REPORT OF

THE INDEPENDENT PANEL ON BEST PRACTICES

WASHINGTON, D.C.
29 AUGUST 2013

EXECUTIVE SUMMARY

The Best Practices Panel has reviewed and made 40 important recommendations in 12 areas, to include: (1) Organization and Management; (2) Accountability; (3) Risk Management; (4) Program Criticality and Acceptable Risk; (5) Planning and Logistics; (6) Lessons Learned; (7) Training and Human Resources; (8) Intelligence, Threat Analysis, and Security Assessments; (9) Programs, Resources and Technology; (10) Host Nations and Guard Forces Capability Enhancement; (11) Regular Reevaluation; and (12) Change Management – Leadership, Communication and Training. Some of the Best Practices Panel's recommendations echoed the findings of previous boards, panels, and reports, but none more crucial than DS' overall placement and reporting within the Department.

One clear and overarching recommendation, crucial to the successful and sustainable implementation of all of the recommendations in this report, is the creation of an Under Secretary for Diplomatic Security. Presently as in the past history, DS reports to the Undersecretary for Management (M). The M family is large, complex and deals with a myriad of Department of State issues such as personnel, budget, procurement, medical services, contracting and a host of other key matters. However, the Department's present direction of expeditionary diplomacy, operating with an increased number of temporary and permanent posts in complex, high-risk environments, requires an organizational paradigm change with an Under Secretary for Diplomatic Security as the lynchpin necessary to safely enable the Department's mission.

With threats to our diplomatic personnel and missions continuing to increase, it is paramount that the Department work from a new perspective with the proposed Under Secretary for Diplomatic Security, other relevant Bureaus and external organizations to advance the Best Practices Panel recommendations. Doing so will better prepare the Department to mitigate the ongoing stream of political violence, terrorism, criminal, and intelligence-related threats. Adversaries who seek to do us harm are both resilient and determined. It is incumbent on the Department to provide its personnel the best possible security through improved organizational structure, risk management process, resources, tactics, and training, to ensure United States policy imperatives can be effectively and safely pursued. The panel's recommendations – if adopted and implemented – will further strengthen the Department's ability to protect its personnel and work more safely on a global platform to achieve American foreign policy goals and objectives.

The comments and recommendations in this report are not intended, nor should they be interpreted, as a commentary or assessment of the performance of any individual or element within the Department, but only as the Panel's judgment on best security management practices.

TABLE OF CONTENTS

EXECUTIVE SUMMARY I
TABLE OF CONTENTS II
INTRODUCTION 1
OVERVIEW 1
METHODOLOGY 2
ORGANIZATION AND MANAGEMENT 3
ACCOUNTABILITY 6
RISK MANAGEMENT 7
PROGRAM CRITICALITY AND ACCEPTABLE RISK 10
PLANNING AND LOGISTICS 11
LESSONS LEARNED 13
TRAINING AND HUMAN RESOURCES 15
INTELLIGENCE, THREAT ANALYSIS, AND SECURITY ASSESSMENTS 17
PROGRAMS, RESOURCES, AND TECHNOLOGY 20
HOST NATIONS AND GUARD FORCES CAPABILITY ENHANCEMENT 24
REGULAR REEVALUATION 26
CHANGE MANAGEMENT - LEADERSHIP, COMMUNICATION AND TRAINING 27
CONCLUSION 28
FINAL NOTE 29
APPENDIX A: PANEL MEMBERS A-1
APPENDIX B: LIST OF CONTACTS B-1
APPENDIX C: REFERENCE DOCUMENTS C-1
APPENDIX D: ACRONYM LIST D-1
APPENDIX E: LIST OF RECOMMENDATIONS E-1

INTRODUCTION

The Accountability Review Board (ARB) for Benghazi recommended that the Department of State (hereinafter referred to as the Department) establish a panel of outside independent experts with experience in high risk, high threat areas to support the Bureau of Diplomatic Security (DS), identify best practices from other agencies and countries, and regularly evaluate United States (U.S.) security platforms in high risk, high threat posts. Subsequent to this recommendation, the Department convened a panel of outside independent experts (hereinafter referred to as the Panel) on 9 April 2013. The Panel, which collectively has over 168 years of public and private security-related service, was chaired by Mark Sullivan[1], with Todd Keil[2], Richard Manlove[3], Raymond Mislock, Jr.[4], and Timothy Murphy[5] as additional members. During the course of its review, the Panel visited 10 U.S overseas missions, of which five were or had been high threat posts, and met with over 200 individuals who provided their views concerning security best practices that might be considered by the Department. The Panel was fully supported by the Department and had unimpeded access to documents, personnel, and organizations within the Department. The Department also facilitated Panel meetings with organizations outside the Department and visits to several overseas posts. The following report reflects the independent views of the Panel, based upon the members' best professional judgment, experience and analysis of best practices informed by their extensive interviews, travel and research.

OVERVIEW

The tragedy in Benghazi is another chapter in the long history of attacks against U.S. diplomatic installations and personnel. A brief summary of the most significant events would include the 1979 Embassy hostage taking in Tehran, the 1983 and 1984 Embassy bombings in Beirut and Kuwait, the 1998 simultaneous Embassy bombings in East Africa, the 2004 attack on the U.S. Consulate in Jeddah, the 2012 attacks on U.S. facilities in Cairo, Tunis, Khartoum, and Benghazi, and, more recently, the February 2013 attack on the U.S. Embassy in Ankara, Turkey.

Dozens of other attacks of lesser impact have occurred and even more have failed or been thwarted. These security incidents directly threaten key, long-term U.S. foreign policy objectives. With global flashpoints such as those in Syria, Iran, North Korea, North Africa, and

[1] Former Director of U.S. Secret Service

[2] Former Diplomatic Security Officer and Assistant Secretary with the Department of Homeland Security (DHS) for Infrastructure Protection

[3] Former Senior Advisor to the United Nations Department of Safety and Security (UNDSS) and Principal Security Advisor for UN Operations in Iraq

[4] Retired DuPont Chief Security Officer, FBI Agent and CIA Security Director, former Overseas Security Advisory Council (OSAC) Co-Chair, Past President and Life Member of the International Security Management Association (ISMA)

[5] Former Deputy Director of the Federal Bureau of Investigation (FBI) and current ISMA member as Vice President (VP) Corporate Compliance for MacAndrews & Forbes Holdings, Inc

the Levant on the rise, other attacks will undoubtedly be mounted in the future, and it is vital that critical shortfalls in the Department of State's approach to enterprise risk management not be allowed to negatively impact U.S. strategic policy goals.

The threat notwithstanding, it is also critical to establish a perspective on these incidents. The Department currently relies on DS to provide a secure environment for the conduct of American foreign policy. Every day DS successfully protects the lives of approximately 35,000 U.S. employees under Secretary of State and Chief of Mission authority worldwide, as well as the lives of approximately 70,000 family members of these employees. An additional 40-45,000 locally engaged staff (LES) are also protected during working hours. In sum, with 2,000 special agents, and its network of engineers, couriers, civil service personnel and other critical staff, DS successfully protects almost 150,000 employees and family members during business hours, and about 100,000 U.S. employees and family members around the clock. Approximately 275 foreign service posts abroad, comprising thousands of buildings and residences, also fall under the Department's responsibility and the DS protective security purview.

It is essential that the U.S. Government (USG) do everything it can to enhance its ability to safeguard personnel who serve on the frontlines of diplomacy in difficult and oftentimes dangerous locales. The Best Practices Panel, convoked with this goal, looked across a wide spectrum of private, government, and non-governmental organizations to glean effective measures to enhance the Department's ability to ensure a safe and secure environment for employees and programs. Not surprisingly, the panel found that many institutions -- and even governments -- refer to DS as the "Gold Standard" for security and seek to model their services after DS. Nevertheless, any successful organization must continuously evolve and improve to adjust with a fluid and dynamic environment.

METHODOLOGY

In conducting its research the Panel focused on issues that were strategic in nature, while touching on several key operational and tactical matters of particular importance. The best practices identified by the Panel, if implemented, will serve to improve the security of Department of State operations not only in high threat areas, but also globally. In this regard the Panel recalled that the East Africa bombings in 1998 occurred at posts that were not designated high threat. In the August 2013 closure of posts in the Middle East and North Africa due to the potential for terrorist attacks, only four of 19 were designated as high threat. The Panel's view was that its recommendations should be realistic, achievable, and measureable. The approach of the Panel was further refined through meetings with representatives of international organizations, host governments, private sector companies with global operations, and Department of State personnel at all levels. Particular emphasis was placed upon interviews with those serving at high threat posts the Panel visited.

The findings and recommendations of the ARB, as well as the recommendations of other Department of State reports and management studies, were reviewed in the context of the Panel's

own independent assessment and observations of the Department's security-related operations. Best practices were then identified to address shortcomings and provide mechanisms for further consideration by the Department.

ORGANIZATION AND MANAGEMENT

The Omnibus Diplomatic Security and Antiterrorism Act of 1986 created DS as a direct result of the bombing of the Embassy and Marine Barracks in Beirut, Lebanon in 1983. Foremost among the purposes of this Act, Congress set forth the responsibilities of the Secretary of State. The Act also established the Assistant Secretary of Diplomatic Security to head DS.[6] This law clearly established the Secretary of State as ultimately accountable for the safety and security of the Department and its personnel. Further, this law clearly established the Assistant Secretary for Diplomatic Security as the Department's senior security executive with global responsibilities delegated from the Secretary of State.

Ambassadors, in their Presidential appointment letters, are designated as directly accountable for the safety and security of their posts and all personnel serving under their authority as Chief of Mission. Management of this responsibility is delegated by the Ambassador to the Regional Security Officer (RSO), who is the senior DS Agent at post. After meeting with Ambassadors, RSOs, agency heads, and other personnel at overseas posts, many in high threat locations, the Panel concluded that the security-related responsibilities and accountabilities of each were well understood by all parties. The direct line of authority from the Ambassador to the RSO, utilizing the Country Team and Emergency Action Committee when necessary, was seen as critical to effective post security management and responding to dynamic threats.

However, at the headquarters level, the same clear lines of authority and understanding of responsibilities are not as well defined or understood. This has led to stove-piped support to posts and lack of understanding of security related coordination requirements among DS, the Under Secretary for Management, and the Regional Bureaus, as noted by the Benghazi ARB.[7] In fact, some senior Foreign Service officers and DS Agents who met with the Panel identified the Under Secretary for Management (M) as the senior security official in the Department responsible for final decision making regarding critical security requirements. This role was not identified by Congress in the Diplomatic Security Act of 1986 and is a potential root cause for the confusion, lack of clear lines of authority, and communication at the headquarters level.

To effectively, efficiently, and securely operate in today's dynamic threat environment, organizational management must be based on clear and well-defined lines of authority which

[6] PL 99-399, "Omnibus Diplomatic Security and Antiterrorism Act of 1986, Title I, Section 102, 103, 105).

