PROTECTING AMERICAN INTERESTS ABROAD: U.S. CITIZENS, BUSINESSES AND NONGOVERNMENTAL ORGANIZATIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS AND INTERNATIONAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

APRIL 3, 2001

Serial No. 107–16

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

75–955 PDF WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

CONTENTS

PROTECTING AMERICAN INTERESTS ABROAD: U.S. CITIZENS, BUSINESSES AND NON-GOVERNMENTAL ORGANIZATIONS

TUESDAY, APRIL 3, 2001

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS AND INTERNATIONAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:08 a.m., in room 2247, Rayburn House Office Building, Hon. Christopher Shays (chairman of the subcommittee) presiding.

Present: Representatives Shays, Putnam, Gilman, Platts, Otter, Kucinich, and Tierney.

Staff present: Lawrence J. Halloran, staff director and counsel; Thomas Costa, professional staff member; Alex Moore, fellow; Jason M. Chung, clerk; David Rapallo, minority counsel; and Earley Green, minority assistant clerk.

Mr. PUTNAM [presiding]. A quorum being present, the Subcommittee on National Security, Veterans Affairs and International Relations' hearing entitled, "Protecting American Interests Abroad: U.S. Citizens, Businesses, and Non-governmental Organizations" is hereby called to order.

The Chair recognizes Mr. Shays from Connecticut for an opening statement.

Mr. SHAYS. Thank you, Mr. Chairman.

During our hearing on counterterrorism strategy last week, witnesses described a significant new contextual element of U.S. security planning in the post-cold war world: widespread resentment fostered by our global military and economic dominance. Unable to challenge our preeminence by frontal assault, our adversaries vent their frustrations through sidelong, or asymmetrical, attacks on Embassies, naval vessels, and other valuable, but vulnerable, national assets.

Individuals and corporate facilities are also at risk. As diplomatic and military facilities abroad are hardened against attack, terrorists and transnational criminals look for softer targets. American businesses and tourists have always been potential symbols and valuable pawns in the deadly game of international terror, kidnapping, and ransom. Today, more than ever, private interests abroad are the victims of publicity-hungry, cash-starved terrorists.

An effective, comprehensive national security policy to combat terrorism should acknowledge this harsh new reality and include

the private sector in programs to prevent, as well as respond to, lawlessness aimed at Americans abroad. Nongovernmental organizations [NGO's], performing humanitarian missions in some of the most isolated, devastated parts of the world should have access to security information and training to minimize the risks of their inherently dangerous work.

So we asked our witnesses this morning to describe current Federal efforts to enhance the security of U.S. citizens and businesses overseas. They will describe some recent progress toward greater awareness of new threats and closer public/private cooperation to prevent loss of life and property.

But the nascent effort faces significant challenges coming to grips with the dynamic, multidimensional, interconnected problems of economic espionage, cybercrime and fanatical terrorism that ignore old rules and old boundaries. Many corporations are reluctant to report extortion and kidnapping, calculating the costs of official entanglements and attendant publicity to be higher than the ransom. Definitional and jurisdictional barriers can impede the flow of information and fragment Federal efforts to help.

Kidnapping and ransom insurance premiums should not be a routine cost of doing business abroad. A U.S. passport should not mark our citizens as targets. We look to our witnesses today to help us understand how national security policies and programs to counter terrorism can operate more effectively to protect American lives and property abroad.

All those testifying this morning bring considerable expertise, experience, and breadth of perspective to our discussion.

I thank you for your time and for your assistance with the subcommittee's ongoing oversight of terrorism at home and abroad.

Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you, Mr. Shays.

[The prepared statement of Hon. Christopher Shays follows:]

DAN BURTON, INDIANA
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MINORITY MEMBER

ONE HUNDRED SEVENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

Majority (202) 225–5074
Minority (202) 225–5051

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS,
AND INTERNATIONAL RELATIONS
Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2548
Fax: 202 225-2382
GROC.NS@mail.house.gov
http://www.house.gov/reform/ns/

Statement of Rep. Christopher Shays
April 3, 2001

During our hearing on counterterrorism strategy last week, witnesses described a significant new contextual element of U.S. security planning in the post-Cold War world: widespread resentment fostered by our global military and economic dominance. Unable to challenge our preeminence by frontal assault, our adversaries vent their frustrations through sidelong, or asymmetrical, attacks on embassies, naval vessels and other valuable, but vulnerable, national assets.

Individuals and corporate facilities are also at risk. As diplomatic and military facilities abroad are hardened against attack, terrorists and trans-national criminals look for softer targets. American businesses and tourists have always been potent symbols and valuable pawns in the deadly game of international terror, kidnapping, and ransom. Today, more than ever, private interests abroad are the victims of publicity-hungry, cash-starved terrorists.

An effective, comprehensive national security policy to combat terrorism should acknowledge this harsh new reality and include the private sector in programs to prevent, as well as respond to, lawlessness aimed at Americans abroad. Non-governmental organizations (NGOs) performing humanitarian missions in some of the most isolated, devastated parts of the world should have access to security information and training to minimize the risks of their inherently dangerous work.

So we asked our witnesses this morning to discuss current federal efforts to enhance the security of U.S. citizens and businesses overseas. They will describe some recent progress toward greater awareness of new threats and closer public/private cooperation to prevent loss of life and property.

Statement of Rep. Christopher Shays
April 3, 2001

But the nascent effort faces significant challenges coming to grips with the dynamic, multi-dimensional, interconnected problems of economic espionage, cyber-crime and fanatical terrorism that ignore old rules and old boundaries. Many corporations are reluctant to report extortion and kidnapping, calculating the costs of official entanglements and attendant publicity to be higher than the ransom. Definitional and jurisdictional barriers can impede the flow of information and fragment federal efforts to help.

Kidnapping and ransom insurance premiums should not be a routine cost of doing business abroad. A U.S. passport should not mark our citizens as targets. We look to our witnesses today to help us understand how national security policies and programs to counter terrorism can operate more effectively to protect American lives and property abroad.

All those testifying this morning bring considerable expertise, experience and breadth of perspective to our discussion. Thank you for your time and for your assistance with the Subcommittee's oversight of terrorism at home and abroad.

Mr. PUTNAM. We're also pleased to have the chairman emeritus of the International Relations Committee, Mr. Gilman from New York.

Would you like to have an opening statement?

Mr. GILMAN. Thank you, Mr. Chairman.

I want to welcome—first of all, I want to tell you how much we appreciate your conducting this hearing at this time. It's particularly important since we just concluded a hearing with Chairman Shays on antiterrorism.

I want to welcome our distinguished panelists who are here with us today. I want to thank them for taking the time to be with us.

As our world has drawn closer together over the last 30 years as a result of improved travel and communications, Americans have benefited from these improvements perhaps as no other nation on Earth. Advances in travel, communication, however, are available to all. And those who would harm American interests have occasionally turned their hate or greed against our American citizens abroad in recent years.

For example, a total of 12 Americans were killed and 18 injured in 14 terrorist attacks just in Israel in the West Bank, in Gaza, between September 13 and November 17 of last year. There were some 37 Americans kidnapped in 1999, not to mention the many who were not reported.

Threats against Americans abroad range from physical harm to unfair economic practices that include stealing intellectual property and computer hacking. It is among the first and most important functions of the consular officials of our diplomatic service to provide aid and assistance to American citizens abroad.

With regard to terrorism, Mr. Chairman, any agency representing our government overseas should join with our Department of State to promote the safety of Americans. And our recent hearing, conducted by Chairman Shays, underscored the fact that we had over some–40 agencies that have some responsibility in terrorism, but without any proper central control, without any proper agency that would handle all of these and bring them together in some centralized function.

In combating the scourge of terrorist attacks directed against our people abroad, timely information-sharing among responsible agencies is certainly a logical and appropriate response. It's for that reason that many of us on this committee feel that we should be adopting a centralized system of control of the agencies that are spread out throughout our government.

I'm interested to hear from our witnesses today and how they believe our Nation may better work to improve the economic and physical security of our citizens who work abroad, live abroad, have businesses abroad.

Thank you very much, Mr. Chairman.

Mr. PUTNAM. Thank you very much.

I'm pleased to welcome the ranking member, Mr. Kucinich from Ohio, for an opening statement.

Mr. KUCINICH. Thank you very much, Mr. Chairman. Members of the committee, good morning. Good morning to the witnesses. I'm glad to have all of you here.

Last week, the subcommittee held a hearing on combating terrorism. The focus of that hearing was on threats to governmental interest. The focus of today's hearing is on threats to nongovernmental interest. This includes violence against U.S. citizens, U.S. companies and, importantly, nongovernmental organizations.

With respect to the last group, I'm particularly interested in finding out what specific U.S. programs are designed to help human rights groups and others delivering humanitarian assistance.

You know, certainly some of the questions that are being posed here today I think we need to go over and pay close attention to. You know, what threats do you face? How does the U.S. Government address those threats? And, third, what could the U.S. Government do better? I think that these are some of the logical and compelling questions which we will be reviewing today.

Just as we need a comprehensive assessment of the threat against governmental interests, we also need to ensure that resources to protect nongovernmental interests are allocated efficiently.

I also think it would be helpful if in our discussions today we could address the root causes underlying threats to the security of nongovernmental interests; in other words, to describe incidents that we've faced is important, and the manner in which the U.S. Government responded is important, but also, I think it would be helpful to address some of the motivations which might be behind those confrontations, such as U.S. foreign policy.

The actions of U.S. companies may affect security issues. For example, oil company executives point out that their employees have been kidnapped repeatedly in Nigeria. But these officials do not address some of the extenuating circumstances that deal with those kidnappings, such as human rights abuses by the oil companies. That's something that I think needs to be looked at; otherwise we are dancing in the dark here on some of these security issues.

I'd like to submit for the record several reports issued by Human Rights Watch that criticize oil companies for their role in harsh treatment of workers who attempt to raise grievances, the exploitation of natural resources of indigenous populations and environmental damage caused by their enterprises.

In one case from January 4, 1999, Human Rights Watch reported that the Chevron Co. supplied helicopters and boats to Nigerian security forces that attacked two communities, killed several people, and burned several villages.

Last week, several witnesses testified there's a growing sense of resentment against the United States. Since this resentment sometimes manifests itself as violence against nongovernmental, as well as governmental, interests, perhaps a greater focus on the cause of the resentment would be in order.

I'm certainly proud to be a Member of the U.S. Congress here, representing my constituency and my country. I'm also interested in what my country can do that would be better to protect citizens abroad.

Thank you very much, Mr. Chairman. I will submit my full statement for the record.

Mr. PUTNAM. Thank you, sir. Without objection, the reports will appear in the record after your statement.

[The prepared statement of Hon. Dennis J. Kucinich follows:]

Opening Statement
Representative Dennis J. Kucinich

Ranking Member
Subcommittee on National Security,
Veterans Affairs, and International Relations

April 3, 2001

GOOD MORNING. LET ME WELCOME ALL OUR WITNESSES HERE TODAY. I AM GLAD YOU COULD BE WITH US.

LAST WEEK, THIS SUBCOMMITTEE HELD A HEARING ON COMBATING TERRORISM. THE FOCUS OF THAT HEARING WAS ON THREATS TO GOVERNMENTAL INTERESTS. THE FOCUS OF TODAY'S HEARING IS ON THREATS TO NONGOVERNMENTAL INTERESTS. THIS INCLUDES VIOLENCE AGAINST U.S. CITIZENS, U.S. COMPANIES, AND, IMPORTANTLY, NONGOVERNMENTAL ORGANIZATIONS.

WITH RESPECT TO THIS LAST GROUP, I AM PARTICULARLY INTERESTED IN FINDING OUT WHICH SPECIFIC U.S. PROGRAMS ARE DESIGNED TO HELP HUMAN RIGHTS GROUPS AND OTHERS DELIVERING HUMANITARIAN ASSISTANCE.

BASED ON A PRELIMINARY REVIEW, THE CURRENT GOVERNMENTAL STRUCTURE SEEMS TO TILT IN FAVOR OF PROTECTING COMMERCIAL ENTITIES. ALTHOUGH THE OVERSEAS SECURITY ADVISORY COUNCIL ALLOWS NONCOMMERCIAL ENTITIES TO AFFILIATE, IT FOCUSES PRIMARILY ON COMMERCIAL ASSETS. IN ADDITION, THE F.B.I. PROGRAM CATERS TO CORPORATIONS AND GOVERNMENT AGENCIES.

ONLY U.S.A.I.D. APPEARS TO PERFORM A SUBSTANTIAL SERVICE IN PROVIDING GRANTS AND SECURITY TRAINING TO N.G.O.s. OVERALL, HUMAN RIGHTS ORGANIZATIONS APPEAR TO HAVE LITTLE AMERICAN ASSISTANCE TO COUNTER SECURITY THREATS, ALTHOUGH I WELCOME INFORMATION TO THE CONTRARY.

IN THIS RESPECT, I WAS HAPPY TO SEE THAT THE CHAIRMAN INVITED AMBASSADOR JAMES BISHOP, WHO NOW WORKS AS DIRECTOR OF THE DISASTER RESPONSE UNIT FOR "INTER-ACTION" — A COALITION OF OVER 150 NONGOVERNMENTAL ORGANIZATIONS OPERATING WORLDWIDE. WITH HIS EXPERIENCE BOTH INSIDE AND OUTSIDE THE GOVERNMENT, PERHAPS HE CAN PROVIDE THE SUBCOMMITTEE WITH ADDITIONAL INSIGHT ON THESE ISSUES.

FINALLY, I WOULD JUST MAKE A CLOSING OBSERVATION. THE SUBCOMMITTEE POSED THE FOLLOWING ISSUES TO THE WITNESSES: FIRST, WHAT THREATS DO YOU FACE? SECOND, HOW DOES THE U.S. GOVERNMENT ADDRESS THOSE THREATS? AND THIRD, WHAT COULD THE U.S. GOVERNMENT DO BETTER?

I THINK THESE ARE LOGICAL AND COMPELLING QUESTIONS. JUST AS WE NEED A COMPREHENSIVE ASSESSMENT OF THE THREAT AGAINST GOVERNMENTAL INTERESTS, WE ALSO NEED TO ENSURE THAT RESOURCES TO PROTECT NONGOVERNMENTAL INTERESTS ARE ALLOCATED EFFICIENTLY.

THE FOCUS OF THIS HEARING MAY BE OVERLY NARROW IN ONE RESPECT, HOWEVER, IN THAT IT DOES NOT ADDRESS THE ROOT CAUSES UNDERLYING THREATS TO THE SECURITY OF NONGOVERNMENTAL INTERESTS. IN OTHER WORDS, WITNESSES WERE ASKED TO DESCRIBE ONLY THE INCIDENTS THEY FACED AND THE MANNER IN WHICH THE UNITED STATES GOVERNMENT RESPONDED. WITNESSES WERE NOT ASKED TO SPEAK ABOUT THE MOTIVATION

BEHIND SUCH ATTACKS, SUCH AS THE IMPACT OF UNITED STATES FOREIGN POLICY.

PLAN COLOMBIA, FOR EXAMPLE, CONCEIVABLY COULD HAVE A SIGNIFICANT IMPACT ON WHETHER UNITED STATES INTERESTS AND INDIVIDUALS ARE TARGETED IN COLOMBIA. AS THE OIL COMPANIES WILL POINT OUT, ONE COLOMBIAN PIPELINE WAS ATTACKED 154 TIMES IN 2000.

BUT THERE ARE MANY ACTIONS BY THE UNITED STATES GOVERNMENT THAT MAY HAVE CONTRIBUTED TO THIS THREAT. FOR INSTANCE, THE UNITED STATES IS PROVIDING HELICOPTERS AND OTHER MILITARY SUPPORT TO THE COLOMBIAN ARMY AT THE SAME TIME THE STATE DEPARTMENT HAS REPORTED THAT THE ARMY IS GUILTY OF SEVERE HUMAN RIGHTS ABUSES.

IN ADDITION, THE COLOMBIAN ARMY COORDINATES WITH ILLEGAL PARAMILITARY UNITS THAT ENGAGE IN BRUTAL MASSACRES. THE STATE DEPARTMENT'S FAILURE TO DESIGNATE COLOMBIA'S MOST NOTORIOUS PARAMILITARY GROUP, THE UNITED SELF-DEFENSE FORCES OF COLOMBIA, AS A TERRORIST GROUP, MAY ALSO BE A CONTRIBUTING FACTOR.

SIMILARLY, THE ACTIONS OF U.S. COMPANIES ALSO MAY AFFECT SECURITY ISSUES. FOR EXAMPLE, OIL COMPANY EXECUTIVES POINT OUT THAT THEIR EMPLOYEES HAVE BEEN KIDNAPED REPEATEDLY IN NIGERIA. BUT THESE OFFICIALS DO NOT ADDRESS THEIR OWN COMPLICITY IN CONTRIBUTING TO THIS THREAT.

I WOULD LIKE TO SUBMIT FOR THE RECORD SEVERAL REPORTS ISSUED BY HUMAN RIGHTS WATCH THAT CRITICIZE OIL COMPANIES FOR THEIR ROLE IN THE BRUTALIZATION OF WORKERS WHO ATTEMPT TO RAISE GRIEVANCES, THE EXPLOITATION OF NATURAL RESOURCES OF INDIGENOUS POPULATIONS, AND THE ENVIRONMENTAL DAMAGE CAUSED BY THEIR ENTERPRISES.

IN ONE CASE FROM JANUARY 4, 1999, HUMAN RIGHTS WATCH REPORTED THAT THE CHEVRON COMPANY SUPPLIED HELICOPTERS AND BOATS TO NIGERIAN SECURITY FORCES THAT ATTACKED TWO COMMUNITIES, KILLED SEVERAL PEOPLE, AND BURNED SEVERAL VILLAGES.

LAST WEEK, SEVERAL WITNESSES TESTIFIED THAT THERE IS A GROWING SENSE OF RESENTMENT AGAINST THE UNITED STATES. SINCE THIS RESENTMENT SOMETIMES MANIFESTS ITSELF AS VIOLENCE AGAINST NONGOVERNMENTAL AS WELL AS GOVERNMENTAL INTERESTS, PERHAPS A GREATER FOCUS ON THE CAUSES OF THIS RESENTMENT IS IN ORDER.

THANK YOU, MR. CHAIRMAN.

TOC = PAGE >

THE PRICE OF OIL

Corporate Responsibility and Human Rights Violations in Nigeria's Oil Producing Communities
Order online

Human Rights Watch
New York · Washington · London · Brussels

Printed in the United States of America.
ISBN: 156432-225-4
Library of Congress Catalog Card Number: 99-60123

TABLE OF CONTENTS

ACKNOWLEDGMENTS

This report was written by Bronwen Manby, researcher in the Africa Division of Human Rights Watch, based on research in the Niger Delta in July 1997, subsequent correspondence with the major oil companies operating in the region, and information provided by Nigerian human rights and environmental activists. The report was edited by Peter Takirambudde, executive director of the Africa Division; Mike McClintock, deputy program director; and Wilder Tayler, general counsel. Elizabeth Thapliyal, Associate in the Africa Division, prepared the report for production.

Human Rights Watch would like to thank its NGO partners who contributed to the report by assisting our research and providing additional information. In particular, we wish to thank the committed and courageous activists of Environmental Rights Action, without whom the report could not have been written. We would also like to thank all those who agreed to meet with us and be interviewed for the report, especially the many residents of oil producing communities of the Niger Delta.

TOC | PAGE >

I. SUMMARY

This report is an exploration of human rights violations related to oil exploration and production in the Niger Delta, and of the role and responsibilities of the major multinational oil companies in respect of those violations. The Niger Delta has for some years been the site of major confrontations between the people who live there and the Nigerian government security forces, resulting in extra-judicial executions, arbitrary detentions, and draconian restrictions on the rights to freedom of expression, association, and assembly. These violations of civil and political rights have been committed principally in response to protests about the activities of the multinational companies that produce Nigeria's oil. Although the June 1998 death of former head of state Gen. Sani Abacha and his succession by Gen. Abdulsalami Abubakar has brought a significant relaxation in the unprecedented repression General Abacha inflicted on the Nigerian people, and General Abubakar appears committed to ensuring the installation of an elected civilian government in May 1999, human rights abuses in the oil producing communities continue and the basic situation in the delta remains unchanged. As this report went to press, the fatal shooting by security forces of tens of youths demonstrating for the oil companies to withdraw from Nigeria was reported, and the deployment of large numbers of soldiers and navy to the delta to suppress such protests.

Since the death of Abacha, there has been a surge in incidents in which protesters have occupied flow stations and closed production or taken oil workers hostage. In the context of increasing threats to the safety of their workers and of damage to their property, oil companies legitimately require security for their personnel and property; but equally there is an even greater need for companies to ensure that such protection does not result in further human rights abuses. The oil companies share a responsibility to oppose human rights violations by government forces in the areas in which they operate, in addition to preventing abuses by their own employees or contractors. Companies have a duty to avoid both complicity in and advantage from human rights abuses, and a company that fails to speak out when authorities responding to corporate requests for security protection commit human rights abuses will be complicit in those abuses.

Human Rights Watch traveled to the Niger Delta in 1997 to investigate human rights violations in connection with the suppression of protest at oil company activities. We found repeated incidents in which people were brutalized for attempting to raise grievances with the companies; in some cases security forces threatened, beat, and jailed members of community delegations even before they presented their cases. Such abuses often occurred on or adjacent to companyproperty, or in the immediate aftermath of meetings between company officials and individual claimants or community representatives. Many local people seemed to be the object of repression simply for putting forth an interpretation of a compensation agreement, or for seeking effective compensation for land ruined or livelihood lost.

We subsequently corresponded with the five multinationals with the largest share of Nigerian production, asking them to comment on our findings about particular incidents at their facilities, as well as their approach to human rights and community relations in general and their relationships with the Nigerian authorities in respect of security and other issues. This correspondence has continued during 1998. The most ample responses were received from Shell, a Dutch-British company, which has faced the most high profile international focus on its responsibilities in Nigeria. Responses on several cases

were also received from Chevron and general information was provided by Mobil: both companies have faced pressure in the U.S., where they are based, concerning corporate responsibility in Nigeria. Elf, headquartered in France, answered most of our questions, though it avoided some, without giving much detail or taking the opportunity to provide background information on its operations; while Agip, an Italian state-owned company, provided an uninformative two page general response to our inquiries and failed to answer many questions. The difficulty that Human Rights Watch, a well known international organization with access to the press worldwide, has had in getting several of the oil companies to pay attention to its concerns appears to be representative of their response to local communities.

In many cases, even where they did respond in connection with particular incidents, companies denied knowledge of government attacks on individuals protesting company action or inaction, or sought to justify security force measures as appropriate responses to threats to company personnel or property. Most of the companies cited in the report failed publicly to criticize security force abuses related to their operations. There were also cases in which witnesses reported that company staff directly threatened, or were present when security force officers threatened communities with retaliation if there were disruption to oil production.

The Role and Responsibilities of the International Oil Companies

The multinational oil companies operating in Nigeria face a difficult political and economic environment, both nationally and at the level of the oil producing communities where their facilities are located. Successive governments have misspent the oil wealth which the oil companies have helped to unlock, salting it away in foreign bank accounts rather than investing in education, health, and other social investment, and mismanaging the national economy to the point of collapse. At the same time, the government has in the past failed to fund its share of the joint ventures operated by the multinationals, and has played the different oil companies against each other so that it has not been easy—even for Shell, the industry giant—to insist that the government contribute towards the investment needed to keep the industry functioning. At the community level, the companies are faced with increasing protests directed at oil company activities and the lack of development in the delta; these have included incidents of hostage-taking, closures of flow stations, sabotage, and intimidation of staff. While the political environment has improved for the oil majors with the death of General Abacha and the succession to the presidency of Gen. Abdulsalami Abubakar, it is unclear what the position will be with the scheduled inauguration of a civilian government in June 1999, and unlikely that relations between the multinationals and the Nigerian government, military or civilian, will ever be entirely smooth.

Acknowledging the difficult context of oil operations in Nigeria does not, however, absolve the oil companies from a share of responsibility for the human rights abuses taking place in the Niger Delta: whether by action or omission they play a role.

In countries characterized by severe human rights violations, like Nigeria, corporations often justify their presence by arguing that their operations will enhance respect for rights, but then adopt no substantive measures to achieve that end. Corporations doing business in these states take on a special obligation to implement proactive steps to promote respect for rights and to ensure that they do not become complicit in violations. The dominant position of the oil companies in Nigeria brings with it a special responsibility in this regard to monitor and promote respect for human rights. Given the overwhelming role of oil in the Nigerian national economy, the policies and practices of the oil companies are important factors in the decision making of the Nigerian government. Because the oil companies are operating joint ventures with the government they have constant opportunities to influence government policy, including with respect to the provision of security for the oil facilities and other issues in the oil producing regions. All the oil companies operating in Nigeria share this responsibility to promote respect for human rights.

In addition to these general responsibilities, the oil companies operating in Nigeria have specific responsibilities in respect of the human rights violations that take place in connection with their operations. These responsibilities must be seen against the context of oil production in Nigeria and the fact that the security provided to keep the oil flowing benefits both the Nigerian government and the oil companies, since disputes which threaten production affect the revenue of both.

Many of the cases investigated by Human Rights Watch which have led to security force abuses concern claims that oil companies have not abided by environmental standards or provided compensation in accordance with the law for damage resulting from oil exploration and production. Other cases concern claims that the oil multinationals have not provided compensation which community members believe to be due to the traditional landholders, although the realities of the Nigerian legal system make it difficult to establish or enforce such an obligation. Often, the Nigerian government effectively entrusts the oil companies themselves to provide the facts on such matters as land claims and valuation, environmental impact assessments, agreed terms of compensation for property and labor, assessment of sabotage, and damage claims. Most negotiations for compensation are bilateral, between the community affected and the oil company concerned, although government structures may play a nominal monitoring role. The process of valuation, negotiation, and payment is therefore in practice controlled almost entirely by the company. The affected communities are in an unequal bargaining position, largely obliged to accept whatever compensation is offered by the companies in such situations. Although there are independent lawyers and environmental groups attempting to monitor oil company compliance with the law and assist the oil communities in pressing their claims, their activities have in the past been seriously hindered by security force harassment, office raids, detentions, and other repressive measures.

Oil companies are legitimately concerned to prevent damage to their facilities and to the environment and to protect their personnel. Security arrangements between the oil companies and the Nigerian government are inevitable, as are internal oil company provisions for security responses in the event of incidents of hostage taking, sabotage, or intimidation. At the same time, the companies emphasize their commitment to avoid violent confrontations between community members and security forces, while underlining a legal obligation to inform the Nigerian authorities when there is a threat to oil production.

However, Human Rights Watch is concerned at the level of secrecy that surrounds the arrangements relating to security for oil installations: not one of the oil companies with which we corresponded responded to our requests to be given access to the parts of the Memorandum of Understanding or Joint Operations Agreement with the Nigerian government governing security, nor to internal guidelines relating to protection of their facilities. Given the abuses that have been committed by the Nigerian security forces in protecting oil installations, most notoriously in Ogoni, it is all the more important that there be transparency in these arrangements and clear commitments from the oil companies to monitor security force performance related to their operations, take steps to prevent abuses, andpublicly protest violations that do occur. Yet none of the oil companies publish regular, comprehensive reports of allegations of environmental damage, sabotage, claims for compensation, protest actions, or police or military action carried out on or near their facilities. Often, based on Human Rights Watch's correspondence, the companies claim to be unaware that arrests, detentions and beatings have taken place in the vicinity of their facilities, despite assertions that they are concerned to maintain good relations with the communities where they operate.

Human Rights Watch believes that the oil companies have responsibilities to monitor security force activity in the oil producing region in detail and to take all possible steps to ensure that human rights violations are not committed. These responsibilities are reinforced when the company has itself called for security force intervention, especially by the military or by notoriously abusive forces such as the Mobile Police, or if the company has made payments to the security forces in return for protection. In particular, Human Rights Watch recommends that:

· Companies should include in written agreements with the Nigerian government relating to the regulation of the oil industry, especially any agreements relating specifically to security, provisions requiring state security forces operating in the area of company operations to conform to the human rights obligations the government has assumed under the International Covenant on Civil and Political Rights, the African Charter on Human and Peoples' Rights and other international human rights and humanitarian norms.

· Companies should make public the provisions of their security agreements with state entities and private organizations.

· Companies should insist on screening security force members assigned for their protection, to ensure that no member of the military or police credibly implicated in past human rights abuses is engaged in protecting oil facilities. Companies should similarly screen security staff in their direct employment.

· Companies should investigate abuses that do occur, and make public and private protests to the authorities where excessive force is used, or where arbitrary detentions or other abuses take place. Companies should publish details of such incidents in their annual reports both in Nigeria and in the country of their head office.

· Companies should publicly and privately call on the Nigerian authorities to institute disciplinary or criminal proceedings, as appropriate, against those responsible for abuses and to compensate the victims. Companies should monitor the status of such investigations and press for resolution of the cases, publicly condemning undue delay.

· Companies should adopt internal guidelines surrounding the provision of security for their facilities, emphasizing the need to ensure respect for human rights, and should take disciplinary action against any employee that does not follow such guidelines.

The following sections summarise the background to human rights abuses in the delta, and give examples of particular incidents in which companies have failed to take these steps.

