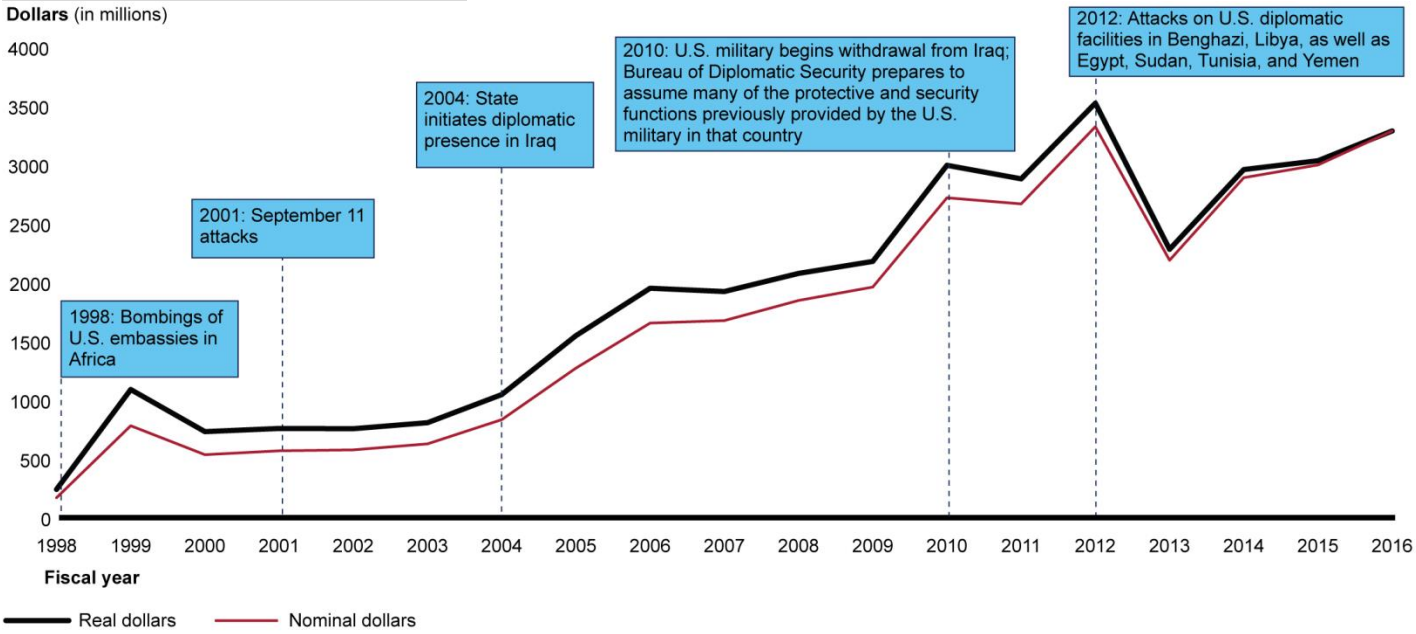
Total funding for Diplomatic Security operations was almost $4.8 billion in fiscal year 2016. Total funding for Diplomatic Security includes its bureau managed funds as well as other funding—such as personnel salaries—managed by other bureaus and offices but necessary for Diplomatic Security operations. Diplomatic Security's bureau managed funds ($3.3 billion in fiscal year 2016) are composed of funds received through annual appropriations, fees collected through visa processing, reimbursements from other agencies, and appropriated funds carried over from prior fiscal years. These funds support regular, ongoing operations and Overseas Contingency Operations (OCO) for temporary, war-related operations. State directed an additional $1.5 billion to Diplomatic Security and its employees in 2016, through other bureaus and offices.

Key Findings

Diplomatic Security's Bureau Managed Funds Have Increased Considerably Since 1998

In fiscal year 2016, Diplomatic Security's bureau managed funds totaled approximately $3.3 billion. Bureau managed funds have increased in response to multiple security incidents since the 1998 bombings of the U.S. embassies in Kenya and Tanzania. (Fig. 1 shows that Diplomatic Security's bureau managed funds had tremendous growth from 1998 through 2016 in both real and nominal dollars.)

Figure 1: Historical Trend in Department of State Bureau of Diplomatic Security Managed Funds, 1998-2016



Source: GAO analysis of Department of State (State) budget data. | GAO-17-681SP

Data Table for Figure 1: Historical Trend in Department of State Bureau of Diplomatic Security Managed Funds, 1998-2016

Fiscal Year	Nominal Value	Real Value
1998	172	243
1999	784	1092
2000	538	734
2001	571	761
2002	579	759
2003	630	810
2004	836	1049
2005	1274	1550
2006	1657	1953
2007	1678	1925
2008	1849	2079
2009	1963	2181
2010	2722	2998
2011	2670	2883
2012	3326	3526
2013	2191	2284
2014	2893	2962
2015	3001	3037
2016	3290	3290

Overseas Contingency Operations Funding Has Made Up a Large Share of Diplomatic Security's Bureau Managed Funds

From 1995 to 1998, Diplomatic Security's bureau managed funds averaged about $173 million annually. After the 1998 bombings in Africa, bureau managed funds grew to $784 million in 1999 as Congress provided Diplomatic Security with emergency supplemental funding to address security vulnerabilities at posts worldwide. By fiscal year 2009, bureau managed funds had grown to about $2.0 billion, largely due to new security procedures put in place after 1998 as well as the need to provide security for diplomats in the conflict zones of Iraq and Afghanistan. Bureau managed funds increased in 2010 to $2.7 billion and in 2012 to $3.3 billion, as the U.S. military began to withdraw from Iraq and Diplomatic Security assumed many of the protective and security functions previously provided by the U.S. military in that country. Congress appropriated less funding in 2013 to the Worldwide Security Protection account because, according to Diplomatic Security, appropriated funds were carried over from prior years. The subsequent increases in funding for that account in 2014 through 2016 followed the 2012 attack in Benghazi, Libya.

Total Funding for Diplomatic Security Also Includes Personnel Salaries and Other Programs

Since 2012, OCO supplemental funding has made up 34-62 percent of Diplomatic Security's bureau managed funds. For example, in fiscal year 2016, OCO funding totaled over $2.0 billion—or 62 percent—of bureau managed funds for that year. According to a bureau official, State's OCO funding was intended to be temporary funding to support operations in Iraq, Afghanistan, and Pakistan but continues to exist, given the security situation in those countries, and has expanded beyond those three countries. Some State officials are concerned that if OCO is discontinued, State would not have sufficient funding to provide necessary security

Point of Contact

For more information, contact:

Michael J. Courts, (202) 512-8980, courtsm@gao.gov

services. For fiscal year 2018, the administration is requesting less OCO funding than the final appropriated amount for fiscal year 2017.

Funding for Diplomatic Security operations totaled almost $4.8 billion in fiscal year 2016. This amount includes both bureau managed funds—which were almost $3.3 billion—and other funding directed to Diplomatic Security and its employees but managed by other bureaus and offices within State (personnel salaries, Antiterrorism Assistance funding, guard services funding, and fraud prevention and detection fees), which totaled almost $1.5 billion. For example, State's Bureau of Budget and Planning manages the salaries of Diplomatic Security personnel. Funding for Diplomatic Security personnel increased from $12 million in 2000 to $419 million in 2016. In addition, State allocates funding to its Bureau of Overseas Buildings Operations for security construction at overseas facilities.

Oversight Questions

1. What impact has Diplomatic Security's increased funding had on its ability to carry out its mission? Are current funding levels sufficient?

2. What are State's plans for utilizing future Diplomatic Security funding? Will there be additional carryover funds in future years, as in 2013?

Enclosure II: Diplomatic Security Staffing Challenges

Enclosure II: Diplomatic Security Staffing Challenges

Background

The Department of State's (State) Bureau of Diplomatic Security (Diplomatic Security), which is responsible for the protection of State's people, property, and information, relies on a broad workforce to carry out its mission and activities. Its workforce includes direct-hire personnel, military support, and contractors. Posts also engage locally employed staff.

Issue

Over the last 2 decades, Diplomatic Security's mission and activities have expanded in response to a number of security incidents, which has led to a dramatic increase in the size of its workforce. The growth in its responsibilities overseas began with the 1998 attacks in Africa and continued with the U.S. policy of maintaining a diplomatic presence in war zones such as Afghanistan and Iraq and other increasingly hostile environments. In addition, the September 11, 2001, terrorist attacks underscored the importance of enhancing domestic security, including Diplomatic Security's investigative capacity, technical programs, and counterintelligence work. This sustained and at times rapid growth has taxed Diplomatic Security's ability to staff positions with the appropriate level of experience and skills.

Key Findings

Diplomatic Security's Workforce Continues to Grow

Diplomatic Security's workforce—numbering over 51,000 direct-hire, other U.S. government, and contract personnel as of May 2017—has experienced continued growth in almost all staffing categories. We previously reported in 2009 that Diplomatic Security's direct-hire work force doubled from 1998 to 2008. Since then, it has increased by another 36 percent to 3,488 personnel in 2017. If State's current hiring freeze is lifted, Diplomatic Security officials told us that they plan to hire an additional 384 special agents in 2017 through 2018. The number of other U.S. government personnel reporting to Diplomatic Security increased by 60 percent, driven largely by the expansion of the Marine Security Guard program after the 2012 Benghazi attacks. Diplomatic Security increased its contracted and support staff by 22 percent. (Table 1 provides information on the increases in Diplomatic Security staff from 2008 through 2017; see app. IV for further staffing details.)

Table 1: Department of State Bureau of Diplomatic Security Staffing Summary, 2008 and 2017

	Direct-hire	Other U.S. government	Contract and support staff	Total
2008	2,568	1,241	37,566	41,375
2017	3,488	1,989	45,870	51,347
Percent change	36	60	22	24

Source: GAO analysis of Department of State data. | GAO-17-681SP

Distribution of Domestic and Overseas Positions Is under Review

In response to a Benghazi Accountability Review Board recommendation, State established a panel to reexamine Diplomatic Security's organization and management. In 2013, the panel reported that, in part, Diplomatic Security had become more focused on its law enforcement and personnel protection functions. This was not surprising, according to the panel, given that Diplomatic Security provided security in two war zones and numerous other high-threat posts. Simultaneously, Diplomatic Security had experienced an increased demand on its domestic criminal

Figure 2: Special Agents Escort a Fugitive from Thailand upon Returning to the United States

Source: Department of State. | GAO-17-681SP

Experience Gaps Persist

State Has Increased the Number of Special Agents Meeting Language Requirements

Point of Contact

For more information, contact:

Michael J. Courts, (202) 512-8980, courtsm@gao.gov

investigative and dignitary protection programs.

Nonetheless, the panel noted that Diplomatic Security's primary mission is "to provide a secure environment for the conduct of U.S. foreign policy" and stated that Diplomatic Security should reflect this priority in its allocation of manpower and other resources. For example, the panel recommended that Diplomatic Security review personnel allocations both domestically and abroad. As of June 2017, Diplomatic Security had completed an initial classified review of its staffing and begun a follow-on study to (1) determine how Diplomatic Security has distributed its staff relative to its priorities; and (2) develop a methodology to assess the quantity, mix, and distribution of Diplomatic Security staff worldwide. According to Diplomatic Security, the second study is expected to result in two tools that Diplomatic Security can use for evaluating its staffing levels: one for domestic staffing and one for overseas staffing.

In fiscal year 2010, we reported that 34 percent of Diplomatic Security's positions were filled with officers below the position's grade. In 2013, the organization and management panel noted that many Diplomatic Security regional director positions were filled by officers holding ranks below the levels established for that position (not including agents posted to Baghdad, Iraq). The panel recommended that Diplomatic Security prioritize filling these positions with at-grade personnel. While State concurred, as of June 2017, it had not identified any new, concrete actions for implementing this recommendation. Instead, State noted that it "will continue to make every effort to place at-grade, experienced, and highly qualified individuals into these positions."

As of December 2016, Diplomatic Security had 422 staffed language-designated positions (LDP), of which 304—or 72 percent—were filled with special agents who met the language requirement. This is an improvement since 2009, when we reported that only 47 percent of Diplomatic Security special agents at LDPs met the requirement. Officials cited two reasons for this increase in compliance: (1) greater agency emphasis on the need for agents to have language skills following the 2012 Benghazi attacks and (2) increased emphasis on speaking rather than reading skills. As a result, Diplomatic Security has an increased number of "asymmetrical" language requirements, where the speaking-level requirement is higher than the reading-level requirement. Diplomatic Security also adopted the "Alert" language training program, which provides special agents with speaking skills relevant to their technical work, particularly for languages spoken at certain high-threat posts. State officials told us that agents can become proficient in 10 weeks using this program, versus 30 weeks typically required for traditional methods.

Oversight Questions

1. To what extent will Diplomatic Security's proposed staffing tools ensure that it has the appropriate quantity, mix, and distribution of staff to address its overseas and domestic responsibilities?
2. What steps has Diplomatic Security taken to ensure that its positions are filled with appropriately experienced staff?
3. What is State doing to further close the gaps in Diplomatic Security's LDPs?