[7] Benghazi ARB, page 6, Para 3, *"Communication, cooperation and coordination among Washington, Tripoli and Benghazi functioned collegially at the working-level but were constrained by a lack of transparency, responsiveness, and leadership at the senior levels. Among various Department bureaus and personnel in the field, there appeared to be very real confusion over who, ultimately, was responsible and empowered to make decisions based both on policy and security considerations."*

support routine global security operations, but which also have the ability to be agile and flexible when supporting posts in high threat environments, particularly during times of increased threat or crisis. Collaboration is essential to ensure that all individuals who have responsibilities related to policy and programs, security and safety, personnel, resources, facilities, administration and intelligence work together to ensure a cohesive effort when conducting global operations. The Department's senior security executive must have the safety and security of personnel, facilities, and enabling operations overseas as a clear and primary focus. The threats Foreign Service personnel face require the Department's security function not be relegated to the same status as other important, but distinctly different, support functions. Today, Diplomatic Security is only one of eleven diverse support and administrative functions reporting to the Under Secretary for Management.[8] This is a significant span of control issue and, if unaddressed, could contribute to future security management failures, such as those that occurred in Benghazi.[9]

Organizations that take advantage of the full capability of their security services are those in which there is a single leadership focal point for security at the senior executive governance level. This leader is responsible for organizing, planning, budgeting, and implementing the organization's protection, which is aligned and integrated with its overall institutional goals and objectives. A common best practice in the private sector is to focus all security efforts through a Chief Security Officer who has direct access to the Chief Executive Officer[10] and works with Executive and Business leadership to ensure clear risk mitigation efforts that enable business objectives. An effective security function must be co-equal to the other organizational components and have a "seat at the table" to ensure strategic accountability, common understanding of risk, and corresponding mitigation options and costs. The integration of security as an enabling element at every stage of the planning and operational process, through a single leadership focal point at the executive governance level, increases the likelihood of program success with the least amount of risk.

When speaking with various U.S. Government agencies, international organizations and the private sector, it was also pointed out to the Panel that the placement of the security function within an organization's structure is a statement of how that organization values security and its personnel. Placement is critical to demonstrate to those both within and outside of the agency

[8] May 2012 Department of State Organizational Chart shows following reporting to M: Administration, Budget and Planning, Consular Affairs, Diplomatic Security and Foreign Missions, Foreign Service Institute, Comptroller and Global Financial Services, Human Resources, Information Resource Management, Office of Medical Services, Overseas Buildings Operations and Office of Management Policy, Rightsizing and Innovation

[9] Benghazi ARB, page 8, Para #2," *"The Board recommends that the Department re-examine DS organization and management, with a particular emphasis on span of control for security policy planning for all overseas U.S. diplomatic facilities."*

[10] In a recent benchmarking survey of the senior security executives (Chief Security Officers) conducted by the International Security Management Association (ISMA), in the 152 multinational companies represented, 89% of the senior security executives reported that their position was two levels or less from their Chief Executive Officer (CEO) and 62% were only one level or less below their CEO.

that the organization understands that an effectively integrated security apparatus is critical to enabling mission success.

The placement of Diplomatic Security within M has led not only to confusion with regard to clear lines of authority, responsibility, and accountability for security within the Department, but also is not in keeping with the provisions of the Foreign Affairs Manual (FAM),[11] 1 FAM 014.5, Organization and Planning Principles, which states that *"Organizational layers should be limited to the minimum number consistent with effective span of control and performance of mission. The addition of nonessential supervisory layers increases problems associated with establishing clear delegation of responsibility and authority, transmission of information, work flow, clearances, operational costs, and morale."*

The current diverse and complex Departmental support elements managed today by the Under Secretary for Management in addition to Diplomatic Security's dynamic and real time demands, is not a best practice for effective span of control and performance of mission as required by the FAM.[12] Furthermore, in the Panel's judgment, the current positioning of DS today is no longer consistent with the intent of the Diplomatic Security Act of 1986 when moving the Office of Security outside of the Administration Bureau. Today's reality is that DS remains as one among many within the mostly Administrative functions of the Department.

The security challenges of the 21st century, when combined with the necessity to conduct foreign policy in high threat environments, require a further elevation of the security function within the Department. In the judgment of the Panel, an Under Secretary for Diplomatic Security is needed to fully integrate and balance security requirements in support of U.S. foreign policy. *This is the lynchpin to ensure that this critical function enables the Department to safely and securely conduct its mission around the world.*

The Panel notes that a similar recommendation was made to the Department in 1999 following the East Africa Embassy bombings and approved by the then Secretary of State, but 14 years later never implemented.[13] Based on the Panel's observations and its knowledge and experience, the implementation of this recommendation is essential if the Department is to bring security governance into the 21st Century and align security management with the realities of a post 9/11 threat environment.

[11] Contains the functional statements or organizational responsibilities and authorities assigned to the Department and cites legislation and executive orders relating to the responsibilities of the Department of State.

[12] Today in DoS, official travel to Somalia requires 11 levels of clearance, with the final approval step being M, personally. In contrast, today in the FCO such travel requires two levels of clearance, with the final approval being the equivalent of the Regional Bureau.

[13] Booz-Allen & Hamilton, Security and Intelligence Management Study, Oct 1999.

RECOMMENDATION

1. The Department should, as a matter of urgency, establish an Under Secretary for Diplomatic Security.[14]

ACCOUNTABILITY

During discussions with former and serving Ambassadors, RSOs, and country team members, the Panel concluded that these key players fully understood their accountability and responsibility for security at country-level; however, they were less clear with regard to accountability and responsibility for security at the Department level. Through further meetings with senior managers at the Department level, the Panel confirmed that institutional and individual security accountability and responsibility were neither well-defined nor understood.

Clearly defined accountability and responsibility for security at every level is fundamental for effective security management within an organization. The organization, its component parts, and individuals within have a critical role to play; therefore, their accountability and responsibility must be clearly documented. Leaders and managers who understand their accountability and responsibility for security will ensure that security-related considerations are incorporated in the earliest stages of planning and decision making rather than as an afterthought. As an essential supporting component, security becomes an enabling element necessary to informed decision making. While it is not possible to eliminate all risk, a framework for accountability ensures that risk is managed and accepted at the appropriate level within an organization. However, with that acceptance the organization must understand that even though its best efforts are made to reduce risk, and individual responsibility is clearly defined, casualties may nevertheless occur. In such instances and absent individual negligence, the resulting inquiry into the incident should reflect lessons learned and focus on how to prevent other such incidents.

The Panel reviewed several frameworks for accountability developed by international organizations, multi-national corporations, and foreign government entities. The most effective frameworks are those that are simple yet inclusive and easily understood. They define the accountability of the organization's Chief Executive Officer, Chief Security Officer, Department Heads, Country Representative, Chief Security Officer in the country, heads of agencies in the country and individual staff members. Within the Department this would be analogous to the Secretary of State, Under Secretary for Diplomatic Security, Assistant Secretaries of the Regional Bureaus, Ambassadors, RSOs, Country Teams, and employees.

There must be, in effect, a defined chain of security accountability that informs and enables program success, extending from the Secretary of State to individual employees. The development and implementation of an accountability framework is a Department responsibility,

[14] The proposed Under Secretary for Diplomatic Security is hereinafter referred to as the Under Secretary for Diplomatic Security.

with corresponding accountabilities and responsibilities established by every Bureau, Directorate, Office, Division, Branch, and Section within the Department.

Although it is not the intention of the Panel to develop a proposed framework of accountability for the Department and notwithstanding the security responsibilities delineated in the FAM, the following general description may serve as an example of this best practice. The Assistant Secretaries of the Regional Bureaus would be accountable to the Secretary of State, through the Under Secretary for Political Affairs, for oversight of the implementation all security measures required for the safety and security of overseas missions. They would further be responsible for coordinating with the Under Secretary for Diplomatic Security to ensure that security is given priority at the beginning of the planning process, particularly in advance of opening or reopening missions in high threat areas. The Under Secretary for Diplomatic Security would be responsible for conducting threat and vulnerability assessments to identify risk and recommend mitigating measures for the consideration of the Under Secretary for Political Affairs. Finally, the Secretary would be responsible for ensuring that institutional and individual accountability and responsibility for security are clearly defined within the Department.

Based on field reviews, it was apparent to the Panel that, if properly institutionalized, a framework for accountability ensures that security and risk mitigation are integrated into planning for every activity and operation from the beginning. This is key when developing models for security risk management and program criticality. With a framework for accountability in place there is no confusion with regard to who is accountable and responsible for making decisions based on policy and security considerations.

RECOMMENDATION

2. The Department should develop an accountability framework documenting institutional and individual accountability and responsibility for security throughout the Department.
3. Accountability and responsibility for security should be included in work requirement statements for all Foreign Service (generalist and specialist) employees.
4. The Department should develop an integrated and seamless training program and communications strategy to ensure Department wide understanding and effective implementation of the accountability framework.

RISK MANAGEMENT

During the Panel's field visits, concern was expressed that the response to the attack in Benghazi would be to centralize security decisions at Department level and thus impact embassy ability to conduct foreign policy in high threat environments. The Panel believes implementing an effective risk management model would allow and enable effective decision making in the field while increasing the Department's overview of current threats and mitigating strategies. The Panel therefore pursued the subjects of risk avoidance versus risk acceptance in the context of risk management practices by other organizations.

After numerous discussions in Washington and in the field, the Panel determined that there is no formal risk management model in place for use by either DS or the Department. Risk is managed by experience and intuition, which is important; however, without an established risk management methodology to measure and manage risk, managers very logically tend to be risk adverse. They restrict operations (thereby reducing the organization's exposure to risk) rather than accept that operations can proceed within established risk parameters. Where risk management is not mainstreamed and understood by program and security managers across an organization, security is seen as an impediment to mission accomplishment rather than as an operational enabler. A risk management model makes it possible for an organization to identify security measures and resources required to achieve mission objectives and then determine the level of risk it is willing to accept to accomplish those objectives.

There are numerous security risk management models used by government agencies, international organizations, and the private sector. In general, security risk management is an analytical process that entails the identification of risk that may affect personnel, assets, and operations and provides cost-effective solutions in the form of mitigation strategies to lower risk by reducing the impact and likelihood of an undesirable event. Risk levels are determined by: identifying threats to personnel, facilities or operations; evaluating vulnerability; and, assessing risk in terms of event likelihood and impact. Risk is reduced and thus managed by identifying and implementing mitigating measures. Critical to assessing risk is the identification and assessment of the program requirement, which is the program managers' responsibility. Once security risk mitigation measures, options, and resource requirements are identified by the security component, managers must ensure that those risk mitigation measures are implemented before mission execution. This is an iterative process and a change in any variable requires a review of the process to determine if any adjustment is necessary.

In the absence of a Department risk management process, the fallback position when Inman[15] and Overseas Security Policy Board (OSPB) standards cannot be met either in the short term or ever has been to define missions, such as Benghazi, in such a manner (special mission, temporary facility) that they are not required to meet Inman standards. Waivers for not meeting security standards have become common place in the Department; however, without a risk management process to identify and implement alternate mitigating measures after a waiver has been given, Department employees, particularly those in high threat areas, could be exposed to an unacceptable level of risk.

[15] The security-driven design and building standards for U.S. diplomatic and consular properties.