The Oil Industry and the Oil Producing Communities

Nigeria is the largest oil producer in Africa, and the fifth largest in the Organization of Petroleum Exporting Countries (OPEC). The discovery of oil has transformed Nigeria's political economy, and oil has for the past two decades provided approximately 90 percent of foreign exchange earnings, and 80 percent of federal revenue. Nigeria also has huge reserves of natural gas, yet to be fully exploited. Yet, instead of turning Nigeria into one of the most prosperous states on the African continent, these natural resources have enriched a small minority while the vast majority have become increasingly impoverished: with a per capita gross national product of only U.S.$260 a year, Nigeria is one of the poorest countries in the world. At the same time, the struggle among the elite to gain access to the profits of the oil boom has been a factor in the rule of successive military governments: since independence in 1960, Nigeria has enjoyed only ten years of civilian rule, though the current military regime has committed itself to leave office in May 1999. While minority ethnic groups in Nigeria's multi-ethnic federation have successfully demanded that new states and local government units be carved out to fulfil their hopes of receiving some benefit from the oil money and to compensate for the damage done by oil production, the Nigerian federation has in practice, paradoxically, become ever more centralized and power and money has been concentrated in the hands of fewer and fewer people. Politics has become an exercise in organized corruption; a corruption perhaps most spectacularly demonstrated around the oil industry itself, where large commissions and percentage cuts of contracts have enabled individual soldiers and politicians to amass huge fortunes.

The first discovery of commercial quantities of oil in Nigeria was in 1956; today, the country produces approximately two million barrels per day (bpd) of crude oil. Estimates of Nigeria's oil reserves vary from sixteen to twenty-two billion barrels, mostly found in small fields in the coastal areas of the Niger Delta. According to the Nigerian constitution, all minerals, oil, and gas belong to the Nigerian federal government, which negotiates the terms of oil production withinternational oil companies. Most exploration and production activities in Nigeria are carried out by European and U.S. oil companies operating joint ventures in which the Nigerian National Petroleum Corporation (NNPC), the state oil company, owns 55 or 60 percent; more recent contracts relating to offshore fields have been structured rather as "production sharing contracts" in which the government is not a formal partner. Shell operates a joint venture that produces close to one half of Nigeria's crude production; Mobil, Chevron, Elf, Agip, and Texaco operate other joint ventures, and a range of international and national oil companies operate smaller concessions.

Oil production has had damaging effects on the environment of the oil producing region, though the extent of the damage is subject to dispute. The Niger Delta is one of the world's largest wetlands, and

the largest in Africa: it encompasses over 20,000 square kilometers, of which perhaps 6,000 square kilometers is mangrove forest, and has the high biodiversity typical of extensive swamp and forest areas, with many unique species of plants and animals. Despite decades of oil production, there is surprisingly little good quality independent scientific data on the overall or long-term effects of hydrocarbon pollution on the Delta, yet oil-led development has clearly seriously damaged the environment and the livelihood of many of those living in the oil producing communities. The oil companies operating in Nigeria maintain that their activities are conducted to the highest environmental standards; but Nigerian environmental laws, in most respects comparable to their international equivalents, are poorly enforced.

Occasional large oil spills kill fish and agricultural crops, and pollute water, with serious effects for the communities and families affected, especially on dry land or in freshwater swamp zones where spills are contained in a small area. The long-term effect of these major pollution incidents, regular small spills, and effluent deliberately discharged to the environment is largely unevaluated. Poorly designed causeways and canals used by the oil industry affect the hydrology of the seasonally flooded freshwater swamp and the brackish water of the mangrove forest, again killing off crops, destroying fishing grounds, and damaging drinking water supplies. Compensation for such damage is inadequate, and—in the absence of a properly functioning court system—there is no effective recourse to an independent arbiter to determine the value of the damaged property. The oil companies state that many spills are caused by sabotage, and, in accordance with Nigerian law, they pay no compensation in such cases; but the determination that sabotage has occurred is largely left in their own hands, increasing the chances of injustice. At the same time, in an area of Nigeria where there is great pressure on cultivable and habitable land, land is expropriated for oil production under laws which allow no effective due process protections for landholders and onlyinadequate compensation for the loss of livelihood of those affected. Although the amount of land used for oil production is small, by comparison with the total area of the Niger Delta, the effect on individual landholders can be devastating. The Niger Delta clearly faces many environmental problems that are not the direct responsibility of the oil industry, but these distinctions are irrelevant to those who have their land confiscated or polluted, without receiving compensation to the value of the benefit lost.

While the people of the Niger Delta have faced the adverse effects of oil extraction, they have in general also failed to gain from the oil wealth. The people living in the oil producing communities largely belong to ethnic groups other than the three major groups in Nigeria (Hausa-Fulani, Yoruba, and Igbo), and speak a diverse range of languages and dialects; the largest of these groups are the Ijaw, who collectively form Nigeria's fourth largest ethnic group. Since the creation of the Nigerian state by the British, the peoples of the delta have complained of marginalization by the regional and federal governments who have ruled their affairs. Despite the vast wealth produced from the oil found under the delta, the region remains poorer than the national average; and though in the north of Nigeria poverty is more extreme, the divisions between rich and poor are more obvious in the areas where gas flares light up the night sky.

Nevertheless, oil production itself and oil-based industrial expansion have transformed the local economy, and some in the oil producing communities have benefitted greatly from oil production. Those with full time employment in the oil industry are paid high wages for skilled work, but they are a well-paid minority surrounded by a mass of un- or underemployed; most do not come from the oil producing communities in any event. Contractors to the oil industry, often traditional leaders or those with close links to the military administrations of the oil producing states, also potentially make large amounts of money, often increased by the widescale corruption surrounding the award of contracts for construction and other oil industry projects—from which those in the oil companies in charge of the choice of contractor also benefit. Development spending by the oil companies has also brought schools, clinics, and other infrastructure to remote parts of the country that might otherwise be far more marginalized by the Nigerian government; but many of these projects are inappropriate for the needs of the communities where they are sited, and others are incomplete or shoddily carried out. Although a minority of politicians, traditional leaders and contractors have become rich on the spoils of oil, and hence support the oil industry's activities, the great majority of people from the minority ethnic groups of the oil producing areas have remained impoverished; at the same time, the potential benefits of links to theoil industry have exacerbated conflicts within and among the oil producing communities.

Protest and Repression in the Oil Producing Communities

Anger at the inequities attributed to the oil economy has led increasing numbers of people from the communities in the oil regions to protest the exploitation of what they see as "their" oil—though the constitution provides that all oil is owned by the federal government—without benefit to them or compensation for the damage done to their land and livelihoods. These protests, mostly disorganized and localized, hit the international news headlines during the early 1990s, when the Movement for the Survival of the Ogoni People (MOSOP), led by well-known author Ken Saro-Wiwa, successfully mobilized tens of thousands of Ogonis, an ethnic group of just half a million people occupying a small part of the oil producing region, to protest at the policies of the federal government in relation to the oil wealth, and at the activities of Shell, the oil company that produces almost half of Nigeria's oil. In 1993, Shell was forced to close its production in Ogoni following mass protests at its facilities, citing intimidation of its staff, and the flowstations there remain closed until today, though active pipelines still cross the region. MOSOP's protests provoked a violent and repressive response from the federal government, for which any threat to oil production is a threat to the entire existing political system. Thousands of Ogonis were detained or beaten by the Rivers State Internal Security Task Force, a military body specifically created to suppress the protests organized by MOSOP, and hundreds were summarily executed over a period of several years. In 1994, Ken Saro-Wiwa and several others were arrested in connection with the murder of four traditional leaders in Ogoni. On November 10, 1995, Saro-Wiwa and eight other MOSOP activists were hanged by the military government for those murders, after a trial before a tribunal which blatantly violated international standards of due process and produced no credible evidence that he or the others were involved in the killings for which they were convicted.

Since 1995, no organization has emerged with the cohesion and dynamism of MOSOP, yet protests aimed at oil production take place on a regular basis, and the memory of Ken Saro-Wiwa is respected across the delta. The great majority of these protests are not organized by well-known leadership figures or by recognized political groupings, but by local community members. Many of these protests are never reported, even in the Nigerian national press: only when there is a threat to oil production is reporting guaranteed. Community members demand compensation for use of their land or for oil spills or other environmental damage, employment in oil industry projects, or development projects for their villages. Many protests are aimed at the government as well as the oil companies and relate to claims for a greater part of the revenue derived from oil to be spent in the oil producing region. Sometimes these demands are made by individuals or families in respect of their own land, sometimes youths who feel excluded from the political system and the benefits of oil wealth organize together and successfully halt production at flow stations in their areas, or prevent construction work going ahead, until the international oil companies have satisfied their demands, or part of them. Sometimes these demands are made by individuals or families in respect of their own land. In other cases, youths who feel excluded from the political system and the benefits of oil wealth join together and successfully halt production at flow stations in their areas, or prevent construction work going ahead, until the international oil companies have satisfied their demands, or part of them. On some occasions there has been damage to property, theft, or intimidation of oil company or contractor staff. Sabotage of oil pipelines does occur, though its extent is disputed between the companies and the communities. Incidents of hostage-taking have recently increased, with some of these cases involving attempts to extort money from the oil companies.

In the face of the threat to oil production caused by some of these protests, the Nigerian government has created a number of special task forces handling security in the oil producing areas, of which the most notorious and brutal is the Rivers State Internal Security Task Force, created in response to the Ogoni crisis. Like many other states, those in the delta have also created anti-crime task forces: Operation Flush in Rivers State and Operation Salvage in Bayelsa state have been active in the oil regions. The paramilitary Mobile Police, deployed throughout Nigeria, are also active in the delta; and on occasion, the navy is used to maintain order in the riverine areas. From their side, the oil companies operating in Nigeria hire "supernumerary police," recruited and trained by the Nigerian police force, but paid for by the oil companies. They are supposed to operate only within the perimeter fence of oil facilities. Some of these police are armed, though Shell states that most working on its behalf are not; some operate in plain clothes. In addition, the oil companies state that they hire private firms for routine security provision at

entrance barriers and other duties at their premises; and local "guards" hired from among landholders across whose land pipelines run or where other facilities are built.

Nigeria's new head of state, Gen. Abdulsalami Abubakar, has greatly reduced the repression enforced by his predecessor, Gen. Sani Abacha, who died in June 1998, releasing many political prisoners and relaxing restrictions on freedom of expression, assembly and association throughout Nigeria. The government has withdrawn the Internal Security Task Force from Ogoni. Many Ogoni exiles havebeen able to return, and MOSOP has been able to hold rallies once again. Nevertheless, the response of the security forces to threats to oil production continues to be heavy handed, and in the oil regions human and environmental rights activists report little change. On December 30, 1998, soldiers shot dead at least seven youths protesting in Yenagoa, the capital of Bayelsa State; the following morning, eight others were reported killed, and over the following days a crackdown continued that was still ongoing as this report went to press.

In virtually every community, there have been occasions on which the paramilitary Mobile Police, the regular police, or the army, have beaten, detained, or even killed those involved in protests, peaceful or otherwise, or individuals who have called for compensation for oil damage, whether youths, women, children, or traditional leaders. In some cases, members of the community are beaten or detained indiscriminately, irrespective of their role in any protest. Under the government of General Abacha, activists from human and environmental organizations, especially from political movements attempting to organize resistance to oil company abuses, faced regular harassment from the authorities. While this situation has eased in recent months, the decrees are still in force that allow detention without trial and establish special tribunals to try cases of "civil disturbances" or sabotage without due process protections.

Human Rights Watch investigated a number of cases of protest against oil company activity that have taken place since the 1995 trial and execution of Ken Saro-Wiwa and his eight codefendants, during a one-month visit to the Niger Delta during July 1997 and in subsequent research. The cases we investigated can be grouped under two broad thematic headings. On the one hand, there are those incidents where community members have claimed that operations of oil companies have damaged the material interests of the peoples of the areas in which they operate and have not compensated fully for that damage. The incidents involve disputes over legal obligations to provide compensation for claims of damage, for encroachment on community land or waters, or for access rights, though claims are often couched in terms of community rights to a "fair share" of the oil wealth derived from their land. Accordingly, community members have made demands for compensation for oil company activities, whether in the form of cash payments following spillages or land expropriation, development projects in communities close to oil installations, or employment of local community members as casual laborers when work is being carried out in the vicinity. On the other, there are cases of harassment and apparently untargeted assaults upon community members that are a general consequence of the deployment of security personnel to provide protection for oil operations.

In the worst cases, people have been killed by the paramilitary Mobile Police or other security responding to threats to oil production. In May 1998, two youths were killed on Chevron's Parabe Platform, off Ondo State, by members of the security forces transported to the platform by Chevron to remove two hundred protesters who had closed down production. The protesters had demanded compensation for environmental damage caused by canals cut for Chevron which opened local waterways to the sea. Frequently, protesters are beaten and arbitrarily detained, for periods ranging from hours to weeks or months; sometimes individuals are detained who simply go to oil company or contractors' premises asking for compensation for works being carried out. In one case in 1997, landholders interviewed by Human Rights Watch had been detained overnight and released without charge following a spill on their land which Elf alleged had been caused by sabotage. They had apparently been held on suspicion that they had caused the sabotage despite the lack of evidence to this effect and the uncompensated damage caused to their crops. Following a major Mobil oil spill in January 1998, up to three hundred people who demanded compensation were reportedly detained; in July, further protests over damage done by the spill and delays in compensation payments led to disturbances in which eleven people were reportedly shot dead by police. As this report went to press, the fatal shooting of tens of Ijaw youths calling for the oil companies to withdraw from Nigeria was reported, together

with the deployment of thousands of troops to the Niger Delta region.

The Role of Shell in the Ogoni Crisis

The role of Shell in Nigeria has received by far the most attention internationally, for three reasons: first, because it is the biggest oil producer in Nigeria with the longest history, dominating the industry for as long as oil has been produced and in the early days enjoying a monopoly and a privileged relationship with government; secondly, because Shell's facilities are largely onshore, in or near inhabited areas and thus exposed to community protests; and thirdly, because it formed the main target of the campaign by MOSOP, which accused the company of complicity in what it alleged was the genocide of the Ogoni people.

During the height of the Ogoni crisis, allegations of Shell collaboration with the military were regularly made, even after the company ceased production from its flow stations in Ogoni in January 1993. A document alleged to be a leaked government memorandum from 1994 implicated Shell in planned "wasting operations" by the Rivers State Internal Security Task Force, stating that the oil companies should pay the costs of the operations. The head of the Task Force several times publicly claimed to be acting so that Shell's oil production couldresume. Former Ogoni members of the Shell police have claimed that they were involved in deliberately creating conflict between different groups of people, and in intimidating and harassing protesters during the height of the MOSOP protests in 1993 and 1994; Ogoni detainees have also alleged that they were detained and beaten by Shell police during the same period. Nigerian environmental and human rights activists in the delta also allege that Shell (and other companies) continue to make payments of field allowances to soldiers deployed to its facilities.

Shell has denied all such allegations, and distanced itself from statements by government or security officials calling for repressive responses to protests, while stating that the company had repeatedly expressed its concerns "over the violence and heavy handedness both sides on the Ogoni issue have displayed from time to time." Shell also denied any collusion with the authorities. However, Shell has since admitted having made direct payments to the Nigerian security forces, on at least one occasion in 1993, under duress. Under great public pressure, both inside and outside Nigeria, to intervene on behalf of the accused during the trial and following the conviction of the "Ogoni Nine," Shell wrote to Gen. Abacha pleading for commutation of the death sentences against Ken Saro-Wiwa and his co-accused on humanitarian grounds, but did not make any comment on the unfairness of their trial.

Shell states that its production in Ogoni remains closed, but that it has made attempts to open negotiations with the communities involved in order to resume production, and to undertake development projects aimed at resolving some of the problems faced by the Ogoni. Community members, on the other hand, reported that, while it was still deployed, the Rivers State Internal Security Task Force forced individuals to sign statements "inviting" Shell to return. Shell has also stated at various times over the last few years that it has opened negotiations with MOSOP representatives, though spokespeople for MOSOP have denied this, and challenged Shell's statements that its presence in Ogoni is limited to provision of social programs and attempts to arrange a reconciliation with the Ogoni people, claiming that Shell staff have on occasion entered Ogoni with security force protection to work on pipelines. MOSOP remains opposed to the reopening of Shell's production in Ogoni, stating that the company should "clean up or clear out" by Ogoni Day, January 4, 2000.

Attempts to Import Weapons

During 1996, newspaper investigations revealed that Shell had recently been in negotiation for the import of arms for use by the Nigerian police. In January 1996, in response to these allegations, Shell stated that it had in the past imported side arms on behalf of the Nigerian police force, for use by the "supernumerary police" who are on attachment to Shell and guard the company's facilities (and other oil company facilities) against general crime. The last purchase of weapons by Shell was said to be of 107 hand guns for its supernumerary police, fifteen years before. But court papers filed in Lagos in July 1995 and reported in the British press in February 1996 revealed that Shell had as late as February 1995 been negotiating for the purchase of weapons for the Nigerian police. Shell acknowledged that it had conducted these negotiations but stated that none of the purchases had been concluded. However, the

company stated to Human Rights Watch that it "cannot give an undertaking not to provide weapons in the future, as, due to the deteriorating security situation in Nigeria, we may want to see the weapons currently used by the Police who protect Shell people and property upgraded."

Threats to Community Members

During its investigation of the situation in the delta during July 1997, Human Rights Watch heard disturbing allegations of three separate meetings, two in connection with the same matter, at which eyewitnesses interviewed by Human Rights Watch alleged that Shell staff, or military authorities in the presence of Shell staff had directly threatened community members, using the situation in Ogoni as an example. Two of these meetings had occurred only days before Human Rights Watch interviewed the people present; the third dated back two years, to the period of Ken Saro-Wiwa's trial. In another case, a youth was assaulted by Mobile Police at Elf's Obite gas project, and then threatened by a manager with C&C Construction, a contractor working at the project owned by the Lebanese Chagoury family, which was close to General Abacha. When he refused to withdraw a legal complaint he brought for the assault, despite recommendations that he should "learn the lessons from the Saro-Wiwa trial," armed men from the State Security Service came to look for him, and he fled several days later to Togo. Since returning to Nigeria several months later, he has been detained several times.

Oil Company Failure to Monitor or Protest Abuses

The most serious case in which an oil company is directly implicated in security force abuses continues to be the incident at Umuechem in 1990, where a Shell manager made a written and explicit request for protection from the Mobile Police (a notoriously abusive force), leading to the killing of eighty unarmed civilians and the destruction of hundreds of homes. Shell states that it has learned from the "regrettable and tragic" incident at Umuechem, so that it would now never call for Mobile Police protection and emphasizes the need for restraint to the Nigerian authorities. Nevertheless, in several of the incidents investigated by Human Rights Watch, oil companies, including Shell, or their contractors, called for security force protection in the face of protests from youths, taking no steps to ensure that such protection was provided in a non-abusive way and making no protests when violations occurred.

In July 1997, youths from Edagberi, Rivers State, for example, were detained overnight following a written complaint to the local police station by Alcon Engineering, a contractor to Shell. While it is claimed by Shell that the youths concerned had been engaged in the intimidation of its contractor, and therefore that security force intervention was appropriate, no safeguards were sought to ensure that such intervention was made in a non-abusive manner. Similarly, at Yenezue-Gene, Rivers State, where Shell faces community hostility caused by the construction of a causeway to its Gbaran oil field which had devastated a forest area of great economic importance to local residents, soldiers present at the site had harassed local community members during 1996 and 1997. Shell stated to Human Rights Watch that its contractors had called for police (though not army) assistance, "due to community hostilities." Shell did not report, in response to Human Rights Watch inquiries, that any guarantees had been sought for the good behavior of these police; the company was also unaware of reports of abusive behavior by security forces that community members stated had been made to local Shell personnel.

In an August 1995 incident at Iko, Akwa Ibom State, a community where a defective flare (used to burn off gas released at a well-head) had caused significant damage, Shell's contractor Western Geophysical stated that it had requested naval assistance to recover boats taken by youths who wanted to obtain benefits from the contractor, including employment. Following the naval intervention, Mobile Police came to the village and assaulted numerous villagers, beating to death a teacher who had acted as an interpreter in negotiations between Western Geophysical and the community. Shell has stated to Human Rights Watch that it does not call for military protection, but justified calling the navy in this case due to the terrain; it stated that the Mobile Police had been called by the navy and not by Shell or itscontractor. In its detailed response Shell did not report that the company or its contractor had made any attempt to protest the Mobile Police action, simply reporting that "this incident is unrelated to Western's seismic activities."

In May 1998, when Chevron's Parabe platform was occupied by approximately 200 youths and

production shut down, Chevron acknowledged that it had called for navy intervention, and that the company had flown the navy and Mobile Police to the platform. Despite the serious result of this action, including the shooting dead of two protesters whom it admitted were unarmed, Chevron did not indicate, in response to inquiries from Human Rights Watch, that any attempt had been made to prevent abusive actions by the security forces in advance of the confrontation. Nor did it state that concern had been expressed to the authorities over the incident or that any steps would be taken to avoid similar incidents in future. Chevron's response concerning an earlier case involving a Chevron facility in which a youth was killed by Mobile Police in July 1997 at Opuama, Bayelsa State, similarly included nothing to indicate that it had raised human rights concerns with the authorities over the incident.

Calling for security force protection increases the responsibility of the oil company to ensure that intervention does not result in human rights violations; but even if the security forces have acted on their behalf without a specific company request for assistance companies cannot be indifferent to resulting abuse. Yet in the great majority of cases the oil companies do not report any attempt to monitor or protest human rights violations by the security forces against those who have raised concerns about environmental problems, requested financial compensation or employment, protested oil company activity, or threatened oil production. In a handful of high-profile cases of detention, one or two oil companies have, under consumer pressure in Europe and the U.S., made public statements, but the great majority go unremarked. In none of the cases of abuse researched by Human Rights Watch which had not reached the international press did any of the oil companies indicate that they had registered concern with the authorities. In the cases reviewed, it was generally only after the behavior of the Nigerian authorities had embarrassed the oil companies on the international stage that action of any kind ensued on behalf of those who were abused by the security forces. In other cases, the oil companies said they were ignorant of arrests or beatings that had occurred, although some concerned quite major incidents at their facilities.

Shell, for example, denied knowledge of detentions that took place following major disturbances during June and July 1995 at Egbema, Imo State, during which Mobile Police carried out indiscriminate beatings and arrested more than thirty people, detaining them for several weeks without trial, before releasing them on bail charged with sabotage. Instead, Shell stated that the disputes at that time hadbeen "amicably settled," through negotiations between the community and the military administration. Elf denied to Human Rights Watch that it knew of the beating and detention of an activist at its Obite gas project in October 1998. Agip, when asked about the case of a youth beaten to death by security guards at its Clough Creek flow station, near Egbemo-Angalabiri, did not even respond to community representations nor to inquiries from Human Rights Watch. When several hundred people were arrested following demonstrations over a January 12, 1998 spill from an offshore pipeline near its Qua Iboe terminal, Mobil did publicly distance itself from the arrests, but did not indicate that any protests had been made to the authorities, stating to reporters in Lagos: "It is a security issue. It is nothing to do with Mobil at all."

Shell's Internal Review Since 1995

Since the international focus on its Nigerian holdings in 1995, the Royal Dutch/Shell group has undertaken a major review of its attitude toward communities and issues of human rights and sustainable development. No other oil company operating in Nigeria has, so far as Human Rights Watch is aware, announced any similar review of its policies and practices as a they relate to human rights violations committed in connection with oil company operations. While we welcome this introspection, the test of its effectiveness in changing Shell's practice can only be gauged by its performance on the ground in countries like Nigeria. It is too soon to tell whether this performance will be changed.

Conclusion

There can be no solution to the simmering conflict in the oil producing areas of the delta until its people gain the right to participate in their own governance and until the protection of the rule of law is extended to their communities. The injustices facing the peoples of the delta are in many ways the same as those facing all Nigerians after decades of rule by successive military regimes, yet in the oil producing regions the suppression of political activity, the lack of legal redress for damage to the

environment and the resulting loss of livelihood, and the sheer ubiquity of human rights abuses by the region's security forces have generated greater protest, in turn generating greater repression. While the death of General Abacha and the succession of General Abubakar has recently improved respect for human rights and fundamental freedoms in Nigeria, the situation in the delta remains fundamentally unchanged—as the recent escalation of protest actions has demonstrated.

The first responsibility for resolving these injustices lies with the Nigerian government. Yet the multinational oil companies operating in Nigeria cannot avoidtheir own share of responsibility. It is not enough simply to say that the political environment in Nigeria is as difficult for the oil companies as it is for anyone else, and that the oil industry does not have the power to alter government policy towards the oil regions: the oil companies in many respects contribute towards the discontent in the delta and to conflict within and between communities that results in repressive government responses. The oil companies must take all steps to ensure that oil production does not continue at the cost of their host communities simply because of the threat or actual use of force against those who protest their activities. There is an ever-growing likelihood that, unless corrective action is taken, protest in the oil areas will become violent in an organized and concerted way, with consequent reprisals and an ever-worsening security situation that will harm all those with interests in the delta region, whether residents or companies.

PAGE < TOC PAGE >

Corporations and Human Rights

Recent Human Rights Violations In Nigeria's Oil Producing Region (February 23, 1999)

Oil Companies Complicit in Nigerian Abuses, HRW Press Release, February 23, 1999

The Price Of Oil Corporate Responsibility and Human Rights Violations in Nigeria's Oil Producing Communities, Human Rights Watch Report, February 23, 1999

Human Rights Watch World Report 1999

Resources and Campaigns: Corporations and Human Rights

In late December 1998 and early January 1999, a military crackdown in the Niger Delta area led to the deaths of several tens of people, the torture and inhuman treatment of others, and the detention of more, many of whom are still held in police custody. These abuses took place as a response to demonstrations held by Ijaw youths in Yenagoa, the capital of Bayelsa State, and Kaiama, a community an hour away by road.

On December 11, 1998, youths hold a meeting at Kaiama, Bayelsa State, form the Ijaw Youth Council (IYC) and adopt a declaration, which stated that "All land and natural resources (including mineral resources) within the Ijaw territory belong to Ijaw communities and are the basis for our survival." Accordingly, "We demand the immediate withdrawal from Ijawland of all military forces of occupation and repression by the Nigerian state. Any oil company that employs the services of the armed forces of the Nigerian state to 'protect' its operations will be viewed as an enemy of the Ijaw people." The youths advised "all oil companies staff and contractors to withdraw from Ijaw territories by the 30th December 1998, pending the resolution of the issue of resource ownership and control in the Ijaw area of the Niger Delta."

In anticipation of the deadline, several thousand troops were moved into the Ijaw areas of Bayelsa and Delta states. On December 30, youths supporting the Kaiama Declaration demonstrated peacefully in Yenagoa and in other communities across the Ijaw areas of the delta. In Bomadi, Delta State, the military administrator attended the demonstration. In Yenagoa, however, a peaceful procession was met with force. Up to 2,000 youths holding candles and dressed in

Eyewitness Testimonies

Developments At a Glance

December 11, 1998: Youth gathering at Kaiama, Bayelsa State. Ijaw Youth Council (IYC) formed and a Kaiama declaration adopted.

The youths advised "all oil companies staff and contractors to withdraw from Ijaw territories by the 30th December 1998, pending the resolution of the issue of resource ownership and control in the Ijaw area of the Niger Delta."

On December 30,1998 Supporters of the Kaiama Declaration demonstrated peacefully in Yenagoa and in other communities across the Ijaw areas of the delta.

December 31, 1998: Confrontation at Mbiama junction. Soldiers fired on the youths, killing several and injuring others.

Three truck loads of soldiers went to Kaiama on January 2, 1999 where they carried out reprisals (for deaths of two soldiers) over the next few days.

Sixty-seven people were kept in the burning sun for three days, with no water for a large part of that time, and were severely and repeatedly beaten by the soldiers.

On January 4, 1999, Opia and Ikenyan, two small communities were attacked by about 100 armed soldiers using boats and a helicopter owned by Chevron.

There have been other recent attacks by soldiers on communities in the delta area in recent weeks. Up to nineteen people were reportedly killed by soldiers based at Shell's

soldiers based at Shell's Forcados terminal on the Atlantic coast.

black met early in the morning and processed along the main street. According to eyewitnesses they were peaceful and unarmed. As they approached the entrance to government house, the base of the military administrator of Bayelsa State, Lt. Col. Paul Obi, soldiers posted at the gate fired on the demonstrators. Several were injured and, according to witnesses, one killed during the firing. Others were arrested and taken to the police station. Later in the day, at least three other youths were killed in a further confrontation with soldiers under the command of a Major Oputa.

The next day, youths who had heard of these killings marched towards Yenagoa from Kaiama and other nearby communities. There was a confrontation at Mbiama junction, where the road divides to lead to Yenagoa or Kaiama, and soldiers fired on the youths, killing several and injuring others. An army truck was set on fire on the bridge at Kaiama. One group of youths came past the junction into Yenagoa, and were met by soldiers again at the motor park, and again a number were killed and injured when soldiers fired without warning. Most of these youths were unarmed, but eyewitnesses reported that ten youths armed with rifles came right into Yenagoa and exchanged fire with soldiers, with no casualties; eventually the youths retreated. At least one person not involved in the confrontation was reportedly shot dead by soldiers at this time. Over the next few days, soldiers were stopping youths and checking them for marks indicating they supported "Egbesu," a traditional Ijaw god. Many were beaten severely at road blocks, some were killed. Others were detained.

In Yenagoa, to this day, tens of soldiers and mobile police posted to the small community are continuing to harass local people. In the "black market" slum area, soldiers and mobile police are continuing to rape local women, dragging them from their shacks at night, and threatening them and their husbands with violence if they do not comply. Several tens remain in detention in Port Harcourt, Warri

and Yenagoa to date: several of those injured in the shooting at government house are being kept under surveillance in hospital in Yenagoa.

During the confrontation along the road between Kaiama and Yenagoa, two soldiers were allegedly killed by youths. In retaliation, three truck loads of soldiers went to Kaiama on January 2, where they carried out reprisals for these deaths over the next few days. As the troops came into the village, most people fled, but some were found in their homes and beaten. Houses were ransacked and valuable property and money taken; others were set fire. Women were raped. At least two were shot dead as they tried to escape; others are missing and it is not known if they fled or were killed.

