

CHANGING
THE **RISK**
PARADIGM
FOR U.S. DIPLOMATS



Una Chapman Cox
FOUNDATION

JANUARY 2021

CONTENTS

4

Project
Participants
Advisory
Group

5

Executive
Summary

9

The Problem

13

The Need for
Congressional
Assistance

15

Remedies

19

Appendix A:
Draft text for
amended 22
U.S.C. Chapter
58, Subchapter III
Section 4831

25

Appendix B:
Project
Supporters

28

Appendix C:
Table of
Abbreviations

PROJECT PARTICIPANTS

Project Director

The Honorable Gregory Starr

American Academy of Diplomacy Support Team

Ambassador Ronald E. Neumann, President

Maria Reissaus, Program Director

Destiny Clements, Program Associate

Una Chapman Cox Foundation Support Team

Ambassador Lino Gutierrez, Executive Director

Nicole Brzozowski, Program Manager

Advisory Group

Dr. Graeme Bannerman

Ambassador Thomas Miller

The Honorable Eric Boswell

Ambassador Ronald Neumann

Ambassador Ryan Crocker

Ambassador Richard Olson

Ambassador James Cunningham

Ambassador Anne Patterson

Ambassador Gerald Feierstein

Ambassador Charles Ray

Ambassador Jeffrey Feltman

The Honorable Gregory Starr

Ambassador Robert Ford

Ambassador Francis X. Taylor

Ambassador Lino Gutierrez

Dr. Michael Van Dusen

Ambassador Hugo Llorens

Ambassador Jacob Walles

Ambassador Deborah McCarthy

EXECUTIVE SUMMARY

The State Department's current risk aversion at higher-threat posts obstructs the performance of the most basic functions of a diplomat abroad — to influence host governments, explain, defend, and advance U.S. policies and objectives, and to correctly analyze political, social, and economic developments as well as the effectiveness of U.S. government programs. Each of these functions demands first-hand contacts and observations. Working only by telephone or an occasional meeting inside secure walls is not a substitute for developing the continuing contacts necessary with local officials and populations. In short, the formulation and execution of national security policy is hindered by the lack of access to foreign contacts at higher-threat missions.

U.S. diplomatic and USAID development officers are rarely allowed to travel to meet sources, colleagues, or counterparts in less than fully secured areas or make unscheduled moves. Our U.S. military partners and members of the intelligence community are not encumbered by similar restrictions. Requests by Foreign Service Officers to discreetly meet with subjects and sources or to review remote programs are too often denied, and the ability to observe and report on a country they are expected to know with a high level of expertise is severely limited.

Effective diplomacy to meet national interests requires a method to engage more broadly even in high-threat locations. We believe it is possible; but progress requires change in three simultaneous areas.



1. The language and structure of the Accountability Review Board (ARB) requirement in the Omnibus Diplomatic Security Act of 1986 must change.

The law is widely interpreted within the Foreign Service as creating an overriding requirement to find someone at fault when a security incident involves serious injury or loss of life. A broad selection of former ambassadors and assistant secretaries have reported that ambassadors, deputies, and regional security officers believe decisions to allow travel outside the mission that result in death or serious injury would be judged in terms of their accountability with the presumption that someone erred in their judgment. Too frequently, the decision is to avoid risk by denying travel or requiring an unattainable level of security. Technological advances, such as videoconferencing or teleconferencing can supplement traditional meetings; however, they are not a substitute for face-to-face meetings that build personal relations and trust with foreign contacts, without which real understanding of sensitive issues is not possible. This is particularly true when sensitivities concern internal foreign political concerns.

The U.S. military, intelligence agencies, FBI and Drug Enforcement Agency each have different requirements for managing accountability and risk. The Academy does not equate the levels of acceptable risk for Foreign Service Officers abroad to the levels of risks acceptable for U.S. military assets engaged in combat operations. However, Foreign Service Officers are frequently assigned to high-threat diplomatic missions abroad. Currently, embassies are hampered by an out-of-date accountability process that essentially is at odds with the current requirement to take reasonable risks in the performance of duty.