The Panel has identified the following advantages of implementing a security risk management model:

1. Clear identification of program requirements by program managers, while considering the operational environment. This requires close collaboration with the security component at the earliest stages of program planning.
2. Identification of the unmitigated risk to personnel, facilities and operations, considering the program requirements.
3. Identification of mitigating measures to reduce risk.
4. Identification of associated resource requirements.
5. Identification of residual (unmitigated) risk.
6. Prioritization of programs based on criticality and available security resources.
7. Identification of the responsibilities of security managers at every step in the risk management process.
8. Identification of the responsibility of program managers at every step in the process.
9. Security enables operations rather than impeding them.
10. Risk is being managed rather than avoided.

Had an effective risk management model been in use at the time the decision was made to extend the special mission in Benghazi, the action memorandum would have detailed the program objectives, threats, vulnerabilities, and the security measures required to mitigate the risk.[16] The Department would then have been able to determine if the level of risk was acceptable considering the expected outcome.

RECOMMENDATION

5. The Department should develop and implement a Department-wide risk management model and policy.
6. The Department should consult with Argonne National Laboratory, Infrastructure Assurance Center as well as the United Nations Department of Safety and Security (UNDSS), to inform the ongoing effort of the Office of Management Policy, Rightsizing and Innovation (M/PRI) and DS to develop a risk management model.
7. The Department should develop an integrated and seamless training program and communications strategy to ensure Department-wide understanding and effective implementation of the risk management model and policy.

[16] Action Memo for Under Secretary Kennedy – M; From: NEA-Jeffery Feltman; Subject: Future of Operations in Benghazi, Libya, dated December 27, 2011.

PROGRAM CRITICALITY AND ACCEPTABLE RISK

An agreed risk management model provides an organization with the mechanism to determine the level at which program managers identify programs of such criticality that the organization is willing to expose its personnel to an increased level of risk. For example, if an organization mitigates risk so that the likelihood of an incident is low and the impact of the incident on personnel, facilities, or operations is low, then the corresponding risk is low and the organization will probably proceed with the activity. On the other hand, if the organization takes all possible mitigating measures and the residual risk (the risk remaining after all possible mitigating measures have been taken) is such that it is likely that an incident will occur and the impact of the incident on personnel, facilities, or operations will be high, the organization must then balance the criticality of the program against the risk to the organization should it implement the program.

Program criticality is determined by program managers; risk is determined by security managers. Acceptable risk is the balance between program criticality and residual risk. At the country level it is the Ambassador, advised by the RSO and the Emergency Action Committee (EAC) who balances program criticality and residual risk within the risk management mechanism. It is efficient and effective that such decisions should be made by empowered managers at the most appropriate level. There may, however, be a requirement to conduct critical programs in an environment where the residual risk is so severe that there is a high likelihood its implementation will result in death or serious injury. In such instances, the criticality of the program should be determined by the Regional Bureaus in consultation with Department leadership and direction from the National Security Council and the White House. The Undersecretary for Diplomatic Security should be responsible for evaluating the risk of implementing the critical program and advising the Regional Bureaus and Secretary of State accordingly.

Every organization has an inherent risk threshold concerning the safety and security of its employees. The mechanism for determining that threshold is the security risk management model adopted by the organization. The determination of program criticality, residual risk, the balance between the two, and the level at which each is determined defines acceptable risk and designates accountability at the appropriate decision making level within the organization.

RECOMMENDATION

8. The Department should develop within its risk management model a mechanism to balance program criticality and unmitigated, or residual, risk and identify accountable decision-makers responsible for accepting risk at each level within the organization.
9. The Department should develop an integrated and seamless training program and communications strategy to ensure Department wide understanding and effective implementation of the program criticality decision making process.

10. The Department should consult with Argonne National Labs, Infrastructure Assurance Center, and UNDSS subject matter experts (SMEs) to develop within its risk management model and policy a mechanism to balance program criticality and residual risk.

PLANNING AND LOGISTICS

After numerous discussions with senior leaders at high threat posts, the Panel concluded that a formal planning process would be a best practice for reopening and opening posts. This observation mirrored the view of ARB Recommendation 6[17] and confirmed the validity of that recommendation. The Panel was briefed by M/PRI on recently-published 2 FAM 420 Opening a Post, which documents that, when required, a planning cell will be established in the appropriate regional bureau to conduct a mission analysis and draft an operations plan. Once the course of action is approved, an implementation and support cell is created under the regional bureau Principal Deputy Assistant Secretary to coordinate the support of all necessary bureaus and ensure other agency coordination. The Panel was impressed by the clear accountability of the regional bureaus for ownership of the plan and its implementation, as well as integration of all supporting elements into this deliberate planning process. The FAM also includes organization charts, a process map, and checklists to ensure no key points are overlooked.

It was unclear to the Panel if the core of designated Department-level professional planners stipulated in 2 FAM 420, Exhibit 423.4 would be embedded in the regional bureaus or "loaned" to the regional bureaus to plan specific operations and then return to the control of the Department-level senior planner or planning office. Best practices indicate that in order to have the capability to: conduct strategic planning; review bureau plans; ensure that the standardized planning process and policy are followed by bureau-level planners; and, ensure the efficient distribution of planners to support regional bureau requirements, there should be a Department-level planning cell, led by a senior planner who reports to the Under Secretary for Political Affairs with regard to the use of this valuable resource. A senior planner at the Department level would also ensure that lessons learned by the regional and other bureau planning cells are folded back into the Department planning process and policy so that they are revised as necessary.

DS Exhibit 423.9 to the above FAM is presently being revised to identify the DS focal point for planning. Best practices indicate that there should be one office within DS that is accountable and responsible for planning. Organizationally this office would be analogous to the planning cell within the office of the Under Secretary of Political Affairs, therefore it should be located in the office of the Under Secretary of Diplomatic Security. In making this recommendation, the

[17] *"Before opening or re-opening critical threat or high risk, high threat posts, the Department should establish a multi-bureau support cell, residing in the regional bureau. The support cell should work to expedite the approval and funding for establishing and operating the post, implementing physical security measures, staffing of security and management personnel, and providing equipment, continuing as conditions at the post require."*

Panel is aware that an Office of Planning and Innovation was proposed within DS and never instituted.[18]

The establishment of minimum operating security standards (MOSS) is a proven best practice that is used by a number of international organizations and agencies. MOSS are particularly useful when planning to occupy temporary facilities in high threat areas, as they provide a starting point for the identification of critical equipment or capability such as: communications; emergency action plans; medical equipment; vehicles; facilities; and, training. It is possible that the lack of this equipment or capability could have such an impact on the plan that it cannot be implemented until the equipment or operational support is available. However, the experience with the establishment of strict standards, such as the Inman standards for the construction of facilities, is that they are often waived due to the press of operational requirements. The Panel is therefore concerned that minimum operating security standards would also be established and then waived. By the informed use of the security risk management process, every identified shortfall in meeting a required standard, to include waivers, must be accompanied by a mitigating measure that will reduce the risk to an acceptable level. The mitigating measure must then be agreed and implemented by regional bureaus as advised by DS.

RECOMMENDATION

11. The Department should establish a planning cell, led by a senior planner within the office of the Under Secretary for Political Affairs, to: advise the Undersecretary with regard to strategic planning; support the regional bureaus; establish terms of reference and standards for bureau planning cell officers; ensure the standardization of planning within the regional bureaus; and, include lessons learned in the planning policy.
12. The Bureau of Diplomatic Security should establish one planning office within DS that is accountable and responsible for DS-centric planning that informs DS decision-making and program execution. This office would also be the DS focal point for the larger Department planning process as identified above and be located in the office of the Under Secretary for Diplomatic Security.
13. Waivers to established security standards should only be provided subsequent to the implementation of mitigating measures as agreed by regional bureau or other program managers, advised by DS, and as informed by the Department risk management model.
14. A Department-wide information and training roll-out program should be initiated for 2 FAM 420.

[18] "Office of Planning and Innovation Mission Statement" and "Office of Operational Planning and Innovation Planning Charter", 14 February 2012.

LESSONS LEARNED

From the Panel's interaction with the United Nations (UN), the New York Police Department (NYPD), private sector representatives, Non-Governmental Organization (NGO) representatives, foreign government entities and other USG agencies who operate overseas, one best practice they all follow is an immediate "hot wash" or after-action debriefing of key participants following critical operational events. Whether a man-made crisis, a traumatic event such as Benghazi, or natural disaster, these organizations use this best practice to identify lessons learned, both good and bad, while information and the experiences of personnel involved is still in sharp focus. These lessons are then factored into communications with employees; crisis, tactical and management training; planning and logistics in support of missions; and, new intelligence requirements. This is further programmed into their institutional risk management process to ensure that every event, not just those with a negative outcome, becomes a learning experience for the entire organization. Some organizations, even if not affected by an event, use it as a management exercise to discuss and plan how they would react in similar circumstances. For example, one foreign government organization informed the Panel that within 90 days of the release of the unclassified Benghazi ARB report they had assembled a team to study, dissect, and incorporate the identified lessons learned into their own management and training.

When DS headquarters managers were asked about a lessons learned process in DS they most frequently said none existed or referred to the RSO Knowledge Database. The Panel's research determined that the DS Knowledge Database has not been truly functional for a number of years. Discussions with Foreign Service Officers and RSOs who serve or have served in high threat posts determined that if there is a functional lessons learned process in the Department or DS, they were unaware of it. While some mistakenly identified the ARB process as the lessons learned capability for the Department, even this process does not capture and exploit all the knowledge and experience of Foreign Service Officers and DS personnel who have experienced events when no ARB was conducted. The Panel notes that State Department's Office of Inspector General (IG) has advised that between 1998 and 2012 only 12 ARBs were conducted by the Department. However, according to an official unclassified DS publication, between 1998 and 2012, 273 significant attacks were carried out against U.S. Diplomatic facilities and personnel.[19]

Furthermore, the Panel interviewed RSOs who have opened or reopened posts in high threat areas and all said they were not given a road map, lessons learned from previous similar missions, or standard operating procedures for opening a post. In addition, they were not debriefed by the Department or DS to capture lessons learned after successfully opening the post

[19] U.S. Department of State, Bureau of Diplomatic Security publication, revised July 2013, "Significant Attacks against U.S. Diplomatic Facilities and Personnel, 1998-2012". This report also states, "*This information is not an all-inclusive compilation; rather, it is a reasonably comprehensive listing of significant attacks.*"

to ensure that those best practices could be used by future officers tasked with the same responsibility.

It is noted that in addressing ARB Recommendation 6[20] the Department, through M/PRI, formed a multi-bureau working group tasked with developing a planning model, process map, policy, and check list for opening a post. This resulted in the approval of 2 FAM 240, Opening a Post, on 30 May 2013. Significantly, in reporting the results of the M/PRI led working group to the Undersecretary for Management, the intent to use "lessons learned" to update the policy and model is specifically mentioned.[21] This does not, however, constitute an effective institutional capability within the Department to gather in a timely manner the knowledge and experience of personnel who experienced critical operational events and incorporate that information back into the Department's training, management and security planning functions.