Sixty-seven people were eventually taken to the motor park, among them the traditional leader of the area, Chief Sergeant Afuniama, and several of his advisers, as well as the Anglican priest in Kaiama. These people were kept in the burning sun for three days, with no water for a large part of that time, and were severely and repeatedly beaten by the soldiers. Two of them had parts of their ears cut off with knives; many received matchet (machete) wounds to their heads, or were cut with broken bottles. Most appalling of all, Chief Afuniama was beaten to the point of unconsciousness, and was then killed, in full view of the others there, by soldiers who dropped a large rock on his head. His body was left in the open for most of the day, and was then taken away. It was found a day later floating in the water downstream from the village. At least nine other corpses were brought to the motor park and later taken away.

Eventually, on the third day that these people were held in the motorpark, the Military Administrator of Bayelsa State, Lt. Col. Obi, came to Kaiama, and ordered that most of them be released after giving their details to the commissioner of police, who accompanied him; twenty or more were taken to Yenagoa,

where most of the rest were released, and some taken to hospital. Soldiers were withdrawn from Kaiama after about week, and the people who had fled gradually began to return to the community.

On January 4, 1999, Opia and Ikenyan, two small communities of maybe 500 people each in Delta State, Warri North local government area, were attacked by about 100 armed soldiers using boats and a helicopter owned by Chevron. Community members described to Human Rights Watch how a helicopter of the kind they are used to seeing flying on Chevron's operations flew low over the community: at first they thought nothing of it, since there are two Chevron wells within 100 metres of Opia village, but as the helicopter approached the village it started firing down at them. After staying about half an hour at Opia, the helicopter flew to nearby Ikenyan and did the same thing. A short while later soldiers came to first Opia and then Ikenyan in four boats. Three of these boats were "sea trucks" of the type used by Chevron; the fourth was a military boat with a machine gun mounted on it. As the boats came towards the villages the soldiers started firing, killing at least two people in each place, including the traditional leader of Ikenyan who was approaching them to try to negotiate. Fifteen people from Opia and forty-seven from Ikenyan are still missing: the communities do not know if their bodies have been thrown in the river or taken away or if they have fled and not come back. The soldiers torched each village before they left, destroying virtually all the houses; canoes were sunk and other property destroyed.

In correspondence with a committee appointed by the two communities to take up their case, Chevron has stated that it was informed by the soldiers that the raid on the villages was a "counter attack" by soldiers who had been threatened by youths as they guarded a Chevron drilling rig which Chevron staff had evacuated following the Kaiama Declaration. Chevron expressed no regret for what had happened, and no company representatives have visited the community since the events of

January 4. Members of the community state, however, that they know of no such altercation, and have no idea why they were targeted. Chevron facilities in the area were evacuated in advance of the December 30 deadline set by the Kaiama Declaration and soldiers posted to guard them.

There have been other recent attacks by soldiers on communities in the delta area in recent weeks. Up to nineteen people were reportedly killed by soldiers based at Shell's Forcados terminal on the Atlantic coast. There has also been violence between communities close to Agip's Brass terminal, and many soldiers have been posted to the facility. Human Rights Watch has not, however, been able to investigate these incidents.

The following are two testimonies given to Human Rights Watch by eyewitnesses to these events.

Testimony of A, a man of 56, of Kaiama, Bayelsa State

I can only tell you what I saw with my own eyes. At about ten o'clock in the morning on January 2 I was visiting Chief Ajoko. While I was there I saw a crowd running towards us saying soldiers are coming. We turned to go into the next room of the house to decide what to do, and as we turned three soldiers came and called to us to come out. We went out, Chief Ajoko, myself, and two others, and the soldiers told us to lie on the ground. I was kicked in the hip. The soldiers went away and then came back and said we should move with them. As we went we met Milton Pens Arizia, Moses Ogori, Nairobi Finikumo, Chief Geigei and Aklis Ogbugu. We were all taken to the motor park. As we got there they sat us under the fruit tree. Others were just lying down in the gutter. Chief Ajoko was by me. A soldier just came and just used his knife to cut off the bottom of his ear. The soldier took it and told him he should eat it. He refused, and one other soldier told the first "don't do that." They brought four corpses on a wheelbarrow. In

the evening they took them away.

They took us into the motor park, we were 67 when we went in. They put us in three groups and guarded us with soldiers till morning. There were more than 100 soldiers. They told us to take off our shirts. For some time they told us to look up at the sun when it was very high and they beat us if we closed our eyes. They took sand and sprayed it in our eyes. They said we should do some frog jumps. For some years I have had a problem with my right leg which does not bend properly. Up to today I now have pain in my leg because of the frog jumps. They said we should walk on our knees with our hands on our head. Then we had to lie on our back on top of broken bottles and creep along. They also had broken bottles and used them to cut us on our backs. Then they came with matchets [machetes] and told us to sit on the ground looking forward. They cut me on my head, which started bleeding -- my clothes I was wearing that day are still stained with blood. They were beating us all the time for just anything. Chief Sergeant Afuniama, the traditional leader of Kaiama; T.K Owonaro, the deputy chief of Kaiama; Chief Tolumoye Ajoko, traditional leader of Olobiri; and Pereowei Presley Eguruze, the youth president of Kolokuma-Opokuma local government area, were taken outside for "special treatment." When Chief Afuniama was brought back into the park he fell down unconscious. A soldier came and dropped a stone on his head. He released it twice, and he said "The chief is sleeping." This was in the morning. They left his body until the evening and then took it out.

About ten that evening, January 3, another group of soldiers came, and one of them said "have these people taken water and food," and he fetched water for us. Up to that time we had no water. Some were drinking their urine; about four were ready to give up had water not been given to them. The following morning the governor came, with the commissioner of police and the commissioner of health and education, and

said we should be handed over to the police, who then took names and addresses, and then released us. The MilAd [Military Administrator] said nothing about compensation.

Testimony of B, a young man from Opia Community, Warri North Local Government Area, Delta State (translated from the local dialect of Ijaw).

On January 4, we were here in the village. At about 2-3 pm we saw a Chevron helicopter in blue and white colours flying by on the other side of the river, and then flying along the route of the pipeline. We thought it was on a Chevron operation because they normally fly that way. By the time it got to us it was flying very low, and then it started firing at us. We were surprised, we didn't know what to do, and we ran into the bush. After thirty minutes or so the helicopter was gone. Then some of the community members came back and were calling to the others to come back from the bush. We were gathered here on the river side and discussing what had happened when we saw Chevron boats coming towards us carrying soldiers. Three were Chevron sea trucks (two numbers were 221 and 242), the ones they normally use, and the other one was a military boat with a machine gun mounted on it. They were full of soldiers, maybe more than 100 in all. We ran into the bush again but as we were running they started firing, it was so intense I can't describe it, dugu-dugu-dugu-dugu-dugu. As I was running a bullet wounded me on my leg. When we went into the bush we saw a fire in the community, everything burning.

Then we heard the boats leaving, so we came back carefully, crawling to see if it was safe and watching who was around. No one was there, so we called to the others in the bush to come back. We saw two people lying dead on the ground, Kekedu Lawuru, and Timi Okuru, a woman. We started crying, and called to the others to come. But some did not come back: 15 are missing till today. Maybe the bodies are in the river. About

twenty were injured, of which ten or so were from bullet wounds, the rest from branches and stones as they ran into the bush. Almost all the houses were destroyed, burnt to the ground. All our property was destroyed. We had a boat that could carry 40-50 persons which was sunk in the river. All our canoes were destroyed. We have nothing now, no means of livelihood.

Since then Chevron have not visited or come to their wells which are behind the village. Major Joseph Osadolo from Koko came and sympathised with us on January 6 -- we learnt the soldiers who attacked came from the Mandagho military base by Chevron's operation at Escravos -- and he promised the Military Administrator would come to see what had happened. We were told he would come on January 16, and we all gathered here from the communities where we are refugees, but he only went to the local government headquarters at Koko and did not come here. Up to now nobody has come.

Oil Companies Complicit in Nigerian Abuses

Rights Group Urges Oil Firms to Help Prevent Niger Delta Crackdown

(Lagos, February 23, 1999) -- On the eve of Nigeria's presidential elections, multinational oil companies investing in the Niger Delta are failing to respond adequately to serious human rights abuse in that region, Human Rights Watch charged in a report released today.

"The oil companies can't pretend they don't know what's happening all around them. The Nigerian government obviously has the primary responsibility to stop human rights abuse. But the oil companies are directly benefiting from these crude attempts to suppress dissent, and that means they have a duty to try and stop it."

Kenneth Roth
Executive Director of Human Rights Watch

In its eight months in office, the government of Gen. Abdulsalami Abubakar has released many political prisoners and relaxed some restrictions on freedom of expression and assembly. But the 200-page Human Rights Watch report documents how Nigerian security forces are using brutal methods to suppress dissent in the Niger Delta.

"The oil companies can't pretend they don't know what's happening all around them," said Kenneth Roth, executive director of Human Rights Watch, an international monitoring group based in New York. "The Nigerian government obviously has the primary responsibility to stop human rights abuse. But the oil companies are directly benefiting from these crude attempts to suppress dissent, and that means they have a duty to try and stop it." Roth noted that recent events in the Niger Delta, especially the crackdown on Ijaw communities over the New Year's weekend, indicate that the Nigerian government is continuing to use violence to protect the interests of international oil companies.

In one particularly serious incident on January 4, soldiers using a Chevron helicopter and Chevron boats attacked villagers in two small communities in Delta State, Opia and Ikenyan, killing at least four people and burning most of the villages to the ground. More than fifty people are still missing. Chevron has alleged to a committee of survivors of the attack that this was a "counterattack" resulting from a confrontation between local youths and soldiers posted to a Chevron drilling rig. Community members deny that any such confrontation took place. In any event, the soldiers' response was clearly disproportionate and excessive.

"Whoever wins this presidential election will have to cope with growing violence in the Niger Delta," said Roth. "The oil companies and the new government should commit to taking a new approach in the region, one that is based on zero tolerance for human rights abuse by the police and military."

Related Material

SUMMARY of the Price of Oil report
UPDATE on the situation in the Niger Delta
February 23, 1999
The Price Of Oil: Corporate Responsibility and Human Rights Violations in Nigeria's Oil Producing Communities
Human Rights Watch Report
February 1999

HRW Press Releases

State of Emergency Declared in the Niger Delta
December 31, 1998

Roth noted that the presidential campaign has included little serious debate over events in the Niger Delta and the role of the oil companies in human rights abuse there.

In the report, Human Rights Watch describes numerous other incidents in which the Nigerian security forces have beaten, detained, or even killed people who were involved in protests over oil company activities and individuals who have called for compensation for environmental damage. Victims include youths, women, children, and traditional leaders. In some cases, the abuse occurs after oil companies have requested that security forces intervene.

The report charges that multinational oil companies are complicit in abuses committed by the Nigerian military and police because they fail to condemn them publicly and to intervene with the Nigerian government to help ensure that they do not recur. In many cases, Human Rights Watch found that the oil companies had made no effort to learn what was done in their name by abusive local security forces seeking to keep oil flowing in the face of local objections.

Human Rights Watch strongly criticized the oil companies for excessive secrecy, and called upon them to make public their security agreements with state entities. It urged the companies to insist on screening all security staff assigned to protect company property, to investigate violent incidents, and to publish the results of those investigations. The companies were urged to take all necessary steps to ensure that their legitimate need to safeguard their facilities and personnel does not result in abuses against members of the communities where they operate.

Much of the protest against oil companies' activity in Nigeria has surrounded issues such as environmental pollution and corruption, which lie outside the mandate of Human Rights Watch. But the need to respect civil and political rights, such as freedom of expression and association, fall squarely within the international human rights treaties that Nigeria has signed, such as the International Covenant on Civil and Political Rights.

Nigeria is the largest oil producer in Africa, pumping more than two million barrels a day. This oil is produced by multinational oil companies operating in joint ventures with the Nigerian government. The Dutch-British corporation Royal Dutch/Shell accounts for nearly half of this production and has faced the strongest criticism of its corporate behavior. Perhaps for that reason, Shell responded most fully to questions from Human Rights Watch about its policies and practices and about specific incidents of human rights abuses connected with its operations. The U.S.-based oil corporations Chevron and Mobil also answered some questions, while France's Elf Aquitaine and Italy's Agip provided almost no information at all. None of the oil companies responded to requests to provide details of security arrangements with the Nigerian government.

For More Information:
In Lagos: Bronwen Manby (2341) 584-0288 (c/o Civil Liberties Organisation)
In New York: Peter Takirambudde (212) 216-1223
In New York: Arvind Ganesan (212) 216-1251
In London: Urmi Shah (44171) 713-1995
In Brussels: Jean-Paul Marthoz (322) 736-7838

Mr. PUTNAM. At this time, I ask unanimous consent that all members of the subcommittee be permitted to place any opening statement in the record and that the record remain open for 3 days for that purpose.

Without objection, so ordered.

I ask further unanimous consent that all witnesses be permitted to include their written statements in the record. Without objection, so ordered.

Gentlemen, welcome. We appreciate your being with the committee at this time. As you know, this is a hearing, and we must swear you in. If you would, please stand and raise your right hand.

[Witnesses sworns.]

Mr. PUTNAM. I note for the record that the witnesses responded in the affirmative.

At this time, we'll recognize Mr. John McCarthy, cochair of the Overseas Security Advisory Council, to begin our testimony. And because the panel is so large, we would ask that you maintain, within some reason, the 5-minute rule.

Welcome.

STATEMENTS OF JOHN M. McCARTHY, COCHAIRMAN, OVERSEAS SECURITY ADVISORY COUNCIL; ROBERT F. LITTLEJOHN, FIRST VICE PRESIDENT, INTERNATIONAL SECURITY MANAGEMENT ASSOCIATION; AMBASSADOR JAMES K. BISHOP (RET.), DIRECTOR, DISASTER RESPONSE AND RESOURCE COMMITTEE, INTERACTION; FRANK J. CILLUFFO, SENIOR POLICY ANALYST, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES; AND DR. BRUCE HOFFMAN, DIRECTOR, WASHINGTON OFFICE, RAND CORP.

Mr. MCCARTHY. Thank you very much, Mr. Chairman. Thank you for allowing me to testify at this time before this congressional subcommittee.

I'm here in my capacity as cochairperson of the Overseas Security Advisory Council, U.S. Department of State, representing the private business sector. Perhaps it would be fitting at this point to briefly furnish some background information concerning OSAC and the role it plays in American business.

Both the State Department and private industry have a common interest in protecting their assets and their people. The U.S. Department of State, through OSAC, has been able to build a bridge between the public and private sectors. By teaming together in OSAC, private industry and the public sector have discovered synergies from which both are able to fulfill their obligations.

The goal is very simple: Working together in OSAC, security information is exchanged and analyzed so that the best security practices can be used to address overseas security concerns and better protect the U.S. citizens and assets.

There are many accomplishments associated with OSAC—with the OSAC partnership, many of which will be articulated later by Peter Bergin, the cochair of OSAC for the public sector.

One of the most important responsibilities of American business is to supply a safe and secure workplace for its employees. In the United States, the task is easier than it is overseas. Today, many U.S. companies, particularly those in the extractive industry do

business in high-risk areas of the world. In Colombia, Nigeria, Indonesia, and Angola, U.S. citizens daily face the hard reality of personal security for themselves and their families. Civil war, threats of kidnapping, extortion and terrorism are real problems for business and Americans working in high-risk areas overseas. The security departments of globally involved American companies must have efficient security plans and programs to neutralize security threats and allow employees to focus on their job responsibilities.

Crisis management and emergency response teams, kidnapping and extortion plans, emergency and evacuation programs, as well as good physical security profiles are key to an excellent employee and asset protection program.

My colleague, Mr. Robert F. Littlejohn, vice president of global security, Avon Products, representing American business through the International Security Management Association, will furnish you more information on the life safety issues just mentioned.

Since Mr. Littlejohn will be addressing employee asset protection in depth, I will cover the other security challenges faced by American business when it decides to do business outside the United States, and provide some proposed and currently practiced measures that have applied to meet these challenges.

Much of America's businesses are no longer limited to the U.S. marketplace. As a result, the business risk analysis for these global companies becomes more complicated. The constants that America takes for granted—political stability, honest law enforcement, fair and impartial administration of justice—now become variables.

Due diligence inquiries are the vehicles that American business uses to make informed decisions concerning the feasibility of entering into an overseas business venture. Conducting due diligence inquiries in foreign countries is a problem particularly in emerging nations. Trying to determine indepth background information concerning a foreign country's political system and commercial environment is difficult because of the lack of good and accurate records.

Further, the laws of the country sometimes prohibit disclosure of the type of information that is part of the public domain in the United States.

Without accurate information concerning the commercial environment in a particular company or the individual who will be a future business partner, investment opportunities may be lost. Whether a company is controlled by organized crime, is an instrument for money laundering, is a reverse engineering expert, or otherwise engaged in matters which test the ethics, values, and laws of the United States is a proper subject for due diligence inquiries.

The intelligence units of the U.S. Government have excellent methods of gathering this type of information which can benefit American business and help avoid running afoul with the laws of the United States and the host country in which it seeks to do business. It is here that OSAC and other government agencies can play an important role in making classified information available to the business community in the following manner.

Business and security specialists who are cleared and authorized by the U.S. Government could review the information for its business value. If they decide that the information has a business value

and should be shared, it would be their responsibility to sufficiently sanitize it so that it still has business intelligence value, but its dissemination does not compromise national security.

Information concerning terrorist affiliation, organized crime associations, fraudulent and illegal business practices will be examples of the information American business needs to make an informed business decisions. Other information including, but not limited to, indigenous insurgent affiliation, associations with unsavory political figures, and those engaged in extortion or other crimes that endanger the lives of individuals would also be valuable when conducting due diligence inquiries.

The globalization of American business was made possible in large part through the computer technology developed mainly by American scientists and engineers. Computers are now commonplace, portable, and an indispensable part of the commercial world. The computers and the intellectual property they communicate and store is vulnerable to all kind of attacks. Even though viruses are planted by hackers and they attack them, or cyber-thieves try to steal their stored patents and trade secrets, computers are the main means of communication and file distribution for American global business.

Protection of the computer from unauthorized invasions is a top priority for American business, and it has joined with government efforts to devise plans and efforts to ward off unwanted attacks. Not to do so would threaten the basic fabric of national security.

But American business is struggling against a tough adversary when battling against computer attacks and theft of intellectual property. In fact, it has been said that the world economic battle of the 21st century will be over the intellectual property rights. This is not speculation; the battle has begun.

Protection of computers and the intellectual property they contain is a national security issue of gigantic proportions. It must be remembered that the United States is no longer solely a manufacturing economy, it is also an information and ideas economy. If America cannot adequately protect its intellectual property, it could suffer dire economic consequences.

The U.S. Government, through OSAC, does an excellent job in sharing information regarding international crime and terrorism with U.S. business interests, but much more is needed to help the U.S. companies so they can protect their intellectual property and trade secrets. The government must become increasingly mindful of the dynamics of computer technology and intellectual property protection and develop programs to assist the U.S. companies in protecting their intellectual property and trade secrets.

One such attempt by the government turned out to be essentially meaningless. The Economic Espionage Act of 1996, championed as the solution to a serious theft of intellectual property, could potentially provide the perpetrator with just the information they are attempting to steal.

More serious and meaningful legislation and other programs need to be put in place by the government. More information is needed to be shared with private industry on how to protect its computers and intellectual property.

Other initiatives that can be launched by the public and private sector to build defenses against computer intrusion and protect intellectual property are as follows.

Continue the OSAC initiative since it has been highly instrumental in protecting U.S. business interests abroad; ensure the permanency of the OSAC charter and support legislation establishing and ensuring its budget; enact a mandate to supply information to OSAC so that it can continue to be the premium supplier of American business; provide relief from encryption and export restrictions; ensure that fines are assessed for violators for agreed-to protection programs; the United States must be able to respond extraterritorially to intellectual property violations since some of the countries will be unwilling or unable to respond to cyber attacks; ensure that the FBI, which investigates most of the violations of computer law is adequately staffed, trained, and equipped to meet the vast, changing technical environment in 2001 and beyond; crack down on pirated software, CDs, and movies; develop treaties, bilateral and multilateral conventions and agreements; encourage common international statutes and laws; encourage nation-states to improve their judicial capacities and political will; support global anticorruption legislation and activities; and, provide technical advice to nations seeking help in implementing economic reforms.

Overall, we have to make protection of intellectual property rights a core issue in our relations with the many foreign governments in order to ensure a level playing field for American business.

The spread of transnational crime makes conducting business in a foreign environment also more difficult. Advanced fee schemes, credit card fraud, money laundering put American business at risk of becoming a victim of unscrupulous victims.

The Association of Certified Fraud Examiners estimate that fraud and abuse costs U.S. organizations more than $400 billion annually, with the average organization losing more than $9 per day per employee. The association says the average organization loses about 6 percent of its total annual revenue to fraud and abuse committed by its own employees. This is an enormous cost for American business as a price to pay.

Sharing information and maintaining a reasonable and effective relationship between the public and private sectors through OSAC will enable American businesses to overcome these difficulties. It will give American industry a chance to conduct an efficient and profitable business, not only in the established overseas markets, but also in the new emerging economies, full of promise and hope for the future.

Thank you very much.

Mr. PUTNAM. Thank you, sir.

[The prepared statement of Mr. McCarthy follows:]

Testimony of John M. McCarthy
Director of Corporate Security, Texaco, Inc.
House Committee on Government Reform
Sub-Committee on National Security, Veterans Affairs
And International Relations Washington, D.C.
April 3, 2001

Thank you ladies and gentlemen for allowing me to testify before this Congressional Sub Committee .

I am here in my capacity as the Co-Chairperson of the Overseas Security Advisory Council (OSAC), United States Department of State representing the private business sector. Perhaps it would be fitting at this point to briefly furnish some background information concerning OSAC and the role it plays in American business.

Both the State Department and private industry have a common interest in protecting their assets and their people. The United States Department of State, through OSAC, has been able to build a bridge between the public and private sectors. By teaming together in OSAC, private industry and the public sector have discovered synergies from which both are able to fulfill their obligations.

Meeting under the auspices of the United States Department of State, OSAC is an assembly of approximately 30 senior security professionals representing a cross section of American business and academia. Through the cooperative efforts of these private industry security representatives and the State Department, each is able to communicate about security issues they face in fulfilling their overseas responsibilities.

The goal is very simple, working together in OSAC, security information is exchanged and analyzed so that the best security practices can be used to address overseas security concerns and better protect U.S. citizens and assets. Some of the accomplishments of this partnership include:

- Through the cooperative actions of OSAC and the private sector, security guidelines have been crafted to help American citizens navigate in different cultures and environments. These brochures and manuals cover basic security concepts and are available to business entities at no cost.
- Through the Transnational Crime Committee, OSAC tracks global criminal activity and gives yearly seminars in Washington to update the business community.
- Through the Country Councils Support Committee, OSAC maintains an advisory relationship with American business overseas keeping those employees with security responsibilities abreast of security's best practices and processes. The Committee is also available to the business community for advice concerning security problems.
- Through the Security Awareness and Technology Committee, OSAC develops security awareness techniques and monitors technical security advances to ensure the OSAC affiliates have the latest information concerning computer and

communications infrastructure.

- OSAC also maintains an Electronic Data Base organized to present business risk analysis information in a user friendly environment to ensure the overseas business community is aware of the political and criminal risks of doing business in dangerous areas.
- OSAC also keeps its security information and risk analysis current by employing trained analysts who are available to the private sector for consultation.
- Each year, OSAC provides a comprehensive briefing at its Washington headquarters concerning global risk matters affecting the business community.

OSAC is a good example of corporate tax dollars at work. It is an example of teamwork at its best. It shows that the public and private sectors can work together efficiently, adding value through managing risk, and developing a competitive advantage for American business overseas.

Mr. Peter Bergin, Co-Chairperson representing the government sector of OSAC, will provide you with in-depth information concerning this organization later today.

One of the most important responsibilities of American business is to supply a safe and secure workplace for its employees. In the United States, the task is easier than it is overseas. Today, many U.S. companies, particularly those in the extractive industry, do business in high-risk areas of the world. In Colombia, Nigeria, Indonesia and Angola, U.S. citizens face the hard reality of personal security for themselves and their families. Civil wars, threats of kidnapping, extortion and terrorism are real problems for business and Americans working in high-risk areas overseas. The Security Departments of American companies there must have efficient security plans and programs to neutralize security threats and allow employees to focus on their job responsibilities.

Crisis Management and Emergency Response Teams, kidnapping and extortion plans, emergency and evacuation programs as well as a good physical security profile are key to an excellent employee and asset protection program.

My colleague, Mr. Robert Littlejohn, Vice President Global Security, Avon Products, Inc. representing American business through the International Security Management Association (ISMA) will furnish you more information on the life safety issues mentioned above.

Since Mr. Littlejohn will be addressing employee and asset protection in depth, I will cover the other security challenges faced by American business when it decides to do business outside the United States and provide some proposed and currently practiced measures that have applied to meet these challenges.

Globalization of American Business

As the needs of the western consumer became more sophisticated and the need to expand business objectives increased, American corporations looked beyond the United States

for markets for its products and services. Latin America, Asia and Africa looked like attractive business prospects since they were desirous of improving their economies. These continents also contained a plethora of undeveloped mineral deposits. Through the exploitation of these minerals, the global thirst for energy and quality consumer products could be quenched.

To properly integrate American business with the market place overseas, domestic companies had to export its marketing and manufacturing acumen and people. Preparing for the foreign business experience involves security challenges not experienced in the United States.

Difficulties Encountered in Overseas Security

The United States is blessed with an infrastructure that is sound, secure and basically honest. It maintains a positive climate for business. Its population is well educated, sophisticated, business oriented and possesses an unusually strong work ethic. It has the technical skills as well as well as the manufacturing and marketing processes and programs that have made the United States the undisputed global economic leader. The United States is the envy of the world economically, and possesses a business environment many want to imitate.

American business has accommodated its foreign colleagues by exporting both its political and economic systems. Governments have welcomed these systems and promulgated them to their populations as an elixir that will solve all their economic problems. The promises of these governments were supported by the view of American life and western culture portrayed on television and movie screens. Because of this view of western life, many thought that by embracing the American way, their economies would be secure and gold would line their streets. They failed to realize it took America over 200 years to get where it is today.

The variables involved with doing business overseas are greater than they are in the United States. In the emerging economies of Asia, Africa and Latin America the political systems are not as stable as they are in Europe and the United States. Keeping track of the global political movements can be a full time job for security directors of multinational companies. For small and mid-cap companies, the job is more difficult; they may not have the funding to acquire the information needed to track these political events.

Law Enforcement agencies in the developing world are less sophisticated than they are in the developed world. Many are not trained to handle routine police work let alone the more complicated white collar and computer crimes. As a result, criminal activity increases and the victims are sometimes the expatriate employees of western companies.

Another variable with which western companies must deal is the judicial system of these countries. Many of the legal systems are a hybrid of western procedures weighted in favor of the local people. This puts an added burden on expatriates when enforcing their rights under local law.

Ethnic wars, rumors of wars, civil wars and terrorism also impact foreign investment and make for a very unstable economic environment. The continual fighting in Colombia, Angola and the DR Congo are examples of the dangerous situations western companies must face when they consider doing business outside the United States. Difficult situations need to be neutralized, as much as possible, in order to attract qualified people to work in these high-risk areas. Once these individuals agree to work in these areas, companies must try to duplicate western life as much as possible to keep the employees working there.

Another aspect western companies must deal with is the country's culture. Doing business in the Middle East, for instance, requires an acceptance of a very different culture. The western view of equality for women is alien to the Middle Eastern culture. Also, the public consumption of alcohol is forbidden in the Muslim world, and their idea of pornography is very different from the western view.

These are some of the areas western business must explore before they make the decision concerning their business investment in overseas countries. The prudent company uses its Security Department to look into these variables and do what is commonly called a "Due Diligence" inquiry.

Due Diligence as a Means of Determining Security Risk

Before we discuss Due Diligence we would do well to define it. Due Diligence, according to Black's Law Dictionary, is "such a measure of prudence, activity, or assiduity, as properly exercised by a reasonable and prudent man under the particular circumstances; not measured by any absolute standard, but depending on the relative facts of the case". In other words, it is the process whereby potential business investors make sure that they fully understand everything they can about the anatomy of the company they are considering buying, and the place where they are going to do business. For most investors in small businesses, the transaction will be a once-in-a-lifetime experience and the major portion of their financial worth will likely be tied up in the venture. It will be absolutely imperative for them to ensure, to the maximum extent practical, that they fully understand the details of the business they are buying and the place where they are investing. Exploring the backgrounds of businesses and people before getting involved with them, is the prudent thing to do and an integral part of a "Due Diligence" inquiry.

In the United States, determining the details of a particular business is fairly straightforward. Federal and State laws generally require transparency when it comes to business dealings. The United States Security and Exchange Commission requires full disclosure when a company desires to raise money by attracting public investment, and the states require a similar disclosure when corporations do business in a particular state. The regulations promulgated in the United States are designed to inform the public of the competency of corporations, key personnel and their products before they ask the public to engage them.

So it is, with those who sell professional services to the public. Here, the states have designed strict standards of competency, which lawyers and medical doctors must meet before they are permitted to practice their professions. Further, the legal system holds these professionals and companies accountable if they fail to perform their duties in a reasonable manner.

Information concerning the competency of the military, medical care, education facilities, marketing information, etc. can be found in government publications. Court records contain the criminal history of individuals.

Conducting a "Due Diligence" inquiry in a foreign country, particularly in emerging economies, can be very difficult. The record systems in many of these countries are incomplete at best but mostly non-existent. If record systems do exist, the bureaucratic red tape that must be endured to gain access to the records is very difficult. Sometimes information concerning businesses and people can be obtained through interviews or contacts.

