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

Report of Inspection

Limited-Scope Review of Department of State Counterterrorism Designation and Vetting Procedures

Report Number ISP-I-08-26, June 2008

PURPOSE, SCOPE AND METHODOLOGY OF THE REVIEW

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

PURPOSE

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

- Policy Implementation: whether policy goals and objectives are being effectively achieved; whether U.S. interests are being accurately and effectively represented; and whether all elements of an office or mission are being adequately coordinated.

- Resource Management: whether resources are being used and managed with maximum efficiency, effectiveness, and economy and whether financial transactions and accounts are properly conducted, maintained, and reported.

- Management Controls: whether the administration of activities and operations meets the requirements of applicable laws and regulations; whether internal management controls have been instituted to ensure quality of performance and reduce the likelihood of mismanagement; whether instance of fraud, waste, or abuse exist; and whether adequate steps for detection, correction, and prevention have been taken.

METHODOLOGY

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

United States Department of State
and the Broadcasting Board of Governors

Office of Inspector General

PREFACE

This report was prepared by the Office of Inspector General (OIG) pursuant to the Inspector General Act of 1978, as amended, Section 209 of the Foreign Service Act of 1980, the Arms Control and Disarmament Amendments Act of 1987, and the Department of State and Related Agencies Appropriations Act, FY 1996. It is one of a series of audit, inspection, investigative, and special reports prepared by OIG periodically as part of its oversight responsibility with respect to the Department of State and the Broadcasting Board of Governors to identify and prevent fraud, waste, abuse, and mismanagement.

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

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

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

Harold W. Geisel
Acting Inspector General

Address correspondence to: U.S. Department of State, Office of Inspector General, Washington, D.C. 20522–0308

TABLE OF CONTENTS

KEY JUDGMENTS

- The Public Designations Unit of the Office of the Coordinator for Counterterrorism (S/CT) is unable to fully and quickly engage its interagency counterparts because it does not have access to Intelligence Community Electronic Mail (IC-email). The Office of Inspector General (OIG) team focused on this problem and obtained commitments from S/CT and the Bureau of Intelligence and Research (INR) that should result in IC-email being provided to the Designations Unit soon.

- On February 26, 2008, the Deputy Secretary issued vetting (due diligence) guidelines applicable to all Department of State bureaus and the U.S. Agency for International Development (USAID) to ensure that U.S. assistance funds do not inadvertently go to terrorists. The Deputy Secretary's memorandum strongly reiterated the importance of vetting and established a working group, which began meeting soon thereafter, to ensure these guidelines are being followed consistently by all offices that are providing assistance.

- On April 10, 2008, the Director for U.S. Foreign Assistance issued instructions to all Department bureaus and USAID that FY 2008 funding requests must include a statement of compliance with the Deputy Secretary's guidelines. This timely guidance reiterated the importance of vetting.

The limited-scope review took place in Washington, DC, between January 15 and April 21, 2008. Ambassador Fernando E. Rondon and Senior Inspector Peter J. Antico conducted the review.

CONTEXT

An OIG team reviewed how the Department is organized and the procedures that are in place to carry out its statutory responsibilities in two aspects of the fight against terrorism. First, the Department is mandated to identify and designate terrorist entities and those supporting terrorism, making those entities subject to sanctions. Second, the Department and USAID are required by law and regulation to ensure that U.S. assistance funds do not inadvertently go to terrorists. One important method to prevent this is by vetting the names of organizations and individuals being considered for assistance against lists of designated terrorist entities.

The OIG team reviewed both aspects of this process, focusing particularly on two offices with central roles: S/CT and the Office of Terrorism Finance and Economic Sanctions Policy in the Bureau of Economic, Energy and Business Affairs (EEB/ESC/TFS).

The OIG team also revisited S/CT's inability to comply with a 2006 inspection recommendation[1] that S/CT, in coordination with INR, facilitate the work of S/CT's Designation's Unit by giving it better communications capabilities and easier access to all source intelligence. This review reaffirms the old recommendation, and recognizes the commitment and specific steps that the two offices have agreed upon to reach this goal.