The Academy recommends a reformulation of the law to put in place a system similar to that of other national security agencies. The new system would utilize an internal review process to evaluate precautions taken against known risks and then evaluate the decision and identify any lessons learned in a report to the Secretary of State. The Secretary would, in turn, inform Congress of the results. The review would focus on whether reasonable actions were taken based on known risks at the time. This would bring the process more in line with that used by the Department of Defense (DoD) and the intelligence community (IC). Equally importantly, it would be a tangible message to the officers of the U.S. Foreign Service that Congress understands and supports the need to take reasonable risks in the performance of diplomatic and foreign aid operations abroad. It would signal that Congress wants to assist in developing a culture where the security of our personnel remains important, but the priority must be implementing the foreign affairs and national security policies and operations of the United States.



2. The Department of State must identify best practices and new techniques for operating in high-threat locations.

Certain cadres of officers, to include political officers, economic officers, consular officers, United States Agency for International Development (USAID) field and project officers, would receive required training in advanced operational techniques and procedures to allow them to operate as safely as possible while accepting levels of increased risk. This will take a joint effort by the Foreign Service Institute, the Diplomatic Security Hard Skills Training Center (FASTC), and other agencies to determine best practices. Additionally, management-level officers at various levels will require additional training in managing threats and risk.



3. Culture: To fully benefit from the legal changes and improved tactics and procedures, the foreign affairs agencies will have to take steps to change a culture of risk aversion that has developed over the years.

Senior and mid-level officers, serving domestically and overseas, will require improved education in identifying and managing threats and risks while balancing the need to fulfill foreign affairs-related goals and objectives. Decision makers responsible for approving operations abroad that entail higher risk — typically deputy chiefs of mission and regional security officers — must have more than just new tools and training. They must also have confidence that the foreign affairs institutions and Congress understand that the highest priority is fulfilling major national security priorities, not solely keeping people safe. Careful judgment of the importance of individual policy objectives balanced against risk and threat mitigation measures will always be necessary and never clear cut. All aspects of the problem — importance of the goals, risk, and mitigation — must be considered when judgments are made and things go wrong.



THE PROBLEM

In late 2019 and early 2020, a small group of senior retired U.S. ambassadors, all members of the American Academy of Diplomacy (AAD), engaged several members of Congress and their staff in discussions on the growing level of risk intolerance experienced in U.S. missions abroad with the consequence that American diplomats and aid practitioners could not effectively fulfill their mandates. Subsequent to these initial discussions, the Una Chapman Cox Foundation agreed to fund an AAD project to examine the issue of changing the risk paradigm for U.S. foreign affairs agencies. AAD formed an advisory committee of senior Foreign Service (retired) officers to guide the effort.

STATE DEPARTMENT
PHOTO

U.S. Secretary of
State Michael R.
Pompeo departs
Erbil, Iraq on
January 9, 2019.

By May 2020, the advisory group had agreed upon a project narrative that effectively described the problem.

“The risk mitigation paradigm currently employed for State Department personnel and those of other civilian U.S. government agencies at higher-threat posts is obstructing the performance of the most basic functions of a diplomat abroad — to influence host governments and other foreign interlocutors, to explain, defend, and advance U.S. policies and objectives, and to gain the information and access needed to analyze political, social, economic, and programmatic developments based on first-hand contacts and observations in a foreign country. Diplomacy is an incremental business in which numerous contacts and observations contribute over time to generate larger results. Diplomats are analysts, policy influencers, persuaders, and negotiators. Executing their mission only by telephone or an occasional meeting inside secure walls is not a substitute for developing the continuing contacts necessary with local officials and populations. In short, the formulation and execution of national security policy is hindered by the lack of access to foreign contacts at higher-threat missions. While acknowledging there are increased threats and dangers for staff operating in high-threat countries, the security versus risk equation for travel outside our missions is too heavily weighted toward eliminating risk to our personnel, often preventing them from successfully fulfilling their mission.