Government's Role in "Due Diligence" Inquiries

The United States Government is helping American business perform "Due Diligence" inquiries by furnishing information concerning terrorism in foreign countries, foreign business practices and anecdotal criminal information through the Overseas Security Advisory Council (OSAC), Department of Commerce and other government agencies. Through its analytical staff, OSAC supplies invaluable insight concerning the political and terrorist environment overseas. Its professional analysts brief business executives and security professionals at business meetings and professional conventions.

But is this enough. Are their other areas of security to which business should be privy in order to make an informed business decision regarding investment in an emerging economy.

Today the various types of organized crime are making their way into legitimate business. Corruption in the emerging economies is sometimes very pervasive. Who to deal with and how much a particular potential business partner is involved with corrupt politicians and organized crime types are "Due Diligence" problems American business faces when it decides to invest overseas. Does a company, sell a license for a particular technology to a government controlled company or should it not do business with them since they may try to steal the technology through reverse engineering or commercial espionage.

Of course foreign governments, individuals and companies are anxious to attract foreign investment and will not wear their corruption on their sleeves. In some cases, they will promise anything to obtain an investment commitment then begin to work against their western partner before the ink is dry on the contract.

Whether a company is controlled by organized crime is an instrument for money laundering; is a reverse engineering expert; or otherwise engaged in matters which test the ethics, values and laws of the United States, is a proper subject for "Due Diligence" inquiries. The intelligence units of the United States Government have excellent methods of gathering this type of information, which could benefit American business and help it avoid running afoul of the laws of the United States, and of the country, in which it seeks to do business.

The business community recognizes that some of this information is classified and to reveal it to unauthorized individuals could compromise national security. The United States Government does not play favorites with information and give one company a competitive advantage over another. American business fully understands the position of the United States Government and recognizes that if the information cannot be given to all; it cannot be given to any.

It is here that OSAC and other government agencies can play an important role in making "classified" information available to the business community in the following manner:

- Business and security specialists who are cleared and authorized by the United States Government could review the information for its business value.
- If they decide that the information has business value and should be shared, it would be their responsibility to sufficiently sanitize it so that it still has business intelligence value but its dissemination does not compromise national security.
- Information concerning terrorist affiliation, organized crime associations, fraudulent and illegal business practices would be examples of information American business would be interested in to make an informed business decision.
- Other information including, but not limited to, indigenous insurgent affiliation, associations with unsavory political figures, and those engaged in extortion or other crimes that endanger the lives of individuals would also be valuable when conducting Due Diligence inquiries.

Business, like the government, has a non-delegable duty to protect the lives of its employees and the assets of its company. Any information which impacts on the safety and security of employees is vital in order for a manager to make an informed business decision.

Through this cooperative effort, among the business community, OSAC and the intelligence units, the information gathered by the United States Government would have more meaning as well as add value to the American economy and American investment overseas.

Protecting Intellectual Property

Over the past 25 years, computer technology has progressed from the cumbersome business machines that would fill a good-sized room to hand held palm pilots. Today computers are used so much they virtually eliminate routine business jobs. The computer

is used to communicate, store and transmit all types of information globally. The communication world of business today is reduced to a binary code and available worldwide.

The computer is one of the reasons for the globalization of business. It is the reason why so many employees can be more efficient, since they can be in touch with their work from anyplace in the world. Space and time have no relevance in today's business environment. An employee in Singapore can use his computer to send a request for information to a fellow employee in New York, and when the Singaporean wakes the next morning, he will be able to view the requested information on his computer.

Computers have been inextricably woven into the fabric of American business. If the company's Intranet or network is disabled for any substantial period of time, the business suffers. Orders cannot be filled, meetings cannot be scheduled, products cannot be shipped, and information cannot be exchanged.

In some areas of business, the traditional company has been replaced by "E-Commerce". This is a business that is completely based on the computer. It works in conjunction with traditional business in arranging for ordering and shipping durable goods globally. Because of its ability to handle a myriad of material in cyberspace, it can represent several traditional businesses at one time. It is low cost since it does not require a host of employees to run the business and does not have to maintain warehouses or other physical assets to house its products.

Computers play an important role not only in business but also our daily lives. To illustrate the importance of the computer and the consequences suffered if it is compromised, let's look at the following example:

In a military exercise code-named "Eligible Receiver," 35 hackers hired by the National Security Agency (NSA) gained access to 36 of the 40,000 government networks within four days. They were able to gain control of major power grids and could have disrupted power in Los Angeles, Chicago, Washington and New York.

In testimony to Congress last year, members of a hacker group said they could bring the Internet to its knees in less than an hour. "It is not difficult at all to fool, confuse or corrupt major [domain name] servers."

"The number of technologies that might be turned against the United States continues to expand with each high-tech invention", say several scientists at U.S. high-tech labs. Among the most frightening are the advent of MEMS — micro-electro-mechanical systems. These tiny machines, potentially smaller than a human cell, may one day be injected into the bloodstream as miniature doctors sent to beat back viruses or kill cancerous cells. But they could just as easily be designed as a lethal combination of high-tech and biological warfare, as smart MEMS could be set to infect and kill specific kinds of subjects.

Much of the intellectual property developed in the United States concerns computer hardware and software. America is the world's leader in computer technology and because of this, the United States is the world's target for the theft of intellectual property. If a country does not have a base of operations in the United States from which to launch commercial intelligence or commercial espionage operations, it will soon be out of the "commercial loop".

Security Challenges to Computer Technology and Intellectual Property in American Business

Since computers are such an integral part of the American business landscape, they become the targets of all that want to disrupt the American economy. Information transmitted in the public domain or cyberspace is fair game for anyone to intercept. Also the computer itself as well as its software systems are subject to attack by hackers. These technicians have the uncanny ability to exploit the computer Internet and trace electronic identities through cyberspace back to the computer of origin and disable it and/or steal all its information. By planting virus messages on the machine, they can also destroy the software and the storage capabilities of that machine or any others with which the original computer communicates.

Some additional challenges to computer security are as follows:

- Protective technology cannot be exported to overseas business locations for administrative reasons.
- There is a limited capability to collect business information overseas because of legal regulation.

But American business is struggling against a tough adversary when battling against computer attacks and theft of intellectual property. In fact it has been said that the world economic battle of the 21st Century will be over intellectual property rights. This is not speculation; the battle has begun. Protection of computers and the Intellectual Property they contain is a national security issue of gigantic proportions.

But protection of intellectual property in computers is not the only kind of intellectual property that needs to be safeguarded. Take, for instance, the product theft and deceptive practices that permeate the pharmaceutical industry.

Generic pharmaceutical companies in India are allowed to produce generic versions of U.S. patented drugs for use by citizens in their country. Yet, few of their drugs go to their citizens. Instead they are shipped around the world where they compete with patented drugs. Because of their low prices, Indian generic drug companies are being taken seriously by the United Nations as well as by health care advocates in the U.S.

The U.S. is no longer solely a manufacturing economy. It is also an information and ideas economy. If America cannot adequately protect its intellectual property, it could suffer dire economic consequences.

Government's Role in Protecting Computer Technology and Intellectual Property

The U.S. government, through OSAC, does an excellent job in sharing information regarding international crime and terrorism with U.S. business interests. However, much more needs to be done to assist U.S. companies in protecting their intellectual property and trade secrets:

- The government must become increasingly mindful of the dynamics of computer technology and intellectual property protection, and develop programs to assist U.S. companies in protecting their intellectual property and trade secrets. One such attempt by the government turned out to be essentially meaningless. The Economic Espionage Act of 1996 championed as the solution to the serious threat of theft of intellectual property could potentially provide the perpetrator with just the information they are attempting to steal.
- More serious and meaningful legislation and other programs need to be put in place by the government.
- More information needs to be shared with private industry on how to protect its computers and intellectual property.

Other initiatives that can be launched by the public and private sector is to build defenses against computer intrusion and protect intellectual property are as follows:

- Continue the OSAC initiative since it has been highly instrumental in protecting U.S. business interests abroad.
- Insure the permanency of the OSAC Charter and support legislation establishing and ensuring its budget.
- Enact a mandate to supply information to OSAC so that it can continue to be the premier information supplier to American business.
- Provide relief from encryption export restrictions
- Ensure that fines are assessed for violators of agreed to protection programs.
- The United States must be able to respond extra-territorially to intellectual property violations since some countries will be unwilling or unable to respond to cyber attacks.
- Ensure that the FBI, which investigates most of the violations of computer law, is adequately staffed, trained and equipped to meet the fast changing technical environment in 2001 and beyond.
- Crack down on pirated software, CDs, movies, etc.
- Develop treaties, bilateral and multilateral conventions and agreements.
- Encourage common international statutes and laws.
- Encourage nation states to improve their judicial capabilities and political will.
- Support global anti-corruption legislation and activities.
- Provide technical advice to nations seeking help in implementing economic reforms.

Overall, we have to make the protection of intellectual property rights a core issue in our relations with many foreign governments in order to ensure a level playing field for American business.

Any country that wants high end, high technology investments – any country that wants to catch up economically – needs a strong intellectual property system that instills confidence for investments. Such investments produce jobs and generate wealth for a national economy.

One example of how good intellectual property laws and systems helped a foreign economy is that involving Texas Instruments, a leading U.S. semiconductor manufacturer.

In the early 1980s, Texas Instruments entered into joint ventures for the production of D-RAM chips with Acer of Taiwan and Goldstar of Korea. In return for supplying the technology through patent licenses, Texas Instruments received part ownership of the joint ventures. The combination of U.S. technology and Asian manufacturing know-how resulted in more than a billion dollars of investment in new factories in Asia. The result is that today the combined sales of these joint ventures account for a significant percentage – estimated by some as 40 percent – of the entire global market for D-RAM semiconductor chips. The result is a win-win situation. Texas Instruments receives over half of its annual revenue – more than $2 billion U.S. – from licensing royalties. Acer and Goldstar pump billions more in to local economies in Asia from their manufacturing facilities, producing jobs and wealth for these nations.

Transnational Crime and American Business

American business is very much affected by crime that crosses international borders. Money Laundering, Financial Fraud, and Product Counterfeiting are examples of transnational crime. It is a crime that costs American business millions.

The Association of Certified Fraud Examiners (CFE), an organization composed of experts who deal with discovering and neutralizing fraud, furnished the following facts concerning fraud in American business:

- Fraud and abuse costs U.S. organizations more than $400 billion annually.
- The average organization loses more than $9 per day per employee to fraud and abuse.
- The average organization loses about 6% of its total annual revenue to fraud and abuse committed by its own employees.
- The typical perpetrator is a college-educated white male.
- Men commit nearly 75% of the offenses.
- Median losses caused by men are nearly four times those caused by women.
- Losses caused by managers are four times those caused by employees.
- Median losses caused by executives are 16 times those of their employees.
- The most costly abuses occur in organizations with less than 100 employees.

- The education industry experiences the lowest median losses.
- The highest median losses occur in the real estate financing sector.

Financial fraud, such as credit card fraud and Nigerian "Advance Fee Fraud," is a direct attack against individuals traveling abroad as well as the integrity of the financial systems of this nation. One of the main goals of those investigating this type of crime, is to search out the source of criminal activity aimed at individual victims and U.S. financial institutions around the world. With the globalization of economies and the transnational nature of crime, it has become evident that organized criminal groups increasingly target individuals traveling abroad, as well as the financial institutions of established and emerging economies. Leaders of foreign countries have realized that transnational organized criminal groups are targeting and victimizing individuals through credit card fraud and advance fee fraud.

Credit Card Fraud

Of the two billion dollars in annual losses reported by the credit card industry, it has been estimated that at least one third of these losses are incurred outside of the United States and perpetrated by transnational organized criminal groups. Lost and stolen credit cards have often been the source of exploitation by these criminal groups, however, a new method of credit card fraud is on the rise.

When a credit card is lost or stolen, it is routinely reported as such by the true card holder preventing or diminishing large amounts of potential fraud tied to that account number. The account number is generally "flagged" by the issuing bank and is most times rendered worthless by the credit card company for future fraudulent use by the criminal.

A new scheme known as "skimming" or "cloning" allows criminals to steal or "skim" the vital credit card information maintained on the magnetic stripe without the bearer of that card knowing the card has been compromised. With this information (account number, expiration date, etc.), the criminal can re-encode a separate card which may also be lost or stolen, their own credit card, or any other card that bears a magnetic stripe. Without even knowing it, your account number could be used to make a purchase, and you will not be made aware of this until you receive your credit card statement.

Advanced Fee Fraud Schemes

In the early 1980s, a formidable criminal network emerged from within the large community of Nigerian nationals residing in the U.S. For the last fifteen years, this network has been continuously adapting and improving its exploitation of financial institutions, insurance companies, government entitlement programs, and individual citizens. Other Nigerian criminal activities include: false credit card application fraud, counterfeit access device fraud, manufacturing and distribution of counterfeit financial instruments and false identification, check kiting, telecommunications and computer fraud, and immigration benefit fraud.

The United States Secret Service is internationally recognized as the experts in the investigation of this type of fraud. Secret Service task forces have arrested a number of criminals operating in the United States and abroad resulting in seizures totaling over $8,000,000.

The way this scheme works is that a company or individual will typically receive an unsolicited letter by mail from an individual claiming to be a senior civil servant in one of the Nigerian ministries, usually the Nigerian National Petroleum Corporation. The letter informs the recipient that the government official is seeking the assistance of a reputable foreign company into whose bank account he can deposit funds ranging from 25-60 million dollars. These funds are alleged to be the results of over invoiced government contracts. The initial contact letter sets the stage and is the opening round of a two-layered scheme. The criminal will eventually reach someone who, while skeptical, desperately wants the deal to be genuine.

Once the trap has been set, an alleged problem concerning the deal will suddenly arise. An unforeseen tax or fee payable to the government of Nigeria will have to be paid before the monies can be transferred. The foreign partner will then be provided with a bank account into which these fees should be transferred. Victims from around the world have incurred financial losses conservatively estimated in the hundreds of millions of dollars annually.

While these advance fee schemes emanate solely from within Nigeria, investigations indicate that Nigerians and others based in the United States, Great Britain, and other countries, are acting in complicity to further these schemes. This type of fraud has become so widespread throughout the United States and overseas that the Secret Service instituted a program that tracks these schemes and their victims. The Secret Service is sharing criminal intelligence in the form of bank accounts and telephone numbers known to be associated with advance fee fraud with authorities in Malaysia, Hong Kong, Canada, the U.K., France, and Germany. These investigative leads have resulted in the arrests of criminals and the seizure of illicit proceeds.

Money Laundering

Drug sales in the United States are estimated by the Office of National Drug Control Policy to generate billions of dollars annually, and most of these transactions are in cash. One laundering system used by Colombian drug cartels involves the use of a Colombian Black Market Peso Exchange as a mechanism to place substantial amounts of currency from U.S. narcotics sales into U.S. financial institutions to avoid detection by the Bank Secrecy Act reporting requirements. In simple terms, the Colombian cartels sell drug-related, U.S. based currency to Black Market Peso Exchanges in Colombia, who in turn, place the currency into U.S. bank accounts. The exchanges then sell monetary instruments drawn on their bank accounts to Colombian importers who use the instruments to purchase foreign goods.

Financial institutions are the primary victim of money laundering. Through concerted efforts by the Congress and the Executive branch, laws and regulatory actions have made the movement of this cash a significant problem particularly for the drug cartels. As a result of these successes, the placement of large amounts of cash into U.S. financial institutions has created vulnerabilities for the drug organizations and cartels. Efforts to avoid reporting requirements by structuring transactions at levels well below the $10,000 limit or camouflage the proceeds in otherwise legitimate activity are continuing. Now, drugs cartels are also being forced to devise creative ways to smuggle the cash out of the country.

Product Counterfeiting

Product counterfeiting and product diversions are also transnational problems with which American business deals. When the United States introduces a product into another country, scientists and research analysts attempt to discover its secret formula. They sometimes are able to duplicate it, but more often than not, they produce a product inferior to the American product. They then counterfeit the company's packaging and sell the product as if it were made in America. When the product does not perform according to expectations, the reputation of American business suffers. Further, some of these countries will allow the pirated manufactured goods to be marketed as a generic product thereby competing with the genuine American item for consumption.

Product counterfeiting, particularly in the fragrance business is an ongoing problem of American business overseas. Some countries are riskier places to invest due to the lack of sufficient protective statutes. Furthermore, some countries are not willing to work with American multi-nationals on this issue since doing so means they would have to develop their own products through costly research and development programs.

Product diversion is another problem facing American business. Here products are priced and delivered to a shipping station for export to a particular country. The prices are geared to act as loss leaders so that through this product, the American business will capture a portion of the market share in the destination country. Unscrupulous marketers, after they have purchased the product for export, divert it to the local market and sell it below the market price.

Steps Being Taken to Fight Money Laundering and Product Counterfeiting. In an attempt to thwart this type of transnational crime, the following initiatives are being pursued:

Sharing Information With U.S. Bankers: In addition to the traditional law enforcement investigative efforts, non traditional methods are also being identified and disrupt this system at its most vulnerable choke points, i.e. the financial institutions and businesses in the importing chain - the points at which money is actually laundered. In order to assist the financial and trade community in working to deny the cartel access to their business, a new approach is being coordinated through the Interagency Coordination Group known as the ICG. The members of the ICG include representatives from the Criminal

Investigative Division of the Internal Revenue Service, the United States Customs Service, the United States Postal Service, the Drug Enforcement Administration, the Department of Justice, the Federal Bureau of Investigation and the Financial Crimes Enforcement Network (FinCen). FinCen is further assisting the ICG through its network of partnerships with the financial and trade communities in the United States. Colombia, Panama and Mexico. The network provides the ICG with a "highway" by which to take its knowledge of the system on the road and share that information with affected banks, merchants and officials within the Colombian, Panamanian and Mexico governments.

Sharing information with government officials, bankers and merchants in Colombia and Panama: Reaching farther into the FinCen network, ICG members approached government officials and bankers in Colombia and Panama, as well as merchants in Panama's Canal Free Zone. The ICG's message has been essentially the same as the one it took to the U.S. banks - "We are all faced with a common problem and here is what we know about it. We will benefit by working together to find solutions". The response from all of the groups contacted has been positive, and more specific information exchange initiatives are underway. While these are encouraging developments, there is still much work to be done to counter this money laundering scheme.

Broadening the education effort: As previously mentioned, representatives from the U.S. banking community are reviewing accounts provided by law enforcement to determine the most effective ways to identify suspicious activity resembling money laundering techniques used in the Colombian Black Marker Peso Exchange System. In addition, these banking representatives have begun an information exchange among themselves to share ideas and identify the best approach to counter this Colombian cartel money laundering system.

Concerning product counterfeiting, private industry is leading a coalition of companies to work co-operatively on this problem. This has helped to focus resources and efforts, but a lot of work remains.

The United States Government can help fight this problem by:

- Using its diplomacy and influence, have countries pass meaningful laws protecting intellectual property rights.
- Using its leverage to convince these countries that it is in their best interests to protect copyrights, patents and trade marks because it will attract western investors to begin businesses in their country providing jobs and a better standard of living for their people.

Conclusion

Much of America's major businesses are no longer limited to the United States market place. As a result, the business risk analysis for these new global companies becomes more complicated. The constants that Americans take for granted: political stability, honest law enforcement, fair and impartial administration of justice, now become variables.

Conducting "Due Diligence" inquiries in foreign countries is a problem particularly in emerging nations. Trying to determine background information concerning the basics of a foreign country's political system and commercial environment is difficult because of the lack of good, accurate records. Further, the laws of the country sometimes prohibit the disclosure of the type of information that is part of the public domain in the United States. Without accurate information concerning the commercial environment in a particular country and the individual whom you assume as a business partner, investment opportunities may be lost.

The globalization of American business was made possible through the computer technology developed mainly by American scientists and engineers. Computers are now commonplace, portable, and an indispensable part of the commercial world. The computers and the intellectual property they communicate and store are vulnerable to all kinds of attacks. Even though viruses planted by "hackers" attack them or cyber thieves steal their stored patents and trade secrets, computers are the main means of communication and file distribution for American global business. Protection of the computer from unauthorized invasion is a top priority for American business and it has joined with government efforts to devise plans and programs to ward off unwanted attacks. Not to do so would threaten the basic fabric of national security.

The spread of transnational crime makes conducting business in a foreign environment more difficult. Advanced fee schemes, credit card fraud and money laundering put American business at risk at becoming a victim of unscrupulous criminals. By sharing information and maintaining a reasonable and effective relationship between the public and private sectors through OSAC, American business will be able to overcome these difficulties, and conduct an efficient and profitable business enterprise; not only in the countries of our original heritage, but also in the new emerging economies full of promise and hope for the future.

Thank you for your attention and I will now answer any questions you may have.

John M. McCarthy
Director of Corporate Security
Texaco, Incorporated

Co-Chair
Overseas Security Advisory Council
U.S. Department of State

Mr. PUTNAM. At this time, the Chair would recognize Mr. Littlejohn. Mr. Littlejohn is the first vice president of the International Security Management Association.

Welcome to the subcommittee.

Mr. LITTLEJOHN. Thank you, Mr. Chairman. We are pleased that the subcommittee chose to draw on the expertise of the International Security Management Association in reviewing the safety of Americans working and traveling abroad.

By way of background, ISMA represents private sector senior security executives worldwide. Some 80 percent of our membership works for U.S. companies that compete internationally, representing an aggregate employee base of 10.5 million and aggregate revenues in excess of $3 trillion.

I am the vice president of global security of Avon Products, responsible for security operations in 140 countries. However, today, I testify on behalf of ISMA as the first vice president and a member of the board of directors.

Let me, at the outset, thank both the Overseas Security Advisory Council and the Federal Bureau of Investigation for the assistance that they have provided U.S. business abroad. Although the U.S. business community, as Mr. McCarthy mentioned, is confronted with many issues abroad, we will focus our testimony on the personal safety issues, as the lives of U.S. citizens are by far our most important priority.

We'll look at the risks affecting our employees abroad. We feel that they fall into four general categories: travel, global crime in general, and then, more specifically, kidnapping and terrorism.

Travel: American travelers today face a number of security risks, and we anticipate that these risks will grow as business personnel become more and more mobile. Increased threats have a chilling effect on global commerce. In countries with high levels of street crime, concern for the safety of business travelers will discourage entry into new markets. Moreover, U.S. business concerns are only magnified when coupled with language barriers, cultural issues, and more importantly, uncooperative and corrupt law enforcement personnel.

Global crime issues, with the exception of kidnapping and terrorism: The most significant security problem faced by private enterprise is global criminal activity. This is a nearly ubiquitous problem which, in its most extreme forms, poses a serious threat to foreign commerce. Such crimes threaten, not only the staff and physical assets, but also increase costs, because security provisions, high-risk compensation, and the difficulty in attracting skilled workers and other accommodations are quite expensive.

Kidnapping: Kidnapping for ransom is on the rise worldwide. Perpetrators use kidnapping for a variety of reasons. In Mexico, criminal gangs kidnap for cash. While, in Colombia, guerilla groups use kidnapping to fund their armed struggle against the state.

Terrorism: The U.S. Department of State reported 169 international terrorist attacks in 1999 that targeted U.S. interests specifically. Long-running terrorist campaigns have had an effect of rising insurance premiums and other operating costs for U.S. companies working in certain high-risk countries.

ISMA recommendations: With these issues in mind, our government can and should implement a dozen actions to enhance the protection of U.S. businesses and their people abroad.

First, U.S. Government should expand training programs to enhance the effectiveness of the global law enforcement community. It should work with other nations in providing targeted financial assistance to law enforcement agencies in high-risk countries that are currently unable to provide adequate protection to U.S. business.

The government should require the FBI to send observers to advise U.S. companies when an employee has been kidnapped abroad. The U.S. Government should establish agreements with other companies—countries to expand territorial jurisdiction of law enforcement agencies. The government should use contacts, existing contacts, to facilitate relationships between private companies operating abroad and local law enforcement agencies. And we must create a closer working relationship with Interpol and its member nations.

We must encourage other nations to enact wars against "air rage." The government should create programs that help the private sector companies to adapt crisis management planning and training designed to address threats in high-risk countries.

We must encourage greater cooperation and communication between the security and the commercial branches of government. The Department of State's political branch should provide more timely and accurate reports of global criminal activity, irrespective of political concerns.

The government should require Federal agencies immediately to disclose information with any appropriate security classification that would protect U.S. business abroad.

And, finally, OSAC is the appropriate agency to disseminate information; and we should consider increasing the OSAC funding to expand both its personnel and educational programs.

In conclusion, much more can and should be done to protect Americans working abroad. We believe the recommendations, if adopted, will have a significant impact on improving individual security and also enhancing global opportunities for U.S. business today.

Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you very much, Mr. Littlejohn.

[The prepared statement of Mr. Littlejohn follows:]

Executive Summary

The testimony included in this document represents opinions from a cross section of International Security Managers Association (ISMA) members. Membership in ISMA is restricted to senior security executives of major corporations. Many of its members have previously held senior positions in federal and local law enforcement agencies.

American businesses operating abroad are confronted with two types of security issues: business security and personal security issues. The business security issues include due diligence, intellectual property theft, counterfeiting, and cyber crime. The personal safety issues include travel, global crime, kidnapping and terrorism. It is our belief that in the current global environment, the ability to provide a safe work environment for employees traveling, living, and working abroad is paramount. Although business-related issues are a major concern, the lives of US citizens are by far our most important priority.

This document addresses personal security issues, broken down into four areas of concern: travel, global crime, kidnapping and terrorism. In each of the four areas, we outline the problem, and assess the extent and impact on US business.

I. Travel Summary

American business travelers today face three primary security risks while engaged in international travel:

1. Extreme threats to physical safety (i.e., kidnapping, extortion, or other terrorist acts)
2. Threats to physical safety *and* property (i.e., robbery, assault and car-jacking)
3. Sophisticated scams designed to separate business travelers from cash and other valuable assets

Americans are frequently targeted for a variety of reasons, ranging from politically motivated anti-American sentiment to the misguided perception that all Americans are affluent, and therefore good targets.

Increased threats to American business travelers can have a chilling effect on global commerce. In countries with high levels of street crime, concerns for the safety and security of business travelers discourage new market entries. US business concerns are only magnified when coupled with language barriers, local customs, and often uncooperative or corrupt law enforcement personnel.

II. Crime Summary

With the exception of kidnapping and terrorism, the most significant security problem faced by private enterprise is criminal activities relating to crimes against person and property.

This is a worldwide problem with major debilitating effects on developing economies. In its most extreme forms, it poses a serious threat to foreign investments.

High levels of crime not only pose threats to staff and physical assets, but also increase costs significantly because of security provisions, high-risk compensation, etc. In countries with widely publicized crime problems, private enterprises have found it difficult to attract skilled expatriates.

Companies are increasingly concerned not only about the difficulty of attracting high-quality staff, but also the possibility of litigation by staff if companies are believed to have failed in their duty to provide a safe work environment. In addition to the individual risk, staff morale, and productivity also suffer.

Organized crime is an increasing threat to US business (particularly in Eastern Europe) due to increasingly sophisticated methods, technology, and penetration into government and private sectors through the corruption of officials. Organized criminal activity by close-knit groups is currently a major growth industry. China's triads, Colombia's drug cartels, Italy's Mafia, Japan's *yakuza* and the Cosa Nostra of the US are now some of the world's most profitable multinationals.

III. Kidnapping Summary

Kidnapping for ransom is on the rise around the world. The perpetrators of kidnap for ransom vary from country to country. In Colombia, for example, guerrilla groups use kidnapping to fund their armed struggle against the state. In Mexico, criminal gangs seek to raise quick cash to buy drugs and other commodities. Still other groups, such as Yemeni tribes, use kidnapping to draw attention to their grievances against the government and seek compensation for past injustices.

The victims of kidnapping for ransom also vary from country to country. Although in many cases, locals are the primary targets, when they are employed by American businesses the result is the same. Some kidnapping groups make a point of targeting foreign nationals either because they expect the rewards to be greater or because they wish to attract international attention.

Regardless of motivation, the profits generated from ransom demands and payoffs have risen steadily. It is believed that the number of kidnappings will continue to rise, impacting US businesses in a variety of countries around the world.

IV. Terrorism Summary

And finally, US State Department statistics reported 169 international terrorist attacks in 1999, specifically targeting US interests. In addition to causing hundreds of injuries and deaths each year, terrorist attacks result in financial costs that soar into the billions.

Terrorism has significantly impacted US companies operating in a number of areas around the world. Left-wing guerrillas in Colombia, Ecuador and elsewhere have repeatedly attacked oil pipelines operated or owned by US companies and have kidnapped expatriate personnel. In response to the NATO bombing of Yugoslavia in 1999 the, 'November 17' group carried out attacks targeting branches of US financial institutions in Athens, Greece using anti-tank rockets,

while other ultra-leftist groups responded by bombing US car dealerships, restaurants and warehouses.

Long-running terrorist campaigns have had the effect of raising insurance premiums and other costs for US companies operating in certain countries. Insurers reported in 2000 that if premiums are forced to rise again due to left-wing guerrilla attacks, it will become more cost effective for companies to bear the cost of terrorist damage themselves rather than continue paying for prohibitively expensive coverage.

Increased fortification of government embassies has resulted in making the more accessible, US private commercial interests comparatively easy targets. In Greece, the 'November 17' group confined its attacks on US interests in 1999-2000 to commercial interests but also attacked unfortified German, Dutch and British diplomatic missions and personnel, presumably because they were 'softer' targets than better protected US government interests.