While the review was in progress, the Deputy Secretary issued timely guidance reemphasizing the responsibility of senior officials at the Department and USAID to apply due diligence procedures to prevent U.S. Government assistance money from inadvertently going to terrorists. The guidance also established an interoffice committee chaired by the Bureau of Economic, Energy, and Business Affairs (EEB) to coordinate and strengthen vetting policies and procedures throughout the Department.

[1]Recommendation 8 of ISP-I-06-25A, Inspection of the Office of the Coordinator for Counterterrorism - March 2006.

DESIGNATIONS

Responsibility for Making Designations

The Secretary of State (Secretary) is responsible for identifying state sponsors of terrorism, terrorist organizations, and individual terrorists by: designating a country as a state sponsor of terrorism pursuant to the Export Administration Act, the Arms Export Control Act, and the Foreign Assistance Act;[2] designating an organization as a Foreign Terrorist Organization (FTO) under the Immigration and Nationality Act;[3] listing an individual or entity as engaging in terrorist activity under Executive Order (EO) 13224; and listing an organization as engaging in terrorist activity on the Terrorist Exclusion List under the USA Patriot Act of 2001.[4] Designation activities are carried out under the direction of S/CT, which serves as "the principal adviser to the Secretary of State on international counterterrorism matters" and provides "overall supervision (including policy oversight of resources) of international counterterrorism activities." [5] With these chief roles, S/CT acts as "a primary coordinating mechanism for the Executive Branch in dealing with international terrorism."

State Sponsors of Terrorism

The Designations Unit within S/CT prepares designations of state sponsors of terrorism, which are countries determined by the Secretary to have repeatedly provided support for acts of international terrorism. Current state sponsors of terrorism include Cuba, Iran, North Korea, Sudan, and Syria.

---

[2]Export Administration Act of 1979, as amended (50 U.S.C. App. § 2405); the Arms Export Control Act of 1976, as amended (22 U.S.C. § 2780); and the Foreign Assistance Act of 196, as amended 1(22 U.S.C. § 2371).
[3]8 U.S.C. § 1189.
[4]8 U.S.C. § 1182.
[5]Pub. L. No. 105-277

Foreign Terrorist Organizations

The Secretary is authorized under the Immigration and Nationality Act to designate as FTOs, entities engaged in terrorist activity that threaten "the security of United States nationals or the national security of the United States." [6] There are 44 terrorist organizations currently on the published FTO list, among them, for example, al-Qaeda, the Islamic Resistance Movement (HAMAS) and the Revolutionary Armed Forces of Colombia (FARC).[7]

Executive Order 13224

In accordance with EO 13224, the Secretary may also designate individuals or entities that have committed or pose a significant risk of committing acts of terrorism that threaten the security of U.S. nationals or U.S. national security.

EEB has the lead in representing the Department's views before the Sub-Counterterrorism Security Group (Sub-CSG) in discussions of possible Department of Treasury Executive Order designations. On the other hand, S/CT has primary responsibility before the Sub-CSG for FTO and EO designations pursuant to the Secretary of State authorities.

Terrorist Exclusion List

The S/CT Designations Unit is further responsible for the Terrorist Exclusion List. A Terrorist Exclusion List designation facilitates the U.S. Government's ability to exclude aliens associated with the 59 entities on the list from entering the United States. Beyond immigration consequences, placement on the publicly available list does not entail the legal consequences that flow from FTO designations (see below).

---

[6]Fact Sheet, Office of Counterterrorism, Washington, DC, October 11, 2005, "Foreign Terrorist Organizations (FTOs)." If the Secretary of State, in consultation with the Attorney General and the Secretary of the Treasury, decides to make the designation, Congress is notified of the Secretary's intent to designate the organization and given seven days to review the designation, as the Immigration and Nationality Act requires. Upon the expiration of the seven-day waiting period and in the absence of Congressional action to block the designation, notice of the designation is published in the Federal Register, at which point the designation takes effect.

[7]Two organizations, one Somali and one Bangladeshi, were added to the list in March 2008.

Specially Designated Nationals List

The EEB/ESC/TFS, and several other Department offices including S/CT, prepare nominations to the Department of Treasury's list of Specially Designated Nationals, and evaluate proposed designations made by the Treasury Department's Office of Intelligence and Analysis. The Specially Designated Nationals list, more commonly called the Office of Foreign Assets Control (OFAC) list, consists of thousands of names of individuals and entities. The list includes designations made pursuant to various Executive Orders that address not only terrorism, but also narcotics trafficking, weapons proliferation, illicit diamond trading, and other crimes. EEB/ESC/TFS, with S/CT's participation, chairs the Department committee that reviews proposed new Treasury Department designations to the OFAC list.