Within DS, the Countermeasures Directorate (DS/C) sends security engineers and other appropriate personnel to posts after serious breaches of physical security measures.[22] Following the civil unrest of 2012 in Tunis, Khartoum, Chennai, Sana'a, Islamabad and Jakarta, DS/C experts traveled to these posts to identify what security countermeasures worked, what did not work, and to conduct repairs or retrofitting of damaged equipment and facility security features. This is not a new process, but a long established best practice carried out by DS/C and DS Security Engineers, often with interagency support and SMEs.

However, this same process is not mirrored in the Department or other DS components, and this points directly to the lack of either a DS or Department-wide institutionalized lessons learned process. Some lessons from the attacks of 11 September 2012 were tactical in nature (pointing to the success or failure of certain physical security features) while others, as noted in this report, were strategic (pointing to the lack of an effective planning, risk management and accountability process). While none of these lessons or processes, even when effectively implemented, provide a guarantee against the loss of life in high threat environments, they do enable a well managed organization to improve its protective measures - over time - and methodically adapt to changing threat environments and reduce risk to personnel, facilities and operations around the world.

Finally, as of the date of this report, the DS Agents who survived the attack on the Special Mission in Benghazi, other than through the ARB interviews or Best Practice Panel discussions, have not been debriefed by any entity in DS or the Department for security lessons learned from this tragedy. While the Department has not taken this step, as noted earlier, a foreign government entity advised the Panel that they had completed their own lessons learned of the incident within 90 days of the release of the ARB report.

---

[20] *Ibid.* 15, p. 11

[21] January 29, 2013 Information Memo to M from M/PRI, SUBJECT: Status: ARB Action No.10 – Develop concept for "support cells", page 1, paragraph one, sub-para 3.

[22] An informal DS newsletter, "Profile" is a publication of the Countermeasures Directorate, Bureau of Diplomatic Security, U.S. Department of State, Summer 2013 edition.

RECOMMENDATION

15. The Department should establish a formalized lessons learned process and accompanying FAM policy to ensure a timely debriefing of all personnel who have participated in critical operational events to collect and preserve the knowledge gained from these personnel so that it may be then incorporated into training, management, and policy processes throughout the Department.
16. The Bureau of Diplomatic Security should establish a formalized lessons learned process and ensure that it is integrated into the recommended Department-wide process. The lessons learned process should involve coordination with appropriate DS entities to obtain and incorporate the knowledge and experience of DS personnel.

TRAINING AND HUMAN RESOURCES

Training is viewed by the Panel as critical to the implementation of every recommendation in this report. As security is every employee's responsibility, the recommendations in this report should be promulgated with a supporting Department-wide communications and training plan for all Department employees. The Bureau of Diplomatic Security and the Foreign Service Institute (FSI) should further advance their current partnership by developing integrated and seamless training modules on high threat post operations, accountability, risk management, program criticality, acceptable risk, planning, logistics, and advanced situational awareness. The advanced situational awareness course should be similar to those currently provided by various DOD services and other USG agencies to their employees. The viability of the identified training must be maintained by continuously updating the curriculum though the incorporation of lessons learned into the courses of instruction in an institutionalized and near real-time process.

The Bureau of Diplomatic Security will be unable to meet and sustain existing training requirements, much less additional ones, while at the same time maintaining the current operational tempo, without sufficient resources to have an appropriately sized "training float." One organization that the Panel met with, describing their significant close protection capability, stated "their operational model required their personnel to spend a third of their time deployed on missions, a third in training and a third in administrative, pre-deployment activities and time off from high threat, high stress missions." Given DS' global and domestic responsibilities, this precise delineation of time may not be feasible. However, there is no doubt that the absence of a "training float" negatively impacts DS' abilities to allocate resources to meet its responsibilities.

[redacted]

The Panel strongly endorses the Department's current effort to identify and resource a consolidated, modern, and fully integrated Foreign Affairs Security Training Center, whose facilities are within the mid-Atlantic region and are controlled directly by the Department of State to meet its unique training needs. The challenges of conducting diplomacy in high-threat areas and around the world, combined with the requirement to maintain effective and viable training for DS personnel and Foreign Service Officers, cannot be sustained within the current facility framework. Similarly, the continued practice of begging hat-in-hand for use of other's facilities places Department training programs at the mercy of other agencies' training priorities. This will be especially critical as the Department implements its new High Threat and expanded Foreign Affairs Counter Threat (FACT) training programs. The establishment of such an integrated state-of-the-art facility is a best practice adopted long ago by the Federal Bureau of Investigation (FBI), United States Secret Service (USSS), and the Drug Enforcement Administration (DEA). Given that the Department relies heavily on the U.S. military (particularly the U.S. Marine Corps), other government agencies and private sector enterprises, it is imperative that the new training facility be located within close proximity to the metropolitan Washington, DC area to capitalize on the interagency synergies necessary to ensure closer collaboration, collective responsibility, joint exercises and innovative approaches.

Furthermore, Training (DS/T) should expand its current interaction with its counterparts at the Central Intelligence Agency's (CIA) Office of Security to regularly exchange and benchmark best practices to establish facilities and operate in high threat areas. Training should also expand interaction with Department of Defense (DOD) components, including the Marine Corps, but particularly in the Special Operations and emergency response fields, with whom DS can have profitable interchanges on training doctrine, how DOD elements would actually support an embassy in crisis, joint training as appropriate, and practical exercises to test and validate the results.

RECOMMENDATION

17. The Department should initiate a comprehensive DS and Human Resources (HR) review to determine the requirements for establishing an accurate DS "training float" essential to meeting operational and language training requirement, overseas staffing consistency and other mission essential objectives.
18. The Department should provide DS with the inter-agency support and resources for continued and expanded exchanges and benchmarking between DS Training and appropriate DOD, Intelligence Community (IC), and other USG agency components with a focus on training doctrine, crisis support, and joint training and exercises.
19. The Department should support DS and FSI in the development and provision of advanced situational training, similar to DOD and other USG agencies, for all Foreign Service

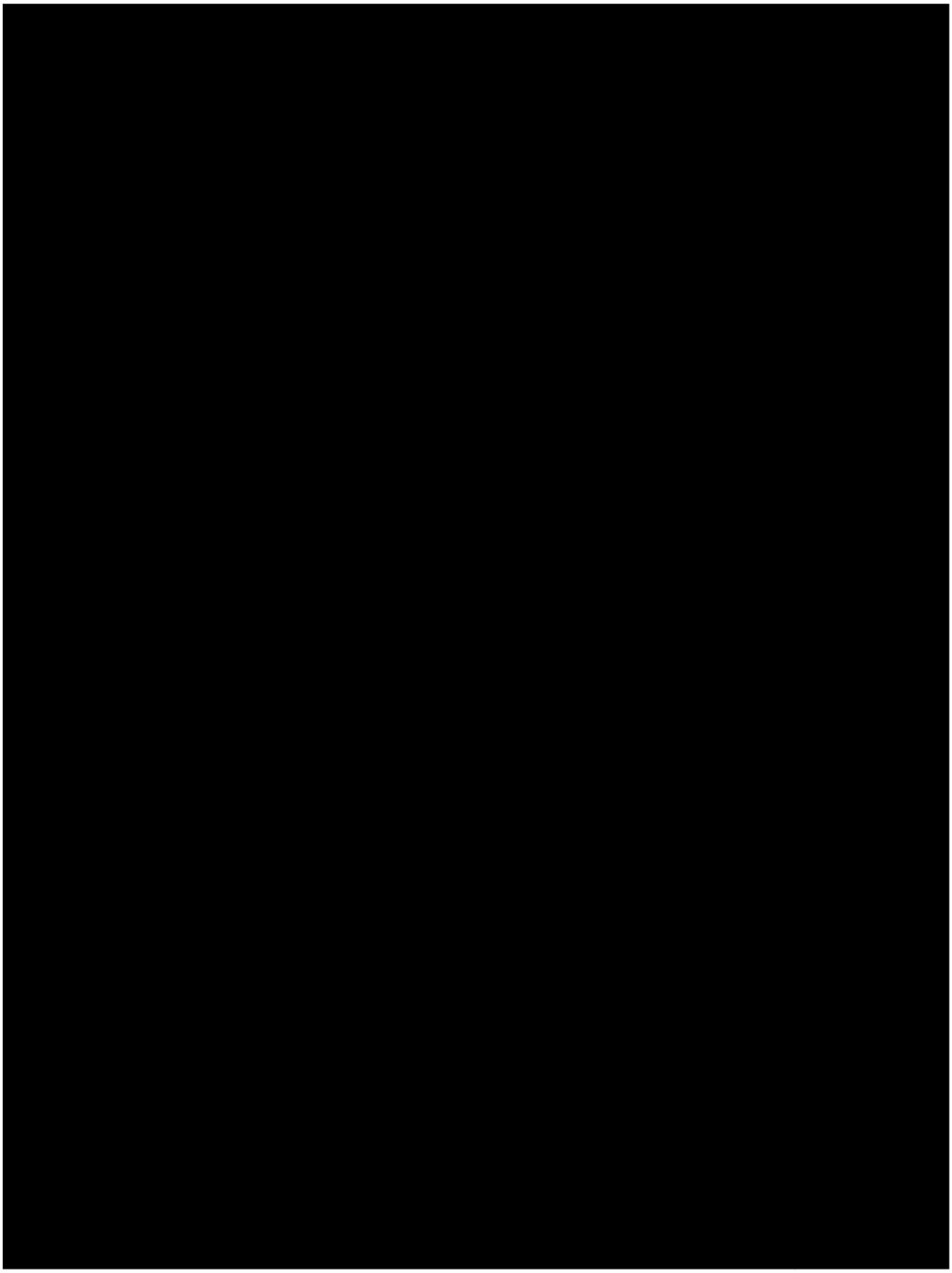
generalist and specialist employees in their initial training classes to enhance their personal safety.