With the aid of Congress, the Department has made great progress in replacing old, insecure, and highly vulnerable facilities abroad with safe and secure embassies and consulates. The risk of losing an entire diplomatic platform and suffering massive loss of life and heavy injuries has been greatly reduced. Congress has generously funded additional security assets such as security officers, armored vehicles, and bodyguards to enhance mobility and travel outside our secure platforms. The Department has a remarkable record of conducting literally millions of moves outside the secure perimeter at our highest-threat posts with few losses, albeit using helicopters or heavily armed and armored convoys. Despite these successes, at high-threat posts Foreign Service and USAID officers are rarely allowed to travel to meet sources, colleagues, or counterparts in less than fully secured areas, nor allowed to move to unscheduled locations or travel outside of secured perimeters. The ability to meet discreetly with subjects and sources or review remote programs is very limited, as is the ability to observe and report on a country they are supposed to know with a high level of expertise. This is not the case with our U.S. military partners or members of our intelligence community.”



The AAD advisory group agreed that a major factor keeping diplomats cloistered is the language and structure of the Accountability Review Board (ARB) requirement in the Omnibus Diplomatic Security Act of 1986. The law is widely interpreted within the Foreign Service as possessing an overriding requirement to find someone at fault if there is a security incident involving serious injury or loss of life, i.e. the first determination after identifying whether injury or loss of life is a security issue is whether the security systems and security procedures for that mission were adequate and who was accountable. Based on their previous experience as ambassadors and assistant secretaries in the Department of State, the advisory group members found that Chiefs of Mission (COM), Deputy Chiefs of Mission (DCM), and Regional Security Officers (RSO) believe decisions made to allow travel outside the mission in high-threat environments that result in death or serious injury would be judged in terms of their accountability with the presumption that someone erred in their judgment. Too frequently the decision by COMs, DCMs, and RSOs is to avoid risk by denying a travel request because the deciding officials feel compelled to demonstrate the purpose of the travel outweighs the risk of injury, something that is difficult to do when the request is to travel outside the perimeter for normal diplomatic and

STATE DEPARTMENT
PHOTO

Deputy Secretary of State Antony “Tony” Blinken speaks with residents during his tour of the Baharka Camp for Internally Displaced Persons in Erbil, Iraq, on Nov. 23, 2015

programmatic activities as opposed to high-priority visits to secured compounds using heavily protected convoys.

As the second major factor, the AAD advisory group strongly believes the foreign affairs agencies will have to take steps to change a culture of risk aversion that has taken hold within our organizations. This will require both education and hard skills training. Senior and mid-level officers, serving domestically and in overseas positions, will require improved education in how to identify and manage threats and risks while balancing the need to fulfill foreign affairs-related goals and objectives. These decision makers require new decision tools and confidence in the foreign affairs institutions and Congress that the highest priority is fulfilling national security priorities.

These two major themes were considered essential by the AAD advisory group, but it was thought prudent to widen the group of experts viewing the problem and possible solutions beyond the initial advisory group. The project narrative was circulated among additional Department of State retirees, senior retirees from USAID, and former U.S. military generals with experience in high-threat theaters working closely with U.S. diplomatic missions. Without hesitation, those contacted signed on in support of the project based on their first-hand observations about the growing level of risk intolerance exhibited by colleagues in the field and their own experiences. Appendix B includes a list of approximately 50 senior U.S. government officials who support this initiative. Additionally, three organizations — The American Foreign Service Association (AFSA), the American College of National Security Leaders (ACNSL), and the USAID Alumni Association's Board of Directors — endorse the call to expand the risk paradigm and amend the ARB process.

THE NEED FOR CONGRESSIONAL ASSISTANCE



PHOTO BY ARCHITECT OF THE CAPITOL

The Department of State and USAID cannot alter the trajectory of growing risk intolerance at high-threat U.S. diplomatic missions abroad by solely implementing internal changes. Congressional assistance will be required.

AAD recommends that the ARB language, first promulgated as part of the Omnibus Diplomatic Security Act of 1986¹, now stated in law as Section 22 of USC 4831-4835², be amended. Originally written when Congress had little confidence that the Department of State was taking security threats and the need for security countermeasures seriously, the law prescribes a very specific and singular investigative method that must be utilized in any case

¹ Public Law 99-399, Aug. 27, 1986, the Omnibus Diplomatic Security and Antiterrorism Act of 1986, 22 USC 4801, Title III – Performance and Accountability, Section 301 – Accountability Review, Section 302 – Accountability Review Board, Section 303 – Procedures, Section 304 – Findings and recommendations by a Board, Section 305 – Relation to other proceedings

² United States Code Title 22 – Foreign Relations and Intercourse; Chapter 58 – Diplomatic Security; Subchapter III – Performance and Accountability, Sections 4831-4835 (22 U.S.C.4831-4835, as amended, 2013)

of serious injury, loss of life, or significant destruction of property at or related to a U.S. government mission abroad, if deemed a security incident. The ARB process, while necessary at the time and useful for several decades thereafter, is now proving to have consequences that are counterproductive to the activities of the Foreign Service.