Process of Forming Designation Proposals

The Public Designations Unit in S/CT is responsible for making recommendations to the Secretary to include entities or individuals for these lists. Counterterrorism designations are formally approved by the Sub-CSG, an interagency committee established under EO 13224 of September 23, 2001, and chaired by the National Security Council. Legal consequences flow from both FTO and EO designations. Individuals or organizations of the United States having dealings with a designated entity may be subject to criminal and civil penalties. Consequences of designations include the freezing of all property, and interests in property, in the United States or under the control of U.S. persons. Designations can and often are challenged in court.

Proposed designations are made on the basis of evidence — sometimes highly classified — that makes the case that a presumed terrorist agent or supporter should be designated. The Public Designations Unit of S/CT prepares FTO and EO designations packages. As there is a legal requirement that FTO listings be reviewed every five years, the Designations Unit must also submit documentary packages for these regular reviews. Once assembled by S/CT, FTO and EO designations packages are circulated for review and concurrence, first to interested offices in the Department and then to the interagency community. Finally, S/CT sends cleared proposed designations to the Secretary for decision.

The Treasury Department's Office of Intelligence and Analysis prepares similar packages for proposed EO designations pursuant to the Treasury Secretary's authority under EO 13224. As members of the Sub-CSG on Terror Finance, several De-

partment offices receive incoming Office of Intelligence and Analysis designations packages for their review. As noted, this review is coordinated by EEB/ESC/TFS, which then presents the Department's agreed response to the Sub-CSG.

Interagency Communications Problems

The OIG team found that S/CT and EEB do not have ready access to IC-email, which is a classified e-mail system used across the U.S. Government by the intelligence community. INR controls access to the Intelligence and Research Information Support System (INRISS), and in order to obtain IC-email, a user must be able to access INRISS. The advantage of having IC-email is that the user can quickly contact members of the interagency intelligence community and share information in a safe classified format. Given S/CT's role as the primary coordinating mechanism for the Executive Branch in dealing with international terrorism, the need for IC-email is apparent and immediate. Indeed, the lack of ready access to highly classified communications and intelligence reporting available on the INRISS system undermines the ability of the Public Designations Unit to support S/CT's mandated leadership role in the U.S. Government's counterterrorism effort.

The OIG team learned of several troubling examples where communication between the Designations Unit and other members of the interagency counterterrorism community was unsatisfactory. In one case, high-level urgent messages failed to reach the Public Designations Unit because the latter does not have access to IC-email. Messages to S/CT must currently be sent to an INR analyst, and then hand-delivered to S/CT. INR analysts who pass such messages are not always available, as happened in the foregoing example. In other cases, communication between the intelligence community and S/CT was insufficient, with non-Department agencies and occasionally their overseas counterparts surprised by the timing of public announcements of FTO designations.

Several workarounds involving INR have been developed to enable the Designations Unit and other responsible Department offices to review highly classified designations packages sent from OFAC, as well as to supply the Designations Unit with information it has tasked the intelligence community with providing in the course of building FTO and EO designations packages. The OIG team concluded that these arrangements are highly unsatisfactory. Indeed, under the circumstances, it is surprising that the Designations Unit is able to do its job as well as it does. There is no question, however, that the work of the Designations Unit would be more effective if the unit could communicate more readily with its intelligence community counterparts.

The complexities of the communications problem are difficult to discuss in an unclassified document; however, the crux of the problem is easily stated: S/CT (and not INR) is the leader of an interagency counterterrorism effort, but is significantly disadvantaged by its lack of easy access to classified reporting and email on INRISS. All of the interagency officials interviewed by the OIG team have ready access to sensitive communications facilities, but S/CT's access is awkward and indirect. It cannot receive Top Secret messages from other interagency personnel who share responsibility for designating terrorist organizations and denying them assistance, nor can it print all source intelligence often required for designations packages, which is received through INR.