ISMA Recommendations

- The US Government has made strides in providing training for foreign law enforcement. We recommend that this training be expanded to raise the overall effectiveness of the global law enforcement community.
- The US should work with other nations to provide targeted financial assistance for resources (equipment, labor, etc.) to law enforcement agencies located in high-incidence countries that are unable to provide adequate protection to US businesses.
- The US Government should seek to establish agreements with foreign countries to expand extraterritorial jurisdiction of law enforcement agencies to provide assistance to Americans victimized by crime.
- The US Government should encourage a close working relationship with Interpol and its 178 member nations to improve communications and training among the global law enforcement community.
- The US Government should enact a policy requiring that the FBI send observers to advise US companies in situations where an employee has been kidnapped abroad.
- The US Department of State should strive to provide even more timely and accurate reports of criminal activity irrespective of the local country's political concerns.
- The US Government should encourage other nations to enact legislation designed to combat and eliminate 'Air Rage'. Currently only Australia, Canada, the UK and US have laws that address this threat.
- The US Government should create programs that encourage and assist private sector companies to adopt effective crisis management plans and training designed to prevent and/ or manage incidents of kidnapping and terrorist attacks in high-risk countries.

- The US Government should use existing government contacts to encourage and facilitate liaisons between private companies and local law enforcement agencies to minimize crime against US citizens abroad.

- The US Government should encourage greater cooperation and communication between security and commercial branches of government to:
  - avoid private sector companies receiving different messages
  - increase candidness of commercial briefings regarding criminal activity in overseas markets
  - stress the importance of due diligence

- The US Government should require federal agencies to immediately disclose any and all information, within the appropriate security classification, that would assist US businesses abroad. OSAC is the appropriate agency to disseminate the information.

- The US Government should increase OSAC funding for expansion of personnel and educational programs.

Conclusion

As previously stated, the four areas of criminal activity identified by ISMA have a significant impact on US businesses and personnel working, traveling and living abroad. Initially, we state that both OSAC and the FBI should provide assistance to US business.

However, more can and must be done to protect Americans abroad. We believe that our recommendations, if adopted, will have a major impact on improving the security of US businesses and personnel abroad.

I. Global Travel

Description of the Problem

The contemporary American business traveler faces several significant security risks while engaged in international travel. These risks include (1) threats to physical safety, such as kidnapping or other terrorist acts, (2) threats to both physical safety *and* property, such as robbery, burglary, and car-jacking, and (3) threats to property involving sophisticated scams designed to separate business travelers from cash and other valuable assets. Americans, in particular, are targets of such crimes owing to factors ranging from politically motivated anti-American sentiment or the misguided perception that all Americans are affluent targets.

Extent of the Problem

Robbery, Assault, and Car-Jacking

Theft of property represents the primary threat facing international travelers, and thieves increasingly rely on violent tactics, thereby increasing the risk to a traveler's physical safety as well as their property. Thieves take advantage of victims in transition, largely unaware or unfamiliar with the surrounding elements. In certain parts of South and Central America, Africa, South Asia, and the Far East, lack of effective law enforcement, highly organized criminal syndicates, political unrest, and anti-American sentiment combine to create extremely hazardous environments. Theft generally falls into one of the patterns identified below:

1. Ground Transportation

   Traveling to and from airports is a serious concern, even in large cities, and airports therein suffer from pervasive "taxi crimes." In Mexico, robbery and assaults on taxi passengers are frequent, with the passenger often subjected to beatings, shootings, and sexual assault. At the Benito Juarez Airport in Mexico City, for example, licensed and registered taxis bear the airport insignia. Patrons secure travel at prepaid booths where they are issued a receipt with the name of the driver and cab number. Unlicensed and unregulated taxis known as "free" taxis solicit unsuspecting travelers, and with long lines at the registered taxi booths, hurried travelers often will avail themselves of the numerous "free" taxi vendors clamoring for business. In many instances, those patrons are driven to remote or isolated locations before being assaulted, robbed of cash, jewelry, and other valuables, and then abandoned. There are even reported incidents "taxi crimes" resulting in the rape or death of unsuspecting victims. In several cases, victims have reported that men in uniforms perpetrated the crime.

   Another tactic- the so-called "express kidnapping"- occurs when a victim is held at gun point and driven from one ATM location to another, and forced to remove cash until the victim reaches his or her credit card limit. The victim is then released in an isolated area. An average of one "express kidnapping" is reported daily. In another recently reported tactic, thieves stop taxis or lone drivers at night, force them to ingest large quantities of

alcohol or narcotics, and then rob them of ATM and credit cards or other valuables. However, it is believed that most express kidnappings are not reported.

In Colombia, Americans hailing taxis on the street are "kidnapped" by accomplices that force their way into the cab. These victims are driven around for a short period of time, stripped of their valuables, and then released outside of town. A variation of this tactic occurs frequently in Thailand, where cab drivers and their accomplices work in concert. Under this approach, an "occupied" taxi stops to pick up the victim. The first occupant is an accomplice who holds the victim at gun or knifepoint while the driver drives them to a remote location where the assault and robbery occurs.

Other means of ground transportation, such as buses and trains, have their unique concerns. Buses are often targets of massive robberies in rural areas- bands of thieves stop busses at gunpoint and systematically rob all bus patrons. Travelers using trains in Russia, Ukraine, other Slavic countries and India have reported that sleeping gas has been pumped into their sleeping cabins and that they were subsequently robbed of their possessions, including passports.

Business travelers renting cars in foreign countries often find themselves a victim of a car jacking or a false-accident scheme. Criminals usually target the expensive cars typically preferred by executives. In the so-called "bump and run" scam, the victim's car is bumped from the rear, usually late at night or in a low traffic area. As the victim exits the vehicle to check for damage, the victim is assaulted, robbed, and car jacked.

A variation of this approach, known as the "smash and grab" is seen in Tanzania and other African countries. In this situation, thieves ram the targeted vehicle, exit their own vehicle, take the incapacitated victim's valuables, and then flee the scene leaving the helpless victim behind.

Still other theft, accomplished by drugging unsuspecting victims, takes place in clubs, restaurants, and other social settings. Such crimes are prevalent in countries including Russia, Ukraine, Mexico, Colombia, Malaysia, and Philippines. Thieves taint targeted victims' drinks with tranquilizers or narcotics, then follow or assist the inebriated victim to isolated locations to rob or otherwise assault him or her.

2. Airport Theft

Not all theft involves physical attack. In some instances, thieves work in teams near airport security devices to steal expensive-looking bags, briefcases, and laptop computers. For example in the "conveyor belt" scam, a security officer spotting a targeted item distracts the traveler at the x-ray machine or metal detector while an accomplice picks up the item and simply walks away. The security officer will then release the victim, who find his/her personal belongings missing and receives little assistance from the offending yet unsuspected officer.

Another version of this scam involves use of a "blocker" who ties up the security line while an accomplice on the other side picks up the targeted item and again walks away. In this situation, security is typically unaware of the illegal transaction until the victim passes through the delayed line to find their bag missing. By that time the accomplice has vanished.

Whether theft occurs as a result of a simple security scam or a violent physical attack, its seemingly unchecked growth in many countries around the world threatens Americans engaged in international travel.

3. Kidnapping and Other Terrorist Acts

Foreign terrorist organizations including Hizballah, Abu Nidal Organization, Hamas, Al-Jihad, and the Sendero Luminoso or 'shining path' continue to rely on terrorist acts in the hope of effecting political change represents a threat to international travelers. During the five-year period from 1995 to 1999, there were one hundred and twenty-eight (128) distinct attacks on civil aviation aircraft, and there is every reason to believe that civil aviation will continue to serve as an attractive target to politically motivated terrorist groups. The publicity surrounding such attacks is the primary vehicle through which many terrorist organizations disseminate their political rhetoric. Usama Bin Ladin, for example, has claimed both the capability and intent to use shoulder-fired surface-to-air missiles to bring down a U.S. airliner to humiliate the United States.

Despite our best efforts, kidnapping and terrorist acts, including airline hijacking, bombings, and sabotage, pose serious threats to traveler safety. Air Watch, a publication of the International Transport Workers Federation, documented 184 incidents of hijacks, attempted hijacks, air rage, sabotage, and other attacks in 2000. The vast majority of these incidents occurred outside the United States. More than a dozen US citizens were kidnapped in Colombia in 1999, twice as many as in 1998.

Air Rage

A related, and increasingly dangerous phenomenon threatening international and domestic air travel is the pattern of violent behavior now called "air rage." Over the past few years, airline industry experts have noted an alarming increase in the number and frequency of violent assaults on airline crews and passengers, including an increase jump in reported unruly passengers from sixty-six (66) in 1997 to over five hundred (500) in 1998. Aggressive and/or violent behavior on board aircraft poses a serious safety risk to in-flight passengers because of the airplane's isolation from outside assistance and lack of means of retreat. Air rage incidents range from simple disturbances and verbal assaults, to violent physical attacks on airline crews, including examples of passengers attacking pilots in an attempt to force planes to crash. Results from such attacks include serious physical injury to crew members and passengers, forced emergency landings, major delays in airports around the world, and emotional trauma for all involved.

4. Confidence Scams and Credit Card Fraud

In many countries, sophisticated confidence scams rob American business interests of millions of dollars each year. Even experienced foreign transaction specialists are taken in by such scams due to the complexity of local laws and the willingness of legitimate entities to participate in elaborate if illicit schemes. In Nigeria, for example, scam operators stage meetings in borrowed offices of Nigerian government officials and transfer documents on official-looking letterhead, complete with official seals, in order to steal millions in complex money transfer schemes.

In another confidence scam, locals posing as state officials or even just inquisitive residents befriend travelers. These individuals obtain personal information, and then contact the traveler's family or company stating that the traveler has been arrested and will soon be incarcerated. The operator offers to bribe the police and secure the traveler's release in exchange for a percentage of the pay-off. This particular operation is usually timed to take place when the traveler is out of communication and cannot be reached, lending credence to the operator's story.

Credit card fraud occurs throughout the world. Reports indicate that in the Ukraine and Russia, for example, store clerks often double-swipe the cards- a profitable and low-risk approach. Often the unsuspecting victim will not notice anything until the credit card statement is received weeks later when the victim is practically powerless. Double charges caught immediately are easily explained as a simple mistake. In another tactic, clerks swipe credit card through a magnetic reader device that stores the number for later use. This method is difficult to detect when performed quickly by competent thieves. Stored numbers are later downloaded to a computer and sold to illegitimate companies in Malaysia and the Philippines, where the stolen numbers can then be placed on fraudulent cards and sold for a profit.

Issues Impacting the Problem

Many of the areas in which these situations are prevalent suffer great disparity in distribution of social wealth, resulting in large underprivileged classes. Those less fortunate are prone to be bold in criminal enterprises to earn a living. In many countries, Americans are thought to be rich, regardless of financial status, and are targeted for many types of crimes. As American businesses expand in foreign countries, particularly to remote areas of the world, U.S. business travelers will continue to be faced with security and safety risks.

Because of the social and economic transitions that many countries are going through, law enforcement personnel are underpaid, poorly trained and under staffed, creating opportunity for graft and corruption within these law enforcement units. In reality, often police officers commit the crimes or at least act as an accomplice or player in the crime.

Countries that are more economically dependent on international commerce may suppress publicity of crimes against business travelers to protect local economies. As a result, the business traveler may unknowingly venture into a crime-ridden area.

Impact On Private Sector Business

The increase in threats to American business travelers has a chilling affect on global commerce. Countries with high levels of street crime increase security and safety concerns for the business traveler. Businesses often avoid areas where personnel are in jeopardy. Individuals cannot effectively conduct business when they are distracted by concerns for personal safety. Most Americans are familiar with personal crimes of this type, but when coupled with language barriers, local customs, and uncooperative or corrupt law enforcement, their concerns are magnified.

II. Global Crime

Description of the Problem

Due to the severe nature of the crimes of kidnapping and terrorism, they will be addressed in separate sections. Criminal activity in all its other forms represents the significant challenge to private enterprise operating abroad. It poses a serious threat to foreign investments, and has a major, debilitating effect on developing economies.

In the form of organized activity by close-knit groups, organized crime is a major growth industry. China's triads, Colombia's drug cartels, Italy's Mafia, Japan's *yakuza* and the Cosa Nostra of the US are now some of the world's most profitable multinationals. Through their increasingly sophisticated methods, their ability to use modern communications technology, their penetration of legal and semi-legal business, and corruption of government officials, these groups pose an increasing threat to legal private business worldwide.

Extent of the Problem

There is little doubt that democratization and economic transition have had the unfortunate side-effect of generating greater criminal activity in many parts of the world. The rise in unemployment, fragmentation of stable communities by economic change, and a relaxation in law and order policies have contributed to this phenomenon. Most obviously, this is present in Eastern Europe and the former Soviet Union, where the former authoritarian political system ensured that crime figures were generally low. In Russia general levels of crime more than doubled in the 1990s and violent crime increased by even greater proportions. There were more than 30,000 murders in 2000, a per capita rate almost three times more than that of the US.

Mass urbanization in many developing countries is also a contributory factor, which leads to breakdown in traditional social and family orders. The breakdown of the old order in emerging markets through industrialization, automation or dislocation caused by war has created a huge underclass. Many are drawn into crime and criminal gangs. In addition to being involved in general street crime, the unemployed in South African townships make easy recruits for criminal gangs that have turned the country into a major transshipment point for drugs and the base for as many as 1,200 crime syndicates.

Alongside structural changes in societies, poor training and lack of resources for law enforcement is a major reason for crime growth. Where public spending has slumped as a result of economic decline, law enforcement agencies have experienced sharp drops in income. In countries where a private sector has emerged for the first time, able officers have moved from the public to private sector to gain much greater incomes. In many countries of Eastern Europe, private security companies have blossomed, staffed largely by former policemen. In some areas, the police have effectively been privatized, offering security provision and response only in return for financial remuneration.

But socio-economic change in the developed world has also led to rising crime rates, and particularly rising rates of violent crime. A declining crime rate in the US from 1992-99 was offset by increases in countries that experienced economic upheaval or continued high levels of unemployment. Many European cities experienced rises in violent crime over this period. Even in generally peaceful New Zealand, violent crime grew by 77% in the 1990s.

Organized Crime

According to UN Development Program (UNDP) estimates, the world's largest crime gangs gross approximately$1.5 trillion a year, rivaling the economic power of multinational corporations and exceeding many nations' GNP. For all the benefits of globalization, progress has come at a high price. In the same way as legitimate mainstream business has breached national boundaries, organized crime has become a trans-national phenomenon. In its international form, organized crime is much more virulent than the sum of its previous national parts. In addition to spreading more broadly than ever before, it has entered areas previously untouched: tax fraud, stock market fraud schemes and computer crime all offer lucrative rewards for criminal organizations.

Criminal organizations have proven to be versatile in exploiting the dramatic rise in global trade, the increase in personal mobility and advances in communications technology. The development of compensatory regulatory measures have not matched advances in global financial systems, so criminal organizations have used the creation of new stock exchanges and the popularity of complicated financial derivatives to expand their money-laundering activities.

The modern global financial system has many points of access and affords possibilities to trade anonymously, to move money rapidly and easily and to obscure both origin and ownership of money. The Bank of New York, which has been under investigation for allegedly moving as much as $10 billion out of Russia on behalf of customers linked to crime gangs, moves more than $600 billion through its system daily in some 115,000 transactions. The volume and speed of this trade, which has tripled in the last five years, offers ideal cover for criminal organizations. This makes preventative measures hard to implement without affecting operational effectiveness.

The other aspect of globalization that provides increased scope for trans-national organized crime is the greater mobility of people in the globalized world. Trans-national ethnic networks resulting from migration are a major resource for organized crime, providing cover, recruits and trans-national linkages that facilitate criminal activity. Immigrant communities are difficult for

law enforcement agencies to penetrate for cultural and linguistic reasons and therefore provide an built-in security mechanism.

For example, Colombian and Mexican crime gangs have used their ethnic networks in the US to help establish dominance over the cocaine trade, while Nigerians based in Thailand have played a central role in trafficking heroin from the golden triangle countries of Southeast Asia to consumer countries. Nor is migration the only manifestation of increased mobility. The ease and speed of cross-border travel provides new opportunities for criminals, while also making them more elusive. This has been the key to Nigerian drug-trafficking groups extending their activities throughout much of southern Africa.

Greater global interaction is also responsible for the prevalence of strategic alliances among criminal organizations in recent years. Based on complementary expertise, the specialization of roles and functions and a convergence of interests that enables these alliances to transcend the problems stemming from divergent criminal cultures and operating styles. These partnerships also enhance the capacity of trans-national criminal organizations to circumvent law enforcement. Mexican and Colombian gangs have successfully used such partnerships for trafficking a number of commodities into the US, while Colombian and Sicilian gangs have cooperated in developing and exploiting major cocaine markets in Western Europe.

At the lower end of the spectrum, where organized crime focuses on racketeering, prostitution, gaming and smuggling, the effect on private industry tends to be indirect, except in certain sectors such as entertainment and leisure. It is the more sophisticated and often semi-legal activities of organized crime that pose the greatest risk to worldwide investors. Above all, this involves companies that become involved with criminal syndicates through association with an apparently reputable company, either through a joint-venture arrangement, or as supplier, sub-contractor or other type of partner.

At best, such an arrangement can raise reputation risk questions for an investor. At worst, it can result in the complete loss of control over a business, as a criminal syndicate slowly takes over control of a joint-venture arrangement. While the risk of expropriation by national governments has receded significantly since the 1970s, subsidiary companies and substantial assets can be lost through involuntary association with organized criminal groups engaged in semi-legal business operations. Such experiences are most common in the Former Soviet Union, Eastern Europe, and China, but can occur in almost any country with substantial criminal penetration of the judicial system and corrupt connections to government officials.

A further major threat to private business is through the use of legal companies for illegal purposes. This concerns money laundering, now a huge worldwide business, funded by the proceeds of narcotics trading and other illegal activities. The Bank of New York scandal is only the largest of a series of allegations against western financial institutions, which have been accused of involvement, unwitting or otherwise, in laundering money from Eastern Europe.

Financial institutions are most vulnerable to fraud. In some 80% of cases, employees or other insiders engage in fraudulent activity. Criminal penetration of a company is often through staff members who are in some way vulnerable. Companies have not yet fully appreciated the scale of

the problem. In a survey conducted in 2000 by UNISYS, some 36% of UK financial institutions still had no anti-fraud strategy, and 95% of board members of financial institutions had received no training in fraud awareness or prevention. A similar lack of preparedness is characteristic of the financial sectors of most countries.

Issues Impacting the Problem

Increasingly complex criminal activities pose a major challenge to law enforcement agencies worldwide. Particularly in developing countries, resource restraints and weak institutional development often mean that law enforcement agencies are unable to combat powerful criminal groups and organizations, and are therefore left vulnerable to corruption. Even in developed countries, law enforcement agencies often still reflect the out-of-date vision of organized crime as a domestic law and order issue rather than the complex, diverse and fragmented phenomenon it has become. The scenario of criminals in Amsterdam controlled by an Englishman in Monaco selling bogus US securities by telephone to South African business people is a jurisdictional nightmare that yet to be adequately addressed. Until the necessary legislation is put in place, and it may take many years before a satisfactory framework is reached, criminal organizations will continue to exploit the many loopholes available to them.

Some efforts have been made to overcome this weakness. Multinational law enforcement task forces, the use of extradition treaties and mutual legal assistance treaties as well as a growing willingness to provide law enforcement training and judicial assistance to other countries are all part of an attempt to reshape law enforcement to counter this problem. The UN adopted in December 2000 a new Convention on Trans-national Organized Crime. Although it may not have much practical impact initially, it is the beginning of a more effective global response to the problems of trans-national crime networks.

Yet states by their very nature remain fixed and static, with ponderous bureaucratic organizations and a relatively high degree of transparency in their operations. Criminal organizations on the other hand are highly mobile, elusive and largely covert. Criminal organizations are far better equipped to prosper in the borderless world than the cumbersome mechanisms established to deter them.

Impact On Private Sector Business

Organized crime and perceptions of organized crime have a major impact on foreign investment flows. High levels of crime pose threats to the security of staff and physical assets, and increase costs significantly because of security provisions, hardship payments, etc. In countries with widely publicized crime problems, high crime levels make it difficult to attract skilled expatriates. Companies are increasingly concerned about the well being of expatriates, partly because of the difficulty of attracting high-quality staff, but also because of the possibility of litigation by staff against companies believed to have failed in their duty of care. Crime against a member of staff can have a major negative impact on staff morale and productivity, beyond the real impact of a particular criminal incident.

Examples:

1. Nigeria

   Criminal activity poses a threat to personnel living in the country, particularly in Lagos and the Niger Delta. As a result of the large supply of cheap weapons, criminals are often better armed than the police. Moreover, police officers and soldiers are sometimes instigators of crime. As a result, foreign investment has been deterred, in large part because of the reluctance of expatriate staff to take up postings. Other factors are also critical in limiting foreign investment, but crime is a major source of concern and increased costs for companies.

2. South Africa

   In South Africa, the sharp rise in crime in the 1990s and the disproportionate impact on expatriates have been the key deterrents for foreign investors. Major security risks to company personnel in South Africa are aggravated robbery, serious assault, car-jacking and theft from vehicles. Last year also saw the development of kidnap for ransom as a minor, but growing problem, particularly targeting foreign executives negotiating deals with criminal South African businessmen. The criminal situation ensures that businesses must adopt a range of precautions, including regular reviews of residences, travel and personal routines and behaviors to reduce risks. This all adds to investment costs.

III. Kidnapping

Description of the Problem

Crime throughout the world has surged steadily in recent years with kidnapping for ransom effectively becoming an established "business" in several countries. Its practitioners include active guerrilla insurgent groups that use ransom proceeds to fund their causes, demobilized rebels and soldiers who have found that the fighting skills perfected in waging guerrilla campaigns have a practical and lucrative application in the kidnapping trade, and criminal gangs that have recognized and exploited weak local and national law enforcement organizations. Ineffective judicial systems pose little risk of capture and incarceration against potentially large and steady ransom payments.

Documenting the exact number of abductions is impossible. A variety of factors explain statistical gaps. Due to its very nature, the crime often goes unreported. Victims' relatives or employers, commonly are warned by kidnappers not to inform or seek the assistance of police/security forces. Alternatively, those most concerned for the victim's safety deliberately avoid authorities because their competence is in question or their complicity in an abduction is suspected. Further, governments can be reluctant sources of kidnapping statistics, preferring not to document either their inability to maintain the security of citizens or to protect visiting or resident foreigners who are important to their economies. Moreover, precise categorization of the crime is prevented by its evolving forms, including similarity to muggings and robberies.

Nevertheless, while existing information indicates that Latin America leads the world in kidnapping, abductions for profit and/or political gain occur in every region of the globe.

Ironically, some of the developing nations where kidnapping is a hazard are exhibiting prospects of evolving as major players and markets in a maturing global economy. Accordingly, investment and expatriate personnel are flowing to the region in ever-greater numbers. Established elites also are prospering and the numbers of the newly wealthy are growing. These trends also swell the population of potential victims. Moreover, economic disparities are glaring. Corruption is growing. The ranks of the unskilled and unemployed are increasing, especially males with a weapons proficiency gained through guerilla groups or from military service, or increasingly from service with the police. Job markets are not growing at the needed pace nor are law enforcement and security capabilities matching the sophistication of criminals.

In sum, the economic and social climate in many regions of the world is fraught with ominous problems that have contributed to the growth in kidnapping. These are unlikely to be resolved in the near term. Prudence dictates a proactive response. Accordingly, the private business sector needs not only to keep itself informed about the dangers of problematic security environments, but also about the available means of protection against threat.

Extent of the Problem

The undisputed global kidnapping leader is Colombia, where active guerrilla groups and professional criminals abduct an average of over ten victims every day. A sampling of other countries where kidnappers pose a significant risk to expatriates and frequent business travelers includes Mexico, Ecuador, the Philippines and Yemen. While the threat level may be higher in these countries, the risk from abduction exists, at some level, in virtually every developing or politically unstable nation that has a weak or ineffective judicial system. The following is an overview of some countries currently experiencing particular problems with kidnapping:

Colombia

Colombia continues to lead the world in kidnapping for ransom. The private anti-kidnapping group Fundación País Libre (Free Country Foundation) reports that during 2000 some 3,706 individuals were abducted in Colombia. This represents an increase of 16 percent over 1999. The majority of victims were Colombians, but during the last four years over 250 foreigners have been abducted. Twenty-one of those victims were American.

The reality in Colombia is that the number of reported abductions may not accurately reflect the severity of the problem. Many abductions are never reported to the police. Rather, kidnappings and ransom negotiations tend to be handled quietly by family members and business colleagues of the victim.

The principal kidnapping practitioners in Colombia are the nation's insurgent groups. Eighty-six percent of the kidnappings that occurred in 2000 were credited to rebel organizations, principally the National Liberation Army (ELN) and the Revolutionary Armed Forces of Colombia (FARC), which use ransom proceeds to help fund their guerrilla war. Common criminals, the nation's

rightwing paramilitary movements, and unknown groups (likely narcotics traffickers) also actively ply the "trade."

The main abduction targets are merchants, managers, and employees of private businesses. Virtually every US citizen is viewed as having the means to pay ransom and is, therefore, a potential victim. Ransom demands for foreigners have ranged as high as $15 million. The largest ransom payment, according to Colombia anti-kidnapping officials, was $3 million paid in 1999.

Abductions often take place either in rural settings or in urban areas where residents have established a pattern of movement. Foreigners engaged in natural resource extraction industries and in engineering projects that take them into rural Colombia are at particular risk. Any American who ventures into guerrilla- or criminal gang-controlled zones is identified as a kidnapping target. In addition, rebel groups increasingly are setting up random roadblocks on the nation's highways. The insurgents use the roadblocks to kidnap motorists who appear to be viable ransom targets. This tactic is locally called "miraculous fishing." In part, as a result of the ubiquitous kidnapping roadblocks, more expatriates and foreigners are abducted in Colombia than in any other nation.

Avoiding rural Colombia does not guarantee safety. A late February 2001 kidnapping of a Japanese auto parts manufacturing executive in Bogota demonstrates that foreigners can be abducted virtually anywhere in the country. Points of vulnerability for expatriates in urban areas are near home, work, or areas routinely visited, such as a country club, shopping center or country vacation home.

Many victims kidnapped by common criminals are later sold to guerrilla groups, who negotiate ransom payment. The guerrillas have the organization and infrastructure to retain and hide victims for extended periods.

Ecuador

The police Anti-Kidnapping Unit dealt with 88 kidnapping incidents in 2000, mostly of businessmen, perpetrated by kidnapping bands composed of Colombians and Ecuadorians. As recently as 1993, the country did not register a single kidnapping for ransom. Since then there have been 147 kidnappings, including 37 incidents in 1999. These figures may understate the number of kidnappings, however, because many abductions are not reported to the authorities and are handled privately. Generally, abductions are most common near the border with Colombia. Insurgents from Colombia cross into Ecuador to take prisoners in order to ransom them later. Criminal gangs may also work in concert or have an informal relationship with Colombian rebels. Sometimes, criminal groups having no political affiliation will claim to be members of a rebel group in order to raise the intimidation level.

A recent high profile abduction involved seven foreign oil workers -- including four Americans -- who were kidnapped in Ecuador's petroleum-rich northeast jungle. The victims were freed March 1 in exchange for $13 million. The seven were part of a group of ten foreign workers who were kidnapped October 12 from an oil camp in the Pompeya jungle region, about 45 miles

south of the Colombian border. Two captives escaped a few days later. The body of American Ronald Sander, an employee of oil company Helmerich & Payne was found Jan. 31. Sander had been shot in the back and was covered in a white sheet scrawled with the words in Spanish: "I am a gringo. For non-payment of ransom. HP Company." Sources said the killing came after the kidnappers refused to budge from an $80 million ransom demand. Negotiators settled on a $13 million ransom in mid-February, just ahead of the kidnappers' deadline to kill a second hostage. Authorities believe the kidnappers are members of the same criminal gang that held seven Canadians and an American for ransom for 100 days in 1999 and that reportedly maintains ties with Colombia's National Liberation Army guerrilla group.

Mexico

Kidnapping for ransom, including the abduction of non-Mexicans, is a significant security concern. The newspaper *Reforma* reported in November 2000 that, according to data from public security organizations and private security companies, kidnapping declined somewhat in 1999, to a total of 510 cases, after registering a major increase to over 600 cases in 1998 and 570 in 1987. These figures probably do not accurately reflect the magnitude of the problem, however. Frequently, associates or families of most victims deliberately do not inform the police, preferring to handle ransom negotiations privately. While the following figure is unsubstantiated, some observers believe there may be as many as 2,000 kidnappings each year in Mexico.

Based on published reports, in 1999, the greatest number of reported kidnappings occurred in the Federal District (19 percent), followed by Baja California (15 percent), Mexico State (12 percent). In 1999, there were two cases involving the kidnapping of wives of European executives and another two involving the children of executives. The average ransom demand in 1999 was $728,000, while the average ransom actually paid was $52,000.

A variation of the kidnap for ransom is the so-called "quicknapping". In this case, victims are kidnapped in taxis that are seized at gunpoint or in carjackings. The victims are taken to ATM machines to withdraw "instant ransoms" and then released. The quicknappings have evolved further into what are locally referred to as "virtual" kidnappings. The victim of virtual kidnapping is usually held for one to three days while the kidnappers arrange a fast ransom payment with the victim's family. Payoffs tend to be in the $10,000-$30,000 range.

Rather than a deterrent, evidence exists that the police are an integral part of the kidnapping problem. In late December 1999, the Federal Preventative Police, a new police unit established to combat organized crime, arrested a police commander and four policemen in Oaxaca State as they collected a $106,000 ransom for a victim they had kidnapped.