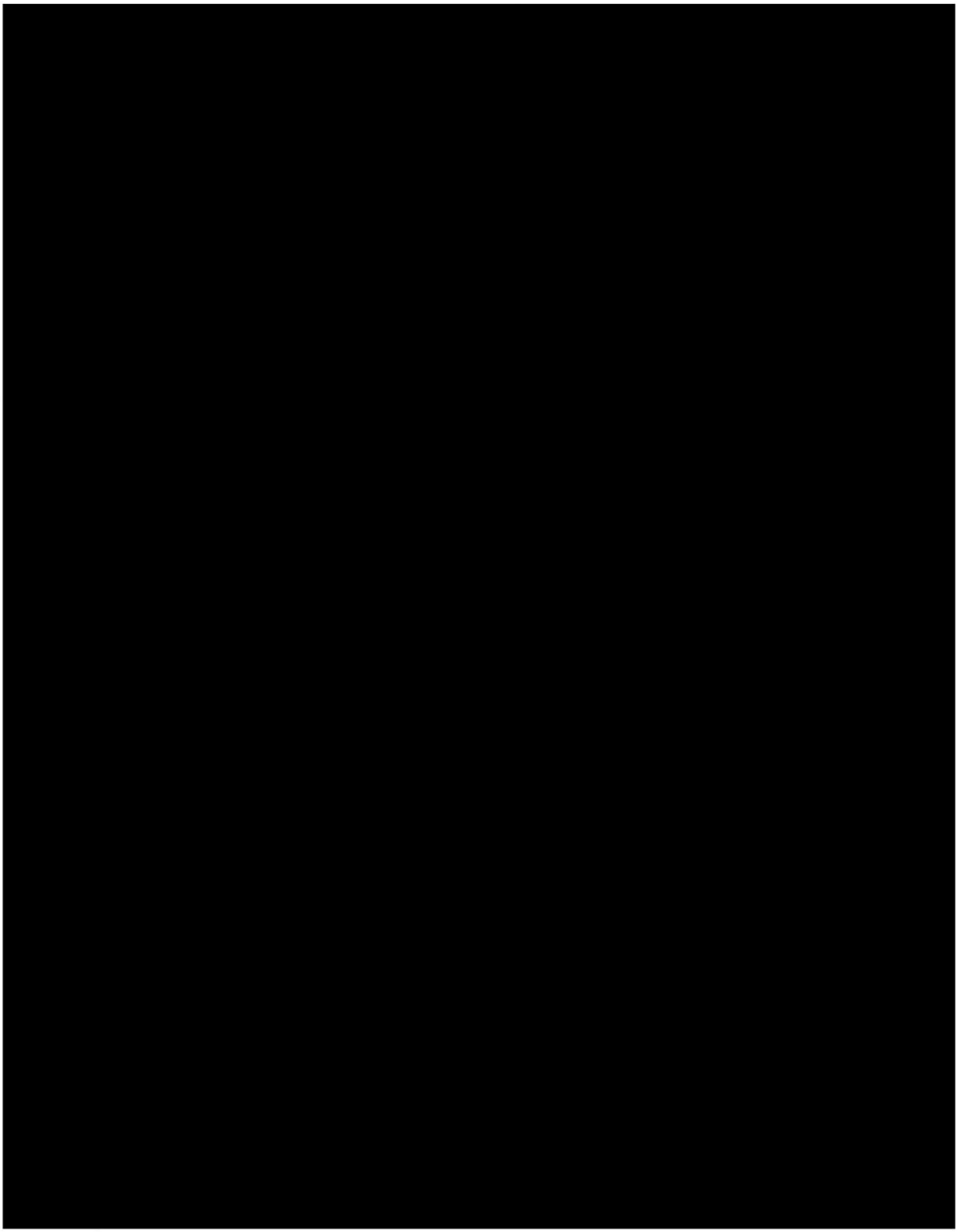
20. The Department should, as a priority, establish a dedicated DS Foreign Affairs Security Training Center within a reasonable distance to the Washington, DC metropolitan area to cost-effectively train agents, Foreign Service personnel, members of the National Foreign Affairs community, and collaborate with training and exercise partners, and implement programs for foreign government security and law enforcement officers.
21. The Department and DS should expand and enhance integrated operational and tactical training with the Marine Corps Embassy Security Group (MCESG) at all levels. This DS/MCESG integrated training should take advantage of the advanced facilities at Quantico and include expanded advanced tactical training between the new rapid deployable MCESG teams and DS MSD.

INTELLIGENCE, THREAT ANALYSIS, AND SECURITY ASSESSMENTS

[redacted]

[23] Booz-Allen & Hamilton, Security and Intelligence Management Study, Oct 1999.





RECOMMENDATION

[redacted]

PROGRAMS, RESOURCES, AND TECHNOLOGY

The Department of State maintains roughly 285 diplomatic facilities worldwide. Attacks on such facilities and U.S. diplomatic personnel are not uncommon and are very likely to continue. History is replete with instances of hostile attacks directed against U.S. personnel, facilities, and interests overseas. Terrorists have proven to be determined over time and readily adapt to the environment to advance their causes. [redacted]

Given terrorists' resilience and resourcefulness, it is essential that the Department and DS harness emerging technology and rapidly deploy it to the field to better protect U.S. facilities, diplomats, and interests. DS has evolved throughout its history by introducing cutting-edge technology, to include hardened buildings, armored vehicle enhancements, and other explosive and attack countermeasures, but this technology is not as consistently and rapidly deployed to posts as mission needs and evolving threats require. Equally important, DS has adapted its policy and application of resources and tactics to better protect U.S. missions and personnel. [redacted]

The Bureau of Diplomatic Security has continuously adapted to meet the challenges presented by hostile adversaries around the world. Following the simultaneous embassy bombings in Dar es Salaam and Nairobi, DS, through the Secure Embassy Construction and Counterterrorism Act (SECCA),[24] researched and developed essential standards for the secure construction of U.S. facilities, which incorporated the latest technologies for blast mitigation, as well as appropriate setback. The SECCA and OSPB measures have been highly successful in protecting our facilities and personnel, and will continue to do so well into the future. Even so, terrorists continue to attack our facilities and have utilized new tactics to attempt to defeat our vehicle barriers, fortified walls, and guard programs. [redacted]

The OBO and DS' Office of Physical Security Programs (PSP) should remain the lead in developing designs and incorporating the latest physical and technical security features to safeguard hardened structures. The Countermeasure's Directorate should also maintain its leading role involving armor programs and certain electronic countermeasures. Overseas Protective Operations (OPO) should maintain the lead on protective services and guard programs. However, the Panel found an urgent need, similar to other USG military and law enforcement agencies, for a new office within DS to manage a "field expedient deployment" program to expeditiously test, evaluate, develop training protocols, and deploy the latest operational tools used to protect U.S. facilities, personnel, and interests.

Based on the Panel's research, this new office should come under the purview of the Assistant Director for Training who also serves as the Chairman of the Special Protective Equipment

[24] 22 USC, Section 4865, Secure Embassy Construction and Counterterrorism Act of 1999

Review Board (SPERB), which makes policy recommendations to the Director. Furthermore, MSD, which reports to the Assistant Director for Training, maintains robust and excellent contacts within DOD and other federal agencies that have extensive Testing and Evaluation (T&E) apparatuses to support their operational and equipment needs. This allows MSD to receive continuous and current information regarding the deployment of emerging technology and/or equipment to support the most advanced operational teams within the USG.

Discussions with members of the Countermeasure's Directorate indicated that they undertake extensive testing and evaluation of equipment before it can be deployed to the field. Although this is comforting in ensuring the efficacy of design standards and equipment, it does not take full advantage of other T&E apparatuses and can lead to extensive evaluation and deployment times. Thus, the Panel recommends the adoption of a best practice of numerous federal agencies which utilize an agile deployment system that permits equipment to be sent to the field while applicable policies and training programs are developed.

As outlined above, the SPERB could be the springboard mechanism for such an initiative in DS with DS/T developing the training protocols and MSD testing the equipment in the training environment before expedient field deployment. Having the policy recommendation entity, testing, evaluation, training, and operational component in one directorate will inevitably ensure that weapons and other vital equipment can be deployed both safely and expeditiously. Moreover, they can leverage their contacts in the special operations community to provide their research and T&E results regarding a particular piece of equipment. Given the high costs associated with T&E and the time required for independent but redundant testing, it may be prudent to rely to the extent possible, on DOD and other agencies research, testing, and evaluation results.

The private sector is often in the forefront with regard to emerging technology, such as mobile communications, which when properly leveraged, can be used as a tool that provides Global Positioning System (GPS) locating, secure communications (through software encryption), and an extensive knowledge resource. [redacted] Nevertheless, their heavy reliance on

commercial means can be a detriment to this goal. Other emergency response teams, like the FBI's Hostage Rescue Team (HRT), and even the Department's Foreign Emergency Support Team (FEST), have the ability through contract or military air assets to expeditiously get to a post needing their services. [redacted]

The Panel recognizes the necessity for situationally based approaches to ambassador/principal officer protection around the world provided directly by DS or a variety of host nation law enforcement and security services. The Panel also must underscore the importance of the consistent application of established procedures, tactics, and deployment and utilization of appropriate protective and response equipment determined by the lead protective organization and the threat environment. DS-managed ambassador/principal officer protective details must be properly resourced with appropriately experienced personnel and evaluated by DS at the headquarters level as part of the RSO program review process.

RECOMMENDATION

29. The Department should establish under the DS Assistant Director for Training/SPERB, a new office for field expedient deployment of hardware, cutting-edge protective technology and procedures.
30. The Department should provide DS the resources to expeditiously review, accept, purchase and deploy non-lethal technology, including millimeter wave devices and acoustic hailing and sonic generation technology.
31. The Department should provide DS with the necessary inter-agency agreements and contract resources for airlift capability for DS' emergency response team from the Office of Mobile Security Deployments, similar to the best practice used by the FBI's HRT and the Department's own FEST.
32. The Department should provide DS information technology support and resources to acquire emerging mobile computing/communication technology platforms. Appropriate cyber security protections must be considered during the acquisition, deployment, and use of this technology.
33. DS should update and ensure adherence to standard operating procedures for ambassador/principal officer protective security operations around the world, and regularly assess the effectiveness of these protective details.

HOST NATIONS AND GUARD FORCES CAPABILITY ENHANCEMENT

[redacted] The critical role played by Host Nation Security Forces (HSNF) and an effective local guard program have been proven repeatedly, but Benghazi has demonstrated yet again the vulnerability of U.S. facilities in countries where there is a willingness to protect U.S. interests, but very little capability to do so. DS recently utilized a computer modeling program to rank high threat posts. When weighted and factored into the process, two important criteria in protecting U.S. facilities were the will and security capabilities of the host nation.

Each year the Department spends extensive resources building new embassy compounds to meet security standards, as well as upgrading existing buildings with physical security features. These hardened facilities, as important as they are in mitigating terrorist threats, can only serve to deter hostile entities from penetrating the compound and the buildings housing U.S. personnel. [redacted] Providing HNSF and guard forces with a vested interest and improved facilities have demonstrated to foster goodwill amongst these first responders and ensures that they are better rested, refreshed, and remain in the area for contingency purposes. This makes them more likely to respond with a concerted and determined focus when an exigency arises. Over time this has proven to be the case and for very little investment can greatly assist in safeguarding U.S. personnel and facilities, particularly important in the hostile environments the USG places its personnel. Equally important is expanded use of contracting officer's authority to award local guard contracts using best value trade-offs when appropriate so that the contract award can be made to other than the lowest priced offeror or highest technical rated offeror. The use of tradeoffs will allow for considerations such as relative importance between cost or price and other significant factors such as past performance, management expertise, technical approach, quality, and delivery method.

For example, Karachi boasts a New Consulate Compound, yet it was nearly overrun late last year when a 60,000-strong crowd attempted to breach the outer wall to the compound. Due to a dedicated HNSF response, to include substantial reinforcements, our personnel in Karachi were not seriously harmed. Fortunately, Consulate Karachi officials had the foresight to work with relevant Post and Department officials to obtain funding to upgrade HNSF living quarters, which adjoins the outer wall of the facility.

Equally important is ensuring that the HNSF responds effectively and capably. In many undeveloped countries, police lack the equipment, resources, and training to mount a skillful response. The Department's Antiterrorism Assistance program (ATA) has been instrumental in building an effective CT capability and in some countries has established a very robust CT partner. Since its inception in 1983, ATA, through DS, has trained roughly 95,000 security and

law enforcement personnel from 154 nations. Nevertheless, policy and legislative restrictions limit the direct impact of the ATA program to developing overall host nation capability and explicitly precludes the use of money, effort and resources to those HSNF that directly support and protect U.S. personnel, facilities, and interests overseas.