All NSC subgroup members interviewed by the OIG team believe that it is crucial for the Designations Unit to have access to INRISS, the INR all source classified intelligence communications platform, particularly for the access it would provide to IC-email. OIG is in no position to assess the relative importance of this need against other priorities in S/CT for which ready access to INRISS is also important. S/CT must make that decision. Nevertheless, the fact remains that the Department is hampering the efforts of its own units to interact quickly, securely, and collegially with other key interagency players in the war on terror.

OIG called attention to this problem in its report on the Inspection of the Office of the Coordinator for Counterterrorism (SBU Report ISP-I-06-25A, issued March 2006). After discussing the Designations Unit, OIG made the following recommendation:

> Recommendation 8: The Office of the Coordinator for Counterterrorism, in coordination with the Bureau of Intelligence and Research, should immediately initiate formal documented discussions to resolve the issue of the Office of the Coordinator for Counterterrorism's access to Bureau of Intelligence and Research data and reach a definitive, mutually acceptable agreement. (Action: S/CT)

This recommendation remains open, in OIG's compliance process after two years. Discussions between S/CT and INR since 2006 led to an unrealized hope that the issue could be resolved when the Public Designations Unit moved into a secure area formerly occupied by INR. But the problem persisted until now, and the recommendation is still open. During the review, however, the OIG team received assurances that INR and S/CT will promptly take specific steps that should finally settle the matter.

Finding A Solution

During the review, INR agreed to increase the number of INRISS logons (authorizations to access the system) that S/CT staffers can use at certain INRISS-equipped workstations in secure S/CT office space. S/CT must decide which of its staffers are assigned logons. S/CT informed OIG, however, that it would assign one of the new logons to the Designations Unit.

INR also agreed to provide an additional workstation for the Designations Unit if it is technically feasible to install it in the Designation Unit's office space.[8]

When these steps have been completed, OIG compliance requirements on this matter should have been satisfied. In the interim, OIG closes recommendation 8 from its report on S/CT (ISP-I-06-25A), and issues the following new recommendation, with action assigned to S/CT, in coordination with INR.

Recommendation 1: The Office of the Coordinator for Counterterrorism, in coordination with the Bureau of Intelligence and Research, should provide the Designations Unit with Intelligence and Research Information Support System capability and Intelligence Community Electronic Mail, in order to facilitate interactions between that key office and its counterparts in the interagency counterterrorism intelligence community. (Action: S/CT, in coordination with INR)

[8]It should be understood that the workstation INR has agreed to provide to the Designations Unit is obsolescent and will need to be replaced with a modernized unit when INR's laudable "e-Intel" (Electronic-Intelligence) initiative achieves its initial operating capability, planned for summer 2008. Under e-Intel, bureaus will be required to procure (and pay for) their INRISS workstations through INR. INR estimates the cost of a new INRISS workstation will be around $1,500. The S/CT Management Officer and the Secretariat have confirmed that funds are available to cover such a purchase for the Public Designations Unit and possibly for other offices in S/CT.

VETTING

Vetting is a term in the counterterrorism community generally used to refer to the process of screening the names of individuals and organizations against various lists of terrorists and their supporters. Vetting is done for several reasons. The OIG team's interest in the matter focused on vetting the names of possible recipients of U.S. Government assistance to ensure that no U.S. Government funds were inadvertently given to terrorists or their sympathizers. Certain types of counterterrorism vetting are required by law. The Department prefers to describe the vetting process as the exercise of "due diligence" because it applies a broader view of what should be involved. Vetting, however, is the word used in several regulations and legislation, and this review employs that term, except in its discussion of new Department guidance on the matter.

Required by Law and Regulation

One of the regulatory bases for vetting is laid out in Homeland Security Presidential Directive No. 6, which directs and authorizes executive departments and agencies to examine their programs to determine where vetting should be applied. It also states that "U.S. policy is to develop, integrate, and maintain accurate and current information about individuals known or suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism."

Appropriations legislation also requires that vetting be carried out in specific areas of the world. For example, the Foreign Operations Appropriations bills for FYs 2003-06 each contained a section entitled "Vetting" for recipients of certain assistance for the West Bank and Gaza. A representative statutory provision states:

> Prior to the obligation of funds appropriated by this Act under the heading "Economic Support Fund" for assistance for the West Bank and Gaza, the Secretary of State shall take all appropriate steps to ensure that such assistance is not provided to or through any individual or entity that the Secretary knows or has reason to believe advocates, plans, sponsors, engages in, or has engaged in, terrorist activity.[9]

[9]Section 566(b) of the Consolidated Appropriations Act, 2004, P.L. 108-199.