Enclosure III: Physical Security of U.S. Diplomatic Facilities

Enclosure III: Physical Security of U.S. Diplomatic Facilities

Background

Responsibility for the security of the Department of State's (State) diplomatic facilities falls principally on State's Bureaus of Overseas Buildings Operations (OBO) and Diplomatic Security (Diplomatic Security). OBO is responsible for the design, construction, acquisition, maintenance, and sale of U.S. diplomatic property abroad. Diplomatic Security is responsible for establishing security and protective procedures at posts and developing and implementing the physical security programs.

State Embarked on an Ambitious Construction Program following the 1998 Embassy Attacks

Issue

Maintaining the physical security of U.S. diplomatic facilities is a critical component of ensuring the safety of U.S. personnel, property, and information. According to OBO, State maintains approximately 1,600 work facilities at 275 diplomatic posts worldwide under chief-of-mission authority. In addition, State has a limited number of temporary work facilities, mostly in dangerous locations such as Afghanistan. All facilities at a post are expected to meet physical security standards set by the Overseas Security Policy Board. In fiscal years 2009 through 2016, State allocated about $11.1 billion to the construction of new, secure facilities and physical security upgrades to existing and acquired facilities. While Diplomatic Security has a few small programs to provide physical security upgrades to facilities abroad, OBO managed most of the allocated funds.

Key Findings

Following the 1998 attacks on U.S. embassies in Kenya and Tanzania, State determined that diplomatic facilities in over 180 posts—more than half of U.S. overseas missions—needed to be replaced to meet security standards. In 1999, State began a new embassy construction program, administered by OBO, to replace these posts.[4] To expedite the delivery of new, secure compounds, OBO adopted a standard embassy design (SED) approach. However, some stakeholders raised concerns about the aesthetics, quality, location, and functionality of those facilities. For example, the 10-acre lot specified by the SED sometimes required situating an embassy far from urban centers, where foreign government offices and other embassies are located. In response to these concerns, State established the "Excellence" approach in 2011. (See fig. 3 for a picture of an embassy built under SED and a rendering of a consulate to be delivered under the Excellence approach.)

Figure 3: Examples of the Standard Embassy Design and the Excellence Approach to Diplomatic Facility Design

Panama City, Panama | Hyderabad, India

Source: Department of State. | GAO-17-681SP

OBO's changes under the Excellence approach focus on producing more innovative, functional, and sustainable embassies that are just as secure as those built using the SED. However, some stakeholders have raised concerns that the new approach may result in embassies that take longer and cost more to build. This would delay getting U.S. personnel into

[4]From 1999 through March 2017, State and other U.S. agencies with overseas staff provided $21 billion to this program.

facilities that meet current security standards. In 2017, we reported that, while the Excellence approach may result in improvements, it carries increased risk to cost and schedule—including up to 24 additional months to develop designs. While OBO is attempting to manage this risk, it does not have performance measures specific to the Excellence goals and, therefore, cannot fully assess the merits of the new approach. We made four recommendations to strengthen performance measures and reporting, monitoring mechanisms, and data systems. While State concurred with these recommendations, they remain open.

[redacted]

Process for Managing Security Risks in Existing Overseas Facilities Has Weaknesses

When facilities do not or cannot meet certain security standards, State works to mitigate identified vulnerabilities through various construction programs and its waivers and exceptions process. However, in 2014, we reported that the waivers and exceptions process had weaknesses. Of the 43 facilities we reviewed, none met all applicable security standards and therefore required waivers, exceptions, or both. However, we found that neither posts nor headquarters systematically tracked the waivers and exceptions and that State had no process to reevaluate waivers and exceptions when the threat or risk changes. Furthermore, posts did not always request required waivers and exceptions or consistently take required mitigation steps. We concluded that with such deficiencies, State cannot be assured it has all the information needed to mitigate facility vulnerabilities. We made 13 recommendations for State to address gaps in its security-related activities, standards, and policies. State generally agreed with our recommendations and, as of June 2017, had addressed five of them.

[redacted]

Lack of Security Standards or Guidance for Temporary Facilities Creates Risk

Future State construction in dangerous posts—such as Kabul, Afghanistan—will likely entail the continued use of temporary office or residential facilities, especially in conflict areas. However, in 2015, we found that in Kabul—without security standards or other guidance to guide temporary facility construction in conflict environments—State inconsistently applied alternative security measures that resulted in insufficient and different levels of security for temporary offices and housing as well as increased costs and extended schedules. We concluded that without temporary facility security standards or guidance, future construction in conflict environments could encounter similar problems. We recommended that State consider establishing security standards or guidance for temporary facilities in conflict zones. State partially concurred and subsequently reported that it was developing additional guidance relating to physical security systems such as Hardened Alternative Trailer Systems, surface-mounted, antiram barriers, and anticlimb wall toppings. As of May 2017, State was continuing to address this recommendation.

Oversight Questions

1. What steps has State taken to mitigate the risks to costs and schedules associated with the Excellence approach to building new embassies?
2. To what extent do State's facilities have or require waivers and exceptions to security standards? What steps has State taken to address weaknesses in its waivers and exceptions program?
3. How extensively does State rely on temporary facilities that have been in place for extended periods of time? What progress has State made in creating additional guidance relating to temporary facilities?

Point of Contact

For more information, contact:

Michael J. Courts, (202) 512-8980, courtsm@gao.gov

Enclosure IV: Physical Security of Diplomatic Residences and Other Soft Targets

Enclosure IV: Physical Security of Diplomatic Residences and Other Soft Targets

Background

The Secretary of State, in consultation with the heads of other federal agencies, is responsible for protecting U.S. government personnel on official duty abroad, along with their accompanying dependents. At overseas posts, the Department of State's (State) Bureaus of Diplomatic Security (Diplomatic Security)—represented by a Regional Security Officer (RSO)—and Overseas Buildings Operations share responsibility for the security of residences and other soft targets overseas.

Addressing Residential Security Vulnerabilities at Overseas Posts

Issue

More than 25,000 U.S. diplomatic personnel live overseas with their families in an environment that presents myriad security threats and challenges. While State has taken measures to enhance security at its embassies and consulates since the 1998 East Africa embassy bombings, these same actions have given rise to concerns that would-be attackers may shift their focus to what they perceive as more accessible targets, such as diplomatic residences, schools, and other places frequented by U.S. personnel and their families. For example, a 2014 posting on a jihadist website called for attacks on American and other international schools in the Middle East. (See fig. 4 for examples of diplomatic residences.)

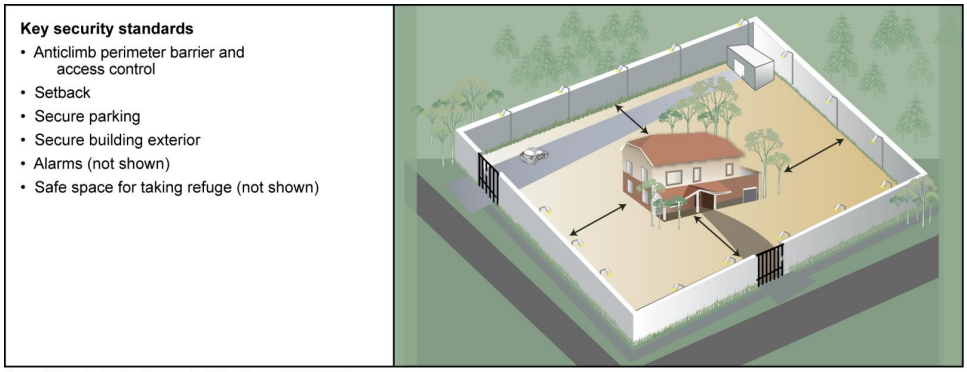
Figure 4: Examples of Diplomatic Residences Overseas

Sources: Department of State (left and center photos); GAO (right photo). | GAO-17-681SP

Key Findings

State acquires housing for overseas personnel by leasing, purchasing, or constructing various types of residences, each of which is subject to a set of security standards. State assesses risks to residences using a range of activities—including a periodic security survey to identify and address vulnerabilities. In fiscal years 2010 through 2016, State allocated about $175 million for residential security upgrades. However, in 2014, we found that State did not complete all residential surveys as required, thereby limiting its ability to address vulnerabilities. In addition, we reviewed 68 overseas diplomatic residences and found that 38 did not meet all of the applicable standards, potentially placing their occupants at risk. In instances when a residence does not and cannot meet applicable security standards, posts are required to either seek other residences or request exceptions, which identify steps to mitigate vulnerabilities. However, we found that Diplomatic Security had an exception on file for only 1 of the 38 residences that did not meet all standards. We concluded that without documenting the necessary exceptions, State lacked a complete picture of security vulnerabilities at residences and information that would enable it to make better risk management decisions. In addition, more rigorous security standards that went into effect in July 2014 would likely increase posts' need for exceptions and lead to costs for upgrades. We made four recommendations regarding the management of risks to residences. State concurred with all four and, as of May 2017, had addressed one. (Fig. 5 portrays key security standards at a notional residence.)

Figure 5: Six Key Categories of Physical Security Standards at a Notional Diplomatic Residence



Source: GAO analysis of the Department of State data. | GAO-17-681SP

Managing Risks to Schools and Other Soft Targets

State has taken a variety of actions to manage risks to schools and other soft targets. These actions fall into three main categories: (1) funding security upgrades at K-12 schools with enrolled U.S. government dependents and off-compound employee association facilities, (2) sharing threat information and providing advice for mitigating threats at schools and other soft targets, and (3) conducting security surveys to identify and manage risks to schools and other soft targets. However, RSOs at most of the posts we reviewed in 2015 were unaware of some guidance and tools for securing these facilities—such as a booklet and compact disc entitled “Security Guide for International Schools” aimed at assisting international schools in designing and implementing a security program. As a result, we concluded that RSOs may not have been taking full advantage of State’s programs and resources for managing risks at soft targets. We recommended that State take steps to ensure that RSOs are aware of existing guidance and tools regarding the security of soft targets. In response, State issued a cable to all diplomatic and consular posts updating policies and procedures for State's Soft Targets Security Upgrade Program for overseas schools and department-chartered employee associations, thereby distributing important information to security personnel who were previously unaware of available guidance and information.

Oversight Questions

1. To what extent has State improved its compliance with security standards at overseas residences? Have the standards implemented in July 2014 affected the number of waivers and exceptions requested?
2. What steps has State taken to ensure that posts conduct residential physical security surveys and request security exceptions, when needed, in a timely manner?
3. To what extent has State adapted its Soft Targets Security Upgrade Program in light of recent public terrorist attacks?

Point of Contact

For more information, contact:

Michael J. Courts, (202) 512-8980, courtsm@gao.gov

Enclosure V: Security Training Compliance

Enclosure V: Security Training Compliance

Background

To help safeguard and prepare U.S. personnel to live and work in some of the most dangerous overseas locations, the Department of State's (State) Bureau of Diplomatic Security (Diplomatic Security) provides training on personal security skills necessary for recognizing, avoiding, and responding to potential terrorism and other threat situations. Diplomatic Security also provides refresher briefings on certain topics, as well as cyber and technical security training. To consolidate the hands-on training that Diplomatic Security provides, State is constructing a training center in Fort Pickett, Virginia, which it expects will be completed in 2019.

Issue

State Does Not Monitor or Evaluate Overall Levels of Compliance with FACT Training

State has a robust security awareness training program provided by Diplomatic Security. For example, State requires specified U.S. personnel traveling for less than 45 days in a calendar year to certain posts to complete its online High Threat Security Overseas Seminar (HTSOS). If specified U.S. personnel are traveling for 45 days or more in a calendar year, State requires that they complete the 5-day Foreign Affairs Counter Threat (FACT) training before departure. Diplomatic Security designed the FACT course to address the dangers that U.S. personnel might face in a number of high-threat, high-risk locations overseas. The course provides hands-on instruction in topics such as detection of surveillance, familiarization with firearms, and awareness of improvised explosive devices (see fig. 6 for examples of other FACT training topics).

Figure 6: Examples of Foreign Affairs Counter Threat Training Topics

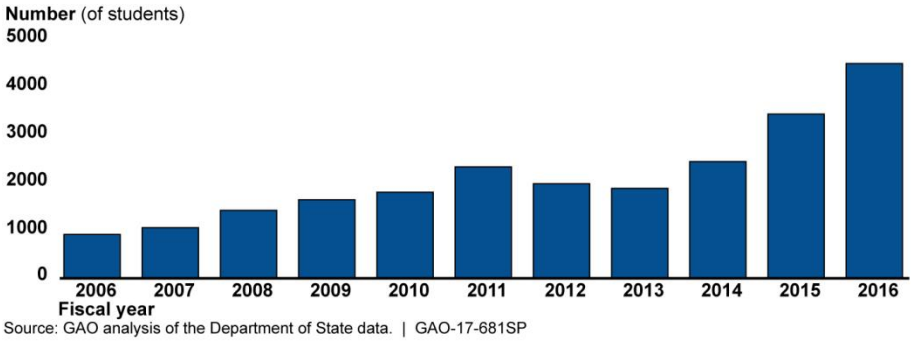
Source: Department of State. | GAO-17-681SP

Key Findings

State's oversight of compliance with the FACT training requirement has weaknesses that limit its ability to ensure that U.S. personnel are adequately prepared for work in high-threat environments. We reported in 2011 and 2014 that State did not have the ability to systematically identify which people required to take the course had not taken it. We made several recommendations to State to improve its management oversight of compliance with mandatory FACT training. These included four recommendations for State to update its policy guidance to reflect changes made to the FACT training requirement in June 2013 (State had doubled the number of countries for which it required FACT training) and to provide clear information on which personnel are required to take FACT training. State concurred with the recommendations and took steps to address them. However, our recommendation that State monitor or evaluate overall levels of compliance with the FACT training requirement remains open. In May 2015, State officials said they were developing a plan to utilize various electronic systems to monitor overall levels of compliance with the FACT training requirement. As of June 2017, State reported that it continues to work on this issue. This lack of oversight is particularly concerning given the significant increase in the number of students taking Diplomatic Security-provided FACT training, from 912 in

fiscal year 2006 to 4,482 in fiscal year 2016 (see fig. 7).