As enacted, the references require one single specific investigative and evaluation process, an ARB, for any security incident that results in loss of life, serious injury, or significant destruction, with an implicit expectation that an error in judgment allowed for the security incident and, therefore, someone must be held accountable. This conclusion is evident from the name of the process, “the Accountability Review Board,” and the judgments of a wide group of senior officers about the influence of the ARB process on accountability and personnel recommendations. The effect over many years of implementation has been to encourage a reluctance to take acceptable levels of risk in approving field operations for Foreign Service Officers abroad. No other department or agency of the federal government operating abroad has specific language in law that requires such a specific and singular investigative response. The two other legs of the U.S. Foreign Affairs triad — the Department of Defense (DoD) and the intelligence community (IC) — follow internally developed investigative procedures when serious incidents occur that take into account the need to accept levels of risk to their personnel in order to achieve success for necessary operations.

AAD and the supporters of this recommendation do not equate the levels of acceptable risk for Foreign Service Officers abroad to the levels of risks acceptable for U.S. military assets engaged in combat operations. However, U.S. Foreign Service Officers are frequently assigned to high-threat diplomatic missions abroad, often in conflict zones, with the full support and understanding of the executive branch and Congress. While there are frequent examples of Foreign Service Officers accompanying military combat personnel performing civilian-political missions, the much larger issue is the need for individual Foreign Service Officers to have greater movement and access to individuals and organizations in various places in high-threat countries. Yet should there be a Foreign Service casualty, the Department of State is mandated to activate an extensive and out-of-date accountability process that has put senior Department of State officials authorizing such actions at odds with the need to take reasonable risks in the performance of duty.

Congress itself recognized the incongruous nature of the law when the U.S. Foreign Service was called to staff embassies and consulates in Afghanistan and Iraq. Understanding that U.S. diplomats had a crucial role to play in these two war zones, Congress passed amendments to the ARB legislation for limited exemptions from the requirement for an ARB, stating that the process need not be used when serious security incidents — serious injury, loss of life, or significant destruction of property — took place at these two diplomatic missions during specific periods.



PHOTO COURTESY OF AMBASSADOR ANNE PATTERSON

REMEDIES

Foreign Service officer talks with an Afghan leader in the Paktika province of Afghanistan.

The Academy believes Congress should amend the language from Title III of Public Law 99-399, the Diplomatic Security and Antiterrorism Act of 1986, now 22 USC 4831-4835, to direct the Secretary of State to develop and use internal investigative procedures into the facts surrounding serious security incidents; convene a high-level internal panel to evaluate the investigation and the incident; and then provide a report of the incident to the Secretary. The Secretary in turn would provide a report of the incident to appropriate congressional committees. This would streamline the serious incident investigation process to a model more in line with that used by DoD and IC. More importantly, it would be a clear message to the officers of the U.S. Foreign Service that Congress understands and supports the need to take reasonable risks in the performance of diplomatic and foreign aid operations abroad. Replacing the ARB language and process, both in name and substance, with methods more typically found in the U.S. government will help reverse a trend toward risk intolerance by

signaling that Congress wants to assist in developing a culture where the security of our personnel remains important, but the priority must be implementing the foreign affairs and national security policies and operations of the United States.

Further, the Department of State, in consultation with others, must identify best practices and new techniques on how to operate in high-threat locations. Certain cadres of officers, to include political and economic officers, consular officers, USAID field and project officers, should receive mandatory training in advanced operational techniques that would allow them to better fulfill their missions at high-threat posts. Advanced training, enhanced operational procedures, and appropriate technical and communications equipment would allow them to operate as safely as possible while accepting levels of increased risk. This will take a joint effort by the Foreign Service Institute, the Diplomatic Security Hard Skills Training Center (FASTC), and other agencies to determine best practices.