Many bureaus and offices across the Department and in the field deliver U.S. Government financial assistance in one form or another. Almost all of them vet the projected recipients of this assistance in some way. While the practice is not universal, the majority of offices have been vetting against the OFAC list (although not all entries on this list are terrorist-related). Some offices now go a step further and also check names against the Government-wide Terrorist Screening Database (TSDB).

Diplomatic Security Assistance to Foreign Security Forces

The Office of Antiterrorism Assistance, of the Bureau of Diplomatic Security, has a special set of vetting requirements mandated under the Leahy Amendment, prohibiting the use of foreign assistance funds to assist foreign security forces where there is credible evidence such forces have committed "gross violations of human rights."[10] Names of possible participants in the Antiterrorism Assistance program are checked against a database of human rights abusers, which is still under development, called the Abuse Case Evaluation System. They are not, however, necessarily checked against the OFAC list or any other counterterrorism list. Additional checks may be run if program managers determine there is a risk that assistance funds could be misdirected to terrorists or their supporters.

Terrorist Screening Center

There are several databases for counterterrorism vetting that are used by different offices in the Department. This report mentions five of the most important: the FTO list, the EO 13224 list, the Terrorist Exclusion List, Treasury's OFAC list; and the TSDB. The TSDB is a Sensitive But Unclassified database containing names and basic biographic data on known and suspected terrorists. It is maintained at the Terrorist Screening Center (TSC) in Virginia, which is managed by the Federal Bureau of Investigation. While the TSDB list is not classified and can be shared with offices in the Department, the intelligence supporting any listing is usually classified and can be reviewed only at the TSC (often through liaison arrangements drawing upon other, all source intelligence community databases). For practical purposes, this

[10]The "Leahy Amendment," sponsored by Senator Patrick Leahy (D-VT), has been separately enacted in several appropriations bills for the Department of State and the Department of Defense. With reference to the Department of State's budget, the amendment was first included in the 1997 Foreign Operations Appropriations Act (Pub. L. No. 104-208) and has been re-enacted, in varying forms, in subsequent State appropriations bills.

means that any Department office needing to vet names against the TSDB list must have approval to use the center. Three Department bureaus have such approval: the Bureau of Consular Affairs, the Bureau of Diplomatic Security, and the Bureau of International Narcotics and Law Enforcement. The deputy director of the TSC is an officer from Consular Affairs, who shares in the management of the facility, so special access arrangements are unnecessary for the Bureau of Consular Affairs. Conversely, the Bureau of Diplomatic Security and the Bureau of International Narcotics and Law Enforcement have negotiated memorandums of understanding with the Federal Bureau of Investigation to use TSC resources. Finally, the USAID, under the policy direction of the Secretary of State,[11] also recently concluded a memorandum of understanding with the Federal Bureau of Investigation to use the facility.

Consular Lookout System

Consular Lookout and Support System (CLASS), a Sensitive But Unclassified listing maintained by the Bureau of Consular Affairs, is sometimes consulted in connection with counterterrorism vetting. The primary purpose of CLASS is to screen visa applicants. If a U.S. Government-funded assistance program will bring foreign participants to the United States, their names will likely be checked against CLASS for visa purposes. There can be exceptions, however, when a traveler is from a visa waiver country. Nevertheless, all U.S. visitors must still be cleared at a U.S. entry point, where visitors' names and passports are checked by immigration officials against the Treasury Enforcement Communications System database. Both lists contain names from the TSDB, and thus contribute to counterterrorism vetting.[12] The names of participants in some field-administered programs, which do not involve travel to the United States (for example, embassy public diplomacy grants and certain USAID projects), may also be vetted against CLASS at post for possible terrorism connections.

[11]As of November 14, 2007, the same individual has been serving as the Department's Director for U.S. Foreign Assistance (F) as well as USAID's Administrator. The incumbent is thus in a position to ensure that both Department of State and USAID take the steps required to practice due diligence or vet all foreign assistance for anti-terrorist considerations.
[12]It is unclear how many TSDB names are replicated in CLASS. The OIG team heard estimates as high as 95 percent for CLASS, and the percentage is believed to be higher for TECS.