Figure 7: Number of Students Taking Foreign Affairs Counter Threat Training from Department of State's Bureau of Diplomatic Security, 2006-2016



Source: GAO analysis of the Department of State data. | GAO-17-681SP

Data Table for Figure 7: Number of Students Taking Foreign Affairs Counter Threat Training from Department of State's Bureau of Diplomatic Security, 2006-2016

Fiscal year /	number of students
2006	912
2007	1054
2008	1417
2009	1637
2010	1794
2011	2325
2012	1973
2013	1873
2014	2433
2015	3428
2016	4482

State Lacks a Clear Requirement for Posts to Provide and Track Refresher Briefings

In addition, in July 2014, State expanded the FACT training requirement to apply to all posts (not just those in high-threat, high-risk locations) by 2019. The gaps we have previously identified in State oversight may increase the risk that personnel do not complete FACT training, potentially placing their own and others' safety in jeopardy.

We reported in 2016 that weaknesses exist in State's guidance on and management oversight of refresher briefings related to transportation security, potentially putting U.S. personnel overseas at greater risk. We found that personnel had difficultly remembering key details covered in new arrival briefings or described the one-time briefings as inadequate. We found that State lacked a clear requirement for Diplomatic Security to provide and track compliance with periodic refresher briefings that could help reinforce information covered in new arrival briefings. In part, this may result from State guidance lacking clarity and comprehensiveness on this matter. Specifically, its guidance states that regional security officers must conduct refresher briefings "periodically" at "certain posts where personnel live under hostile intelligence or terrorist threats for long periods" but does not define "periodically" or "long periods." Further, according to Diplomatic Security officials, there is no requirement for affirming that post personnel have received refresher briefings. We recommended that State clarify existing guidance on refresher briefings, such as by delineating how often briefings should be provided at posts facing different types and levels of threats, which personnel should receive them, and how their completion should be documented.

Point of Contact

For more information, contact:

Michael J. Courts, (202) 512-8980, courtsm@gao.gov

Diplomatic Security headquarters officials stated that most violations of post travel policies are due to personnel forgetting the information conveyed in new arrival briefings. Without effective reinforcement of the information that is covered in new arrival briefings, State cannot ensure that U.S. personnel and their families overseas have the knowledge they need to protect themselves from transportation-related security risks.

Oversight Questions

1. What efforts is State taking to ensure that U.S. personnel are in compliance with all applicable security training requirements, including mandatory HTSOS and FACT training?
2. Does State have the capacity to train the number of U.S. personnel required to take Diplomatic Security-provided FACT training?
3. What steps is State taking to reinforce information covered in new arrival briefings with U.S. personnel and their families?

Enclosure VI: Embassy Crisis and Evacuation Preparedness

Enclosure VI: Embassy Crisis and Evacuation Preparedness

Background

The Department of State's (State) Bureau of Diplomatic Security (Diplomatic Security) is responsible for ensuring that overseas post personnel and their family members are prepared for crisis situations and evacuations.

Issue

From October 2012 to September 2016, in response to various threats, such as terrorism, civil unrest, and natural disasters, State evacuated staff and family members from 23 overseas posts. During this period, several posts—such as Embassy Bujumbura in Burundi and Consulate Adana in Turkey—evacuated post staff or family members on more than one occasion. Overseas posts undergoing evacuations generally experience authorized departure or ordered departure of specific post staff or family members before leading to suspended operations. To help mitigate risks, State requires posts to create Emergency Action Plans (EAP), practice security drills and, if an evacuation is needed, review the event in order to learn from the experience.

Key Findings

Emergency Action Plans Not Updated within Required Time Frames and Not Readily Usable

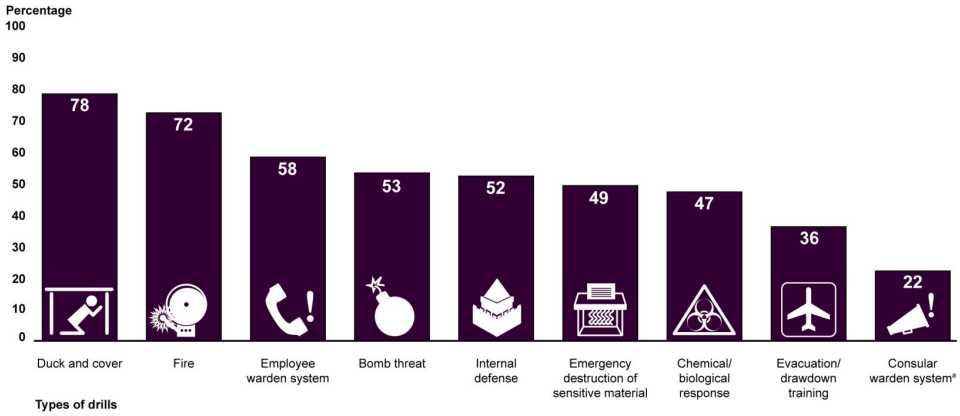
State requires every post to update its EAP on an annual basis. EAPs contain information to assist overseas posts in responding to emergencies, such as checklists of response procedures and decision points to help determine when to evacuate post staff or family members. In 2017, we found that, from fiscal years 2013 through 2016, a quarter of overseas posts, on average, were late completing required annual EAP updates. While the completion rate improved from 46 percent to 92 percent of posts completing updates on time in fiscal years 2013 and 2016, respectively, our review of a nongeneralizable, judgmental sample of EAPs from 20 posts that had been approved by Diplomatic Security showed that only 2 of 20 had updated all key EAP sections. We also found that EAPs are viewed as lengthy and cumbersome documents that are not readily usable in emergency situations, as required by State policy. We recommended that State take several actions to improve their EAPs, such as developing a procedure to ensure that overseas posts complete comprehensive, annual EAP updates on time; develop a monitoring and tracking process to ensure EAP updates are reviewed; and make the EAP more readily usable during emergency situations. State agreed with all of our recommendations and reported that it has started to address them. For example, State is developing a redesigned EAP that will minimize redundancy, group content according to posts' planning and response needs, and make the EAP better organized and more user-friendly.

Few Posts Report Completing All Required Drills to Prepare for Crisis and Evacuations

Posts are required to conduct nine types of drills each fiscal year to prepare for crises and evacuations. In 2017, we found that, on average for fiscal years 2013 through 2016, posts worldwide reported completing 52 percent of required annual drills; posts rated high or critical for political violence or terrorism reported completing 44 percent of these drills. Overall, less than 4 percent of posts reported completing all required drills during fiscal years 2013 through 2016. As shown in figure 8 below, 78 percent of posts reported completing duck-and-cover drills, but only 36 percent of posts reported completing evacuation training drills. We

recommended that State improve the completion and reporting of required drills. State concurred and is updating the system it uses to report drills.

Figure 8: Percentage of Overseas Posts that Report Completing Each Type of Drill, Fiscal Years 2013-2016



[a]The consular warden system is a mechanism through which a post reaches out to American citizens in country, typically by phone or e-mail, in the event of an emergency, disaster, or threat, for the purposes of distributing information of interest.

Source: GAO analysis of the Department of State data. | GAO-17-681SP

After an authorized or ordered departure has terminated, State's *Foreign Affairs Handbook* requires post staff to transmit an after-action report listing any lessons learned from the experience to State headquarters. In 2017, we found that, during fiscal years 2013 through 2016, there were 31 evacuations from overseas posts; however, according to State officials, none of the posts submitted the required lessons learned report. These reports could have been used to modify the post's guidance on how to best respond to an emergency situation. According to State officials, these reports also could help staff at other posts learn about the challenges faced by the evacuated posts, identify relevant best practices, and prepare for potential future evacuations. We recommended that State take steps to improve the completion and submission of required lessons learned reports following evacuations from overseas posts. State concurred and has developed tools to improve the process.

Overseas Posts Have Not Submitted Required Lessons Learned Reports following Evacuations

Oversight Questions

1. How much progress has State made ensuring that (1) overseas posts annually update their EAPs and (2) Diplomatic Security comprehensively reviews key EAP sections?
2. What efforts is Diplomatic Security making to ensure that posts complete and report completion of required crisis and evacuation drills within required time frames?
3. What steps is State taking to ensure that overseas posts complete required lessons learned reports following evacuations and submit those reports to State headquarters for analysis?

Point of Contact

For more information, contact:

Michael J. Courts, (202) 512-8980, courtsm@gao.gov

Enclosure VII: Department of Defense Support to U.S. Diplomatic Missions

Enclosure VII: Department of Defense Support to U.S. Diplomatic Missions

Background

The Department of Defense (DOD) has long provided military protection and support for the security and safety of U.S. diplomatic missions and personnel during normal operations and emergencies. This support is particularly critical in times of crisis, such as when DOD provides security reinforcements to facilities under threat or assists with evacuations. Several entities within DOD and the Department of State (State) prepare for and coordinate these efforts. Memoranda of Agreement between State and DOD establish frameworks for cooperation on scenarios requiring security augmentation, crisis response, and evacuation for U.S. diplomatic and consular missions overseas.

Issue

The September 2012 attacks in Benghazi, Libya, and the related wave of protests and threats to U.S. missions in Africa and the Middle East prompted a reexamination of how State and DOD collaborate to provide emergency military protection and other support to overseas posts. The possibility of similar threats and attacks requiring additional DOD support at U.S. diplomatic facilities is spread across a large geographic area. Given the chaos and complexities inherent in such acute crises, and the possibility that unrest could affect multiple U.S. facilities at one time, the need for DOD support will likely continue. From 2013 to 2016, 24 overseas posts experienced some level of increased threat resulting in the evacuation of some or all U.S. personnel. While not all periods of increased threat warrant additional DOD assistance, many do. For instance, in 2014 alone, the U.S. military provided support for embassy reinforcement, military-assisted departures, or evacuations, including in South Sudan, Libya, and Iraq. (Fig. 9 shows one of the DOD units and aircraft that may be used in evacuations or other emergencies.)

Figure 9: The Department of Defense May Use the East Africa Response Force and C-130J Aircraft for Some Evacuations

Source: Department of Defense Combined Joint Task Force-Horn of Africa; U.S. Air Force photo by Staff Sgt. Eric Summers Jr. | GAO-17-681SP

Key Findings

DOD Created Dedicated Military Forces to Increase Support to Diplomatic Posts

As part of the reorganization following the 2012 attacks, DOD—in coordination with State—increased the military resources provided to overseas posts. According to State and DOD officials, this represented a whole-of-government approach to countering threats to U.S. overseas personnel and facilities. Drawing from existing U.S. Marine Corps and U.S. Army units, DOD created three dedicated military forces to respond to crises across Africa and the Middle East: (1) a Special Purpose Marine Air-Ground Task Force for Crisis Response (SPMAGTF-CR) assigned to DOD's U.S. Central Command, which supports U.S. diplomatic missions in the Middle East; (2) a SPMAGTF-CR assigned to U.S. Africa Command, which supports U.S. missions in North and West Africa;

and (3) the East Africa Response Force, a U.S. Army force that supports U.S. diplomatic missions in East Africa. These forces can provide a variety of functions, from security reinforcement during increased threats, to military-assisted departures and evacuation support. According to DOD officials, in 2014, U.S. Africa Command experienced some logistical challenges associated with covering such a large geographic area, with particular concern should multiple crises occur simultaneously.

State and DOD Expanded the Marine Security Guard Program

In 2014, State and DOD announced several changes to the Marine Security Guard (MSG) program, which deploys units of marines to provide certain types of security to U.S. overseas missions. Specifically, in coordination with State's implementation of the Benghazi Accountability Review Board recommendations, DOD has since increased the size of MSG detachments at all posts, with further increases at high-threat posts; accelerated the deployment of additional detachments to other U.S. diplomatic facilities; and created a Marine Security Guard Security Augmentation Unit based in Quantico, Virginia, to provide additional support on short notice. State and DOD officials reported in June 2017 that they have experienced some challenges associated with deploying the increased MSG units, including obtaining sufficient numbers of marines to fill the desired number of units and logistical and other support at some posts. The agencies continue to work to add certain nonlethal weapons to the MSG equipment set.

State and DOD Continue to Update Plans and Polices for Coordination in Times of Crisis

In 2015, we reported on State and DOD's post-Benghazi approach to provide additional military support to U.S. overseas posts. While State and DOD had updated some guidance to reflect the new approach, we recommended that the departments more clearly define the roles, responsibilities, and circumstances under which DOD support would be provided and that they update related interagency and departmental guidance. In response to our recommendations, State and DOD have taken steps to update such interagency guidance. These steps included interdepartmental exercises and other collaboration, which resulted in a joint concept paper and a subsequent December 2016 State-DOD memorandum of agreement outlining common terms, roles, responsibilities, and scenarios under which DOD assistance may be requested, among other things. State and DOD officials have indicated that each department will produce further department-specific guidance in the form of a forthcoming diplomatic cable; a DOD update to a 2013 military order; and a new, related DOD instruction. DOD officials expect to issue the updated order by the end of fiscal year 2017 and to complete the instruction in fiscal year 2018.