Philippines

Local anti crime activists charge that kidnapping is regaining its status as the country's number one "cottage industry." It is believed that, kidnappers are earning an average of nearly $20,950 a day in ransom payments. During the first three months of 2001, at least 25 people were kidnapped. Chinese-Filipinos are the favorite targets of kidnapping gangs because they are

regarded as wealthier than most. As members of a cliquish minority, they are unlikely to report these crimes to the police. US business personnel are also considered attractive targets because of their perceived ability to pay ransoms. In the early 90s, kidnapping was regarded as the most lucrative crime in the country, with ransom payments as high as $1,047,526 per victim. Kidnappings declined in 1994, however, after President Fidel V. Ramos mobilized the government's anti-crime network to pursue kidnapping gangs. Anti-crime advocates assert that kidnap-for-ransom gangs were effectively neutralized during the 31-month presidency of Joseph Estrada under the aegis of Philippine National Police (PNP) Director General Panfilo Lacson. His successor, PNP Deputy Director Leandro Mendoza, a protégé of new President Gloria Macapagal Arroyo, is held in particular suspicion because of his alleged criminal ties. Whether coincident or not, kidnapping for ransom has boomed during Mendoza's tenure.

In addition to crime gangs, the nation's insurgent movements conduct kidnapping for ransom. In April 2000, the rebel Abu Sayyaf Group (ASG) kidnapped 22 people, including 10 foreign tourists, from the resort island in Borneo, Malaysia. The hostages were transported to the Philippines by the ASG where they were held until a ransom payment of a reported $1 million per captive was made by the government of Libya, which negotiated the release of the victims. Two Americans were among the initial group of captives but were able to successfully evade the ASG insurgents.

Yemen

Kidnapping is a significant threat to westerners in Yemen. Traditional tribal elements and Islamic terrorists have a history of abducting foreigners, including Americans.

The more pervasive threat is kidnapping by disgruntled tribesmen seeking to use their victims as bargaining chips for extracting concessions from the government. This remains a constant threat to foreigners who venture onto Yemeni roads outside principal cities. Tourists, engineers, and extraction industry workers are the most frequent targets.

More than 200 foreigners have been abducted in the past decade with most released unharmed. In 1998, however, Islamic extremists abducted 12 foreign tourists, including two Americans. Four of the hostages subsequently were killed in a shootout between their abductors and forces attempting to rescue them.

Impact On Private Sector Business

In Latin America, with the exception of Colombia, which continues to host thriving rebel insurgent movements, the engine driving kidnapping growth is mostly powered by crime rather than politics. In other regions of the world, groups kidnap not only for profit but to draw attention to political causes or bring pressure on the host government to address local or national grievances. The kidnapping of an American is guaranteed to generate media headlines and usually will force the host government, at the very least, to examine the kidnapper's demands in an effort to ensure the hostages are freed.

Regardless of motivation, the profits generated from ransoms have risen steadily. For example, the database of a commercial threat assessment group indicates a sevenfold increase of profits from just over $25 million in 1992 to $182 million by the end of 1994. Of that amount, kidnappings in Mexico alone accounted for $150 million. Indeed some analysts consider the publicly acknowledged payment in 1996 of a $2 million ransom for a Japanese executive as a key event in advertising the profitability of the crime. Still others point to the 1994 kidnapping of a Mexican financier that extracted a $30 million ransom, while the kidnapping the same year of a ranking supermarket executive yielded a reported $50 million.

While such spectacular coups are rare, kidnappers continue to be "pro-business" in their targeting: during the 1990's, between 30 and 40 percent of victims in Latin America were in the business sector, despite otherwise fluctuating rates of actual kidnappings. American business targets are attractive because U.S. citizens are presumed throughout most of the world to be affluent and many companies are insured against kidnapping and prepared to pay large ransoms. For those looking to make a political statement, US business travelers and expatriates are almost always more ubiquitous within a host country than US diplomats and personnel, making them a larger target pool.

The increasing vulnerability to the kidnapping threat will force companies to expend more resources on security. Already, it is more difficult for companies to find people willing to work or travel in countries where the kidnapping threat is significant. Further, businesses may have to withdraw resident employees and restrict or eliminate travel by U.S.-based workers in high-risk areas. Implementing these measures will surely have a negative impact on business operations and may ultimately dictate that companies relocate to safer environments.

IV. Terrorism

Description of the Problem

Terrorist groups have been active throughout the world over the last ten years. The US State Department's own statistics reported 392 international terrorist (involving citizens or the territory of more than one country) attacks in 1999, of which 169 targeted US interests. In addition to causing hundreds of injuries and deaths each year, terrorist attacks result in massive financial costs to governments and private sector companies. For example, the Irish Republican Army (IRA)'s four large bomb attacks in central London and Manchester (UK) between 1992-96 caused at least $2.7 billion in damage as well as disrupting financial sector operations.

Extent of the Problem

Separatist terrorism

Common in Europe since the1970's, separatist terrorism remains a significant concern. Generally directed against domestic government interests and personnel, it can also extend into bomb attacks directed at 'civilian' targets such as financial centers and urban areas to force concessions from governments.

Examples

In December 1999, the Basque separatist terrorist group ETA resumed its campaign after a 14-month cease-fire and killed 23 people in a series of shootings and car bomb attacks across Spain, and injured many more. Police thwarted an attempted grenade attack in September 2000 that was aimed at assassinating Prime Minister Aznar and German Chancellor Gerhard Schroeder during an official event in Hernani (Basque Country). ETA appears likely to expand operations into France in response to French police operations against the group.
Dissident Real IRA recently carried out scores of attacks against military installations in Northern Ireland and attempted 'spectacular' bomb attacks aimed at causing massive damage to high-profile interests in London: MI6 building on 20 Sep 2000; BBC television center 4 Mar 2001. Mainstream Provisional IRA has maintained a cease-fire since July 1997, but it is capable of resuming its terrorist campaign in mainland Britain in the event of a breakdown in political negotiations.

In addition to waging war with government troops in northern Sri Lanka, the Tamil separatist Liberation Tigers of Tamil Eelam (LTTE) also carry out frequent bomb attacks targeting government officials, military installations, commercial interests such as oil depots, and indiscriminate suicide bomb attacks in crowded areas of the capital Colombo. These attacks are aimed at causing as much human and economic damage as possible and reinforce the LTTE message that there will be no peace or stability until its demands have been met. Suicide bomb attacks in Colombo killed over 100 people in 2000, and in December 1999 President Kumaratunga narrowly escaped assassination after a suicide bomber detonated explosives carried in her handbag: 26 killed, 110 injured.

Until 1999, the Kurdish separatist Kurdish Workers' Party (PKK) carried out a similar campaign in Turkey. The group operated an insurgency against government troops in the southeast of the country while also carrying out terrorist attacks in Istanbul and on the Aegean coast, including bomb attacks at popular tourist sites, upscale shopping centers and bus and railway stations. However, since Turkish security forces in February 1999 arrested the PKK leader Abdullah Ocalan in Kenya, the group has scaled down its campaign and ceased terrorist attacks aimed at forcing the creation of an independent Kurdish state.

Often separatist terrorist groups are motivated by religious motives, especially in the case of Islamist groups based in central Asia, China and southeast Asia. These groups have routinely used terrorist attacks as part of their campaigns. For example, Islamic separatist terrorists continue to carry out attacks in the Xinjiang province of China, in border areas of Uzbekistan and Kyrgyzstan, and in the Mindanao province of the Philippines, among other locations.

Left-wing terrorist/guerrilla groups

These groups are based primarily in Latin America. Although politically motivated, they also often have links with criminal groups involved in drug trafficking and kidnapping. Many left-wing guerrillas involved in insurgencies against governments also carry out terrorist attacks in busy urban areas and against economic targets such as oil pipelines and electricity suppliers.

Revolutionary Armed Forces of Colombia (FARC) wages armed insurgency against the state by trying to seize power by force. The group launches armed attacks against security force targets (police stations, military outposts), and also frequently bombs economic infrastructure (oil pipelines/installations, infrastructure). Occasional car bomb/mortar attacks in urban centers, usually against security force installations, kidnap for ransom, and extortion demands against foreign companies are also part of their operations. FARC attacks against economic infrastructure have continued unabated and in the second half of 2000, FARC effectively paralyzed normal activities in the Putumayo department with implementation of so-called 'armed strikes,' in which FARC enforced prohibition on all overland transportation.

Also in Colombia, the National Liberation Army (ELN)'s weakened military capacity has forced the group to increase its level of terrorist activity, especially sabotage of electricity and oil infrastructure. The ELN also attacks road infrastructures, such as bridges, and launches sporadic bomb attacks in urban centers. These include large car bomb attacks against economic and security force targets as well as smaller bomb attacks – generally at night and not designed to cause physical injury against banks. The ELN was responsible for a large percentage of the record 98 bomb attacks against the Cano-Limon-Covenas oil pipeline in 2000. In an effort to extract concessions from the government, the ELN in 1999 intensified its sabotage campaign against the electricity sector, bombing 267 electricity pylons. In the past two years, the ELN has staged a number of mass kidnappings, including the hijacking in April 1999 of a domestic airline flight.

In Peru, the Tupac Amaru Revolutionary Movement (MRTA) has carried out bombings of foreign targets over the last ten years, with special focus on US entities. The MRTA is also involved in kidnappings and assassinations. The most significant recent event centered on the hostage crisis at the Japanese ambassador's residence in Lima. 14 members of the MRTA took hostage guests at a function on 17 December 1996. On 22 April 1997, Peruvian Special Forces stormed the residence. All 14 activists were killed. On 10 September 1998, police arrested nine MRTA guerrillas and found a large cache of armaments. In November 1998, which effectively ended armed activity by the MRTA, additional leaders were arrested. However, a resurgence of armed activity remains a potential security risk.

The Nepal Communist Party (Maoist, NCP-M) started an insurgency in 1996, reportedly borne out of frustration with the country's system of democracy and the emergence of widespread corruption, money politics and organized crime. Most Maoist violence takes the form of attacks against police posts in remote rural areas. Foreign banks based in Kathmandu have received threatening letters demanding money, while foreign aid offices in rural areas have been attacked. Attacks were carried out, most recently resulted in the robbery of 15 Polish tourists in February 2001, may be the work of criminal gangs rather than bona fide insurgents.

In developed countries, there is less threat of guerrilla insurgencies similar to those in Latin America, but several urban left-wing terrorist groups remain active. Of these the most effective is the Revolutionary Organization November 17 in Greece, which has carried out 23 assassinations and numerous bomb and rocket attacks over the last 24 years, targeting government buildings, diplomatic missions and high-profile foreign businesses, as well as

foreign government personnel and wealthy Greek businesspeople. In June 2000, the group killed the British defense attaché as he drove to work in northern Athens. It subsequently claimed that the attaché was actively involved in planning NATO air strikes against Yugoslavia in 1999.

Islamic Extremist Terrorist Groups

Islamic extremist terrorist groups are based primarily in the Middle East and Asia: three of the most significant groups are described below, although there are also groups active in Algeria, Indonesia, the Philippines, Egypt, Lebanon and elsewhere. These groups generally use terrorist violence as part of their campaigns against moderate Muslim or secularist governments, but are often also vehemently opposed to the US government because of interventions against Iraq and Libya, as well as its perceived support for Israel.

The Al-Qaida Islamic extremist group consists of Saudi-born terrorist leader Osama bin Laden's close-knit cadres in Afghanistan and around the world. Its primary aim is the removal of US military forces from the Persian Gulf and Arabian Peninsula. The group directly organizes attacks or supports local groups attacking US military and diplomatic interests in the Middle East and elsewhere. Al-Qaida was responsible for the simultaneous bombings of the US embassies in Nairobi (Kenya) and Dar es-Salaam (Tanzania) in August 1998. Bin Laden supported efforts by an Algerian network in Canada to bomb targets in the US and by Jordanian extremists to attack tourist sites in Jordan; both attacks were to take place on the millennial New Year's eve. Al-Qaida was suspected of being involved in the October 2000 bombing of the USS Cole in Yemen and a number of plots targeting US military and diplomatic facilities in the Persian Gulf in the second half of 2000.

Hamas is the main Islamic faction in Palestinian politics, and has been the main rival to the Palestinian Authority (PA), which is dominated by Yasser Arafat's Fatah faction. However, this security cooperation broke down in late 2000, and Hamas and the related Islamic Jihad group have confirmed their renewed ability to operate with a series of bomb attacks in Israel in late 2000 and early 2001. Islamic Jihad claimed responsibility for a car bomb in Jerusalem in November 2000. Six more recent attacks in Netanya, Hadera, Tel Aviv and West Jerusalem (Israel) appear to have been the work of Hamas. Most have been bombs attached to parked cars or public buses and taxis, although suicide bombing re-emerged in March 2001. Attacks tend to target crowded commercial centers such as markets and shopping centers.

Islamic Movement of Uzbekistan (IMU) has attempted over the last few years to destabilize the whole southern and eastern borderland of Uzbekistan, and also southern Kyrgyzstan. Breakdowns in border security also aid the IMU in the shipment of narcotics. In its largest terrorist attack, the IMU carried out seven bomb explosions in Tashkent (Uzbekistan) on 16 February 1999. At least 15 people were killed, and about 150 people were injured. Those killed and injured in the bombings were mainly bystanders. The attacks were probably designed to assassinate Karimov.

Issues Impacting the Problem

US or NATO-led military interventions against Yugoslavia and Iraq have recently provoked terrorist actions against US interests in third party countries, such as Greece and Italy. US foreign policy interventions in the Middle East in particular are almost certain to provoke some form of terrorist retaliation against US government or commercial interests in the long-term.

In 1998, the US State Department ordered a comprehensive review of security provisions in its diplomatic missions around the world, and demanded that physical security upgrades such as the construction of blast perimeter walls, vehicle barriers and 'setbacks' from public roads be implemented where possible. This increased fortification of US diplomatic missions worldwide, coupled with changes made after the bombing of the US embassy in Beirut in 1982, appears in some cases to have encouraged terrorist groups to target more accessible US private commercial interests. In Greece, the 'November 17' group confined its attacks on US interests in 1999-2000 to commercial interests but also attacked unfortified German, Dutch and British diplomatic missions and personnel, presumably because they were 'softer' targets than better protected US government interests.

Impact on Private Sector Business

Terrorism has had a significant direct impact on US private sector business. Left-wing guerrillas in Colombia, Ecuador and elsewhere have repeatedly attacked oil pipelines operated or owned by US companies, in addition to kidnapping expatriate personnel. In some cases this represents a specific targeting of US companies, while in other countries terrorists have pursued all foreign companies as part of wider campaigns.

In Europe, terrorist groups have frequently targeted US companies in small-scale attacks, to protest against, for example, US military intervention in Yugoslavia or Iraq. Terrorists have targeted US companies because of their high profiles, and the fact that they are perceived as closely linked to, or even identical to, the US government. Long-running terrorist campaigns have had indirect effects on US companies operating overseas.

For example, long-running terrorist campaigns have had the effect of raising insurance premiums and other operating costs for US companies working in certain countries. In 2000, insurers reported that if premiums are forced to rise again because of the risk of guerrilla attacks, it will become more cost effective for companies to self insure.

Terrorist action overseas has deterred US companies from considering investing or operating in certain countries affected by concerted terrorist campaigns. Many companies are reluctant to enter markets where frequent attacks on telecommunications, electricity supplies or roads are liable to disrupt business operations and place personnel at risk.

Mr. PUTNAM. Let the record note that Mr. Platts of Pennsylvania and Mr. Tierney of Massachusetts have joined the subcommittee.

At this time, the Chair recognizes Mr. Bishop. Mr. Bishop is the director of disaster response and resource committee, InterAction.

Welcome to the subcommittee.

Mr. BISHOP. Thank you, Mr. Chairman and members of the subcommittee, for the opportunity to participate in this morning's hearing.

Security for nongovernmental organizations, particularly those NGO's on the front lines of disaster relief and refugee protection and assistance, has become a vital concern among our members.

Mr. PUTNAM. Mr. Bishop, could you move the mic closer, please.

Mr. BISHOP. We greatly appreciate your interest and concern. Where NGO's were once the victims of random violence, they increasingly have become the specific targets of violence by governments, nonstate actors, as well as individuals. Motives include resentment at perceived NGO preference for one of the belligerent parties; a desire to force foreigners out of an area so that there will be no credible witnesses to war crimes and other human rights violations; and the desire of thugs or belligerents to seize the assets NGO's, U.N. agencies, and the Red Cross movement bring to disaster sites.

Death and severe injuries, hostage-taking, rape, and theft have taken an increasing toll among United Nations, NGO, and Red Cross movement field workers during the 1990's. The United Nations keeps the best records, and they report that between January 1992 and the year 2000, a total of 189 field personnel lost their lives on overseas assignments, with 98 murdered.

Our members are dealing each year with incidents in which their personnel are robbed, incarcerated under one pretext or another, and taken hostage by criminals or belligerents. Offices are invaded by loot-seeking soldiers, guerilla bands, crooks, etc. There are near escapes as bullets and grenades strike nearby. Land mines blow off limbs. NGO vehicles slip off back roads taken to avoid mines, and their occupants die.

As security threats have become more lethal and common, NGO's have taken greater care to look after their employees overseas. The process has been encouraged by the sympathetic response of USAID's Office of Foreign Disaster Assistance [OFDA]. It has provided InterAction with over $800,000 to design and field-test two courses, one on provision of health services and complex emergencies and the other on security for field workers.

The further we looked into the subject of security, the more sharply our members appreciated that the government and corporate approaches to overseas security are not appropriate for NGO's.

CARE and Catholic Relief Services cannot retreat to walled and barred compounds or ride through the city in armored cars accompanied by armed bodyguards. The mission of most NGO's is to live among and serve the local poor and disaster stricken. They must remain accessible to their clientele, forgo sidearms, and depend upon their good relations with the local community and constant threat assessments as their primary survival tools. The NGO ap-

proach cannot be one of physical deterrence or retaliation; it has to be acceptance by the population they are serving.

Thus, the InterAction security course relies more on the Mennonites than the U.S. Marines for content. It stresses personal conduct and cultural sensitivity as well as roadblock negotiations, mines avoidance, communications security, vehicle movement controls, and evacuation planning.

The next stage in our collaborative relationship with OFDA on security was approval of a proposal to persuade CEOs of disaster response agencies that security could and should be incorporated into their organizational culture and operations. Twenty-four CEOs and senior managers of leading American and Canadian NGO's spent 2 days last September in a very participatory program. CEO accounts of their successes and problems in trying to promote security awareness and training within their own agencies were very credible to their peers.

The InterAction is pleased with the support it continues to receive from OFDA in addressing its security vulnerabilities.

With respect to the State Department, the help on security has not been financial, but diplomatic. Senior officials of the Bureau of Population, Refugees and Migration have been very accessible and ready to bring—see pressure put on foreign governments impeding access to refugees and internally displaced persons, or refusing visas to relief workers.

There are several security issues which remain unresolved between the U.S. Government and most of our members. I must note at this point that I am not speaking for all of our members in identifying additional help. Most would appreciate receiving funds from the government. As a matter of principle, some of our members do not solicit or accept any U.S. Government funds. And one member which does solicit U.S. funding for the operations of its overseas partners recently informed us that it opposes any U.S. Government funding for NGO security initiatives.

The unmet needs most of our members would like to see the government resolve include coverage of the costs NGO's incur in upgrading their security awareness and procedures. These include the cost of employees hired to supervise security operations, training costs, equipment costs, particularly communications equipment, additional insurance, better protective vehicles and so forth.

Another key issue for our community is eligibility for evacuation by the U.S. Government. I was surprised by reports that members of our agencies had been told by Embassy officers in some evacuations that their foreign citizen spouses and children were ineligible to accompany them. More frequently, American NGO's reported that their third-country employees had been told that there was no room for them in the helicopter or naval vessel conducting the evacuation.

In fairness to Assistant Secretary of State for Consular Affairs, Mary Ryan, and Embassy officers who conduct these hazardous operations, I must admit that we have not sat down with them to seek greater clarity and consistency on this issue. We will seek such a discussion.

Another of our concerns is the growing unwillingness of the U.S. Government to put its personnel in harm's way. When U.S. Gov-

ernment employees assigned to work with NGO's and instructed not to go outside their hotel, to be back across the border by nightfall, are withdrawn under the pretext of a voluntary departure, it is hard for NGO's to provide the humanitarian services the Congress and U.S. people want undertaken.

As our members frequently find themselves involved working alongside U.S. military forces engaged in peacekeeping and humanitarian operations, we have long had a program which involves our staff and members' giving presentations on the respective roles of NGO's and the military at disaster sites. We have helped prepare relevant military manuals and participated in both command post and field exercises. Unfortunately, the information shared often does not reach those assigned to the next intervention. We're trying to identify funding which would give our input greater reach and timeliness.

A 30-minute video placed aboard each assault ship and in pilot ready-rooms, defining the roles of NGO's, would be one approach if we can mobilize the funding. If members of this subcommittee find the concept meritorious, your assistance in providing the funds or directing their use would be greatly appreciated.

Thank you for this opportunity to appear before you this morning and for your attention. I look forward to your comments and questions. Thank you.

Mr. PUTNAM. Thank you, Mr. Bishop.

[The prepared statement of Mr. Bishop follows:]

WRITTEN TESTIMONY BY JAMES K. BISHOP

FOR THE

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS AND INTERNATIONAL RELATIONS

APRIL 3, 2001

MR. CHAIRMAN AND MEMBERS OF THE SUBCOMMITTEE:

THANK YOU FOR THIS OPPORTUNITY TO PARTICIPATE IN THIS MORNING'S HEARING. AS YOU MAY KNOW, INTERACTION IS A COALITION OF 160 AMERICAN NGOS PROVIDING ASSISTANCE IN SUSTAINED DEVELOPMENT, DISASTER RESPONSE AND REFUGE ASSISTANCE AND PROTECTION IN SOME 100 NATIONS ABROAD. THE MEMBERSHIP INCLUDES MOST OF THE MAJO R AMERICAN NGOS ENGAGED IN THESE FIELDS, E.G. CARE, SAVE THE CHILDREN, CATHOLIC RELIEF SERVICES, WORLD LEARNING, THE INTERNATIONAL RESCUE COMMITTEE, WORLD VISION, ETC. THE INTERACTION SECRETARIAT ASSISTS THE MEMBERS IN CONVENING MEETINGS WITH UNITED STATES GOVERNMENT AND UNITED NATIONS AGENCIES. WE PROVIDE TRAINING AND SET AND MAINTAIN STANDARDS. WE ENGAGE IN ADVOCACY ON OUR MEMBERS' BEHALF. WE SERVE AS FOCAL POINT FOR COUNTERPART COALITIONS IN OTHER PARTS OF THE WORLD.

FOR ALMOST SIX YEARS I HAVE SERVED INTERACTION AS DIRECTOR OF ITS DISASTER RESPONSE UNIT, WHICH MEANS THAT I WORK MOST DIRECTLY WITH THE 35 MEMBERS OF OUR DISASTER RESPONSE COMMITTEE. IT IS COMPOSED OF AGENCIES FOCUSED IN WHOLE OR IN PART ON PROVIDING ASSISTANCE TO THOSE AFFECTED BY NATURAL AND MAN MADE DISASTERS ABROAD, WHETHER IN THE SUDAN, NORTH KOREA, INDIA, MOZAMBIQUE, SAN SALVADOR, AFGHANISTAN, THE CONGO OR WEST AFRICA. AS THE NAME CARD SUGGESTS, MOST OF MY PROFESSIONAL LIFE WAS SPENT IN THE U.S. FOREIGN SERVICE, WHERE I WAS ENGAGED IN RESPONSES TO MAN-MADE DISASTERS IN LEBANON, AND LATER AS AMBASSADOR IN LIBERIA AND SOMALIA, AS WELL AS DURING EIGHT YEARS SERVICE AS DEPUTY ASSISTANT

SECRETARY OF STATE, FIRST FOR AFRICA AND THEN FOR HUMAN RIGHTS AND HUMANITARIAN AFFAIRS.

WHERE NGOS ONCE WERE THE VICTIMS OF CRIMINALITY AND RANDOM VIOLENCE, THEY INCREASINGLY HAVE BECOME THE SPECIFIC TARGETS OF VIOLENCE BY GOVERNMENTS, NON-STATE ACTORS, AS WELL AS INDIVIDUALS. MOTIVES INCLUDE RESENTMENT AT PERCEIVED NGOS PREFERENCES FOR ONE OF THE BELLIGERENT PARTIES, A DESIRE TO FORCE FOREIGNERS OUT OF AN AREA SO THERE WILL BE NO CREDIBLE WITNESSES TO WAR CRIMES AND OTHER HUMAN RIGHTS VIOLATIONS, AND THE DESIRE OF THUGS, GANGS OR BELLIGERENTS TO SEIZE THE ASSETS NGOS, UN AGENCIES AND THE RED CROSS MOVEMENT BRING TO DISASTER SITES. IN ADDITION, THERE ARE DISGRUNTLED EMPLOYEES TAKING REVENGE FOR REAL OR IMAGINED SLIGHTS. SOMETIMES THE IDENTITIES AND MOTIVES OF THE PERPETRATORS ARE UNCLEAR, AS IN THE RECENT KIDNAPPING IN CHECHNYA OF KENNY GLUCK, AN AMERICAN WORKING FOR MEDICINES SANS FRONTIERES.

LACK OF RESPECT FOR THOSE PROVISIONS OF INTERNATIONAL HUMANITARIAN LAW OBLIGING BELLIGERENTS TO PERMIT ACCESS TO THOSE AFFECTED BY WAR HAS INCREASED AS NATIONAL LEADERS AND NON-STATE ACTORS HAVE REALIZED THAT THE INTERNATIONAL COMMUNITY RARELY PUNISHES VIOLATORS. THE FACT THAT A HIGHER PERCENTAGE OF NATIONAL AND REBEL LEADERS ARE NOT ONLY WITHOUT SCRUPLE BUT SEMI-LITERATE MAKES INEFFECTIVE WHAT ONE SENIOR UN OFFICIAL RECENTLY LABELED THE "DIPLOMATIC RUT" OF THE CONVENTIONAL PROTECTION APPROACHES OF THE AND SIXTIES AND SEVENTIES.

DEATH AND SEVERE INJURIES, HOSTAGE TAKINGS, RAPE AND THEFT HAVE TAKEN AN INCREASING TOLL AMONG UN, NGO AND RED CROSS MOVEMENT FIELD WORKERS DURING THE NINETIES. THE UNITED NATIONS KEEPS THE BEST RECORDS AND THEY REPORT THAT BETWEEN JANUARY 1992 AND 2000 A TOTAL OF 189 UN FIELD PERSONNEL LOST THEIR LIVES ON OVERSEAS ASSIGNMENTS, WITH 98 MURDERED. THE INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC) HAD NINE OF ITS EXPATRIATE FIELD WORKERS MURDERED IN CHECHNYA AND THREE MURDERED IN BURUNDI IN RECENT YEARS. FRED CUNY, A GIANT IN THE AMERICAN NGO MOVEMENT, DISAPPEARED IN CHECHNYA IN THE MID-NINETIES.

AMONG THE LIABILITIES OF THE DIVERSIFICATION OF THE NGO COMMUNITY IS ITS FAILURE TO MAINTAIN RECORDS OF SECURITY INCIDENTS IN WAYS WHICH WOULD ALLOW COMPILATION OF CASUALTY TOLLS SIMILAR TO THOSE PUBLISHED BY THE UN. BUT OUR MEMBERS ARE DEALING EACH YEAR WITH INCIDENTS IN WHICH THEIR PERSONNEL ARE ROBBED, INCARCERATED UNDER ONE PRETEXT OR ANOTHER, AND TAKEN HOSTAGE BY CRIMINALS OR BELLIGERENTS. OFFICES ARE INVADED BY LOOT SEEKING SOLDIERS, GUERRILLA BANDS, CROOKS, ETC. THERE ARE NEAR ESCAPES AS BULLETS OR GRENADES STRIKE NEARBY. NGO WORKERS DIE AT THE HANDS OF CRIMINALS AND ARE ARRESTED BY LOCAL GOVERNMENTS AFTER THE U.S. GOVERNMENT TAKES MILITARY ACTION AGAINST THE GOVERNMENT. LANDMINES BLOW OFF LIMBS. NGO VEHICLES SLIP OFF BACK ROADS TAKEN TO AVOID MINES AND THEIR OCCUPANTS DIE.

AS SECURITY THREATS HAVE BECOME MORE LETHAL, NGOS HAVE TAKEN GREATER CARE TO LOOK AFTER THEIR EMPLOYEES OVERSEAS. THE PROCESS WAS ENCOURAGED BY THE SYMPATHETIC RESPONSE OF USAID'S OFFICE OF FOREIGN DISASTER RESPONSE (OR OFDA). OUT OF DISCUSSIONS BETWEEN OFDA AND INTERACTION'S DISASTER RESPONSE COMMITTEE CAME AGREEMENT IN THE EARLY 1990S TO POLL OUR MEMBERS ON WHAT THEY SAW AS THEIR MOST PRESSING TRAINING NEEDS. OFDA EXPECTED THE RESPONSE TO BE TRAINING IN HOW TO PROVIDE TECHNICAL SERVICES MORE EFFECTIVELY AT DISASTER SITES. IN FACT, THE TRAINING MOST RESPONDENTS INDICATED WAS AT THE HEAD OF THEIR WISH LIST WAS SECURITY TRAINING.

OFDA ACCEPTED THE RESULTS OF THE POLL AND GAVE INTERACTION A TOTAL OF OVER $ 800,000 TO DESIGN AND FIELD TEST TWO COURSES, ONE ON PROVISION OF HEALTH SERVICES IN COMPLEX EMERGENCIES AND THE OTHER ON SECURITY FOR FIELD WORKERS. WE SET UP A SECURITY ADVISORY GROUP COMPOSED OF SECURITY EXPERTS FROM BOTH OUR MEMBERS AND OUTSIDE PROFESSIONALS. THE FURTHER THE GROUP LOOKED INTO THE SUBJECT OF SECURITY THE MORE SHARPLY THE MEMBERS APPRECIATED THAT THE GOVERNMENT AND CORPORATE APPROACHES TO OVERSEAS SECURITY WERE NOT APPROPRIATE FOR NGOS.