Senior Department officials and mid-level Foreign Service Officers in management positions will require additional training in managing threats and risk — identifying risks and weighing those risks against the imperative to conduct diplomacy and foreign aid programs in volatile and sometimes dangerous countries. The continuing conduct of diplomatic and foreign aid programs must be given a higher priority and emphasis relative to the general threat levels,

to better balance the risk versus reward paradigm that currently skews toward avoiding risk.

To replace the current ARB process, AAD and the supporters of this project suggest that a leaner internal process as outlined below should be the basis for moving forward. The advisory group recommends the law be amended to instruct the Department of State to institute an internal process specific to the Foreign Service, but with similarities to the processes used by DoD and IC when reviewing serious incidents. The internal process should include timely reporting requirements; an inquiry and investigative phase; and a separate analysis and review process with a report to the Secretary, with a subsequent report to the chairmen of the four foreign affairs committees of Congress. An internal Department of State process to investigate and review serious security incidents should include:



A. An initial requirement for an immediate report of the incident, followed within three days by a more detailed report of the incident from the mission involved.



B. An investigation of the incident by Diplomatic Security (DS) using personnel trained in incident investigation as well as security operation abroad, but which must also include agents from the internal affairs/professional responsibility unit. DS would produce a

report of the incident/report of inquiry/ investigation within 60 days. The report must provide an account of what occurred; evidence of who perpetrated the attack, if known or suspected; and whether applicable security procedures were followed. In the event that the security incident was an attack on a U.S. Diplomatic Compound, motorcade, residence, or other facility, the report would determine if adequate security countermeasures were in effect. If the attack was on an individual or group of officers conducting an approved operation outside the mission, the report would determine and report if a proper process was followed in evaluating the requested operation and weighing the risk of the operation. The report would not seek to assign accountability for the incident unless there was an observation that an official breached their duty. At the discretion of the Secretary, additional personnel can be assigned to the incident investigation team.



C. A Serious Security Incident Permanent Coordinating Committee (SSI/PCC) would be convened and chaired by the head of the Office of Management, Strategy and Solutions, (M/SS). The SSI/PCC would be specifically charged with reviewing serious security incidents resulting in deaths, serious injury, or significant destruction of property. Submission of the DS Report of Investigation along with all reporting from the diplomatic

posts with any/all relevant additional evidence and information (CCTV recordings, movement logs, interviews) would be made available for review and full consideration. The voting committee members would include:

- The representative of the Under Secretary of Management, the head of M/SS
- The Assistant Secretary responsible for the region where the incident occurred
- The Assistant Secretary of Diplomatic Security
- The Assistant Secretary for the Bureau of Intelligence and Research
- The Assistant Secretary for Consular Affairs
- An Assistant Secretary Representative from a United States government (USG) agency if that agency was involved

Other attendees (non-voting) at the SSI/PCC providing advice, additional information, or counsel, would include:

- The Department of State legal advisor or deputy legal advisor
- A representative of the Director of National Intelligence (DNI), if appropriate

The SSI/PCC would receive all relevant information on the incident, including all reporting from post or other sources, the DS report, any pertinent intelligence information, and receive a briefing from the DS unit conducting the inquiry. The PCC would determine:

- If the account of the incident is fully described
- If security systems and procedures pertinent to the incident were in place and functioning
- If there is evidence that anyone did not fulfill their duties, and if there is a need for anyone to be referred to the Director General for malfeasance or breach of duty
- Whether there are relevant lessons or outcomes that should be relayed to other U.S. diplomatic missions and/or units within the Department of State
- If there are follow-up measures the Department or other agency involved should take



D. The SSI/PCC findings would be reported by M/SS, along with a copy of the DS incident investigation, in a report to the Secretary. At the discretion of the Secretary,

the report would be provided to the Deputy Secretary of State, the Under Secretary for Political Affairs, the Under Secretary for Management, and the Deputy Secretary or equivalent of any agency who had an employee or was otherwise substantially involved in the incident.

Nothing in this process would preclude the Secretary of State from convening a follow-up public board of inquiry comprised of notable persons to investigate any security incident if it was of such magnitude or significance that an internal process was deemed insufficient to understand and investigate the incident. All the materials gathered in the normal internal process would be provided to any Board of Inquiry the Secretary convenes.