Oversight Questions

3. To what extent is DOD postured with adequate forces and equipment to ensure support to U.S. missions in crisis situations?
4. What is the progress of increasing MSG detachments at identified diplomatic facilities? What challenges exist to providing the personnel or support needed for these additional units?
5. What steps have been taken to ensure that recent State and DOD policy and procedure updates are institutionalized and readily available in future emergencies?

Point of Contact

For more information, contact:

John H. Pendleton, (202) 512-3489, pendletonj@gao.gov

Enclosure VIII: Dissemination of Threat Information

Enclosure VIII: Dissemination of Threat Information

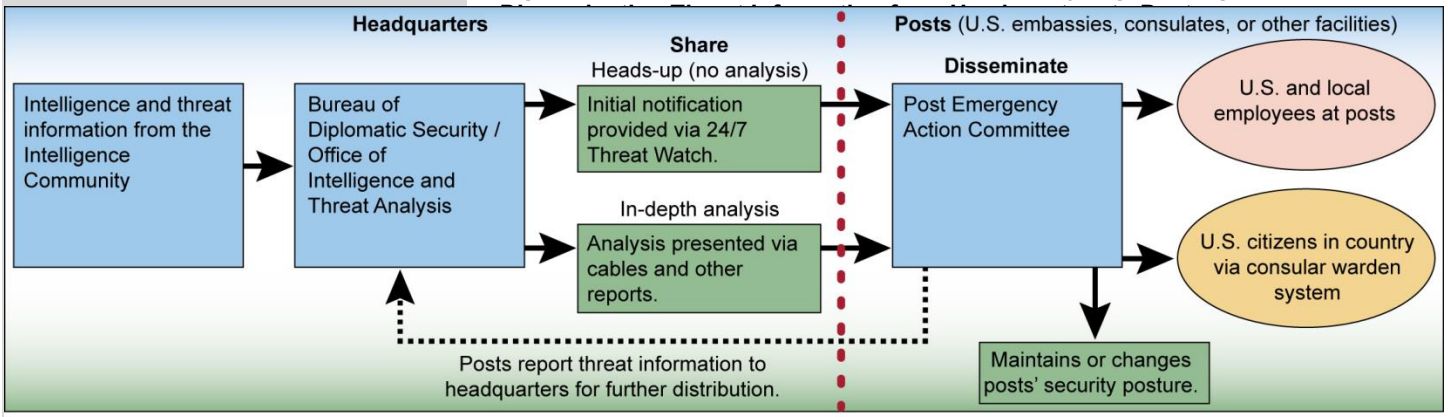
Background

The Department of State's (State) Bureau of Diplomatic Security (Diplomatic Security) is responsible for disseminating threat information to posts. At posts, the Emergency Action Committee (EAC), which includes the Regional Security Officer (RSO) and Consular Officer, among other subject matter experts, disseminates threat information to post personnel, as appropriate. In addition, consular officers are responsible for disseminating information to the nonofficial U.S. community—U.S. citizens living in or traveling through the affected area.

Issue

Diplomatic Security and overseas posts have processes for communicating threat information to post personnel (U.S. employees and locally employed staff) as well as U.S. citizens in country. However, these populations do not always receive important threat information in a timely manner. Diplomatic Security's Office of Intelligence and Threat Analysis, based at State headquarters, analyzes threat information from multiple sources, including the U.S. Intelligence Community, and shares the results of its analysis with posts' RSOs via cables and other reports. Before analyzing the information, Diplomatic Security sends an initial notification to posts, according to bureau officials. In addition, posts collect, analyze, and report threat information to headquarters for further distribution. At posts, RSOs, at the direction of the EAC, may adjust the post's security posture and disseminate threat information to post personnel. In addition, if State shares information with the official U.S. community, its policy is to make the same or similar information available to the nonofficial U.S. community if the threat applies to both. (See fig. 10 for a schematic of State's threat information dissemination process.)

Figure 10: Department of State's Process for Analyzing, Sharing, and



Source: GAO analysis of Department of State information. | GAO-17-681SP

Key Findings

Improper Reporting of Terrorism-Related Threats May Have Endangered Employees, but State Took Steps to Improve Communication

State has taken steps to improve RSOs' reporting of terrorism-related threat information to headquarters. In June 2015, we found that RSOs at some posts designated critical for terrorism were not complying fully with directions from the Secretary of State to use terrorist reporting cables to report all terrorism-related incidents or threats to ensure proper handling and dissemination of the information. For example, we found that in some cases, terrorism-related incidents were not reported in required terrorist reporting cables. We concluded that without comprehensive and accurate reporting, State may lack assurance that it received complete information about terrorist threats that could help prevent and mitigate such threats. We recommended that Diplomatic Security take steps to remind RSOs and posts

of the critical importance of using the proper type of cable to report all terrorism-related threats. In December 2015, State sent guidance to all posts specifying that terrorism-related threats must be reported through terrorist reporting cables to ensure appropriate dissemination of the information. Further, in January 2017, State provided reporting instructions to RSOs to help ensure the timely and accurate reporting of all security-related information through the correct reporting channels.

Problematic Dissemination of Threat Information Can Endanger Overseas U.S. Personnel and Locally Employed Staff

Diplomatic Security uses various methods to communicate threat information to overseas post personnel—both U.S. and locally employed staff. However, in our 2016 report on transportation security, we reported that post personnel do not always receive threat information in time to avoid potential threats. We found that several factors can lead to untimely receipt of transportation-related threat information. We recommended that State address these factors. First, some RSOs reported that they send security notices exclusively to *state.gov* e-mail addresses; however, not all post personnel have *state.gov* e-mail addresses. In one case, this resulted in post personnel traveling through a prohibited area and an embassy vehicle being attacked with rocks and seriously damaged. Second, limited guidance existed for RSOs on how to promote timely communication of threat information. Third, RSOs and other staff at some posts mistakenly believed that RSOs cannot share threat information with the official U.S. community until consular officials received approval from State to share the same information with the nonofficial U.S. community—a clearance process that can take as long as 8 hours. State reported that it is reviewing the option to forward e-mails outside its system. It also reported that it is developing a two-way emergency notification system that would provide a redundant method for distributing messages during crises. In addition, State updated its policy manual to clarify that RSOs' sharing of threat information should not be delayed by the clearance process, according to Diplomatic Security officials.

Infrequent Consular Warden System Drills May Increase Risk to U.S. Citizens in Country

To ensure that overseas posts can disseminate information to U.S. citizens in country in the event of an emergency, disaster, or threat, State requires posts to annually conduct a drill of the consular warden system. The consular warden system is a pyramidal contact system designed to reach the U.S. citizen population. However, we found in 2017 that, on average between fiscal years 2013 and 2016, 78 percent of overseas posts did not report the completion of required consular warden system drills. We concluded that this gap in State's crisis and evacuation preparedness creates a risk that U.S. citizens in country may be insufficiently warned about emergency situations. We recommended that State take steps to improve the completion and reporting of required drills, and State concurred, noting it is forming a working group to review its policies.

Point of Contact

For more information, contact:

Michael J. Courts, (202) 512-8980, courtsm@gao.gov

Oversight Questions

1. How effective have overseas posts' efforts to conduct outreach to the nonofficial U.S. community been in past emergencies?
2. What is the status of State's plan to use new technology to disseminate information to U.S. personnel and U.S. citizens overseas?
3. What steps has State taken to ensure that posts complete the annual tests of the consular warden system?

Enclosure IX: Countering Human Intelligence Threats

Enclosure IX: Countering Human Intelligence Threats

Background

The Department of State's (State) Counterintelligence Division—under the Office of Investigations and Counterintelligence in the Bureau of Diplomatic Security (Diplomatic Security)—is responsible for overseeing State's counterintelligence efforts, including assisting Regional Security Officers (RSO) with implementation at overseas posts.

Issue

Foreign intelligence entities from host nations and third parties are motivated to collect information on a variety of sensitive topics of national importance, including intelligence, defense, and economic information. These entities may attempt to collect information through the use of sophisticated overt, covert, and clandestine means, including human intelligence collection. Because State operates diplomatic posts in many countries, State and other U.S. agency employees at these posts—and their family members—can be targeted by host governments and other entities. National counterintelligence guidance requires that State and other executive agencies implement programs to counter the intelligence threat to U.S. national security and interests by protecting personnel and information.

Key Findings

State Has Enhanced Counterintelligence Measures for Critical Threat Posts

State has established several measures to counter the human intelligence threat at overseas posts. Those measures include (1) requiring all State and other agency personnel serving at these posts to report contacts with foreign nationals, particularly those from countries with critical human intelligence posts; (2) prescreening State personnel assigned to certain posts against 13 criteria designed to identify vulnerabilities and directing other agencies to prescreen their personnel; and (3) briefing personnel about what to expect when working and living in potentially hostile intelligence environments. While State prepares personnel at all posts to be aware of human intelligence threats, it uses enhanced counterintelligence strategies for personnel assigned to posts designated as "critical threat" for human intelligence. For example, personnel at critical threat posts receive counterintelligence briefings before departure and annually while serving at these posts. (See fig. 11.)

Figure 11: Comparison of Counterintelligence Preparation for Critical Threat and Other Overseas Posts

	Before departure →	At post →	Upon departure
Noncritical Threat Posts	• Employee receives routine counterintelligence awareness as part of general training courses.	• Regional Security Officer (RSO) provides arrival security briefing, employee signs acknowledgment form. • Employee completes annual online training.	• RSO debriefs employee.
Critical Threat Posts	• Employee receives routine counterintelligence awareness as part of general training courses. • Diplomatic Security prescreens personnel. • Diplomatic Security provides predeparture briefing.	• RSO provides arrival security briefing, employee signs acknowledgment form. • RSO provides annual refresher briefing. • Employee completes annual online training.	• RSO debriefs employee.

Source: GAO. | GAO-17-681SP

Counterintelligence Efforts at Posts

Diplomatic Security assesses counterintelligence efforts at overseas posts through Counterintelligence Post Surveys and Post Security Program Reviews, making recommendations to improve any gaps identified in countermeasures. In addition, as part of a government-wide effort, the Office of the Director of National Intelligence evaluates State's counterintelligence activities to identify gaps and make recommendations to strengthen State's counterintelligence program.

Coordination among U.S. Government Agencies

State works with other U.S. government agencies in several ways to help identify and assess the human intelligence threats to overseas posts. For example, deputy chiefs of mission convene interagency counterintelligence working groups to monitor threats to their posts and establish post-specific measures to protect U.S. interests. In addition, the Overseas Security Policy Board—an interagency body chaired by the Assistant Secretary of State for Diplomatic Security—establishes threat rankings for overseas posts and develops security standards for these posts, including administrative and procedural requirements to counter human intelligence threats. Furthermore, according to State officials, Diplomatic Security has entered into formal memoranda of understanding with several other agencies to establish standard procedures for counterintelligence information sharing, liaison exchanges, and counterintelligence investigations related to personnel at overseas posts. State is one of the 17 U.S. government agencies—led by the Office of the Director of National Intelligence—that work to protect the nation against intelligence and security threats. (Fig. 12 shows the official seals of the U.S. government's 17 intelligence agencies.)

Figure 12: Official Seals of the 17 U.S. Government Intelligence Agencies That Work to Protect the Nation against Intelligence and Security Threats

Source: GAO. | GAO-17-681SP

Oversight Questions

1. How has the nature and scope of the human intelligence threat faced by State domestically and overseas changed in recent years?
2. How does State ensure that personnel are prepared to live and work at posts facing a high or critical human intelligence threat?
3. How does State evaluate the effectiveness of its human intelligence countermeasures domestically and at overseas posts? How does State adjust its countermeasures, if warranted?

Point of Contact

For more information, contact:

Michael J. Courts, (202) 512-8980, courtsm@gao.gov

Enclosure X: Ensuring Information Security

Enclosure X: Ensuring Information Security

Background

The Department of State (State) created its information security program to address requirements in both the Omnibus Diplomatic Security and Antiterrorism Act of 1986 and the Federal Information Security Modernization Act of 2014 (FISMA). State's Bureaus of Diplomatic Security (Diplomatic Security) and Information Resource Management (IRM) share responsibility for implementing the information security responsibilities in these laws. In May 2017, Diplomatic Security created the new Directorate for Cyber and Technology Security to consolidate relevant elements from other directorates.

Attacks from Foreign Nations Pose Most Frequent Threat

Maintaining Obsolete Technology Increases Costs and Challenges to Ensuring Information Security

Issue

Since 1997, GAO has designated federal information security as a government-wide high-risk area and in 2003 expanded this area to include computerized systems supporting the nation's critical infrastructure.[5] The number of information security incidents reported by federal agencies—including State—increased from 5,503 in fiscal year 2006 to 77,183 in fiscal year 2015. Cyberattacks forced State to shut down its unclassified e-mail system and parts of its public website in both 2014 and 2015 after finding evidence that its systems had been breached. Cyber-based threats to federal systems and information come from unintentional sources, such as natural disasters, coding errors, and careless employees, or from intentional sources, such as disgruntled insiders, hackers, or hostile nations. State's outdated technology makes it increasingly difficult to ensure security. In addition, State's information security program is split between two bureaus, each responsible for aspects of the program. Further, State makes extensive use of contractors to perform information security functions such as the monitoring and assessment of systems. Protecting those systems and information from unauthorized disclosure or alteration is particularly important at State, where inappropriate disclosure could cause catastrophic harm to the nation's diplomacy and security.