CARE AND CRS COULD NOT RETREAT TO WALLED AND BARRED COMPOUNDS, OR RIDE THROUGH THE CITY IN ARMORED CARS ACCOMPANIED BY ARMED BODYGUARDS. THE MISSION OF MOST NGOS IS TO LIVE AMO NG AND SERVE THE LOCAL POOR AND DISASTER STRICKEN. THEY MUST REMAIN ACCESSIBLE TO THEIR CLIENTELE, FOREGO SIDE ARMS, AND DEPEND ON THEIR GOOD RELATIONS WITH THE LOCAL COMMUNITY AND CONSTANT THREAT ASSESSMENTS AS THEIR PRIMARY SURVIVAL TOOLS. THE NGO APPROACH CANNOT BE ONE OF PHYSICAL DETERRENCE OR RETALIATION. IT HAS TO BE ACCEPTANCE BY THE POPULATION T HEY ARE SERVING. THUS THE INTERACTION SECURITY COURSE RELIED MORE ON THE MENNONITES THAN THE U.S. MARINES FOR CONTENT. IT STRESSED PERSONAL CONDUCT A ND CULTURAL SENSITIVITY AS WELL AS ROADBLOC K NEGOTIATIONS, MINES AVOIDANCE, COMMUNICATIONS SECURITY, VEHICLE MOVEMENT CONTROLS, AND EVACUATION PLANNING. THAT COURSE IS NOW BEING CONDUCTED WITH VARIOUS MODIFICATIONS ALL AROUND THE WORLD BY OUR MEMBERS, OTHER NGOS, AND THE BRITISH NGO RED R, WHICH SPECIALIZES IN TRAINING. OFDA IS HELPING TO SUBSIDIZE THE COURSE PRESENTATIONS BY RED R. THROUGHOUT THE PROCESS OF CURRICULUM DEVELOPMENT AND PILOTING, THERE WAS CLOSE COLLABORATION WITH UN SECURITY OFFICIALS, AS WELL AS WITH THOSE OF THE RED CROSS MOVEMENT, AND INVOLVEMENT AT ALL LEVELS OF EUROPEAN NGOS.

OFDA NEXT ASKED INTERACTION TO PREPARE G UIDELINES FOR SECURITY PLANNING, WHICH WE DID GLADLY. NGOS PRESENTING PROJ ECT PROPOSALS FOR DISASTER RESPONSE SUBSEQUENTLY HAVE BEEN REQUIRED TO STATE WHETHER OR NOT THEY HAVE A SECURITY PLAN FOR EACH POST COVERED BY THE PROPOSAL PREPARED IN ACCORDANCE WITH INTERACTION'S GUIDELINES. THEY MUST EXPLAIN WHY NOT, IF THEY DO NOT. STATE'S BUREAU OF POPULATION, REFUGEES AND MIGRATION (BPRM), ANOTHER MAJOR SOURCE OF FUNDING FOR NGOS ENGAGED IN DISASTER RESPONSE, PARTICULARLY CARE OF REFUGEES, IS IN THE PROCESS O F INCORPORATING A SIMILAR PROVISION IN THE GUIDELINES IT IS COMPOSING. MEANWHILE A NUMBER OF OUR MEMBERS HAVE DEVELOPED THEIR OWN SECURITY GUIDELINES AND HANDBOOKS. I HAVE BROUGHT A SAMPLING. MORE UPGRADED THE LEVEL OF RESPONSIBILITY FOR SECURITY WITHIN THEIR OWN ORGANIZATIONS.

OFDA'S RECENT DIRECTOR ROY WILLIAMS WAS A LONGTIME PROPONENT OF THE VIEW THAT SENIOR MANAGEMENT HAS TO BECOME PARTISANS OF GREATER ATTENTION TO SECURITY IF THE NEEDED CHANGES IN AGENCY CULTURE AND PRACTICES ARE TO ACHIEVED. THUS THE NEXT STAGE IN OUR COLLABORATIVE RELATIONSHIP WITH OFDA ON SECURITY WAS APPROVAL OF A PROPOSAL TO PERSUADE CEOS OF DISASTER RESPONSE AGENCIES THAT SECURITY COULD AND SHOULD BE INCORPORATED IN THEIR ORGANIZATIONAL CULTURE AND OPERATIONS. WITH OFDA'S FINANCIAL SUPPORT, TWENTY-FOUR CEOS OF LEADING AMERICAN AND CANADIAN NGOS SPENT TWO DAYS LAST SEPTEMBER IN A VERY PARTICIPATORY PROGRAM INVOLVING PRESENTATIONS FROM THE RAND CORPORATION, THE ICRC, THE INTERNATIONAL FEDERATION OF RED CROSS AND RED CESCENT ACTIVITIES (IFRC), RED R, ETC. THERE ALSO WAS AMPLE TIME FOR DISCUSSION AMONG THE CEOS, WHOSE ACCOUNTS OF THEIR SUCCESSES AND PROBLEMS IN TRYING TO PROMOTE SECURITY AWARENESS AND TRAINING WERE VERY CREDIBLE TO THEIR PEERS. WE ARE ABOUT TO UNDERTAKE THE FIRST OF TWO IMPACT SURVEYS. MEANWHILE OUR MEMBERS AND OTHER NGOS HAVE A SEMINAL WORK WRITTEN FOR THE SEMINAR BY KOENRAAD VAN BREBANT ENTITLED *MAINSTREAMING THE ORGANIZATIONAL MANAGEMENT OF SAFETY AND SECURITY*, A FOLLOW-ON TO THE AUTHOR'S EARLIER *OPERATIONAL SECURITY MANAGEMENT IN VIOLENT ENVIRONMENTS.*

IN FEBRUARY OF THIS YEAR WE RECEIVED OFD A'S APPROVAL TO USE AVAILABLE FUNDING TO MOVE TO THE NEXT STEP IDENTIFIED BY THE SEPTEMBER SEMINAR PARTICIPANTS. CONSULTANTS ARE NOW EXAMINING WHAT SECURITY RESPONSIBILITIES INTERNATIONAL NGOS, PRIMARILY OUR MEMBERS, ARE ASSUMING FOR THE SECURITY OF THEIR NATIONAL STA FF. IS THERE JUST A WAVE FROM THE EXPATS AS THEIR HELICOPTER CLEARS THE EVACUATION SITE, OR ARE NATIONAL STAFF SECURITY NEEDS BEING PAID SERIOUS ATTENTION ?

AS THIS INVENTORY OF PROGRAMS SUGGESTS, INTERACTION IS PLEASED WITH THE SUPPORT IT CONTINUES TO RECEIVE FROM OFDA IN ADDRESSING ITS SECURITY VULNERABILITIES. WITH RESPECT TO BPRM THE HELP HAS NOT BEEN FINANCIAL BUT DIPLOMATIC. SENIOR BPRM OFFICIALS HAVE BEEN VERY ACCESSIBLE AND READY TO S EE PRESSURE PUT ON

FOREIGN GOVERNMENTS IMPEDING ACCESS TO REFUGEES AND IDPS, OR REFUSING VISAS TO RELIEF WORKERS. WHEN THE OCCASIONAL INADEQUATE PERFORMANCE OF UN AGENCY OFFICIALS HAS BECOME A SECURITY PROBLEM, BPRM HAS HAD A QUIET WORD WITH THE HEAD OF A UN AGENCY IT FUNDS. WHEN EFFORTS TO ENGAGE THE UN AGENCIES IN A SERIOUS DISCUSSION ABOUT NGO/UN SECURITY COOPERATION IN THE FIELD WERE STONEWALLED BY MIDLEVEL UN OFFICIALS, A DIRECT APPROACH BY BPRM TO THE HEAD OF THE UN AGENCY RESPONSIBLE FOR THE ROADBLOCK BROKE IT, AND AN ENCOURAGING DIALOGUE IS NOW UNDERWAY.

THERE ARE SEVERAL SECURITY ISSUES WHICH REMAIN UNRESOLVED BETWEEN THE USG AND MOST OF OUR MEMBERS. I SHOULD NOTE AT THIS POINT THAT I AM NOT SPEAKING FOR ALL OF OUR MEMBERS IN IDENTIFYING ADDITIONAL HELP MOST WOULD APPRECIATE RECEIVING FROM THE GOVERNMENT. AS A MATTER OF PRINCIPLE, SOME OF OUR MEMBERS DO NOT ACCEPT ANY U.S. GOVERNMENT FUNDS. AND ONE MEMBER WHICH SOLICITS U.S, FUNDING FOR THE OPERATIONS OF ITS OVERSEAS PARTNERS RECENTLY INFORMED US THAT IT OPPOSES ANY U.S. GOVERNMENT FUNDING FOR NGO SECURITY INITIATIVES.

THE MOST IMPORTANT UNMET NEED MOST OF OUR MEMBERS WOULD LIKE THE GOVERNMENT TO RESOLVE IS COVERAGE OF THE COSTS NGOS INCUR IN UPGRADING THEIR SECURITY AWARENESS AND PROCEDURES. THESE INCLUDE THE COSTS OF EMPLOYEES EITHER HIRED TO SUPERVISE SECURITY OPERATIONS OR DIVERTED FROM OTHER DUTIES, THE COSTS OF ASSIGNING PERSONNEL TO THE FIELD TASKED SPECIFICALLY WITH THIS RESPONSIBILITY, TRAINING COSTS, EITHER IN-HOUSE OR VIA RED R, EQUIPMENT COSTS, PARTICULARLY COMMUNICATIONS EQUIPMENT, ADDITIONAL INSURANCE, BETTER PROTECTED VEHICLES, ETC. AS THOSE WHO KNOW NGOS WILL APPRECIATE, THE NGOS HAVE DIVERSE VIEWS ON MECHANISMS FOR AMERICAN GOVERNMENT ASSISTANCE. SOME WANT OFDA AND BPRM TO ADD AN ADDITIONAL PERCENTAGE TO THEIR INDIRECT COSTS TO COVER THESE EXPENSES. OTHER MEMBERS WOULD LIKE OFDA AND BPRM TO APPROVE AS AN ADDITIONAL LINE ITEM IN THEIR BUDGETS AN ALLOCATION FOR SECURITY COSTS. I PROBABLY HAVE NOT DONE FULL JUSTICE TO THE SKILLS OF OUR FINANCIAL OFFICERS, SOME OF WHOM MAY HAVE IDENTIFIED OTHER FORMULAE.

ANOTHER KEY ISSUE IS ELIGIBILITY FOR EVACUATION BY THE U.S. GOVERNMENT. HAVING RUN SEVERAL OF THESE FROM VARIOUS POSITIONS, INCLUDING A SEAT ON THE LAST DEPARTING HELICOPTER, I WAS SURPRISED BY REPORTS THAT MEMBERS OF OUR AGENCIES HAD BEEN TOLD BY EMBASSY OFFICERS IN SOME EVACUATIONS THAT THEIR FOREIGN CITIZEN WIVES AND CHILDREN WERE INELIGIBLE TO ACCOMPANY THEM. MORE FREQUENTLY AMERICAN NGOS REPORTED THAT THEIR THIRD COUNTRY EMPLOYEES HAD BEEN TOLD THERE WAS NO ROOM FOR THEM IN THE HELICOPTER OR NAVAL VESSEL. IN FAIRNESS TO MARY RYAN AND EMB ASSY OFFICERS WHO CONDUCT THESE HAZARDOUS OPERATIONS, I MUST ADMIT THAT WE HAVE NOT SAT DOWN WITH MARY AND HER COLLEAGUES TO SEEK GREATER CLARITY AND CONSISTENCY ON THE ELIGIBILITY OF NGOS FAMILY MEMBERS AND THIRD COUNTRY EMPLOYEES OF AMERICAN NGOS FOR EVACUATION. WE WILL SEEK SUCH A DISCUSSION.

I MENTIONED EARLIER THE DIFFICULTY ENGAGING THE UN SYSTEM IN A SERIOUS DIALOGUE ABOUT ITS SECURITY RESP ONSIBILITIES TOWARD ITS NGO PARTNERS. MUCH OF THIS IS VERY PERSONALITY DEPENDENT, AND UN STAFF HAS RUN VERY SERIOUS RISKS TO ASSIST NGOS. BUT IN OTHER CASES, NGOS HAVE BEEN NEEDLESSLY EXPOSED BY DANGER BY THE UNWILLINGNESS OF SOME UN OFFICIALS TO SHARE INFORMATION, COMMUNICATIONS , OR EVEN NEWS THAT THEY WERE ABOUT TO EVACUATE. A S A MAJOR FUNDER OF THE UN AGENCIES ENGAGED IN DISASTER RESPONSE ,WE HOPE TO HAVE THE U.S,. GOVERNMENT'S CONTINUED SUPPORT SHOULD THE TALKS NOW UNDER WAY BETWEEN US AND THE UN NOT REACH A CONCLUSION WE BELIEVE MEETS OUR NEEDS.

ANOTHER OF OUR CONCERNS IS THE GROWING UNWILLINGNESS OF THE U.S. GOVERNMENT TO PUT ITS PERSONNEL IN HARM'S WAY. SOMETHING IS SERIOUSLY WRONG WHEN ALL USAID OFFICERS ASSIGNED TO A COUNTRY, INCLUDING THOSE CHARGED WITH LIAISON WITH NGOS OPERATING IN LOCALES MUCH MORE DANGEROUS THAN THE CAPITAL, ARE REPORTED UNCONVINCINGLY BY THE STATE DEPARTMENT TO HAVE SIMULTANEOUSLY DECIDED TO TAKE ADVANTAGE OF AN AMBASSADOR'S DECLARATION OF A VOLUNTARY DEPARTURE. WHEN U.S. GOVERNMENT EMPLOYEES ASSIGNED TO WORK WITH NGOS ARE INSTRUCTED NOT TO GO OUTSIDE THEIR HOTEL, OR TO

BE BACK ACROSS THE BORDER BY NIGHTFALL, IT ALSO IS HARDER TO PROVIDE THE HUMANITARIAN SERVICES THE CONGRESS AND THE U.S. PEOPLE WANT UNDERTAKEN.

AS OUR MEMBERS FREQUENTLY FIND THEMSELVES WORKING ALONGSIDE U.S. MILITARY FORCES ENGAGED IN PEACEKEEPING AND HUMANITARIAN OPERATIONS, WE HAVE LONG HAD A PROGRAM WHICH INVOLVES OUR STAFF AND MEMBERS GIVING PRESENTATIONS ON THE RESPECTIVE ROLES OF NGOS AND THE MILITARY AT DISASTER SITES. WE HAVE HELPED PREPARE RELEVANT MILITARY MANUALS AND PARTICIPAT ED IN BOTH COMMAND POST AND FIELD EXERCISES. UNFORTUNATELY THE INFORMATION SHARED OFTEN DOES NOT REACH THOSE ASSIGNED TO THE NEXT INTERVENTION. WE ARE TRYING TO IDENTIFY FUNDING WHICH WOULD GIVE OUR INPUT GREATER REACH AND TIMELINESS. A 30 MINUTE VIDEO PLACED ABOARD EACH ASSAULT SHIP AND IN PILOT READY ROOMS WOULD BE ONE APPROACH, IF WE CAN MOBILIZE THE FUNDING. IF MEMBERS FIND THE CONCEPT MERITORIOUS YOUR ASSISTANCE PROVIDING THE FUNDS OR DIRECTING THEIR USE WOULD BE APPRECIATED.

THANK YOU FOR THIS OPPORTUNITY TO APPEAR BEFORE YOU THIS MORNING AND FOR YOUR ATTENTION. I LOOK FORWARD TO YOUR COMMENTS AND QUESTIONS.

Mr. PUTNAM. Mr. Cilluffo and Dr. Hoffman testified last week as well. Their expertise spans terrorism issues from broad strategy to protection of individuals. We appreciate your willingness to participate with us again today.

The Chair recognizes Mr. Cilluffo, senior policy analyst, Center for Strategic and International Studies.

Mr. CILLUFFO. Thank you, Mr. Chairman.

Mr. Chairman, distinguished members, it is a privilege to appear before you today on this important matter. Threats, particularly terrorist threats facing nonofficial American interests overseas, are an underexamined and often underappreciated aspect of the emerging threat environment. Given the breadth and depth of the subject, to run through this in approximately 5 minutes is a tall order, especially for me, as I've rarely had an unspoken thought.

One can hardly turn on the news without coming across a reference to terrorism, kidnapping, or piracy. Just to provide you with a brief snapshot, yesterday, Philippine President Arroyo declared an all-out war against the Abu Sayyaf in response to threats that they would decapitate American hostage, Jeffrey Schilling.

Over the weekend, the Basque separatist group, ETA, threatened Spanish tourist resorts and warned of "undesirable consequences" to Spanish tourism and economic interests.

During the past month, there were high-profile kidnappings in Mogadishu, Somalia, in Nepal, in Bangladesh, and Egypt.

At the beginning of March, four of five American oil workers returned home after 5 months in captivity in the Ecuadorian jungle. The fifth had been killed, presumably to hasten ransom payments.

U.S. citizens and facilities have long served as a lightning rod for terrorist activity abroad. Official U.S. Government facilities are our most visible international symbols of power and culture. Because of past terrorist actions, the U.S. Government has been hardening diplomatic and military facilities, making them less susceptible to attack. I would like to note the efforts that Mr. Gilman has put forward in this area. These efforts have been ratcheted up in the wake of the twin bombings of the U.S. Embassies in Kenya and Tanzania in 1998.

While these efforts are a good beginning, we need to examine the issue more holistically. These efforts encourage the terrorist, who often takes the path of least resistance, to select from soft targets; it displaces risk.

In addition, business now increasingly symbolizes the United States. U.S. companies overseas, particularly those with strong brand recognition, are equated with American power and culture. Unfortunately, not everyone views these favorably. A Hamas training manual expounds that it is foolish to hunt a tiger when there are plenty of sheep to be had.

Terrorism is a multifaceted problem. The intent differs from group to group and incident to incident. But the means, violence and intimidation, remain the same. Government is not in a position to be the sole protector. The private sector must better understand the risks and take greater responsibility for its own security.

Terrorism is nothing new. It has always been the weapon of the weak to target the strong. It is also dynamic. While it may be possible to lessen our vulnerability to the terrorist threat, prophylaxis

and protection efforts alone will not be sufficient since the terrorist will simply shift their modus operandi and target selection.

For example, following the two successful counterterrorism operations by the Israelis in Entebbe in 1976 and the German GSG–9 operation in Somalia in 1977 against hijacked aircraft, terrorists changed their tactics almost overnight, moving away from hijacking to bombing aircraft. This illustrates the back-and-forth nature of the struggle: measure, countermeasure, counter-countermeasure, and on it goes.

Terrorists are no longer content with the land and the air. They have also taken to the sea. The bombing of the U.S.S. *Cole,* the aquatic Hamas suicide bomber, and the LTTE Sea Tiger attack on Trincomalee Harbor all point to a growing maritime terrorist trend. Cruise ships present ripe targets. One should consider terrorist or pirate attacks as a possible next step, whether they are politically or economically motivated.

Throughout the 1960's, 1970's and 1980's, groups chose their actions with an ear cocked for popular support and an eye trained on State funds. Of late, however, there has been a shift toward radical religious views and extreme nationalism. Neither of these necessarily places the same constraints on violence as before. In fact, radical and violent actions could bolster rather than undermine support for the cause.

These terrorists no longer seek a seat at the negotiating table. Rather, they want to blow up the table altogether and build their own table in its place.

Usama bin Laden's fatwah makes clear that civilians, not just American officials are targets on al-Qaeda's radar screen.

Funds from States that support terrorism are dwindling, but by no means depleted entirely. Terrorist organizations have had to search for a new source of funding for their wars. Organizations intensified their moneymaking operations, drugs, kidnapping, extortion, and a whole host of other illicit activity.

Kidnapping, of course, is nothing new to terrorists either, but there is a new twist. More and more terrorists take hostages for money, not for publicity. The $64,000 question is how much is going into their coffers to further their terrorist campaigns and/or how many of these enterprises are transforming into outright criminal enterprises, Kidnapping, Inc., if you will.

Kidnapping abroad has evolved into a highly lucrative crime. The perpetrators are more sophisticated and savvy than ever before. Moreover, indigenous law enforcement may be outgunned, outmanned, and outskilled. Worse still, in some countries, the local law enforcement is part of the problem with high levels of corruption making protector and predator almost synonymous.

Though accurate statistics are notoriously difficult to obtain, the majority of global abductions occur in Latin America. In the previous decade, business people accounted for roughly 40 percent of the victims. International companies, particularly those with strong corporate images, may be more likely targets, owing to their deep pockets.

While South America is the global kidnapping center, Southeast Asia is the global piracy hub. What kidnapping is to land, piracy is to seas. There has been a dramatic increase in the frequency and

severity of piracy. The International Maritime Bureau reports that attacks by pirates increased by 57 percent from 1999 to 2000. This is a total of 469 reported attacks on ships, leaving 72 people dead.

Business leaders must also expand their concept of security to include not only the physical, bricks and mortar, but also the cyber. We are aware of our cyber vulnerabilities due to major government exercises that we have conducted on our own systems. We have also seen what can be done. Luckily, at this point, most of the perpetrators have been young adults, but someone was able to disable the emergency 911 systems in south Florida.

There is certainly no shortage of bad actors with views inimical to the United States. What we have not yet seen is the convergence of intent and capabilities where the real bad guys exploit the real good stuff. Admittedly, the global good guys are at a disadvantage in the cyber realm. In essence, we've created this global village without a police department.

In addition, U.S. businesses are at risk from foreign intelligence services in foreign companies, be they friend or foe, for losses from economic industrial espionage are enormous but almost impossible to quantify exactly.

While information relating to product design and trade secrets are the most obvious targets, information such as marketing plans, bid proposals, pricing structures and customer lists also rank very high on a competitor's wish list.

In conclusion, as government targets become more difficult to attack and U.S. corporations and businesses expand overseas, terrorists and kidnappers have indicated they will likely continue to expand their focus to include nonofficial Americans, be they U.S. corporations, humanitarian workers, or international tourists.

The private sector needs to be part of the solution. We need to expand the national security planning table to include them. We have the opportunity to integrate the private sector into the overall antiterrorism-counterterrorism framework and to attempt to prevent threats and mitigate risk, not merely respond to events after they have occurred.

The U.S. Government must also continue to sharpen its own antiterrorism and counterterrorism capabilities. The first line of defense is good intelligence. Multidisciplinary intelligence collection is crucial to provide indications and warning of possible attack, including insights into the culture and mindsets of terrorist organizations, and to illuminate key vulnerabilities that can be exploited and leveraged to disrupt terrorist activities before they occur.

While a robust technical intelligence capability is crucial, our human intelligence capability must be enhanced. In addition, we must enhance intelligence-sharing between the public and private sector.

We must also cultivate good relations and connections abroad. Terrorism is a transnational problem that demands a transnational solution. I just look to the preempted bombings in the millennium and the support that we got from the Jordanians to give a clear insight as to how important that can be.

Companies also ought to establish direct contact with indigenous law enforcement agencies and security services, and the U.S. Gov-

ernment ought to help facilitate these meetings and ensure that small to medium-sized companies are included.

More and more, the public and private sectors have overlapping duties. We must realize that we cannot protect everything everywhere all the time. But we do have the opportunity develop a comprehensive plan and strategy to combat terrorism in all its forms. And I highlight and really do appreciate the work of this subcommittee on assuring that we get to that point. Once developed, implementing and sustaining such efforts must be a high priority for U.S. national security.

Mr. Chairman, I'm pleased that the Congress in general and your subcommittee in particular have recognized these needs and will reform our Nation's policies and posture and guide it accordingly.

Thank you for your time.

Mr. PUTNAM. Thank you, Mr. Cilluffo.

[The prepared statement of Mr. Cilluffo follows:]

Center for Strategic & International Studies
Washington, DC

Protecting American Interests Abroad: U.S. Citizens, Businesses, and Non-Governmental Organizations

Statement of
Frank J. Cilluffo
Senior Policy Analyst
Center for Strategic and International Studies
To the
Subcommittee on National Security, Veterans Affairs, and International Relations
U.S. House Committee on Government Reform

Chairman Shays, distinguished committee members, I appreciate the privilege of appearing before your committee again on a related matter of critical importance to our nation's security – namely, to examine the security threats, particularly terrorist threats, posed to non-official American interests overseas. This is an under-examined and often under-appreciated aspect of the threat. Yet, it is only with the understanding that the threat to non-official Americans (U.S. persons not on official business) overseas is growing that we can begin to integrate the private sector into our overall antiterrorism and counterterrorism framework.

One can hardly turn on a news program or pick up a newspaper without coming across a reference to terrorism, kidnapping, or piracy. Just to provide you with a brief snapshot of the scope of the challenge, just yesterday, Philippine President Arroyo declared "an all out war against the Abu Sayyaf." This comes in response to threats made by Abu Sayyaf that they would decapitate American hostage Jeffrey Schilling and present his head to President Arroyo on her birthday this Thursday. Over the weekend, the Basque separatist group "Basque Fatherland and Liberty" (Euzkadi Ta Askatasuna, a.k.a. ETA) threatened Spanish tourist resorts and warned of "undesirable consequences" to "Spanish touristic-economic interests."

Last week, two of the nine United Nations aid workers seized in a raid on the Doctor's Without Borders compound in Mogadishu several days prior by soldiers of Somalian warlord Muse Sudi Yalahow were released. And Maoist insurgents in Nepal added a policeman to the 100 or so hostages they already possess, sparking a huge search for him.

The week before that, kidnappers released a British engineer in Bangladesh after he, and two Danes, had been seized in the jungle while surveying a road for a Danish firm. The kidnappers were not interested in furthering any political goals, but were merely interested in the ransom.

The week before that, an Egyptian tour guide abducted his four German charges in Luxor, Egypt, threatening to kill them unless he received custody of his children, now living in Germany. And the week before that, four American oil workers returned home after five months in captivity in

the Ecuadorian jungle. The previous month, the kidnappers shot and killed one of the American hostages.

U.S. citizens and facilities have long served as a lightning rod for terrorist activity abroad. Official U.S. government facilities are our most visible international symbols of power and culture. Because of past terrorist actions, the U.S. government has been hardening government and official facilities, making them less susceptible to attack. These efforts have been ratcheted-up in the wake of the twin bombings of the US embassies in Nairobi, Kenya and Dar es Salaam, Tanzania in 1998.

U.S. efforts (prophylaxis and target hardening) encourage the terrorist, who often takes the path of least resistance, to select from soft targets. Put another way, these efforts have displaced the risk to the private sector. Even though government facilities can be a more appealing strategic target, they are also better defended. Thus, the increased risk to business is in many ways an ironic, negative by-product of governmental efforts. Of course, while the government has made a good start –it still has a ways to go.

In addition, business now increasingly symbolizes the United States. U.S. companies overseas, particularly those with strong brand recognition, are equated with American power and culture. Unfortunately, not everyone views these favorably. These companies present tempting targets because of what they represent. But companies go knowingly into potentially dangerous areas because they must seek out new opportunities to compete, to grow, and to turn a profit.

Thus terrorists have begun to look for easier prey and found non-official Americans abroad. A *Hamas* training manual expounds that it is foolish to hunt a tiger when there are plenty of sheep to be had.

Terrorism is a multifaceted problem. The intent differs from organization to organization, but the means – violence and intimidation – remain constant. Government is not in a position to be the sole protector. The private sector must better understand the risks and take greater responsibility for its own security. But while the onus of protection is shifting from Uncle Sam to the private sector, the non-governmental sector need not act alone.

As terrorists look to criminals, as criminals emulate businesses, and as businesses run intelligence operations, the threat is "going private." It is difficult to apportion responsibility for protection and security. It is clear, however, that the private sector must be integrated into the broader framework of antiterrorism and counterterrorism planning. Public-private partnerships and strong leadership establish a framework within which to work on preventing terrorism, not simply managing risk.

Big, Dangerous World

Terrorism is nothing new. It has always been a weapon of the weak against the strong – used most often to further a specific purpose. Terrorists choose symbolic targets as much to make a point as to cause damage. These would-be targets can be identified and better protected – but the unfortunate reality is that no defense can guarantee safety one hundred percent of the time.

Hence, while it may be possible to lessen our vulnerability to the terrorist threat, prophylaxis and protection efforts alone will not be sufficient since the terrorist will simply shift modus operandi.

Commercial airliners have long been a primary terror target. But, with focused efforts and diligence, the number of attacks has decreased, even as the overall number of terrorist incidents has increased – demonstrating the value and possibility of hardening targets. The hijacking of Air France Flight 139 in July 1976 by terrorists, and its subsequent re-routing to Entebbe, Uganda, prompted a highly successful raid by an Israeli commando team. In the end, the hostages were freed, no ransom was paid, and the terrorists' demands went unmet.

In October of the following year, four terrorists (led by Zohair Youssef Akache) hijacked a 737 bound for Germany from the Balearic Islands. After flitting around Europe and the Middle East, the plane was finally landed in Mogadishu, Somalia. While there, the "crack" German anti-terrorist unit GSG-9, along with two British Special Air Services members on loan, successfully stormed the aircraft and rescued the hostages. Here too, the situation was resolved by the use of force without payment of ransom.

Following these two successful counter-terror operations, terrorists changed tactics, moving away from hijacking aircraft to bombing them. This illustrates the back and forth nature of the struggle – measure, countermeasure, counter-counter measure.

For terrorists, calculated violence raised public awareness of their political agendas. Groups chose their actions with an ear cocked for popular support and with an eye on trained on state funds. These two factors placed constraints on the level of violence because terrorists sought a seat at the negotiating table and could not completely disregard the existing system they wanted to become a part of.