Tightening Vetting Procedures

Procedures for counterterrorism vetting, and whether vetting is conducted at all, vary widely throughout the Department. Different lists are consulted by different offices, and a few offices have negotiated special arrangements to conduct vetting at the TSC. The inefficiencies and potential vulnerabilities in these arrangements have been apparent both at the interagency and Department level, but interagency efforts have so far failed to establish a Government-wide set of standards and procedures for counterterrorism vetting prior to awarding U.S. Government assistance.

Without clear, Government-wide agreement on vetting standards, the Department began its own assessment of the issue about a year ago. The Department's initiative, which the OIG team learned about during the early stages of this review, resulted in the Deputy Secretary's issuance of a memorandum entitled: State and USAID Funding and the Risks of Terrorist Funding. [13] This guidance clarifies due diligence procedures to ensure that U.S. Government assistance money will not inadvertently go to terrorists or their supporters. The memorandum also lists the tools available, including vetting, to achieve this goal and the circumstances under which varying procedures might be followed.

Importantly, the guidance also announces the creation of a Department working group chaired by EEB to facilitate implementation of these guidelines. Such implementation will be critical to the success of this initiative.

The Deputy Secretary's guidance thoroughly addresses many of the questions raised in this OIG review. The guidance reminds senior officials, including Department Assistant Secretaries and USAID Assistant Administrators, of their responsibility to conduct a risk-based assessment of any new assistance program and make "the final decision about what review process is appropriate for any particular program." The guidance also states:

[13]The Deputy Secretary's February 26, 2008 memorandum was sent to the USAID Administrator, Under Secretaries, Assistant Secretaries and Assistance Coordinators. As attachments, it contained Guidance for Risk-Based Assessment and Procedures for Reviewing Program Recipients. The guidelines were sent to the field in State 020628 of February 28, 2008.

> A single fixed procedure for preventing inadvertent benefits to terrorists or their supporters – a "one size fits all approach" – for all programs is not appropriate. Instead, safeguards and scrutiny should be highest in areas with greatest risk.
>
> Where a program is assessed to be particularly high-risk, such that it entails a high risk of support to terrorists or their supporters, but there are significant foreign policy reasons for proceeding, additional guidance should be sought from the Under Secretary level or above, and the Office of the Legal Adviser must be consulted with respect to applicable legal requirements.

The guidance then outlines the following basic procedures that apply to all programs:

> Even when the risk of providing inadvertent benefits to terrorists is minimal, certain basic procedures are generally appropriate. For example, the names of grantees and contractors must be checked against the Specially Designated Nationals list administered by the Department of Treasury's Office of Foreign Assets Control in all cases.

Basic Department contracting and grant regulations must also be met in all cases, including making "a responsibility determination as to whether the [primary] recipient of the funds meets certain business and ethical standards," which the recipient would obviously fail to meet if found to have ties to terrorism, and making the same determination for subgrantees and subcontractors.

An attachment to the guidance lists additional procedures that might be employed, depending on the nature of the program and the level of risk entailed, including several possible checks against counterterrorism lists, such as the Terrorist Exclusion List and intelligence databases. Regarding this last suggestion, the guidance notes:

> Such database checks are not feasible across all Department grants and programs, but the Department is seeking to establish additional capacity to do such checks when the circumstances warrant this level of due diligence.

The OIG team considers this guidance to be an important milestone as the Department addresses this complex problem. The guidance correctly emphasizes that, prior to undertaking new assistance programs, senior Department and USAID officials must evaluate the risks associated with the new initiative, notably any risks that funds might be inadvertently diverted to terrorists. Moreover, the guidance points out that these risks have to be weighed against the potential benefits to be

derived from the program, and that, in certain circumstances, the benefits may justify some degree of risk. In particularly high-risk environments, the guidance rightly calls for the matter to be referred to the Department's highest-level officials for decision.

In the OIG team's view, the guidance provides the framework for addressing the issue of preventing possible diversions of U.S. Government assistance monies to terrorists. The efficacy of the guidance will be seen in the implementation stage, notably whether serious risks are identified.