Key Findings

In 2016, we surveyed 24 federal agencies—including State—to identify the sources of malicious attacks on their high-impact systems—any system that holds sensitive information, the loss of which could cause individuals, the government, or the nation catastrophic harm. Consequently, these systems warrant increased security to protect them. Eighteen of these 24 agencies—including State—identified cyberattacks originating from nation states as the most serious and frequent threat to the security of their systems. They identified e-mail cyberattacks as the most serious and frequent delivery method. We made recommendations to the Office of Management and Budget (OMB) to improve security over federal systems, including those at State.

State relies on several aging and obsolete technology systems, which require significant resources to operate and create challenges to ensuring information security. We found that State spent about 87 percent of its information technology budget on operating and maintaining its computer systems in 2015. This segment of State's technology budget increased by approximately $109 million between 2010 and 2015. A State official stated that the increase is largely due to the cost of maintaining the infrastructure, including meeting security requirements. For example, three of State's visa systems were more than 20 years old. The software for one of these systems is no longer supported by the vendor, creating

[5]In February 2015, we further expanded this area to include protecting the privacy of personally identifiable information.

challenges related to information security. State is planning to upgrade the software to a newer version that also is not supported by the vendor. As a result, we recommended that State identify and plan to modernize or replace legacy systems, consistent with OMB guidance.

[redacted]

Roles and Responsibilities for Information Security Need Additional Definition

FISMA directs State and other agencies to designate a Chief Information *Security* Officer (CISO)—who, at State, reports to the Chief Information Officer in IRM—to develop, document, and implement a department-wide information security program that protects the agency from cyberattacks. In a 2016 report, we evaluated 24 federal agencies to determine whether they followed FISMA and other requirements defining the CISO's responsibilities. Twenty-two of the 24 agencies—including State—had defined almost all CISO responsibilities properly. However, we found that State had assigned responsibility for responding to information security incidents—a FISMA-designated CISO responsibility—to Diplomatic Security without also defining the CISO's role in that activity. We concluded that not having a defined role may limit the CISO's ability to effectively oversee State's information security incident response process. We recommended that State define the CISO's role in department policy for ensuring that State had procedures for incident detection, response, and reporting. State concurred with the recommendation and noted that IRM and Diplomatic Security coordinate communications for the incident response process.

[redacted]

Oversight of Information Technology Contractors Needs Improvement

Under FISMA, State's Chief Information Officer must create an information security program that protects agency information and information systems, including those operated by contractors. Although State conducted system security control assessments and other oversight measures, in 2014 we found that State's oversight of information technology contractors needs improvement. For example, we reported that State's policies require contractors to protect personally identifiable information and system authorization, but the contract for one system that we reviewed did not contain language that communicated these requirements. We also found that State did not always ensure that its system security control assessments evaluated the extent to which background investigations had been conducted for contractor employees and, therefore, that State lacked assurance that contractor employees could be trusted with access to government information and systems. We recommended that State develop procedures to improve the oversight of contractor-operated systems. State agreed with our recommendations.

Points of Contact

For more information, contact:

Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov

Oversight Questions

1. Given State's numerous facilities worldwide and extensive use of contractors, what unique information security challenges, if any, does it face? How does it manage its global cybersecurity program?
2. Given the rapidly changing nature of technology, how does State assess and address threats to its systems and users from changing cyber threats?
3. How will the new Directorate for Cyber and Technology Security improve State's capability to address cybersecurity issues?
4. To what extent, if any, does assigning CISO responsibilities to multiple bureaus increase State's risk for duplication, overlap, or fragmentation of information security responsibilities?

Enclosure XI: Status of Recommendations Made in Reports following the Benghazi Attack

Enclosure XI: Status of Recommendations Made in Reports following the Benghazi Attack

Background

The Secretary of State is generally required by law to convene Accountability Review Boards (ARB) in cases of serious injury, loss of life, or significant destruction of property involving U.S. diplomatic missions or personnel abroad, and in any case of a serious breach of security involving intelligence activities of a foreign government directed at a mission abroad. State has convened 12 ARBs since 1998. ARBs are responsible for reporting their findings about the circumstances of the attack and making recommendations.

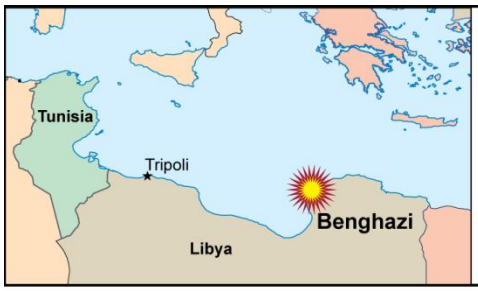
State Reported Having Addressed 268 of 287 Recommendations from Interagency Security Assessment Teams

State Reported Having Addressed 26 of 29 Recommendations from Benghazi ARB

Issue

On September 11, 2012, the acquired facilities at the U.S. Special Mission in Benghazi, Libya, came under attack (see fig. 13). Tragically, four U.S. officials were killed, including the U.S. Ambassador. In response to the attack, the Department of State (State), working with the Department of Defense, formed Interagency Security Assessment Teams to evaluate the security at 19 dangerous posts. Those teams made a number of recommendations to improve physical and procedural security at each post. In addition, an ARB was convened in response to the Benghazi attack; it resulted in 29 recommendations, including several concerning how State manages risk at dangerous posts. Furthermore, two of State's actions resulting from that ARB led to additional reports that included more recommendations.

Figure 13: September 2012 Attack on U.S. Special Mission in Benghazi, Libya



On the night of September 11, and into the morning of September 12, a series of attacks involving arson, small-arms fire, machine-gun fire, and rocket-propelled grenades descended on the U.S. Special Mission in Benghazi, Libya. Terrorists also attacked a nearby annex and U.S. personnel moving between the facilities.

Sources: Department of State (text); Map Resources (map). | GAO-17-681SP

Key Findings

The Interagency Security Assessment Teams assessed all facilities at the 19 posts for any security vulnerabilities—physical or procedural. Their assessments resulted in 287 recommendations including for State to install physical security upgrades, improve security procedures, and construct or acquire new or replacement facilities. State officials told us that State immediately began implementing the recommendations. In addition, State created the new High Threat Programs Directorate within its Bureau of Diplomatic Security (Diplomatic Security) to ensure that those posts facing the greatest risk receive additional, security-related attention. As of June 2017, State reported having addressed 268 of the 287 recommendations.

In December 2012, the ARB that State convened to investigate the Benghazi attack released the report of its investigation. The ARB made 23 unclassified recommendations[6] in six areas: (1) overarching security considerations; (2) staffing dangerous posts; (3) training and awareness; (4) security and fire safety equipment; (5) intelligence and threat analysis; and (6) personnel accountability. In addition, the ARB, according to State, made six classified recommendations. State accepted

[6]This number excludes the ARB's 21st recommendation, which State reported it is addressing as classified recommendation four.

all 29 of the ARB's recommendations and pledged to fully implement them. For example, in response to the ARB, State expanded the mandatory Foreign Affairs Counter Threat training requirement to all dangerous posts (and, subsequently, to *all* posts by 2019). As of June 2017, State reported having addressed all but three of the ARB's recommendations.

[redacted]

State Reported Having Addressed 28 of 35 Recommendations from the Panel on Diplomatic Security Organization and Management

In response to the Benghazi ARB's second recommendation, State established a panel to evaluate the organization and management of Diplomatic Security. In May 2013, the panel provided its report to State. It made 35 recommendations in three areas: (1) organization, (2) training, and (3) management. State accepted 29 of the panel's 35 recommendations. For instance, State did not accept a recommendation for Diplomatic Security to establish a chief of staff position at the GS-15 level within its Principal Deputy Assistant Secretary's office, noting that no other bureau has an equivalent position.[1] As of June 2017, State reported having addressed 28 of the 29 recommendations it accepted. For example, as a result of the panel's report, Diplomatic Security is undertaking a strategic review of its staffing.

[redacted]

State Reported Having Addressed 36 of 40 Recommendations from the Panel on Best Practices

In response to the Benghazi ARB's fourth recommendation, State established a panel to help Diplomatic Security identify best practices for operating in dangerous environments. The panel provided its report to State in August 2013. It made 40 recommendations in 12 areas, including organization and management; program criticality and acceptable risk; lessons learned; training and human resources; intelligence, threat analysis, and security assessments; and host nations and guard forces' capability enhancement, among others. State accepted 38 of the panel's 40 recommendations. State did not accept the panel's first recommendation, that it establish an Under Secretary for Diplomatic Security. It asserted that doing so would compound the "stove-piping" that the ARB and others reported in the wake of the Benghazi attack. In addition, State did not accept the panel's 13th recommendation, which stated that waivers to established security standards should only be provided subsequent to the implementation of all mitigating measures. State noted that in time-sensitive situations, exceptions might be appropriate when some mitigating measures are in place. As of June 2017, State reported having addressed 36 of the 38 recommendations it accepted. For example, as a result of the panel's report, Diplomatic Security created a Strategic Advisory Unit within Diplomatic Security to advise and perform ad hoc analysis for the Assistant Secretary.

Oversight Questions

1. What efforts is State taking to close the remaining Benghazi-related recommendations?
2. What effect, if any, has implementing the Benghazi-related recommendations had on the security of diplomatic facilities, personnel, and information?
3. Since 1998, 12 attacks have resulted in the formation of ARBs. What is the status of all recommendations made by the 12 ARBs?

Point of Contact

For more information, contact:

Michael J. Courts, (202) 512-8980, courtsm@gao.gov

[1]For the remaining five recommendations, State reported that it did not fully accept two, but tried to meet their intent, and that it closed three without accepting or declining them because the recommendations were outside its purview.

Appendix I: Scope and Methodology

This special publication is largely based on previously published GAO work. To generate a list of possible key issues, we reviewed past products concerning the Department of State's (State) Bureau of Diplomatic Security (Diplomatic Security), by GAO, State's Inspector General, and the Congressional Research Service. Working with GAO's subject matter experts, we narrowed the list of issues and identified potential oversight questions. We interviewed cognizant agency officials in Washington, D.C., and Arlington, Virginia, from State—including from the Bureaus of Management, Diplomatic Security, Overseas Buildings Operations (OBO), and Information Resource Management—the Department of Defense, and the U.S. Agency for International Development. We used these interviews to refine our key issues, gain updated information and data, follow up on actions taken regarding our past recommendations, and identify relevant lessons learned. We also worked with the officials to determine what portions of our past classified or restricted work could be presented in a public product. We then synthesized this information to provide a balanced and comprehensive overview for each issue and to formulate oversight questions.

We updated relevant data when possible and performed additional data reliability assessments when necessary. These additional assessments were conducted only on data that we had not previously reported; all other data were assessed as part of our work for our previously published reports. We assessed the reliability of various types of data—funding, staffing, and training—from Diplomatic Security and, as appropriate, its partner agencies. Specifically, we assessed the reliability of the following data:

- Diplomatic Security bureau managed funds, from fiscal years 2010 to 2016.[1] (We used previously reported data for fiscal years 1998 to 2007, and updated previously reported data for fiscal years 2008 to 2009.)

[1]In this report, Diplomatic Security bureau managed funds include funds received through annual appropriations, fees collected through visa processing, reimbursements from other agencies, and appropriated funds carried over from prior fiscal years. Bureau managed funds do not include other funding (personnel salaries, Antiterrorism Assistance funding, guard services funding, and fraud prevention and detection fees) directed to Diplomatic Security and its employees but managed by other bureaus and offices.

- Dedicated allocations to Diplomatic Security and OBO for physical security at diplomatic facilities for fiscal years 2015 to 2016. (We used previously reported data for fiscal years 2009 to 2014.)
- Diplomatic Security staffing numbers for its workforce of direct-hire employees, other U.S. government support staff, and contractors. (We used previously reported data for 1998, 2008, and 2011.)
- Number of students who completed Diplomatic Security-provided Foreign Affairs Counter Threat training for fiscal years 2011 to 2016. (We used previously reported data for fiscal years 2006 to 2010.)

To assess the reliability of the data, we interviewed cognizant officials about how the data were produced and their opinion of the quality of the data, specifically the data's completeness, accuracy, and comparability to previously reported data. We also worked with the cognizant officials to identify any limitations associated with the data and to mitigate those issues or note these limitations in our report, as appropriate. In addition, we updated previously reported data on the percentage of Diplomatic Security employees who do not speak and read foreign languages at the level required by their positions and interviewed knowledgeable officials to corroborate and clarify the data. We determined that the data mentioned above were sufficiently reliable for our purposes.

We prepared this report under the authority of the Comptroller General to conduct work on his initiative because of broad congressional interest in the oversight and accountability of providing security to U.S. personnel working at diplomatic missions and to assist Congress with its oversight responsibilities.