The Panel has identified a critical section in the Foreign Assistance Act of 1961, which permits up to $1,000,000 to be spent directly to train those HNSF assigned to protect U.S. missions and personnel. If this legislation can be amended to increase the amount, to include a new funding stream directed to DS Training, then an agile mechanism will allow DS/T to utilize elements from both ATA and MSD to train and then exercise HSNF with local guard elements and other U.S. mission assets in a bilateral exercise to the benefit of the USG, host nation, and specifically the affected post. As much as possible, training would be performed in-country or regionally (if facilities are available), and in the U.S. as appropriate. Ideally, this unit would be located adjacent to or within a few minutes response time of the primary USG compound in-country. This focused training would initially be directed at the identified high threat posts to ensure that the most threatened missions receive the necessary support both quickly and strategically. As this is a focused policy to the benefit of a mission and not a country, the ultimate mechanism and funding stream should be separate from the CT bureaus funding of the ATA program.

RECOMMENDATION

34. The Department should seek an amendment to the Foreign Assistance Act of 1961 which would provide budgeting authorization and associated program management authority directly for DS to enable it and its embassy RSOs to provide training and equipment support to, and exercise on a regular basis with, those foreign security services that are assigned to protect the diplomatic community in compliance with the Vienna Convention on Diplomatic Relations, but are lacking in adequate knowledge, skills and/or equipment.
35. The Department should allocate funding for building basic infrastructure for host nation security and local guard forces assigned, deployed, or contracted to protect U.S. facilities, where those entities do not have the resources to provide facilities, particularly in the high-threat or other posts where such support is crucial for the safety and security of Department personnel and facilities.
36. The Department should increase its legislative effort to gain and expand DS' authority for "Best Value" contracting, the tradeoff between the lowest priced and the highest technically rated contractor, for local guard programs at high risk and other posts where necessary. The Department should further provide DS the resources to develop and implement local guard program initiatives to "invest in loyalty", a best practice utilized by other USG agencies, focused on enhanced guard pay, benefits, stipends, training (regionally or in the U.S.), uniforms, equipment, and personnel development programs.

REGULAR REEVALUATION

With the completion of this report, the current Best Practices Panel will dissolve. The ARB intended that this not be a one-time effort, but a continuing and regular support function to DS and the Department. However, regular evaluations and input will not support DS if identified best practices are not followed and adapted to the Department's and DS' mission requirements. The Panel discovered that many key issues that it focused on in this report as best practices were included in recommendations made 14 years ago in a report commissioned by the Department.[25] This report was largely ignored by the Department and did not receive wide circulation within either the Department or DS at the time, based on the Panel's discussion with DS and Department personnel.

The report focused on three categories of key opportunities for improvement: organizational structure; risk management; and, intelligence dissemination. A number of specific recommendations were made in this report, but the most important were never adopted or instituted by the Department. The report also included a best practice survey of other U.S. government agencies and the private sector. In the 27 years since DS' creation, the Department has received a significant amount of best practice input from 18 ARBs and a number of independent panels, such as the current one. Through any number of long existing and effective bilateral interagency and allied foreign government exchanges, the OSPB, and the role model for private-public partnerships - the Overseas Security Advisory Board (OSAC), the Department and DS have had a better opportunity than most USG agencies to harvest best practices from a wide variety of SMEs. The failure has not been in the Department's ability to obtain SME guidance and best practice input, but rather in the lack of a corporate approach to adapting and implementing those best practices to the Department's mission requirements and operating environments. In the Panel's judgment and supported by our interaction with the appropriate elements of foreign governments, other USG agencies and the private sector, DS Agents and DS as an organization were frequently identified as the "go to" SMEs for protecting personnel, facilities and operations not just on high-threat posts, but around the world and at home.

The Panel observes that the challenge for the Department and DS has not been in obtaining regular best practice and SME input, but in incorporating that knowledge into operations and management capabilities.

RECOMMENDATION

37. The Department should institutionalize the ISAT process to conduct regular annual reevaluations of all HTP and other post as required.

[25] In 1999, as a result of the ARBs conducted following the 1998 embassy bombings, the Department of State contracted Booz-Allen and Hamilton with the objective of examining the Board's recommendations on security and intelligence management.

38. The Department should appoint a multi-disciplinary Advisory Board of outside SMEs to institutionalize regular and independent input on security management and best practices for protecting personnel, facilities, and global operations, with a focus on high threat posts.
39. Members of this Advisory Board should be nominated by the Under Secretary for Diplomatic Security and appointed by the Secretary for three year terms, with one third of its members rotating off annually. This Board should be administratively supported by permanent staff and should provide direct input to the Under Secretary for Diplomatic Security.

CHANGE MANAGEMENT - LEADERSHIP, COMMUNICATION AND TRAINING

The best practices recommended by the Panel are realistic, achievable and measurable. Their implementation does not require the expenditure of significant additional resources; however, their implementation will require a significant cultural shift within the Department. An integrated change management strategy is therefore required to institutionalize these recommendations – they should not be farmed off piecemeal in a check list fashion similar to the ARB responses, but should be addressed in a Department-wide and comprehensive manner.

Key to this process is the vision and leadership of the Secretary as he executes his security-related responsibilities delineated in the Diplomatic Security Act. The Secretary must be directly engaged in supporting the change management process, emphasizing that it is necessary for the security of all civilian U.S. personnel on official duty abroad and their dependents. In this regard the Secretary plays a visible role by: defining his strategic vision, which should be simple and easily understood; inspiring the change; selecting the right team to manage the change process; and, communicating directly with Department personnel.

The experience of other similar organizations managing change is that successful change requires consultation and involvement by management at every level in the organization. In developing the policy to implement the Panel's recommendations, managers must consult with and avail themselves of the extensive experience of their staff members. This consultation, conducted within the parameters of the Secretary's strategic vision, should be inclusive and lead to the development of specific policies and procedures to implement the key recommendations of the Panel's report.

Change is not necessarily a welcomed process; therefore, a Department-wide communications strategy must be devised and implemented to inform Department employees and gain their support for the change. Basic to such a strategy is early and frequent communication from Department leadership concerning the purpose for the change and the status of its implementation. The communications strategy should take full advantage of all means of communication, such as e-mails and bulletins; however, town hall meetings with senior leaders and other such personal leadership techniques may be the most effective.

Once the policies and procedures have been agreed by the Department, and if the change is to become institutionalized and lasting, it must be accompanied by an agreed and comprehensive training strategy. It is envisioned that as a minimum such a strategy would include the immediate training of personnel at headquarters and in the field, as well as further continuing training to be conducted at the appropriate level by FSI and DS/T. The ramifications of the Panel's key recommendations are such that they cannot be included in work requirement statements without the incumbent having received the training necessary to implement the requirement, thus both an immediate training requirement and a long-term training requirement are necessary.

As noted earlier in this report, personnel serving today under the authority of Chief of Mission, clearly understand the roles of the ambassador and RSO in providing for the safety and security of all personnel at post. The change management process recommended by the Panel provides the Department with a path forward to ensure that the same clarity exists throughout the Department.

RECOMMENDATION

40. Using this section as a blueprint, the Secretary should establish a comprehensive change management strategy throughout the Department that is led by the Deputy Secretary for Management and Resources.

CONCLUSION

The bombing of the American Embassy in Beirut, Lebanon in April 1983 and subsequent bombing of the U.S. Marine barracks in October 1983 led to the Inman Report, which in turn led to the Inman security standards for building U.S. Embassies and facilities overseas. The Inman Report gave birth to the U.S. Diplomatic Security Act of 1986 which created the Bureau of Diplomatic Security and the Diplomatic Security Service. [redacted]

Although the Panel was informed of the "new normal" and "expeditionary diplomacy" which require the execution of foreign policy in high threat areas despite the risk involved, the Department has no institutional mechanism that will allow it to operate in such environments. It is unlikely that temporary facilities, in areas such as Benghazi, will ever meet Inman standards. The Department therefore identifies missions with special terminology to avoid its own high, but unattainable, standards and then approves waivers to circumvent those standards, thus exposing those serving under Chief of Mission authority to an unacceptable level of risk.

The present environment requires a new paradigm in which an Under Secretary for Diplomatic Security leads a 21st century security organization providing the Department the expert advice, guidance and support to manage risk by defined processes in order to achieve foreign policy goals while enhancing the security of all serving overseas under Chief of Mission authority. Key

to this approach is the establishment of a framework for accountability and a model for risk management, institutionalized through continuous training and supported by a robust lessons learned process. The Department's Foreign Service Officers and DS agents, many of whom have served in high threat locations, have the experience, knowledge and expertise required to adapt and implement the best practices proposed in the present report. It is the view of the Panel that the Department has been presented with a unique opportunity and moment in time to ensure that the sacrifice made in Benghazi will result in positive change.

FINAL NOTE

This report is dedicated to those Department of State employees who have given their lives in the service of our country.

To the men and women of DS with whom we met, we hope that we have kept our pledge to recommend best practices that will address many of the challenges that you face as you provide a safe and secure environment for the conduct of U.S. foreign policy.

We also wish to take this opportunity to thank the Department, particularly overseas posts that hosted our visits and the Bureau of Diplomatic Security, for the outstanding support provided to the Panel during this most important endeavor.

APPENDIX A: PANEL MEMBERS

PANEL MEMBERS

Mark Sullivan (Chairman)

Todd Keil

Richard Manlove

Raymond Mislock, Jr.

Timothy Murphy

STAFF

Erika Lichliter

Stephanie Murdock

MARK SULLIVAN - CHAIRMAN

Mark Sullivan was a Federal Agent for almost 35 years with 29.5 years as a Secret Service Agent. From May 2006 – February 2013 he was the Agency's 22nd Director.

Prior to being appointed Director, he held several leadership positions including Deputy Director and Assistant Director for Protective Operations. As Assistant Director for Protective Operations he was responsible for the protection of the President, Vice President, their families, former Presidents and their spouses, other national leaders, and Visiting Heads of State. He was also responsible for the planning and implementation of security for National Special Security Events.

Upon retirement, he became a partner at Global Security and Intelligence Strategies, Washington, DC, specializing in threat assessments, risk management, cyber security and investigations.

TODD KEIL

Todd M. Keil has more than 29 years of experience in global security operations and management, intelligence and law enforcement, and threat assessment and risk mitigation in the government and the private sector. He is currently a Senior Advisor at TorchStone Page, LLC, providing world-leading individuals and organizations with end-to-end risk avoidance solutions.

Mr. Keil was appointed in December 2009 by President Barack Obama as the Assistant Secretary for Infrastructure Protection at the U.S. Department of Homeland Security. His office was responsible for protecting the assets of the United States essential to the nation's security, public health and safety, economic vitality, and way of life. These assets are divided into 18 separate sectors as diverse as critical manufacturing, banking and finance, commercial facilities and information technology. Mr. Keil served in this position until February 2012. Prior to his appointment, Mr. Keil worked in corporate security management positions at Texas Instruments, Inc., and the Welsh-Sullivan Group, LLC.