The Department of State, within 90 days of the completion of the report to the Secretary of State, would provide a report of the incident to the chairmen of

the relevant congressional foreign affairs committees.

The Department of State Inspector General should not be a part of the incident investigation for security incidents but would fulfill their mandated role through inspections or reviews to ensure the Department follows the proper procedures for addressing serious security incidents.

Nothing in this report or suggested legislation should in any way alter the responsibility of the Department of Justice to investigate and take appropriate action regarding any such incident.

The American Academy of Diplomacy, the Una Chapman Cox Foundation, and our supporters, in Appendix A, have provided a proposed amended text for Section 22 U.S.C. 4831-4835, for consideration by relevant congressional personnel and committees.



APPENDIX A

Draft Text for amended

22 U.S.C. Chapter 58, Subchapter III - PERFORMANCE AND ACCOUNTABILITY

Section 4831 INVESTIGATION OF SERIOUS SECURITY INCIDENTS (formerly *Accountability Review Boards*)

(a) In general

- (1) Convening the Serious Security Incident Investigation and Permanent Coordinating Committee process;

In any case of any serious security incident involving loss of life, serious injury, or significant destruction of property at, or related to, a United States Government (USG) diplomatic mission abroad, and in any case of a serious breach of security involving intelligence activities of a foreign government directed at a USG mission abroad, a Security Incident Inquiry (SII) into the event shall be convened by the Department of State and a report produced for the Secretary providing a full account of what occurred; whether security provisions pertinent to the incident were in place and functioning; whether any malfeasance or breach of duty took place that materially contributed to the outcome of the incident; and relevant security improvements or follow-up measures that might be recommended. A Security Incident Inquiry need not be convened where the Secretary determines that a case clearly involves only causes unrelated to security.

- (2) Department of Defense facilities and personnel;

The Secretary of State is not required to convene a Security Incident Inquiry in the case of an incident described in paragraph (1) that involves any facility, installation, or personnel from the Department of Defense with respect to which the Secretary has delegated operational control of the overseas security functions to the Secretary of Defense pursuant to Section 4805 of this title. In any such case, the Secretary of Defense shall conduct an appropriate inquiry. The Secretary of Defense shall report the findings and recommendations of such inquiry, and the action taken with respect to such recommendations, to the Secretary of State and Congress.

- (b) Deadlines for convening a Serious Security Incident Investigation and Permanent Coordinating Committee process:

- (1) In general

The Secretary of State shall convene the Serious Security Incident investigation and then the subsequent Permanent Coordinating Committee process (SSI/PCC) not later than 60 days after the occurrence of an incident

described in subsection (a)(1) of this section, except that such 60-day period may be extended for one additional 60-day period if the Secretary determines that the additional period is necessary;

(2) Delay in cases involving intelligence activities

With respect to breaches of security involving intelligence activities, the Secretary of State may delay the establishment of a SSI/PCC if, after consultation with the chairman of the Select Committee on Intelligence of the Senate and the chairman of the Permanent Select Committee on Intelligence of the House of Representatives, the Secretary determines that the establishment of a SSI/PCC would compromise intelligence sources or methods. The Secretary shall promptly advise the chairman of such committees of each determination pursuant to this paragraph to delay the establishment of a SSI/PCC.

(c) Notification to Congress

Whenever the Secretary of State convenes an investigation and SSI/PCC in response to a serious security incident, the Secretary shall promptly inform the chairman of the Committee on Foreign Relations of the Senate and the Chairman of the Foreign Affairs Committee of the House.

Section 4832. Security Incident Investigation and Permanent Coordinating Committee

(a) The Serious Security Incident inquiry process will consist of two distinct elements: a security inquiry investigative phase, and a review panel phase conducted by high-level Department of State officials.

(1) The security investigation process will utilize Diplomatic Security resources and any other investigative personnel deemed necessary. A Report of Investigation will be prepared at the conclusion of the investigation which will describe what, when, and where the security incident occurred; who was involved; an accurate account of the casualties, injured, and damage done; and a review of security procedures in place at the time of the attack.