We conducted this performance audit from January 2017 to September 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Attacks against U.S. Diplomatic Missions and Subsequent Legal and Policy Changes

U.S. diplomatic missions have faced numerous attacks that were followed by legal and policy changes. Between 1998 and 2016, there were 419 attacks against U.S. diplomatic interests, according to the Department of State's Bureau of Diplomatic Security. Several of the deadly attacks against U.S. personnel and facilities overseas were followed by new legislation, independent reviews with corresponding recommendations, or both. For example, the Omnibus Diplomatic Security and Antiterrorism Act of 1986,[1] which followed the attacks against the U.S. embassy in Beirut, Lebanon, in 1983, established the Bureau of Diplomatic Security and set forth its responsibility for post security and protective functions abroad. The Secure Embassy Construction and Counterterrorism Act of 1999,[2] which followed the Africa embassy bombings of 1998, set requirements for colocation of all U.S. government personnel at an overseas diplomatic post (except those under the command of an area military commander) and for a 100-foot perimeter setback for all new U.S. diplomatic facilities.

In addition, the Secretary of State is generally required by law to convene an Accountability Review Board (ARB) following incidents that result in serious injury, loss of life, or significant destruction of property involving U.S. diplomatic missions or personnel abroad.[3] An ARB is responsible for reporting its findings about the circumstances of an attack and making recommendations as appropriate. Since 1998, 12 attacks have resulted in the formation of an ARB, the most recent of which was formed in

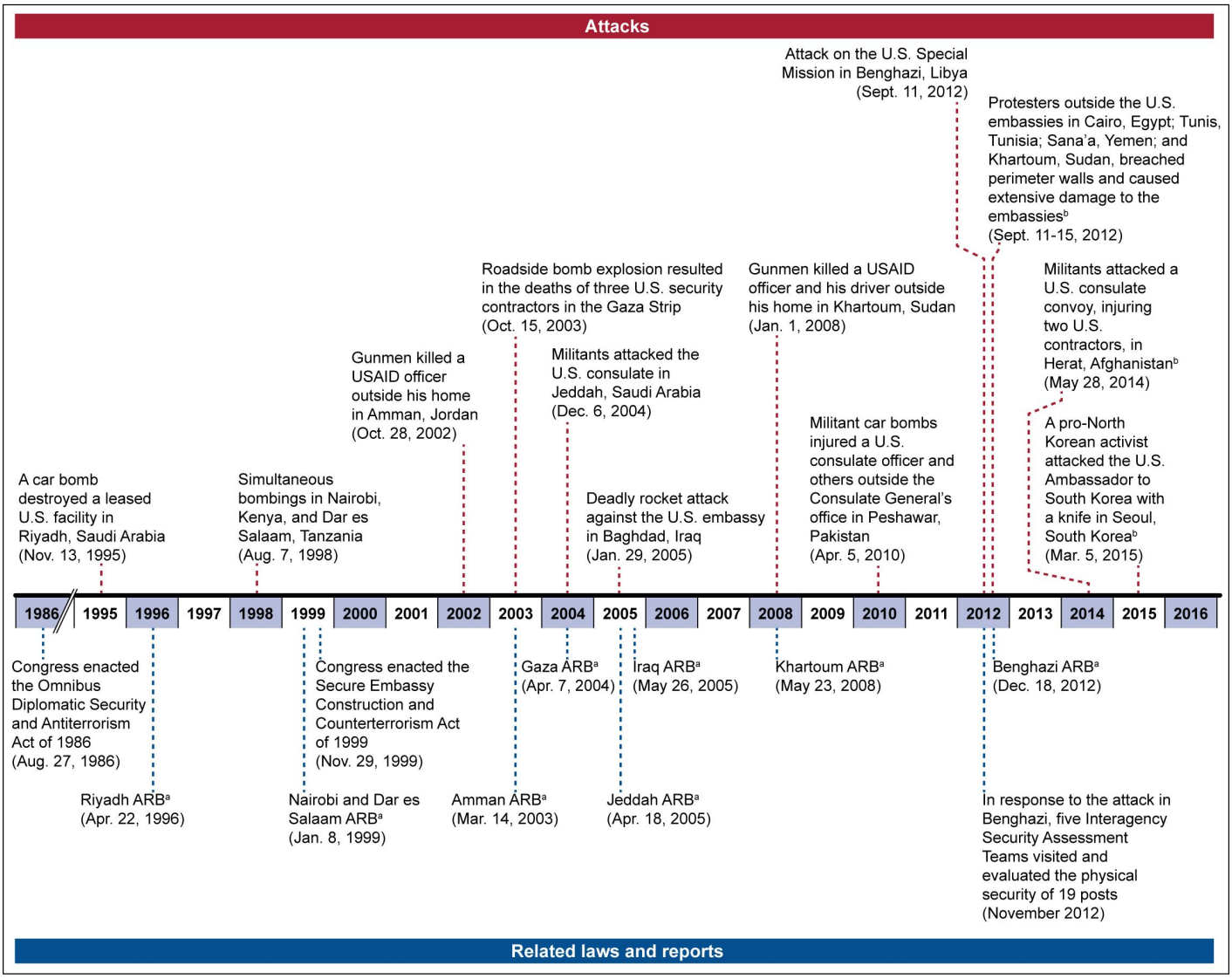
[1]Pub. L. No. 99-399 (codified at 22 U.S.C § 4801 *et seq*).

[2]Pub. L. No. 106-113, div B, § 1000(A)(7) (incorporating by reference H.R. 3427 of the 106th Congress and codified at 22 U.S.C. § 4865).

[3]22 U.S.C. § 4831. The Secretary of State was not required to convene ARBs for incidents occurring in Afghanistan between 2006 and 2014 or in Iraq between fiscal years 2006 and 2017 because of the ongoing wars in both countries.

response to the 2012 attacks in Benghazi. (See fig. 14 for a time line of selected attacks and related laws and reports.)

Figure 14: Time line of Selected Attacks against U.S. Missions and Related Laws and Reports, 1986–2016



Legend: ARB=Accountability Review Board; USAID=U.S. Agency for International Development.

Source: GAO analysis of Department of State documentation and other sources cited above. | GAO-17-681SP

[a]Date of ARB report provided to the Secretary of State.

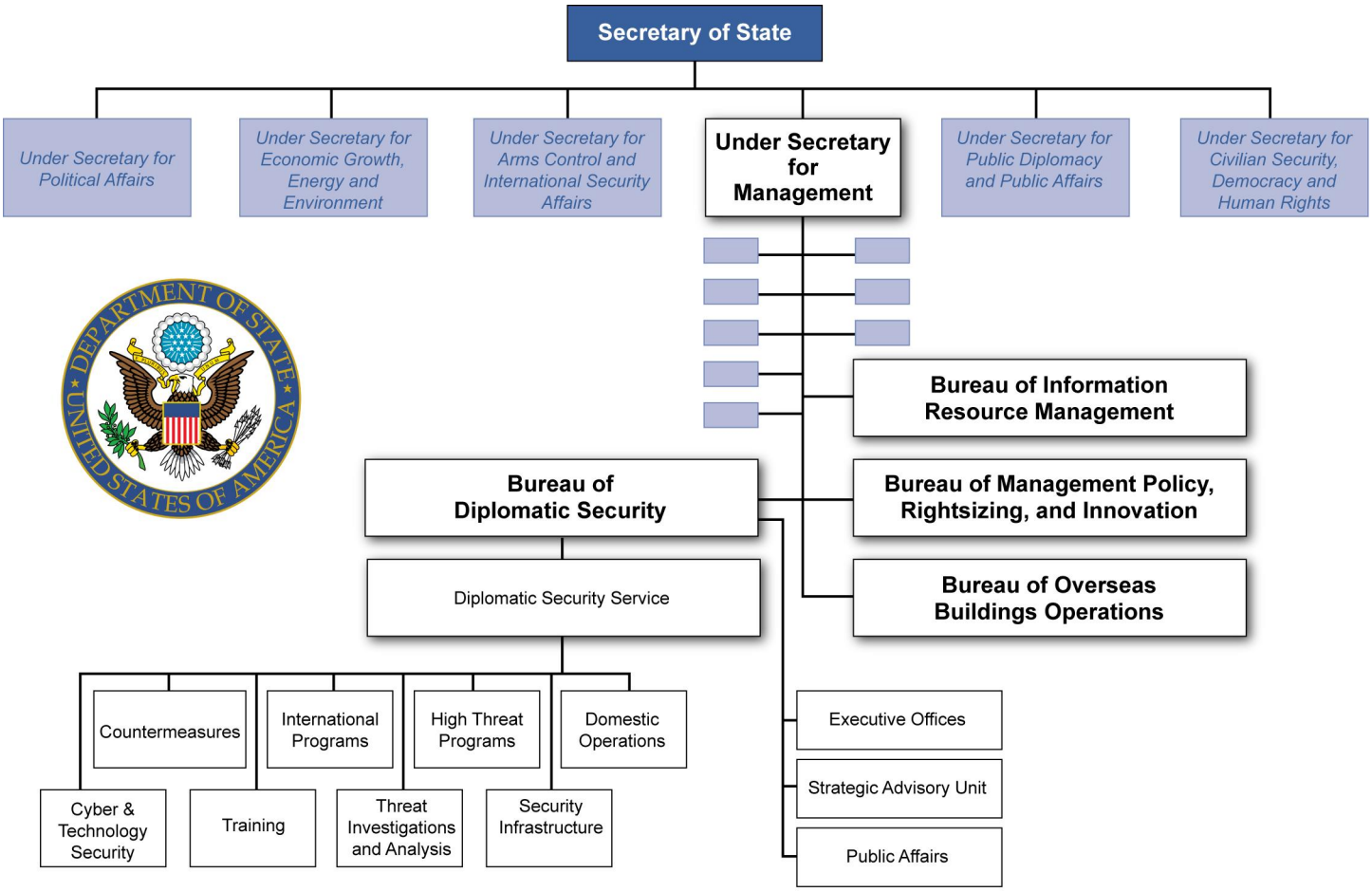
[b]No ARB convened; ARBs not required for attacks in Afghanistan.

Appendix III: Diplomatic Security Responsibilities, Components, and Collaboration with Other U.S. Agencies

The Department of State's (State) Bureau of Diplomatic Security (Diplomatic Security) has responsibilities set forth in State's Foreign Affairs Manual[1]; to help meet its responsibilities, the bureau relies on multiple organizational components within State. (Fig. 15 highlights State offices with key security responsibilities.) State also collaborates with other U.S. government agencies to secure U.S. missions overseas.

[1]See 1 FAM 261.1

Figure15: Department of State Organizational Chart of Offices with Key Security Responsibilities



Source: Department of State. | GAO-17-681SP

Diplomatic Security-Related Responsibilities

As established by the 1961 Vienna Convention on Diplomatic Relations, host country governments are required to protect the diplomatic personnel and missions of foreign governments.[2] More than two decades later, following an attack against the U.S. embassy in Beirut, Lebanon, Congress enacted the Omnibus Diplomatic Security and Antiterrorism Act of 1986 to provide enhanced diplomatic security and to combat international terrorism. The act assigns the Secretary of State responsibility for providing security for all diplomatic operations, in consultation with the heads of other federal agencies that have personnel or missions abroad. The act also created Diplomatic Security to provide a broad range of security and protective functions internationally and domestically. In addition, the act specifies that other federal agencies will cooperate with State to fulfill all security operations of a diplomatic nature.

Diplomatic Security Components

The Bureau of Diplomatic Security is State's security and law enforcement arm. The bureau's eight operational directorates—listed below—are collectively known as the Diplomatic Security Service. In addition, Diplomatic Security has three administrative offices that assist the mission: Executive Office, Strategic Advisory Unit, and Public Affairs.

- *International Programs:* Directs the formulation, planning, coordination, policy development, and implementation of security programs that protect U.S. diplomatic missions for most posts. Manages high-profile security programs such as the Embassy Local Guard Program, Emergency Action Planning, the Worldwide Protective Services Program, Surveillance Detection, and the Marine Security Guard Program.
- *High Threat Programs:* Directs the formulation, planning, coordination, policy development, and implementation of security programs that protect U.S. diplomatic missions at high-threat, high-risk posts. Manages security programs to include personnel recovery, tactical and strategic planning, special operations, evacuation operations, and State's responses to international crises at high-threat, high-risk

[2]Vienna Convention on Diplomatic Relations, Apr. 18, 1961, 23 U.S.T 3227, 400 U.N.T.S. 95.

posts. Diplomatic Security created this directorate following the 2012 attack on Benghazi to ensure that those posts facing the greatest risk—now designated as high-threat, high-risk posts—received additional, security-related attention.