Mr. Keil also held numerous key positions at the U.S. Department of State's Diplomatic Security Service over 22 years of service, culminating his career as the Regional Director for Western Hemisphere Affairs, where he championed protection of U.S. government facilities, personnel, and national security information. In Foreign Service positions at U.S. embassies in Indonesia, Ireland, and Austria, he provided a broad range of security and law enforcement management and risk mitigation expertise advising U.S. ambassadors, and in primary liaison roles with a wide network of global law enforcement, intelligence, and security agencies. From 1994 to 2000, he held a leadership position on the protective detail that provided personal protection for two Secretaries of State.

RICHARD MANLOVE

Richard Manlove served with the United Nations from 1993 to 2008 in a variety of positions. From 2007 to 2008 he was the Principal Security Advisor for United Nations Operations in Iraq. Prior to that assignment he served from 1994 to 2007 in a number of senior management positions within the Department of Safety and Security (previously the Office of the United Nations Security Coordinator), where he specialized in peacekeeping operations, field assessments, and policy development. He served from 1993 to 1994 as the Chief Security Officer for the United Nations Observer Mission in Liberia.

Since his retirement from the United Nations in 2008, Mr. Manlove has been appointed to a number of United Nations' Boards of Inquiry considering attacks on United Nations personnel. From 2010 to 2011 he returned to the Department of Safety and Security to advise on the transition from MNF-I – provided security to Iraqi security in support of United Nations operations.

Earlier, Mr. Manlove served for 26 years in the U.S. Army in a variety of Infantry and political-military command and staff assignments to include four years on the Army General Staff.

RAYMOND MISLOCK, JR.

Raymond Mislock, Jr. is a Director in Pamir Consulting LLC, with recognized expertise in corporate security management, global risk management, trade secret protection and economic espionage investigations in the corporate sector, having served as the Chief Security Officer for DuPont from 1999 to October 2011. Immediately prior to joining DuPont, Mr. Mislock served for two years as the Security Director for the Central Intelligence Agency, responsible for managing Agency information, personnel, technical and physical security operations worldwide.

Prior to his Agency service, Mr. Mislock completed a 25-year career with the Federal Bureau of Investigation as the Special Agent in Charge of the FBI's National Security Division of the Washington Field Office where he directly managed counterintelligence, counterespionage and counterterrorism investigations. His Bureau career included a three-year special assignment to the U.S. Department of State as the Director of Counterintelligence in the Bureau of Diplomatic

Security and one year at the National Security Council, Office of Intelligence Policy, as the Director of Counterintelligence Programs.

He served as DuPont's representative to and former Co-Chair of the U. S. Department of State's Overseas Security Advisory Council and is a former member of the Leadership Board of the FBI's Domestic Security Alliance Council. Mr. Mislock is a Life Member, former Board member and past President of the International Security Management Association. He entered active duty in the U.S. Navy in 1968 and served as the Officer in Charge of a Swift Boat in Vietnam from May 1969 to February 1970.

TIMOTHY MURPHY

Timothy P. Murphy is a Vice-President at MacAndrews and Forbes, a private, diversified holding company. Prior to joining MacAndrews and Forbes, Mr. Murphy was the Deputy Director of the Federal Bureau of Investigation. Mr. Murphy spent 23 years in the FBI and prior to his FBI career served as a police officer. He held a number of operational positions in the FBI in a variety of field offices nationwide, investigating matters as diverse as counterterrorism, organized crime, and drugs, and he also served as an FBI pilot. He served in various management roles, to include serving as a special assistant to the FBI Director—a position that gave him a unique, high-altitude view of the global FBI from both operational and administrative perspectives. He served as the Special Agent in Charge of the Cincinnati field office, as the Bureau's chief financial officer, and then the Associate Deputy Director before becoming the Deputy Director in 2010.

In his last two FBI positions, Mr. Murphy oversaw the operational and administration aspects of a workforce that was more than 35,000 strong, spread throughout 56 national offices and more than 60 international offices. This included all operational aspects of the Counterterrorism, Counterintelligence, Criminal, Cyber and Intelligence programs, as well as human resources, training, strategy management, facilities management, records management, security, financial management, information technology, inspection and internal audit, and leadership development.

Mr. Murphy maintains close ties to the law enforcement and intelligence communities, and is frequently consulted for his expertise in global criminal and security issues. He is member of the Police Executive Research Forum, the International Association of Chiefs of Police, the Overseas Security Advisory Council (he is also a member of the New York OSAC Executive Committee), the Domestic Security Advisory Council, the FBI Agents Association, the FBI National Academy Associates, and the International Security Management Association.

ERIKA LICHLITER

Erika Lichliter works for the Department of State as a Procurement Analyst in the Executive Directorate for the Office of Management Services, Contracts and Procurement of the Bureau of Diplomatic Security (DS/EX/MGT/CAP). Ms. Lichliter provides advice and guidance to DS Program Offices on all phases of acquisition planning, pre and post award procurement procedures, and assists in the development of DS procurement policies and procedures.

STEPHANIE MURDOCK

Stephanie Murdock works for the Bureau of Diplomatic Security as a Procurement Analyst in the Office of Management Services Resource Unit. Ms. Murdock is responsible for analyzing, maintaining and reviewing budgets and procurement orders for the Executive Office of Diplomatic Security. Stephanie Murdock began working for the Bureau in 2010 as an Administrative Assistant within the Office of Management Services, Logistical Support Division. Prior to her employment with the Bureau she spent 6 years in the private sector as an Office Manager working in budgets, procurement and management.

APPENDIX B: LIST OF CONTACTS

DEPARTMENT OF STATE AND OTHER U.S. GOVERNMENT

[redacted]

UNITED NATIONS

[redacted]

NYPD

[redacted]

PRIVATE SECTOR

[redacted]

ROME

[redacted]

VIENNA

[redacted]

GENEVA

[redacted]

[redacted]

NAIROBI

[redacted]

JUBA

[redacted]

CAIRO

[redacted]

BEIRUT

[redacted]

SANAA

[redacted]

AFOSI

[redacted]

LONDON

[redacted]

[redacted]

IMF

[redacted]

TEL AVIV

[redacted]

APPENDIX C: REFERENCE DOCUMENTS

1 FAM

2 FAM 420

2 FAM 423.4

2 FAM 423.9

12 FAM 400

Action Memo for Acting Assistant Secretary Starr – DS, From DS/T – Mark Hipp, Subject: High Threat Training Strategy Implementation, May, 2013

Action Memo for Under Secretary Kennedy – M, From: NEA-Jeffery Feltman, Subject: Future of Operations in Benghazi, Libya - Dated 12/27/11 **(Sensitive But Unclassified – SBU)**

Advanced Security in the Field, United Nations Training CD

Air Force Office of Special Investigations Mission Brief

Argonne National Laboratory Resilience Publications – Selected Resources – June 2013

AS/NZA ISO 31000:2009 – Risk Management – Principles and Guidelines

ASIS Chief Security Officer Guideline 2008

ASIS Chief Security Officer (CSO) Organizational Standard, ASIS CSO.1-2008, American National Standard

ISMA/OSAC Benchmarking Survey Report

Basic Security in the Field, Staff Safety, Health, and Welfare, United Nations Training CD

Benghazi Accountability Review Board Implementation, Fact Sheet, Office of the Spokesperson, U.S. Department of State, May 20, 2013

Benghazi Accountability Review Board Report, Unclassified

Benghazi Accountability Review Board Report, **Classified Secret/NOFORN**

Booze Allen – Security and Intelligence Management Study – October 1999

Bureau of Diplomatic Security – Bureau Priorities and Strategy FY 2013 – FY 2015

Bureau of Diplomatic Security – Organization Structure, Authorities and Responsibilities

Construction Vulnerability and Protective Measures Indices for the Enhanced Critical Infrastructure Protection Program – Argonne National Laboratory – US Department of Energy

Comprehensive Timeline of Events – Benghazi, Last Edit 201221126

Diplomatic Security Service Office of Training & Performance Standards (TSP), April 26, 2013

Diplomatic Security Service, Office of Mobile Security Deployments Briefing, (undated)

Director's Note by DSS Director Greg Starr, The New High-Threat Directorate, dated May 15, 2013

DS Deliberate Planning History (Undated)

DS Deliberate Planning Process – OPORD – Operations Order (Undated)

DS Deliberate Planning Process Office of Operational Planning and Innovation (OPI) (Undated)

DS/HTP Proposed DOS Deliberate Planning Process, Planning and Support Cell (PSC). 1/15/2013

Foreign Assistance Act of 1961

FY 2014 Bureau Resource Request, Bureau of Diplomatic Security

Handbook for United Nations Designated Officials for Security, United Nations Department of Safety and Security 2012

Information Memo For Under Secretary Kennedy – M, From DS – Gregory B Starr, Acting, Subject: Accountability Review Board Recommendations concerning High Threat Training for DS Agents (Recommendation 17, Taskers 31-31), dated April 9, 2013

Information Memo For Under Secretary Kennedy – M, From M/PRI – Alaina B. Teplitz, Subject: Status: ARB Action No. 10 – Develop concept for "support cells"

Intermediate Risk Analysis for Fusion Center Analysts – Course Modules – National Protection and Programs Directorate – Office of Infrastructure Protection – Department of Homeland Security

Introduction to Risk Analysis for Fusion Center Analysts – State of Brighton Exercise Materials - National Protection and Programs Directorate – Office of Infrastructure Protection – Department of Homeland Security

Leveraging an Established Relationship, The Diplomatic Security Special Agent Afloat Program, by LtCol David Monroe, USMCR, Marine Corps Gazette, August 2012

Memorandum of Agreement Between the U.S. Department of State and the United States Marine Corps – Change Date: May 5, 2011

NSP – Quarterly Security Report – January – March 2013

Office of Operational Planning and Innovation (DS/DSS/OPI) – Department of State – Bureau of Diplomatic Security – Draft – February 14, 2012

Office of Security, Global Response Staff, PAC 2013, Central Intelligence Agency

Omnibus Diplomatic Security and Antiterrorism Act of 1986

OSI Fact Book – Global Reliance Special Edition 2013

President's Letter of Instruction to Chiefs of Mission

Profile, Summer 2013, Publication of Countermeasures Directorate, Bureau of Diplomatic Security, U.S. Department of State

Report to Congress on Actions Taken By the Department of State in Response to the Program Recommendations of the Accountability Review Board on the Death of Four Official Americans in Benghazi, Libya, September 11, 2012, Published January 2013

Report of the Accountability Review Boards, Bombings of the U.S. Embassies in Nairobi, Kenya and Dar es Salaam, Tanzania on August 7, 1998, U.S. Department of State Electronic Archive

Report on Diplomatic Security Organization and Management, May 2013

Risk Analysis Guidebook – National Protection and Programs Directorate – Office of Infrastructure Protection – 2013 – Department of Homeland Security

Risk Steering Committee – DHS Risk Lexicon – 2010 Edition

Secure Embassy Construction and Counterterrorism Act of 1999

Securing U.S. Diplomatic Facilities and Personnel Abroad: Background and Policy Issues – CRS Report for Congress, May 7, 2013

Security and Business Continuity Accountability Framework – A Guide to Roles and Responsibilities for IMF Personnel – Third Edition