(2) The Serious Security Incident Permanent Coordinating Committee (SSI/PCC) will meet to review the report, all other reporting relevant to the incident, and evidence available (such as video recordings). The SSI/PCC will, upon completion of their review, provide a report to the Secretary of State on the incident, outcomes, and any possible recommendations. The SSI/PCC will be primarily composed of Assistant Secretary-level personnel in the Department, and at a minimum include:

- (A) The representative of the Under Secretary to Management and chair of the SSI/PCC, the head of the Office of Management, Strategy and Solutions (M/SS);
- (B) The Assistant Secretary responsible for the region where the incident occurred;
- (C) The Assistant Secretary to Diplomatic Security;
- (D) The Assistant Secretary for the Bureau of Intelligence and Research;
- (E) The Assistant Secretary for Consular Affairs;
- (F) An Assistant Secretary-level representative from any involved USG agency;
- (G) Other personnel may be added as deemed necessary or appropriate.

Section 4833. Investigation and Inquiry Procedures

- (a) Regarding requirements for an internal investigation, analysis, and reporting system for Serious Security Incidents as outlined in Section 4831:
 - (1) The Department of State shall develop an internal investigative protocol to ensure the proper investigation of security incidents described in Section 4831, which shall be referred to as the Serious Security Incident Investigation process, and shall be promulgated in relevant foreign affairs manuals.

- (2) The Serious Security Incident inquiry process typically commences upon reporting of the incident from the diplomatic mission where the event transpired, followed by detailed reporting within three days that provides additional details and information.
- (3) The Diplomatic Security Service shall assemble an investigative team to establish what occurred; report on evidence of who perpetrated the attack, if known or suspected; and whether applicable security procedures were followed. In the event the security incident was an attack on a US Diplomatic Compound, motorcade, residence, or other facility, the report shall determine if adequate security countermeasures were in effect. If the attack was on an individual or group of officers, employees, or family members conducting operations or movements outside the mission, the investigation must determine whether proper security briefings and procedures were in place and whether adequate consideration of threat and weighing of risk of the operation or movement took place.
- (4) If during the investigation, evidence comes to light that an employee did not fulfill their duties and this breach contributed in a material fashion to the incident, the investigative team shall include these observations or reports in the Report of Investigation.

- (5) Confidentiality: During the investigative process, the Department shall adopt such procedures with respect to confidentiality as deemed necessary, including procedures relating to the conduct of closed proceedings or the submission and use of evidence in camera, to ensure in particular the protection of classified information relating to national defense, foreign policy, or intelligence matters. The DNI shall establish the level of protection required for intelligence information and for information relating to intelligence personnel contained in the report. Members of the SSI/PCC will respect these measures, though the level of the classification of the final report to the Secretary will be determined by the SSI/PCC, taking into account the material therein.

Section 4834. Findings and Recommendations by the SSI Permanent Coordinating Committee

(a) Findings

The DS Report of Investigation, all evidence and reporting, and any other relevant information shall be provided to the Serious Security Incident Permanent Coordinating Committee (SSI/PCC). The SSI/PCC shall examine the facts and circumstances surrounding the serious injury, loss of life, or significant destruction of property at or relating to a United States government mission abroad or surrounding the serious breach of security involving intelligence activities

of a foreign government directed at a United States government mission abroad and shall make written findings determining:

- (1) If the incident abroad did constitute a serious security incident as determined in Section 4831, and that the incident was security related;
- (2) If the incident involved a diplomatic compound, motorcade, residence, or other mission facility, whether the security systems, security countermeasures, and security procedures operated as intended, and whether such systems worked to materially mitigate the attack or were found to be inadequate to mitigate the threat and attack;
- (3) If the incident involved an individual or group of officers conducting an approved operation outside the mission, the SSI/PCC would determine and report if a valid process was followed in evaluating the requested operation and weighing the risk of the operation. The report would not seek to assign accountability for the incident unless there was a conclusion that an official breached their duty.
- (4) The impact of intelligence and information availability, and whether the mission was aware of the general operating threat environment or any more specific threat intelligence or information and took that into account in ongoing and specific operations;

(5) Such other facts and circumstances that may be relevant to the appropriate security management of U.S. missions abroad.