- *Domestic Operations:* Oversees criminal investigations domestically and abroad related to State personnel, facilities, and visiting foreign dignitaries, including passport and visa violations, counterintelligence investigations, and use of force incidents involving State personnel. Oversees the protection of the Secretary of State, the U.S. Ambassador to the United Nations, foreign dignitaries, and other persons of interest.
- *Training*: Formulates and implements all security and law enforcement training programs and policies for Diplomatic Security. Directs the formulation, coordination, and implementation of security and law enforcement training programs that promote the professional development of Diplomatic Security personnel. Oversees specialized security training at overseas posts on a regular and emergency basis and provides emergency security support to posts abroad during periods of high threat, crisis, or natural disaster.
- *Threat Investigations and Analysis*: Directs, coordinates, and conducts the analysis of terrorist threats and hostile activities directed against U.S. government personnel, facilities, and interests abroad. Conducts protective intelligence investigations, coordinates foreign-government and private-sector requests for assistance relating to terrorist incidents, and directs the operations of the Diplomatic Security Command Center and the Overseas Security Advisory Council.
- *Security Infrastructure*: Manages all matters relating to security infrastructure in Diplomatic Security functional areas of personnel security and suitability and insider threats. Formulates strategic operational planning, priorities, and funding for security infrastructure operations.
- *Countermeasures*: Manages, plans, and develops policy for worldwide physical and technical security countermeasures programs. Represents State in negotiations with other federal agencies on issues regarding physical and technical security countermeasures. Directs the offices of Physical Security Programs, Security Technology, and Diplomatic Courier Service.
- *Cyber and Technology Security:* Manages cyber and technical elements of State's security program. In May 2017, Diplomatic Security created this new directorate by consolidating cyber

technology and investigative support elements from other directorates. The goal is to increase State's ability to enable secure innovation in areas such as e-mail messaging services, Wi-Fi, cloud services, mobile communications, and social media.

Other State Bureaus and Offices Collaborate with Diplomatic Security

To complete parts of its mission, Diplomatic Security collaborates with other State entities, most notably the overseas missions and the Bureaus of Overseas Buildings Operations (OBO) and Information Resource Management (IRM).

- *Overseas Missions:* At posts, the Chief of Mission (Ambassador or Principal Officer), is ultimately responsible for the security of facilities, information, and all personnel under chief-of-mission authority.[3] He or she is assisted by Diplomatic Security, which is represented at post by a head special agent known as the Regional Security Officer (RSO). RSOs—working with assistant RSOs and other security personnel—are responsible for implementing a wide range of duties such as protecting personnel and property, documenting threats and residential vulnerabilities, and identifying possible mitigation efforts to address those vulnerabilities. The overseas missions also play a role in setting post-specific security measures and funding some physical security upgrades, with approval from Diplomatic Security. In addition, each post has an Emergency Action Committee (EAC) that provides guidance in preparing for and responding to potential changes in risk that might affect the safety and security of the post and the American citizens in country. The EAC may include the Ambassador, Deputy Chief of Mission, Principal Officer, Defense Attaché, Political Officer, Economic Officer, RSO, Management Officer, Consular Officer, Public Affairs Officer, Human Resources Officer, Medical Officer, U.S. Agency for International Development (USAID) Mission Director, Community Liaison Office Coordinator, and others, including non-State officials, as appropriate. Further, as the 2005 Iraq Accountability

[3]Per the Diplomatic Security Act of 1986, the Secretary of State is responsible for the protection of all U.S. government personnel on official duty abroad, other than those assigned to a U.S. military commander. In addition, the President instructs ambassadors and others designated as chief of mission to take direct and full responsibility for the security of the mission and all the personnel, "whether inside or outside the chancery gate."

Review Board (ARB) noted, all mission personnel bear "personal responsibility" for their own and others' security.[4]

- *Overseas Buildings Operations (OBO):* OBO manages the acquisition, design, construction, maintenance, and sale of U.S. government diplomatic property abroad. Through the Capital Security Construction Program, OBO replaces and constructs diplomatic facilities to provide U.S. embassies and consulates with safe, secure, functional, and modern buildings. In addition, OBO tracks information on State's real properties, including residences; provides funding for certain residential security upgrades; and funds and manages the Soft Targets Program, State's program for providing security upgrades to schools attended by U.S. government dependents and off-compound employee association facilities.
- *Information Resource Management (IRM)*: State's Chief Information Officer leads IRM to provide the information technology and services State needs to carry out its foreign policy mission. The Federal Information Security Modernization Act of 2014 (FISMA) directs the heads of federal agencies, including State, to designate a Chief Information Security Officer to develop, document, and implement a department-wide information security program.

In addition, the Office of Management Policy, Rightsizing, and Innovation (M/PRI) tracks State's implementation of ARB recommendations. Diplomatic Security, OBO, IRM, and M/PRI all report to the Under Secretary for Management.

Other U.S. Agencies Also Play a Role in Securing U.S. Missions Overseas

Diplomatic Security coordinates its work overseas with a number of U.S. government entities and agencies:

[4]In addition, State communicated the responsibility of all overseas employees to practice good personal security in response to a GAO report that found that information concerning personal security was not reaching the intended audience and that post management and personnel were generally uninformed of recent changes in the security arena. See GAO, *Overseas Security: State Department Has Not Fully Implemented Key Measures to Protect U.S. Officials from Terrorist Attacks Outside of Embassies*, GAO-05-642 (Washington, D.C.: May 9, 2005).

- The Overseas Security Policy Board (OSPB) develops security standards for executive agencies working overseas. Chaired by the Assistant Secretary for Diplomatic Security, OSPB includes representatives from approximately 20 U.S. agencies with personnel overseas, including intelligence, foreign affairs, and other agencies. State incorporates the OSPB's physical security standards in the *Foreign Affairs Handbooks*. Diplomatic facilities overseas—whether permanent, interim, or temporary—and residences are required to meet the standards applicable to them. The OSPB standards vary by facility type, date of construction or acquisition, and threat level. If facilities do not meet all applicable standards, posts are required to request waivers, exceptions, or both.
- The Department of Defense (DOD) has long provided military protection and support for the security and safety of U.S. diplomatic missions and personnel during normal operations and emergencies. For example, DOD provides Marine Security Guards at some U.S. diplomatic missions to help protect U.S. personnel, classified material, and property. DOD support is particularly critical in times of crisis, such as when DOD provides security reinforcements to facilities under threat or assists with evacuations. Several entities within State, DOD, and the military branches prepare for and coordinate these efforts. Memoranda of Agreement between State and DOD establish frameworks for cooperation on scenarios requiring security augmentation, crisis response, and evacuation for U.S. diplomatic and consular missions overseas.
- USAID maintains its own Office of Security, which is responsible for the physical security of its facilities and coordination with Diplomatic Security.
- Other agencies operating overseas—such as the Departments of Commerce or the Treasury—may also have security offices, but none of them operating under chief-of-mission authority maintain their own facilities outside of Diplomatic Security's responsibility.

Appendix IV: Bureau of Diplomatic Security Staffing Levels

The Department of State's Bureau of Diplomatic Security (Diplomatic Security) employs a broad workforce of over 51,000 individuals to carry out its mission and activities. Its workforce includes direct-hire security specialists and management support staff, military support, and contractors. See table 2 for a description of each position and a comparison of Diplomatic Security staffing levels in fiscal years 2008, 2011, and 2017.[1]

Table 2: Department of State's Bureau of Diplomatic Security Staffing Numbers in Fiscal Years (FY) 2008, 2011, and 2017

Position	Staff as of FY2008	Staff as of FY2011	Staff as of FY2017	Percent change from 2008 to 2017	Description
Direct-hires[a]					
Special agents	1,585	1,870	2,110	33	Special agents are the lead operational employees of Diplomatic Security. Special agents serve as Regional Security Officers (and assistants) abroad, where they manage all security requirements. Domestically, special agents primarily conduct investigations and provide protective details to the Secretary of State and foreign dignitaries. Special agents also serve in headquarters positions that support and manage all Diplomatic Security operations.
Criminal investigator	44	73	95	116	Diplomatic Security posts Civil Service criminal investigators at domestic field offices to conduct criminal investigations—including visa and passport fraud cases—alongside the Foreign Service special agents.
Security Engineering Officers and Security Technical Specialists	293	340	351	20	Engineers and technicians service and maintain security equipment at posts overseas as well as provide for information security domestically and overseas.
Couriers	98	101	106	8	Couriers ensure the secure movement of classified U.S. government materials across international borders.

[1]We reported Diplomatic Security staffing levels for fiscal years 2008 and 2011 in two previously published reports. See GAO, *State Department: Diplomatic Security's Recent Growth Warrants Strategic Review,* GAO-10-156 (Washington, D.C.: Nov. 12, 2009) and GAO, *Diplomatic Security: Expanded Missions and Inadequate Facilities Pose Critical Challenges to Training Efforts,* GAO-11-460 (Washington, D.C.: June 1, 2011).

Position	Staff as of FY2008	Staff as of FY2011	Staff as of FY2017	Percent change from 2008 to 2017	Description
Security Protection Specialists	0	38	19	NA	Security Protection Specialists are intended to serve as supervisors on protective details in Iraq, Afghanistan, and Pakistan. Diplomatic Security is phasing out the Security Protection Specialist role and reassigning their duties to the Regional Security Officers.
Management support staff	548	600	807	47	Management support staff includes nonagent Civil Service employees who provide managerial, administrative, investigative, and analytical services.
Direct-hires subtotal	2,568	3,022	3,488	36	
Other U.S. government					
Marine Security Guards	1,134	1,170	1,880	66	Marine Security Guards' primary role is to protect personnel and prevent the compromise of national security information and equipment. Marine Security Guards control access to State facilities overseas.
Seabees	107	116	109	2	Seabees are active duty navy construction personnel with skills in building construction, maintenance, and repair essential to State facilities and security programs located worldwide.
Other U.S. government subtotal	1,241	1,286	1,989	60	
Contract and support staff					
Private security contractors	2,000	1,377	1,939	-3	Private security contractors are U.S. citizens who provide protective details for dignitaries in critical threat environments in Iraq, Afghanistan, Pakistan, and Israel.
Diplomatic Security guards and surveillance detection	33,491	35,150	40,050	20	Diplomatic Security guards provide perimeter security to post compounds as well as security at residences of post staff. Surveillance detection teams augment post security by identifying suspicious activity outside of post compounds.
Support contractors	1,300	1,680	2,657	104	Diplomatic Security also employs contractor support staff at headquarters who provide administrative support.
Uniformed protective officers	775	848	1,224	58	Officers provide security at domestic facilities, such as State headquarters.
Subtotal	**37,566**	**39,055**	**45,870**	**22**	
Total	**41,375**	**43,363**	**51,347**	**24**	

Legend: Diplomatic Security=Bureau of Diplomatic Security; State=Department of State.

Source: GAO analysis of Department of State data. | GAO-17-681SP

[a]The number of direct-hire staff does not include locally employed staff. Diplomatic Security was unable to provide a definitive number of all locally employed staff for all 3 fiscal years.

Appendix V: GAO Recommendations regarding the Bureau of Diplomatic Security

Over the course of our work on the Department of State's (State) Bureau of Diplomatic Security (Diplomatic Security) and related efforts, we have identified conditions that affect the success of its programs and recommended a range of improvements that should be considered in program planning and implementation. For example, we have made recommendations on the need for State to address gaps in its security-related activities, standards, and policies, such as developing a process to ensure that mitigating steps agreed to in granting waivers and exceptions for older, acquired, and temporary work facilities have been implemented. We have also made recommendations on the need for improved information sharing between Diplomatic Security directorates, such as sharing information with each other on the residential security exceptions they have processed to help provide Diplomatic Security with a clearer picture of security vulnerabilities at residences and enable it to make better risk management decisions. State and its partner agencies have generally concurred with our recommendations and have taken steps to address a number of them, several of which are noted in the enclosures. In addition, we have identified several existing conditions—such as gaps in State oversight of personnel compliance with mandatory security training and many overseas diplomatic residences not meeting all applicable security standards—that continue to challenge the U.S. government's ability to protect its people, property, and information around the world.

In letters addressed to the Secretary of State, we identified which of these recommendations we believe should be given high priority for implementation. As of August 14, 2017, State had 27 open recommendations that have been deemed by GAO as being among the highest priorities for implementation. Of the 27 priority recommendations, 24 are listed below (see table 3) and are related to this report in four areas, as follows:

- *Security of overseas personnel*. Fully implementing GAO's priority recommendations on personnel security, such as those related to the Foreign Affairs Counter Threat (FACT) training, would help ensure that State personnel are prepared to operate in dangerous situations.

- *Security of overseas facilities.* Fully implementing GAO's priority recommendations on physical security at overseas posts, such as those regarding risk management associated with physical security of diplomatic facilities, will improve the safety and security of personnel serving overseas, particularly in high-threat locations.
- *Transportation security*. Fully implementing recommendations related to transportation security would improve State's efforts to manage transportation-related security risks overseas.
- *Information security.* Fully implementing GAO's priority recommendation regarding obsolete computer systems will improve State's ability to secure its information technology systems and access to potentially sensitive information.

GAO will continue to monitor State's progress in implementing these recommendations and will update their status on the GAO website at http://www.gao.gov.