Coordination of Vetting

As noted, the Deputy Secretary's February 26, 2008, guidance announced formation of an EEB-led working group to focus on implementation. The guidance stated that the group would "convene a meeting for all bureaus and USAID to review existing best practices and respond to questions arising from this guidance and its implementation [and] organize follow-up meetings as needed."

This report pointed out that vetting procedures vary widely in grant-making offices across the Department. While recognizing that the delivery of assistance by Department offices and USAID is not — and could never be — a fully centralized effort, vulnerabilities were created by overly decentralized past practices. The new working group has a broad mandate, but will require focused leadership from EEB and other key principals, including the Director of U.S. Foreign Assistance, to ensure that all participating offices practice the required measure of due diligence and/or vetting.

The Director of U.S. Foreign Assistance provides leadership for foreign assistance policy, planning, and budgeting; and reviews and approves all Department and USAID assistance programs and activities. These programs and activities are described in the Department's annual requests for funding through the Foreign Operations appropriations cycle and later detailed in corresponding operational plans. Changes to programs and activities throughout the course of the year are approved by the Director of U.S. Foreign Assistance and, once Congress is notified, updated in the operational plans. These operational plans, buttressed by the budget justification and the appropriations bill, permit a full picture of the type of programs underway, which offices are implementing them, and at what cost. The documents thus provide the Department, USAID, and the working group with an overview of the range of programs that require due diligence procedures and for which vetting may be necessary. These steps ultimately remain the responsibility of implementing offices, which directly manage the programs and make decisions about safeguards.

The working group held the first organizational meeting on March 5, 2008. For the moment, the procedures are a work in progress, but the working group's stated intention is to apply lessons learned and best practices from all bureaus and USAID. Subsequent meetings, under the leadership of EEB, with the Office of the Director of U.S. Foreign Assistance support, are expected to explore these lessons and practices more fully and offer guidance to the Department and USAID on appropriate due diligence procedures in particular situations. USAID is already using the TSC and it appears that the Department itself may need to make greater use of this center. The OIG team was assured by the Office of the Director for U.S. Foreign Assistance that it would not approve budget requests for assistance programs without accompanying statements that antiterrorist concerns had been taken into account. The key will be implementation.

An important step in this direction was the issuance by the Office of the Director of U.S. Foreign Assistance of an April 11, 2008, memorandum on Approval of Foreign Assistance Funding in FY 2008. This document directed all bureaus and USAID to include a statement with all assistance requests attesting that due diligence procedures would be applied to the program in accord with the Deputy Secretary's guidelines.

FORMAL RECOMMENDATION

Recommendation 1: The Office of the Coordinator for Counterterrorism, in coordination with the Bureau of Intelligence and Research, should provide the Designations Unit with Intelligence and Research Information Support System capability and Intelligence Community Electronic Mail, in order to facilitate interactions between that key office and its counterparts in the interagency counterterrorism intelligence community. (Action: S/CT, in coordination with INR)

	Name	Date of Appointment
Director for U.S. Foreign Assistance	Henrietta Fore	11/07
Assistant Secretary, Economic, Energy and Business Affairs	Daniel S. Sullivan	06/06
Assistant Secretary, Intelligence and Research	Randall M. Fort	08/06
Coordinator for Counterterrorism	Dell L. Daily	06/07

ABBREVIATIONS

CLASS	Consular Lookout and Support System
Department	Department of State
EEB	Bureau of Economic, Energy and Business Affairs
EEB/ESC/TFS	EEB/ Office of Terrorism Finance and Economic Sanctions Policy
EO	Executive Order
FTO	Foreign Terrorist Organization
IC-email	Intelligence Community Electronic Mail
INR	Bureau of Intelligence and Research
INRISS	INR Information Support System
OFAC	Office of Foreign Assets Control, Department of Treasury
OIG	Office of Inspector General
S/CT	Office of the Coordinator for Counterterrorism
Secretary	Secretary of State
Sub-CSG	Sub-Counterterrorism Security Group
TSC	Terror Screening Center
TSDB	Terrorist Screening Database
USAID	U.S. Agency for International Development

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

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

You may also write to
Office of Inspector General
U.S. Department of State
Post Office Box 9778
Arlington, VA 22219
Please visit our website at oig.state.gov

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