(A) Reporting findings

The SII/PCC shall submit a report of the findings (which may be classified to the extent deemed necessary by the committee) and, if made, any recommendations to the Secretary of State. After suitable consideration, and within 90 days of receipt of the report, the Secretary of State shall provide a report of the incident and findings to the chairmen of the Senate Foreign Relations Committee and the House Committee on Foreign Affairs.

(B) Personnel Recommendations

Should the SII investigative team find reasonable cause to believe any individual described in Section 4833 (b)(1)(C) has breached the duty of that individual or uncovers lesser failures in performance related to the incident, it shall be reported to the SSI/PCC. If the SSI/PCC members find reasonable cause as well, it shall be reported to the Director General of the Foreign Service for appropriate action.

Section 4835. Relation to Other Proceedings

(a) Nothing in this subchapter shall be construed to create administrative or judicial review remedies or rights of action not otherwise available by law, nor shall any provision of this subchapter be construed to deprive any person of any right or legal defense which would otherwise be available to that person under any law, rule, or regulation.

(b) Nothing in this process would preclude the Secretary of State from convening a follow-up public board of inquiry made up of notable persons to investigate any security incident if it was of such magnitude or significance that an internal process was deemed insufficient to understand and investigate the incident. All the materials gathered in the normal internal process would be provided to any Board of Inquiry the Secretary convenes.



APPENDIX B

AAD FS Risk Paradigm Change Project Supporters

As of December 20, 2020

Aarnes, Anne, USAID	Feltman, Jeffrey D., Amb.
Allen, John R., Gen. USMC	Ford, Robert S., Amb.
Arellano, Hilda M. "Bambi", USAID	Garber, Larry, USAID
Bever, James A., USAID	Hammink, William P., USAID
Bodde, Peter W., Amb	Hill, Christopher R., Amb.
Brownfield, William R., Amb.	Jones, Deborah K., Amb.
Campbell, John F., Gen. U.S. Army	Jones, Stuart E., Amb.
Connelly, Maura, Amb.	Kennedy, Patrick J., Amb. (M)
Cohen, David, USAID	Llorens, Hugo, Amb.
Crocker, Ryan C., Amb.	McCarthy, Deborah, Amb.
Crowley, Christopher, USAID	McChrystal, Stanley A., Gen. US Army
Cunningham, James B., Amb.	McKinley, P. Michael, Amb.
Dunford, Joseph F., Gen. USMC	McMaster, H.R., Lt. Gen. US Army
Eikenberry, Karl, Lt. Gen US Army/Amb.	McNeill, Dan K., USArmy
Feierstein, Gerald M., Amb.	Miller, Thomas J., Amb.

Myers, Desaix “Terry”, USAID	Sisson, Andrew, USAID
Neumann, Ronald E., Amb.	Stall, Thomas H., USAID
Nicholson, John W. Jr., US Army	Starr, Gregory B., Asst. Sec. DS
Olson, Richard G., Amb.	Stephenson, James “Spike”, USAID
Patterson, Anne W., Amb	Thomas-Greenfield, Linda, Amb.
Pickering, Thomas R., Amb.	Van Egmond, Alan, USAID
Ray, Charles A., Amb.	Votel, Joseph L., Gen. US Army
Rodriguez, David M., Gen US Army	Walles, Jacob, Amb.
Romero, Peter F., Amb.	

Groups that support

American Foreign Service Association
American College of National Security Leaders
USAID Alumni Association’s Board of Directors

APPENDIX C

TABLE OF ABBREVIATIONS

AAD	American Academy of Diplomacy
ACNSL	American College of National Security Leaders
AFSA	American Foreign Service Association
ARB	Accountability Review Board
COM	Chief of Mission
DCM	Deputy Chief of Mission
DG	Director General
DNI	Director of National Intelligence
DoD	Department of Defense
DS	Diplomatic Security
IC	Intelligence Community
M/SS	Office of Management, Strategy and Solutions
ROI	Report of Investigation
RSO	Regional Security Officers
SII	Security Incident Inquiry
SSI/PCC	Serious Security Incident Permanent Coordinating Committee



© Copyright 2021 American Academy of Diplomacy
1200 18th Street, NW, Suite 902
Washington, DC 20036
202.331.3721

www.academyofdiplomacy.org