Table 3: GAO Open Priority Recommendations regarding the Department of State's Bureau of Diplomatic Security, as of August 14, 2017

GAO report	Open priority recommendations:
Countering Overseas Threats: Gaps in State Department Management of Security Training May Increase Risk to U.S. Personnel. GAO-14-360. Washington, D.C.: March 10, 2014.	To strengthen State's ability to ensure that U.S. civilian personnel are in compliance with the FACT training requirement, the Secretary of State should take the following actions: • Identify a mechanism to readily determine the universe of assigned U.S. civilian personnel under chief-of-mission authority who are required to complete FACT training. • Take steps to ensure that management personnel responsible for assigning personnel to designated high-threat countries consistently verify that all assigned U.S. civilian personnel under chief-of-mission authority who are required to complete FACT training have completed it before arrival in the designated high-threat countries. • Take steps to ensure that management personnel responsible for granting country clearance consistently verify that all short-term, temporary duty U.S. civilian personnel under chief-of-mission authority who are required to complete FACT training have completed it before arrival in the designated high-threat countries. • Monitor or evaluate overall levels of compliance with the FACT training requirement among U.S. civilian personnel under chief-of-mission authority who are subject to the requirement.
GAO report:	**Open priority recommendations:**
Diplomatic Security: Overseas Facilities May Face Greater Risks Due to Gaps in Security-Related Activities, Standards, and Policies. GAO-14-655. Washington, D.C.: June 25, 2014.	To improve the consistency and data reliability of State risk management data, the Secretary of State should take the following action: • Direct the Under Secretary for Management to identify and eliminate inconsistencies between and within the *Foreign Affairs Manual*, the *Foreign Affairs Handbook* (FAH), and other guidance concerning physical security. To strengthen the applicability and effectiveness of State's physical security standards, the Secretary of State should work through the Bureau of Diplomatic Security or, in his capacity as chair, through the Overseas Security Policy Board (OSPB) to take the following actions: • Develop physical security standards for facilities not currently covered by existing standards. • Clarify existing flexibilities in the FAH to ensure that security and life-safety updates to the OSPB standards and *Physical Security Handbook* are updated through an expedited review process. • Develop a process to routinely review all OSPB standards and the *Physical Security Handbook* to determine if the standards adequately address evolving threats and risks. • Develop a policy for the use of interim and temporary facilities that includes definitions for such facilities, time frames for use, and a routine process for reassessing the interim or temporary designation. To strengthen the effectiveness of State's ability to identify risks and mitigate vulnerabilities, the Secretary of State should direct the Bureau of Diplomatic Security to take the following actions: • Routinely ensure that necessary waivers and exceptions are in place for all work facilities at posts overseas. • Develop a process to ensure that mitigating steps agreed to in granting waivers and exceptions have been implemented. To strengthen the effectiveness of State's risk management policies, the Secretary of State should take the following action: • Develop a risk management policy and procedures for ensuring the physical security of diplomatic facilities, including roles and responsibilities of all stakeholders and a routine feedback process that continually incorporates new information.

GAO report:	Open priority recommendations:
Diplomatic Security: State Department Should Better Manage Risks to Residences and Other Soft Targets Overseas. GAO-15-700. Washington, D.C.: July 9, 2015.	To enhance State's efforts to manage risks to residences, schools, and other soft targets overseas, the Secretary of State should direct the Bureau of Diplomatic Security to take the following actions: • Institute procedures to improve posts' compliance with requirements for conducting residential security surveys. • Take steps to clarify existing standards and security-related guidance for residences. For example, the Bureau of Diplomatic Security could conduct a comprehensive review of its various standards and security-related guidance for residences and take steps to identify and eliminate gaps and inconsistencies. • Develop procedures for ensuring that all residences at posts overseas either meet applicable standards or have required exceptions on file.
GAO report:	**Open priority recommendations:**
Diplomatic Security: State Should Enhance Its Management of Transportation-Related Risks to Overseas U.S. Personnel. GAO-17-124. Washington, D.C.: October 4, 2016.	To enhance State's efforts to manage transportation-related security risks overseas, the Secretary of State should direct the Bureau of Diplomatic Security to take the following actions: • Create consolidated guidance for Regional Security Officers that specifies required elements to include in post travel notification and transportation security policies. For example, as part of its current effort to develop standard templates for certain security directives, the Bureau of Diplomatic Security could develop templates for transportation security and travel notification policies that specify the elements required in all security directives as recommended by the February 2005 Iraq Accountability Review Board as well as the standard transportation-related elements that the Bureau of Diplomatic Security requires in such policies. • Create more comprehensive guidance for Bureau of Diplomatic Security reviewers to use when evaluating posts' transportation security and travel notification policies. For example, the checklist that Bureau of Diplomatic Security reviewers currently use could be modified to stipulate that reviewers should check all security directives for Bureau of Diplomatic Security-required elements recommended by the February 2005 Iraq Accountability Review Board. The checklist could also provide guidance on how to take the presence or absence of these required elements into account when assigning a score to a given policy. • Clarify whether or not the FAH's armored vehicle policy for overseas posts is that every post must have sufficient armored vehicles, and if the Bureau of Diplomatic Security determines that the policy does not apply to all posts, articulate the conditions under which it does not apply. • Develop monitoring procedures to ensure that all posts comply with the FAH's armored vehicle policy for overseas posts once the policy is clarified. • Implement a mechanism, in coordination with other relevant State offices, to ensure that Emergency Action Committees discuss their posts' armored vehicle needs at least once each year. • Clarify existing guidance on refresher training, such as by delineating how often refresher training should be provided at posts facing different types and levels of threats, which personnel should receive refresher training, and how the completion of refresher training should be documented. • Improve guidance for Regional Security Officers, in coordination with other relevant State offices and non-State agencies, as appropriate, on how to promote timely communication of threat information to post personnel and timely receipt of such information by post personnel. • Take steps, in coordination with other relevant State offices and non-State agencies, as appropriate, to make travel notification systems easily accessible to post personnel who are required to submit such notifications, including both State and non-State personnel.

GAO report:	Open priority recommendation:
Information Technology: Federal Agencies Need to Address Aging Legacy Systems. GAO-16-468. Washington, D.C.: May 25, 2016.	To address obsolete information technology investments in need of modernization or replacement, the Secretary of State should direct the Chief Information Officer to take the following action: • Identify and plan to modernize or replace legacy systems as needed and consistent with the Office of Management and Budget's draft guidance, including time frames, activities to be performed, and functions to be replaced or enhanced.

Source: GAO. | GAO-17-681SP

Appendix VI: Related GAO Products

This appendix provides a list of recent GAO products related to each enclosure.[1] Copies of most products can be found on our website: http://www.gao.gov/.

GAO also has done work on some of the key issues identified in the enclosures that resulted in Sensitive But Unclassified or Classified products. (Report numbers with an SU suffix are Sensitive But Unclassified, and those with a C suffix are Classified.) Sensitive But Unclassified and Classified reports are available to personnel with the proper clearance and need-to-know, upon request. For a copy of a Sensitive But Unclassified or Classified report, please call or e-mail the point of contact listed in the related enclosure.

Enclosure I: Diplomatic Security Funding

State Department: Diplomatic Security Challenges. GAO-13-191T. Washington, D.C.: November 15, 2012.

State Department: Diplomatic Security's Recent Growth Warrants Strategic Review. GAO-10-156. Washington, D.C.: November 12, 2009.

Enclosure II: Diplomatic Security Staffing Challenges

Department of State: Foreign Language Proficiency Has Improved, but Efforts to Reduce Gaps Need Evaluation. GAO-17-318. Washington, D.C.: March 22, 2017.

State Department: Diplomatic Security Challenges. GAO-13-191T. Washington, D.C.: November 15, 2012.

State Department: Diplomatic Security's Recent Growth Warrants Strategic Review. GAO-10-156. Washington, D.C.: November 12, 2009.

[1]Enclosure IX is not included because GAO has not yet published a product on that Bureau of Diplomatic Security-related topic.

Enclosure III: Physical Security of U.S. Diplomatic Facilities

Embassy Construction: State Needs to Better Measure Performance of Its New Approach. GAO-17-296. Washington, D.C.: March 16, 2017.

Afghanistan: Embassy Construction Cost and Schedule Have Increased, and Further Facilities Planning Is Needed. GAO-15-410. Washington, D.C.: May 19, 2015.

Diplomatic Security: Overseas Facilities May Face Greater Risks Due to Gaps in Security-Related Activities, Standards, and Policies. GAO-14-655. Washington, D.C.: June 25, 2014.

Diplomatic Security: Overseas Facilities May Face Greater Risks Due to Gaps in Security-Related Activities, Standards, and Policies. GAO-14-380SU. Washington, D.C.: June 5, 2014.

Enclosure IV: Physical Security of Diplomatic Residences and Other Soft Targets

Diplomatic Security: State Department Should Better Manage Risks to Residences and Other Soft Targets Overseas. GAO-15-700. Washington, D.C.: July 9, 2015.

Diplomatic Security: State Department Should Better Manage Risks to Residences and Other Soft Targets Overseas. GAO-15-512SU. Washington, D.C.: June 18, 2015.

Enclosure V: Security Training Compliance

Diplomatic Security: State Should Enhance Its Management of Transportation-Related Risks to Overseas U.S. Personnel. GAO-17-124. Washington, D.C.: October 4, 2016.

Diplomatic Security: State Should Enhance Management of Transportation-Related Risks to Overseas U.S. Personnel. GAO-16-615SU. Washington, D.C.: September 9, 2016.

Diplomatic Security: Options for Locating a Consolidated Training Facility. GAO-16-139T. Washington, D.C.: October 8, 2015.

Diplomatic Security: Options for Locating a Consolidated Training Facility. GAO-15-808R. Washington, D.C.: September 9, 2015.

Countering Overseas Threats: Gaps in State Department Management of Security Training May Increase Risk to U.S. Personnel. GAO-14-360. Washington, D.C.: March 10, 2014.

Countering Overseas Threats: Gaps in State Department Management of Security Training May Increase Risk to U.S. Personnel in High-Threat Countries. GAO-14-185SU. Washington, D.C.: February 26, 2014.

Diplomatic Security: Expanded Missions and Inadequate Facilities Pose Critical Challenges to Training Efforts. GAO-11-460. Washington, D.C.: June 1, 2011.

Enclosure VI: Embassy Crisis and Evacuation Preparedness

Embassy Evacuations: State Should Take Steps to Improve Emergency Preparedness. GAO-17-714. Washington, D.C.: July 17, 2017.

Embassy Evacuations: State Should Take Steps to Improve Emergency Preparedness. GAO-17-560SU. Washington, D.C.: June 28, 2017.

Enclosure VII: Department of Defense Support to U.S. Diplomatic Missions

*Interagency Coordination: DOD and State Need to Clarify DOD Roles and Responsibilities to Protect U.S. Personnel and Facilities Overseas in High-Threat Areas. G*AO-15-219C. Washington, D.C.: March 4, 2015.

Enclosure VIII: Dissemination of Threat Information

Embassy Evacuations: State Should Take Steps to Improve Emergency Preparedness. GAO-17-714. Washington, D.C.: July 17, 2017.

Embassy Evacuations: State Should Take Steps to Improve Emergency Preparedness. GAO-17-560SU. Washington, D.C.: June 28, 2017.

Diplomatic Security: State Should Enhance Its Management of Transportation-Related Risks to Overseas U.S. Personnel. GAO-17-124. Washington, D.C.: October 4, 2016.

Diplomatic Security: State Should Enhance Management of Transportation-Related Risks to Overseas U.S. Personnel. GAO-16-615SU. Washington, D.C.: September 9, 2016.

Combating Terrorism: Steps Taken to Mitigate Threats to Locally Hired Staff, but State Department Could Improve Reporting on Terrorist Threats. GAO-15-458SU. Washington, D.C.: June 17, 2015.

Enclosure X: Ensuring Information Security

Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority. GAO-16-686. Washington, D.C.: August 26, 2016.

Information Technology: Federal Agencies Need to Address Aging Legacy Systems. GAO-16-468. Washington, D.C.: May 25, 2016.

Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems. GAO-16-501. Washington, D.C.: May 18, 2016.

Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs. GAO-15-714. Washington, D.C.: September 29, 2015.

Information Security: Agencies Need to Improve Oversight of Contractor Controls. GAO-14-612. Washington, D.C.: August 8, 2014.

State Department Telecommunications: Information on Vendors and Cyber-Threat Nations. GAO-17-688R. Washington, D.C.: July 27, 2017.

Enclosure XI: Status of Recommendations Made in Reports following the Benghazi Attack

Diplomatic Security: Overseas Facilities May Face Greater Risks Due to Gaps in Security-Related Activities, Standards, and Policies. GAO-14-655. Washington, D.C.: June 25, 2014.

Diplomatic Security: Overseas Facilities May Face Greater Risks Due to Gaps in Security-Related Activities, Standards, and Policies. GAO-14-380SU. Washington, D.C.: June 5, 2014.

Appendix VII: GAO Contact and Staff Acknowledgments

GAO Contact

Michael J. Courts, 202-512-8980 or CourtsM@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following individuals made key contributions to this report: Thomas Costa (Assistant Director), Miriam Carroll Fenton (Analyst-in-Charge), Esther Toledo, Mason Calhoun, David Dayton, Neil Doherty, David Hancock, Thomas Johnson, Owen Starlin, and Sally Williamson.

The following individuals provided technical assistance and additional support: Joshua Akery, J.P. Avila-Tournut, Jeffrey Baldwin-Bott, Amanda Bartine, John Bauckman, Aniruddha Dasgupta, Mark Dowling, Wayne Emilien, Ian Ferguson, Justin Fisher, Brian Hackney, Brandon Hunt, Guy LoFaro, Michael Rohrback, and Martin Wilson.

In addition, each GAO report cited in the preceding enclosures and in appendix VI includes a list of staff who contributed to that product.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, LinkedIn, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov and read The Watchblog.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548