Staff Bulletin - Planning and Approval Procedures for Missions to Fund-Designated High Risk Locations, IMF, December 20, 2012

Strategic Plan, FY 2010-2013, Diplomatic Security International Programs, Deputy Assistant Secretary Charlene Lamb, May 2010

Significant Attacks Against U.S. Diplomatic Facilities and Personnel, 1998-2012, U.S. Department of State, Bureau of Diplomatic Security

Summary of Principal Recommendations, The Inman Report, Report of the Secretary of State's Advisory Panel on Overseas Security (undated)

United Nations Security Management System, Security Policy Manual, Chapter II, Section B, Framework of Accountability for the United Nations Security Management System, February 4, 2011

United Nations Security Management System, Security Policy Manual, Chapter II, Section C, Terms of Reference for the Executive Group on Security, May 5, 2009

United Nations Security Management System, Security Policy Manual, Chapter IV, Security Management, Section N, Policy For United Nations Minimum Operating Security Standards (MOSS), April 20, 2009

United Nations Security Management System, Security Policy Manual, Chapter V, Compliance With Security Policies and Procedures, Section G, Boards of Inquiry, November 8, 2012

U.S. Department of State, Bureau of Diplomatic Security, Office of Security Technology, Special Projects 2013 **(Sensitive But Unclassified – SBU)**

U. S. Department of State Cable, May 17, 2013, Subject: Visit of Benghazi ARB-Recommended Best Practices Panel **(Sensitive But Unclassified – SBU)**

U.S. Department of State Cable, December 9, 2012, Subject: Security Environment Threat List (SETL) – 2012-2013 **(SECRET/NOFORN)**

APPENDIX D: ACRONYM LIST

AFOSI	Air Force Office of Special Investigations
ARB	Accountability Review Board
ARSO	Assistant Regional Security Officer
ATA	Antiterrorism Assistance Program
CIA	Central Intelligence Agency
CT	Counterterrorism
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOD	Department of Defense
DoS	Department of State
DS	Diplomatic Security
DS/C	Countermeasures Directorate
DS/T	Training
EAC	Emergency Action Committee
EFP	Explosively Formed Penetrators
FACT	Foreign Affairs Counter Threat
FAM	Foreign Affairs Manual
FBI	Federal Bureau of Investigation
FCO	Foreign and Commonwealth Officer
FEST	Foreign Emergency Support Team
FS	Foreign Service
FSI	Foreign Service Institute
FY	Fiscal Year
GPS	Global Positioning System
HNSF	Host Nation Security Forces
HTP	High Threat Posts Directorate
HR	Human Resources
HRT	Hostage Rescue Team

IC	Intelligence Community
IG	Inspector General
INR	Bureau of Intelligence and Research
IP	International Programs
ISAT	Interagency Security Assessment Teams
ISMA	International Security Management Association
ITA	Intelligence and Threat Analysis
LES	Locally Engaged Staff
M	Management
MCESG	Marine Corps Embassy Security Group
MOSS	Minimum Operating Security Standards
M/PRI	Management Policy, Rightsizing and Innovation
MRAP	Mine Resistant Ambush Protected
MSD	Mobile Security Deployment
NCTC	National Counterterrorism Center
NGA	National Geospatial Agency
NGO	Non-Governmental Organization
NSA	National Security Agency
NYPD	New York Police Department
OBO	Overseas Building Operations
OPO	Overseas Protective Operations
OSAC	Overseas Security Advisory Council
OSPB	Overseas Security Policy Board
PSP	Office of Physical Security Programs
RSO	Regional Security Officer
SECCA	Secure Embassy Construction and Counterterrorism Act
SME	Subject Matter Expert
SPERB	Special Protective Equipment Review Board

T&E	Testing and Evaluation
TDY	Temporary Duty
TIA	Threat Investigations and Analysis Directorate
UN	United Nations
UNDSS	United Nations Department of Safety and Security
U.S.	United States
USG	United States Government
USSS	United States Secret Service
VP	Vice President

APPENDIX E: LIST OF RECOMMENDATIONS

ORGANIZATION AND MANAGEMENT

1. The Department should, as a matter of urgency, establish an Under Secretary for Diplomatic Security.

ACCOUNTABILITY

2. The Department should develop an accountability framework documenting institutional and individual accountability and responsibility for security throughout the Department.
3. Accountability and responsibility for security should be included in work requirement statements for all Foreign Service (generalist and specialist) employees.
4. The Department should develop an integrated and seamless training program and communications strategy to ensure Department wide understanding and effective implementation of the accountability framework.

RISK MANAGEMENT

5. The Department should develop and implement a Department-wide risk management model and policy.
6. The Department should consult with Argonne National Laboratory, Infrastructure Assurance Center as well as the United Nations Department of Safety and Security (UNDSS), to inform the ongoing effort of the Office of Management Policy, Rightsizing and Innovation (M/PRI) and DS to develop a risk management model.
7. The Department should develop an integrated and seamless training program and communications strategy to ensure Department-wide understanding and effective implementation of the risk management model and policy.

PROGRAM CRITICALITY AND ACCEPTABLE RISK

8. The Department should develop within its risk management model a mechanism to balance program criticality and unmitigated, or residual, risk and identify accountable decision-makers responsible for accepting risk at each level within the organization.
9. The Department should develop an integrated and seamless training program and communications strategy to ensure Department wide understanding and effective implementation of the program criticality decision making process.
10. The Department should consult with Argonne National Labs, Infrastructure Assurance Center, and UNDSS subject matter experts (SMEs) to develop within its risk management model and policy a mechanism to balance program criticality and residual risk.

PLANNING AND LOGISTICS

11. The Department should establish a planning cell, led by a senior planner within the office of the Under Secretary for Political Affairs, to: advise the Undersecretary with regard to strategic planning; support the regional bureaus; establish terms of reference and standards

for bureau planning cell officers; ensure the standardization of planning within the regional bureaus; and, include lessons learned in the planning policy.

12. The Bureau of Diplomatic Security should establish one planning office within DS that is accountable and responsible for DS-centric planning that informs DS decision-making and program execution. This office would also be the DS focal point for the larger Department planning process as identified above and be located in the office of the Under Secretary for Diplomatic Security.
13. Waivers to established security standards should only be provided subsequent to the implementation of mitigating measures as agreed by regional bureau or other program managers, advised by DS, and as informed by the Department risk management model.
14. A Department-wide information and training roll-out program should be initiated for 2 FAM 420.

LESSONS LEARNED

15. The Department should establish a formalized lessons learned process and accompanying FAM policy to ensure a timely debriefing of all personnel who have participated in critical operational events to collect and preserve the knowledge gained from these personnel so that it may be then incorporated into training, management, and policy processes throughout the Department.
16. The Bureau of Diplomatic Security should establish a formalized lessons learned process and ensure that it is integrated into the recommended Department-wide process. The lessons learned process should involve coordination with appropriate DS entities to obtain and incorporate the knowledge and experience of DS personnel.

TRAINING AND HUMAN RESOURCES

17. The Department should initiate a comprehensive DS and Human Resources (HR) review to determine the requirements for establishing an accurate DS "training float" essential to meeting operational and language training requirement, overseas staffing consistency and other mission essential objectives.
18. The Department should provide DS with the inter-agency support and resources for continued and expanded exchanges and benchmarking between DS Training and appropriate DOD, Intelligence Community (IC), and other USG agency components with a focus on training doctrine, crisis support, and joint training and exercises.
19. The Department should support DS and FSI in the development and provision of advanced situational training, similar to DOD and other USG agencies, for all Foreign Service generalist and specialist employees in their initial training classes to enhance their personal safety.
20. The Department should, as a priority, establish a dedicated DS Foreign Affairs Security Training Center within a reasonable distance to the Washington, DC metropolitan area to cost-effectively train agents, Foreign Service personnel, members of the National Foreign

Affairs community, and collaborate with training and exercise partners, and implement programs for foreign government security and law enforcement officers.

21. The Department and DS should expand and enhance integrated operational and tactical training with the Marine Corps Embassy Security Group (MCESG) at all levels. This DS/MCESG integrated training should take advantage of the advanced facilities at Quantico and include expanded advanced tactical training between the new rapid deployable MCESG teams and DS MSD.

INTELLIGENCE, THREAT ANALYSIS, AND SECURITY ASSESSMENTS

[redacted]

PROGRAMS, RESOURCES, AND TECHNOLOGY

29. The Department should establish under the DS Assistant Director for Training/SPERB, a new office for field expedient deployment of hardware, cutting-edge protective technology and procedures.
30. The Department should provide DS the resources to expeditiously review, accept, purchase and deploy non-lethal technology, including millimeter wave devices and acoustic hailing and sonic generation technology.
31. The Department should provide DS with the necessary inter-agency agreements and contract resources for airlift capability for DS' emergency response team from the Office of Mobile Security Deployments, similar to the best practice used by the FBI's HRT and the Department's own FEST.
32. The Department should provide DS information technology support and resources to acquire emerging mobile computing/communication technology platforms. Appropriate cyber security protections must be considered during the acquisition, deployment, and use of this technology.
33. DS should update and ensure adherence to standard operating procedures for ambassador/principal officer protective security operations around the world, and regularly assess the effectiveness of these protective details.

HOST NATIONS AND GUARD FORCES CAPABILITY ENHANCEMENT

34. The Department should seek an amendment to the Foreign Assistance Act of 1961 which would provide budgeting authorization and associated program management authority directly for DS to enable it and its embassy RSOs to provide training and equipment support to, and exercise on a regular basis with, those foreign security services that are assigned to protect the diplomatic community in compliance with the Vienna Convention on Diplomatic Relations, but are lacking in adequate knowledge, skills and/or equipment.
35. The Department should allocate funding for building basic infrastructure for host nation security and local guard forces assigned, deployed, or contracted to protect U.S. facilities, where those entities do not have the resources to provide facilities, particularly in the high-threat or other posts where such support is crucial for the safety and security of Department personnel and facilities.
36. The Department should increase its legislative effort to gain and expand DS' authority for "Best Value" contracting, the tradeoff between the lowest priced and the highest technically rated contractor, for local guard programs at high risk and other posts where necessary. The Department should further provide DS the resources to develop and implement local guard program initiatives to "invest in loyalty", a best practice utilized by other USG agencies, focused on enhanced guard pay, benefits, stipends, training (regionally or in the U.S.), uniforms, equipment, and personnel development programs.

REGULAR REEVALUATION

37. The Department should institutionalize the ISAT process to conduct regular annual reevaluations of all HTP and other post as required.
38. The Department should appoint a multi-disciplinary Advisory Board of outside SMEs to institutionalize regular and independent input on security management and best practices for protecting personnel, facilities, and global operations, with a focus on high threat posts.
39. Members of this Advisory Board should be nominated by the Under Secretary for Diplomatic Security and appointed by the Secretary for three year terms, with one third of its members rotating off annually. This Board should be administratively supported by permanent staff and should provide direct input to the Under Secretary for Diplomatic Security.

CHANGE MANAGEMENT - LEADERSHIP, COMMUNICATION AND TRAINING

40. Using this section as a blueprint, the Secretary should establish a comprehensive change management strategy throughout the Department that is led by the Deputy Secretary for Management and Resources.