Of late, however, there has been a shift towards radical religious views and extreme nationalism. Neither of these necessarily places the same constraints on violence as before. In fact, radical and violent actions in this "new world" could bolster, rather than undermine, support for "the cause."

While again we cannot generalize, some terrorists no longer seek a seat at the negotiating table. Rather, they want to blow the table up altogether, and build their own table in its place. Usama bin Laden issued a fatwah stating "...kill[ing] the Americans and their allies – civilian and military – is an individual duty for every Muslim who can do it in any country...We – with God's help – call on every Muslim who believes in God and wishes to be rewarded to comply with God's order to kill the Americans and plunder their money wherever and whenever they find it." This *fatwah* makes clear that civilians, not just government officials, are targets on Al Qaeda's radar screen.

The linkage between terrorism and radical Islamic fundamentalism grows. The focus seems to be shifting away from the Middle East and towards Afghanistan. Additionally, terror networks are coming to have private patrons and are developing transnational connections, providing channels for raising funds, training, weapons, supplies, and propaganda. Organizations with similar interests and/or objectives will share personnel and/or intelligence and have learned

valuable lessons from others' successes and failures. Terrorists are also organized as a network of networks. They tend to be loosely affiliated, bound by a common goal – today's *fellow travelers* if you will.

Funds from states that support terrorism are dwindling, but by no means depleted entirely. The fall of the Soviet Union ended the stream of money that funded many terrorists. As a result, terrorist organizations had to search for a new source of funding for their wars and because their ambitions have grown. To survive and to prosper, organizations intensified their extant revenue generating ability: drugs, kidnapping, extortion, and other illicit activities.

The linkage between terrorists and narcotics is strong, and getting stronger (but is beyond the scope of this testimony). Suffice it to say narcotics provide a substantial source of funding and have deepened the connection between terrorists and organized crime. Kidnapping is also nothing new to terrorists. They have been taking hostages since day one to gain media attention and ransom money. But there is a new twist - more and more terrorists take hostages for money – not for publicity.

Kidnapping has become big business. The $64,000 question is how much money is going into their coffers to further their terrorist campaigns and how many of these organizations are transforming into outright criminal enterprises – "Kidnapping, Inc.," if you will?

Decadent Guerillas

Kidnapping abroad has evolved into a highly lucrative crime. It has gone from being a terrorist media tool to an industry raking in large piles of cash. The perpetrators are more sophisticated and savvy than ever before. And things are likely to worsen before improving.

Abductions come to resemble military operations, complete with detailed surveillance and top of the line weapons. There are quasi-corporate structures in place for kidnapping. Organizations are divided into subdivisions. Some are dedicated to research and surveillance, some to the actual abduction, others to hold the person, and still others to handle the negotiations. There is even a domestic trade in hostages as they are sold from group to group.

In addition, there are local concerns. The indigenous law enforcement personnel may be outgunned, outmanned, and outskilled. Worse still, in some countries the local law enforcement is part of the problem, with high levels of corruption making protector and predator almost synonymous.

The possibility of substantial remuneration also attracts the most basic thugs, those without any "professionalism." They are more erratic, more dynamic and therefore more difficult to deal with making negotiations more challenging. You do not know what is going on in their minds and they may be itchier with the trigger finger.

A recent New York Times article on kidnapping reports that there are now variations on the theme as new forms, or techniques, associated with kidnapping emerge: "Express" where people are held and required to take out the maximum amounts of money possible from ATMs until the

account is empty; "Tiger" where a foreigner's freedom is ransomed to their families back home; and "Bad-on-bad" where one gang seizes members of another during negotiations to garner favorable terms. Despite these fancy alternatives, most kidnappers abduct someone to recover a ransom.

It bears recognizing that statistics on the subject are notoriously difficult to ascertain and the statistics are underreported. Governments, at least the US government, does not monitor all international kidnapping, but only specific elements of it. The private sector is unwilling to discuss the topic for fear of weakening consumer confidence or for advertising its weaknesses. Insurance companies and security firms, who provide kidnap and ransom insurance as well as ancillary services like security, intelligence, and negotiation, also remain tight-lipped. Thus the numbers cited tend to represent only a portion of the whole.

That said, the majority of all global abductions occur in Latin America. In the previous decade, business people represented roughly 40% of the victims. These abductions can cost an individual company millions of dollars. International companies, particularly those with a strong corporate image, may be more likely targets owing to the knowledge that they have deep pockets.

Colombia has the largest incidence of kidnapping in the world. Kidnapping is second only to narcotics in illegal revenue-producing practices. The Colombian authorities recently reported that 3,706 people were kidnapped last year, 22 of them were foreigners, and 140 were children. These numbers may increase as the guerillas increase their war chests to combat Plan Columbia and may expand beyond the Colombian borders. The FARC announced a 10% tax on those people or enterprises with assets that exceed $1 million, non-payment could result in kidnapping. Colombian police state that the FARC made roughly $110 million since announcing the policy last April. The ELN has also been heavily involved in kidnapping for ransom for years. They begin their surveillance and target acquisition procedures at the airport, when would-be targets are deplaning – a different kind of "customs" altogether.

The guerillas are not the only ones profiting from kidnapping. Local criminal gangs have been known to abduct people, then sell them to the guerillas. Things have deteriorated to the point that radio stations air programs allowing the hostage's relatives to call in and have their messages broadcast to the jungle encampments.

Kidnapping is not confined only to Columbia. Brazil, Mexico, Ecuador, Venezuela, Honduras, El Salvador, and Costa Rica all have experienced a rise in kidnapping for ransom. Lest history be forgotten, Ecuador had its own high-profile kidnapping less than six months ago which was only recently resolved this month after a ransom payment. A group suspected to be former FARC members snatched ten oil workers, five of whom were from the United States, out of the jungle. Abducted in October, the kidnappers killed one of the hostages this past February to force the company's hand and pay ransom. They were abducted despite beefed up security efforts on the part of the Ecuadorian government that sought to curb spillover of reprisals for Plan Columbia.

These techniques are not confined to Latin America. Abu Sayyef, "Bearer of the Sword" in Arabic, achieved widespread international prominence through their high profile kidnapping from a luxurious resort, despite previous terrorist actions and a history of kidnapping and piracy.

The group founded by Abdurajak Abubakar Janjalani, who participated in the war in Afghanistan, began kidnapping in 1991. It has a violent past, including allegedly bombing busses, shopping centers, and even a church. They have kidnapped such diverse people as Spanish nuns, Hong Kong fishery workers, and a US bible translator. Among their demands after kidnapping various guests and resort employees, they claimed to be interested in an independent Muslim state and the sought the release of convicted Afghan terrorists from US prisons. But at the end of the day they "settled" for $1 million per hostage.

Clearly kidnapping pays. According to authorities in the Philippines, Abu Sayyef purchased their arms with the $5.5 million dollars in ransom monies received from previous kidnappings. Their large coffers attract new recruits. The number of their members reportedly jumped from 200 to 1000. This sudden surge in wealth distorted the local economy. At one time, the Philippine peso was worth substantially less in Manila than in Jolo. The basic micro-economic rules of supply and demand still apply, Western hostages, previously going for $100,000, now command $1million. Feliciano Belmonte, the Philippine House Minority floor leader compared Abu Sayyef's leader, "Commander Robot," to Bill Gates.

Hostages serve as a meal ticket and a hall pass. Governments and private organizations are less willing to risk injury to hostages by the use of force where the group still holds hostages – though a major assault was finally laid on.

Recently the Philippine military chief established a special force to assist the police in curbing the recent spate of kidnappings as part of an effort to curb crime. The police would gain access to the military intelligence system and their experience. The unit would receive joint police-military training.

The Philippines is certainly not the only country to experience a threat by kidnappers to the tourism industry. The recent kidnapping of four German tourists by their tour guide in Luxor, Egypt and the Basque ETA also highlight this risk. Luxor was the site of the 1997 massacre of 58 tourists by Islamic militants. According to Swiss federal police the attack was ordered "directly or indirectly" by Mustafa Hamza, a member of the al-Gamaa al-Islamiya and represented a fundamental shift in target selection. It also greatly affected Egypt's desirability as a tourist destination and prompted a strict safety operation by the Egyptians. Though tourism is now booming, it was depressed for several years.

Kidnapping is particularly difficult to address because it is rooted in the weaknesses and disparities of foreign, sovereign powers. Many kidnappings are local. The lives of those who have are a valuable commodity and the have-nots are willing and able to capitalize. Many of the driving factors lie outside US control, making those features that we can recognize and address more valuable still.

It is also important to note that there are often competing, and in some cases divergent, interests at stake. Sovereign nations, the United States included, have a vested interest in not negotiating so as to thwart future attempts and bring the perpetrators to justice. While the victim's family, and possibly the employer, simply want their loved one returned safely, this is a highly emotional, highly volatile situation. Stability and calm go a long way towards reaching a positive resolution.

Of course joint and foreign training provides an invaluable tool for beginning to address the issue. The FBI's International Law Enforcement Academy in Budapest and the soon to be established academy in the United Arab Emirates greatly assists cooperation, and builds the trust and understanding of their anticrime counterparts abroad.

We would also do well to pay attention to the Central Asian republics. The lure of oil and natural resources present a powerful draw. However, the region is fast becoming a terror hub. The Taliban and Usama bin Laden have been expanding their influence. In addition, as Arnaud de Borchgrave reported in recent conversations with Pakistan's General Pervez Musharraf, the West's constant focus on bin Laden has transformed him into a "cult figure."

The Taliban uses some of its wealth to support and succor terrorists, notably the Islamic Movement of Uzbekistan. In September 2000, the State Department designated the IMU as a terrorist organization because it "...threatened the lives of civilians and regional security and undermined the rule of law." US presence in the region presents a very tempting target, particularly after we cut our ties with Afghanistan and have imposed further sanctions.

Despite these new developments, the terrorist's main goal is to use violence to disrupt a stable society to achieve some change. The scope of their ambitions has increased and the scope of their reach has as well. They no longer confine themselves to the land. Several organizations have rediscovered the sea.

Maritime Terror

The bombing of the USS Cole, the Hamas suicide bomber, and the LTTE attack on Trincamolee Harbor, Sri Lanka point to a growing maritime terror trend.

In October of 2000, suicide bombers used a shaped charge mounted on a skiff to kill 17 US sailors and wound 39 others aboard the USS Cole while at port in Aden, Yemen. As with other high profile bombings, the attack on the Cole will presumably lead to copycat attacks.

The bombing of the USS Cole also serves as a grim reminder that terrorists will continue to probe and will strike where they can. The Cole merely stopped to "gas and go" en route to the Persian Gulf. Additionally, they will try and expand their scope, controlling whatever territory and/or channels possible.

Also in October 2000, the Liberation Tamil Tigers of Eelam mounted a well-organized attack on Trincamalee harbor, injuring 40 people as well as destroying two crafts by guns and a large passenger craft by explosion. In November, a *Hamas* suicide bomber attempted to attack an

Israeli patrol craft. The vessel exploded without seriously injuring anyone or the vessel. These three attacks provide the first look at a new, or newly applied, form of maritime terrorism.

As reported by Jane's Intelligence Review, the LTTE have developed a maritime division, with some 3000 personnel, between 100-200 surface and underwater vehicles, underwater demolition teams, marine engineering and boat-building capabilities, and a maritime school and academy. These represent substantial resources dedicated to maritime activities and reflect dangerous objectives.

They seek to control Sri Lanka's northern waterway and to disrupt the Sri Lankan Navy. A maritime corridor provides continued access to guns and supplies, and prevents Navy interdictions of the same. By controlling shipping channels they could exert further pressure on the Sri Lankan government. Of course, this disruption to shipping poses a problem to businesses everywhere that rely on ships to transport their goods.

The Sea Tigers, the naval branch of the LTTE, have attacked and looted commercial vessels, in classical pirate fashion. They have also used commercial vessels as bait for Sri Lankan Naval craft, attacking a commercial ship to provoke a response, then overwhelming the Naval vessel with superior numbers or by the use of land based material. The LTTE's commercial vessels now also pose a danger. Often, those ships engaged in illegal activities, like smuggling and gun running, are wired to explode – making interdiction that much more dangerous and costly.

Here too, there is a shift in target selection and a change in modus operandi. Effective use of terror tactics on the water merely expands the potential scope of the terrorist threat.

While South America is the global kidnapping center, South East Asia is the global piracy hub.

Kidnapping on the Seas

Pirates have been around since there were ships to pillage. What kidnapping is to land, piracy is to the seas. There has been a dramatic increase in the frequency and severity of piracy – particularly in South East Asia.

The International Maritime Bureau reports that attacks by pirates increased by 57% from 1999 to 2000. This is a total of 469 reported attacks on ships, with 72 people killed, and 99 people injured. Attacks in Indonesia account for a quarter of the global total. As with kidnapping above, the statistics tend to reflect only a portion of the whole owing to a reticence in reporting of incidents.

In many cases, the pirate vessels are highly technologically sophisticated and are heavily armed. They carry automatic weapons and rocket launchers, and have top of the line navigational and positioning systems. Except for the weapons, the equipment is dual use, meaning that it is available on the open market. They are much quicker and more nimble than their targets. The pirates zoom up to their prey, board, and overwhelm the crew and commandeer the vessel.

The ship itself is often the treasure. Pirates will hijack the vessel, then repaint and rename her, sell the cargo, and send her back out to search for other victims. Alternatively, the pirates will attack the crew, including rape and murder, then leaving the vessel to drift, presenting a substantial hazard.

Cruise ships present ripe targets. One should consider terrorist, kidnap, or pirate attacks on cruise ships could be the next logical step – whether politically or economically motivated.

There is an increasing connection between the pirates and the drug cartels. The seized vessels are often used to smuggle narcotics. The drug and gunrunning outfits will support the pirates by bribing officials. This relationship is particularly strong in southern India, in the LTTE's sphere of influence, while southern China's powerful gangs and triads engage exert substantial control over regional piracy.

Piracy and kidnapping disrupt the flow of businesses. There is a premium on reliability. Not knowing whether your goods will arrive or whether your people will survive decreases that reliability.

The danger of disruption is not limited to the high seas or remote jungles. High tech companies in the booming metropolis could be at risk.

Cyber

Technology is central to modern business – but with this comes vulnerability. The cyber threat to companies is real and comes in many guises. Likewise, the range of possible perpetrators is broad, varying from corporate competitors to foreign countries to terrorists. These actors may be motivated by financial and/or political considerations, or perhaps other reasons altogether. Terrorists, for instance, may turn to cybercrime as yet another means of finance.

Almost all the Fortune 500 corporations have been victims of cybercrime – which is itself already a multi-billion dollar business. Yet, there is no accurate accounting of the damage that has been done to date. In part, this is due to underreporting of attacks/losses. Plainly, this is not the sort of news that shareholders want to hear. Equally (if not more) disturbing, however, is the fact most companies are simply unaware that "virtual" intruders have made off with their intellectual property.

And even when the loss is apparent, who the perpetrator is may not be. As an illustration of such anonymity, consider that authorities are currently investigating a massive cyberfraud scheme – incorporating, among other things, the theft of at least a million credit card numbers from some forty U.S. financial institutions in twenty States. The identity of the hackers is not yet known, though it is believed that the attack originated in Russia and the Ukraine.

Cybercrime, however, is at the low end of the spectrum of threats faced by corporations. To date, no severe incidents of nation-based cyberwarfare have been detected. But just think of what could happen if the really bad guys exploited the really good stuff and became more techno-savvy. While it may be disturbing to contemplate the potential of combining physical

attacks with equally meticulous cyber attacks, it is only a matter of time until this convergence occurs.

Business leaders must, therefore, expand their concept of security to include not only the physical (bricks and mortar) but also the virtual. Industry should not be alone in wrestling with Internet protection, of course. To the contrary, government must lead by example and put its own house in order. And, at the same time, the public and private sectors must cooperate and work together as never before.

Admittedly, the good guys are at a disadvantage in the cyber realm. The Internet knows no borders – but law enforcement remains bound by physical jurisdictions or lines on a map. Put another way, we have created a global village without a police department. For this reason, as well as others, cyber threats pose one of the most serious challenges for business and government alike in the twenty-first century.

Economic and Industrial Espionage

"Espionage" is defined as an "intelligence activity directed toward the acquisition of information through clandestine means and proscribed by the laws of the country against which it is committed." This does not cover legitimate economic intelligence collection and analysis through legal means, nor strategic acquisitions or the like.

"Economic espionage" refers to state-sponsored collection, often directly involving a nation's foreign intelligence service, tasked to aid or support a specific company. "Industrial espionage" refers to clandestine collection by companies and individuals such as information brokers against their competitors. But the distinction between the two is unclear, especially in countries with state-owned or state-subsidized enterprises.

Companies and foreign governments also have an enormous interest in acquiring proprietary information and trade secrets. The American Society for Industrial Security pegs the losses to U.S. firms in excess of $1 trillion last year. Information age companies rely on proprietary information for their successes.

These intangibles are vulnerable to theft. For example, in the biotechnology and software realms, it often costs many millions of dollars in research and development to design a product that is ultimately boiled down into ten pages of useful text. Therefore, it makes basic economic sense to recruit an insider to provide you with a copy of the formula. At a fraction of the cost, you end up with the same product as your competitor, and you can spend your savings on gaining market share, advertising, and developing core competencies.

While information relating to product design and trade secrets are the most obvious targets, information such as marketing plans, bid proposals, pricing structures, and customer lists, also rank very high on a company's wish list. And, US companies abroad need to be wary of the infrastructure that supports their projects. Foreign security services as well as other companies have been known to plant employees. A favored ploy involves inserting a "mole" into the

corporation with the express purpose of purloining secrets, a technique employed by many countries and at the heart of intelligence tradecraft.

But the most common information thief, and every company's weakest link, are employees and former employees. The same technology that was intended to empower the employee can be exploited against the employer. Of course, some companies simply hire away those individuals with the requisite knowledge at four or five times their current salary. Even at that rate, it is still a bargain, and much cheaper than underwriting the cost of research and development. Sherlock Holmes summed it up well when he remarked, "Whatever one man can invent, another can discover."

In 1996, Congress enacted the Economic Espionage Act to increase the protection afforded to trade secrets. The law provides stiff penalties and covers both acts that benefit a foreign government and acts that benefit private parties. But there have been comparatively few cases brought under the Act due to the very stringent requirements. Western countries, longtime US military allies, do not shrink from economic espionage. Our cooperation over affairs of state does not exclude our competition in "les affaires."

Conclusion

As government targets become more difficult to attack, and as US corporations and businesses expand overseas, terrorists have indicated they will likely continue to expand their focus to include non-official Americans, be they US corporations, humanitarian workers or international tourists. Terrorists will not have to look very hard: US businesses, humanitarian organizations, and tourists span every corner of the globe.

Terrorists pose a dynamic threat to American interests abroad. Hardened government facilities make non-official Americans potentially more attractive targets. Thus the private sector needs to be part of the solution. We need to expand the national security policy planning table to include them. We have the opportunity to integrate the private sector into the overall antiterrorism and counterterrorism framework, and to attempt to prevent threats and mitigate risk, not merely respond to events after they have occurred.

Companies must understand that they are at risk from terrorists, kidnappers, pirates, and spies and that these threats can substantially affect their earnings and their reputation. In addition, they are responsible for their employees' continued safety. For businesses the bottom line is the bottom line and terrorism, kidnapping, piracy, and economic espionage cost them money.

Insurance companies offer to indemnify companies for loss arising from kidnapping, ransom, and extortion. K&R insurance is a multi-million dollar a year market. Most firms tend not to advertise their policies so as not to advertise the potential upside to the kidnapper of millions of dollars. In some cases, the insurance companies insist on secrecy for the very same reason.

Companies have an interest in keeping quiet. On one hand, not to advertise their vulnerabilities, and on the other, not to undermine shareholder and consumer confidence. Clearly there would be a benefit to consciousness raising and education without exposing or embarrassing anyone.

There are means for the private sector to present fewer vulnerabilities – but in order to capitalize on them, non-official Americans must first be aware that they may be in danger. Prevention of a problem begins with the awareness that there is something wrong. Non-official Americans are like the proverbial ostrich with its head in the sand. Yet non-official Americans should not be so surprised when they get kicked in the most obvious place.

Depending on the policy, the insurer will negotiate with the kidnapper, pay off the ransom, and even provide post-traumatic event counseling. Policies cover kidnapping and hijacking, but also cover extortion, blackmail, and property damage exposure, including trade secrets and proprietary information.

Consulting firms provide complementary services, working with the business to prevent trouble. Many are well staffed with former government officials and employees. They provide the full spectrum of preventive consulting services, training courses, and on the ground support. Some know the "going rate"; others have their own sets of eyes and ears to provide warning.

Added to this is the desire to expand and the need to explore. Companies go abroad, hire these firms, and run these risks because there is money to be made. Therefore, we must devise a means of minimizing exposure to the private sector. While the private sector must shoulder some responsibility for protection, the federal government can provide assistance.

We ought to support public-private partnerships like the Overseas Security Advisory Council (OSAC), the Critical Infrastucture Assurance Office (CIAO), and the Awareness of National Security Issues and Response Program (ANSIR) on the federal side, and the numerous private sector equivalencies.

The U.S. government must also continue to sharpen its own antiterrorism and counter-terrorism capabilities. The first line of defense is good intelligence. Multi-disciplinary intelligence collection is crucial to provide indications and warning of a possible attack (including insights into the cultures and mindsets of terrorist organizations) and to illuminate key vulnerabilities that can be exploited and leveraged to disrupt terrorist activities before they occur. To date, signals intelligence has provided decision makers with the lion's share of operational counterterrorism intelligence. National technical means cannot be allowed to atrophy further. While a robust technical intelligence capability is crucial, our human intelligence capability must also be enhanced - especially needed against low-tech terrorists who area also less susceptible to non-human forms of intelligence collection. In addition, we must enhance intelligence sharing between the public and private sectors.

We must also cultivate good relations and connections abroad. Terrorism is a global problem. Transnational cooperation and understandings necessarily must be high priorities. Developing good working relations now could save lives in the event of a crisis.

Companies must follow suit. They ought to establish direct contact with the indigenous law enforcement agencies and the security services. Government ought to help facilitate these meetings. There should also be regularized channels set up, as much as possible considering

individualized corporate need, to make future meetings possible for small to midsize companies as well.

More and more, the public and private sectors have overlapping duties. We must realize that we cannot protect everything, everywhere, all the time. But we do have the opportunity to develop a comprehensive plan and strategy to combat terrorism in all its forms. Once developed, implementing and sustaining such efforts must be a high priority for U.S. national security.

Mr. Chairman, I am pleased that the Congress in general, and your subcommittee in particular, has recognized these needs and will reform our nation's policies and posture and guide it accordingly. Thank you for the opportunity to share my thoughts with you today. I would be pleased to try to answer any questions you may have.

Mr. PUTNAM. The record will note, the gentleman from Idaho, Mr. Otter, has joined the subcommittee.

The Chair now recognizes Dr. Bruce Hoffman, director of the Washington office for the RAND Corp.

Welcome.

Mr. HOFFMAN. Thank you very much. Thank you, Mr. Chairman and distinguished members of the subcommittee for the opportunity to testify in this matter.

While the volume of worldwide terrorism fluctuates from year to year, one trend remains constant. Since 1968, the United States is annually head of the list of countries targeted by terrorists. Indeed, for more than 3 decades, terrorists have targeted the United States and its citizens more than any other country. This phenomenon is attributable as much to the geographical scope and diversity of America's overseas commercial interests and the number of our military bases on foreign soil as to the U.S. stature as the lone remaining superpower.

Terrorists are attracted to American interests and citizens abroad precisely because of the plethora of available targets, the symbolic value inherent in any blow struck against perceived American, quote-unquote, imperialism, expansionism, or economic exploitation, and not the least because of the unparalleled opportunities for exposure and publicity from the world's most extensive news media that any attack on an American target assures.

The reason why the United States is so appealing to target to terrorists suggests no immediate reversal of this trend. It is, as one commentator has noted, the price that the West and, in particular, the United States as leader of the free world, pays for its hegemony.

Moreover, regardless of what the United States actually does, we are perhaps irrevocably perceived as a status quo power and, therefore, attacked for real or imagined grievances. Indeed, as the lone remaining superpower, the acute feelings of anger and resentment toward the United States was cited last week before this committee by Senator Rudman and General Boyd, in short, the world's continued enmity.

The main problem that we face in protecting American citizens and interests abroad from both current and future threats rubs up against one of the fundamental axioms of terrorism. Hardening one set of targets often displaces the threats onto other softer targets. In other words, security measures may successfully thwart plans or actual terrorist operations or even deter terrorists from attacking, but they may not eliminate the threat entirely, which may mutate into other, perhaps even more deadly forms.

Determined terrorists, accordingly, will simply identify vulnerabilities and hence potential targets, adjusting or modifying their means and method of attack to execute a completely different kind of operation that still achieves their goal.

Therefore, in the current context of heightened threats to U.S. diplomatic facilities and military forces overseas, as we harden the range of American diplomatic and military targets long favored by terrorists, we doubt this will eliminate the terrorist threat completely but risk displacing it onto softer, more vulnerable and more accessible unofficial nongovernmental targets, that is, ordinary

American tourists and travelers, business people, and otherwise unwary citizens.

The implications involving a potential increase in maritime terrorist attacks following the successful assault on the U.S.S. *Cole* are particularly chilling. It is horrifying to contemplate a U.S.S. *Cole* suicide attack on a cruise ship steaming into a Caribbean, Mediterranean or U.S. port, much less any other unprotected harbor.

The general pattern of terrorists attacking a wide variety of, quote-unquote, soft American targets is, however, already well established. For example, according to the U.S. Department of State, a total of 778 Americans have been killed by terrorists overseas between 1968 and 1999, the last year for which published Department of State statistics were available.

Let me pause for a second and say that in a country where murder rates hover around 16,000 persons per year and where the annual incidents of violent crime regularly exceeds a million, the risks to U.S. citizens traveling and working abroad need to be put in an admittedly discomforting perspective of just how safe we are as Americans living and working in our own borders.

But, that aside, of the 778 fatalities, half were private citizens, ordinary travelers, tourists and businessmen; 319 were U.S. Service personnel; and 63 were American diplomats. Accordingly, although the attacks on our two Embassies in East Africa in 1998 and the more recent assault on the U.S.S. *Cole* are seared into our collective consciousness, they actually mask the threats that perhaps affect ordinary citizens far more than diplomats and soldiers and sailors.

Equally significant is the fact that 83 percent of Americans killed by terrorists between 1968 and 1999 died in attacks in which they were specifically targets. Clearly, American citizens traveling, living and working overseas who have no ostensible or official connection with the U.S. Government are indeed already firmly in the terrorist cross hairs.

This should not conceal the fact that at times individuals are targeted not necessarily because they are U.S. citizens but because they are westerners in general and hence opportunistically regarded by terrorists as desirable for their potential to bring large cash ransom payments for their release.

These basic patterns of terrorism are evident in the key incidents reported during 2000 that have continued into the present year. In addition to the attack on the U.S.S. *Cole,* four American climbers were kidnapped by members of the Islamic Movement of Uzbekistan last August. That same month, an American, Jeffrey Schilling, was seized by the Abu Sayyaf organization in the Philippines, a group that had previously kidnapped two other American citizens—a Protestant missionary and a Roman Catholic priest.

In November, an American who headed a program of the U.S. Republican Institute in Azerbaijan, a nongovernmental organization, was found murdered in Baku, apparently the victim of a robbery. And in January 2001, a U.S. citizen in Chechnya, there as a part of the humanitarian aid mission, Action Against Hunger, was kidnapped.

As the latter incidents evidence, threats to Americans working for international humanitarian relief organizations and similar nongovernmental organizations present a special problem. These people are under increased threats for a number of reasons. According to Randolph Martin, senior director for operations at the New York-based International Rescue Committee, there are at least six reasons that NGO's are targeted: The overall increase in the number of conflicts in the past decade to which these organizations are being deployed; a general absence of the rules of war in these conflicts and the proliferation of so called irregular fighters, many of whom also include criminals and bandits interested as much in plunder as in the realization of a political agenda; a prevailing perception of aid operations as especially soft targets; the eroded acceptance of neutrality amongst these groups; and, within the NGO's themselves, a lack of security combined with the skeptical if not adversive altitude on the part of some for the need for security and protective measures.

These views dovetail with those of another American citizen, in fact a former student of mine, who works with a U.S.-based aid organization in a particularly conflict-ridden country in Africa. In a recent e-mail she wrote to me: The first threat we face is basic—and I am quoting—threats against expatriates by terrorists, guerrillas, paramilitaries and others to gain publicity or to enhance panic and fear or to attempt to get the aid agencies to withdraw altogether. The second threat is common banditry of theft that is common anywhere but enhanced in a country of war facing severe economic difficulties. The third threat that we face is being caught in the cross fire, whether it be stray bullets hitting expatriate houses, rebel ambushes on the roads, hitting mines, or being caught in the field during a rebel attack. This third threat is often the most difficult to predict.

Based on the observations of this aid worker, the help provided by the local U.S. Embassy appears to be ingenuous but limited.

In general, therefore, the problem with NGO's and the security of NGO's overseas appears to be twofold. On the one hand, the NGO's themselves may have in the past paid too little attention to their own security and could have provided insufficient training before deployment. While, on the other hand, it often falls to the local American Embassy to fill this void, whose efforts and activities in this respect can be limited as much by insufficient resources as by too few personnel.

In conclusion, it should be recognized that terrorism is not a problem that can be solved, much less ever completely eradicated. No country with the breadth and magnitude of the overseas interests and presence that the United States has can reasonably expect to hermetically insulate or seal itself off completely from any and every manifestation of this threat. In this respect, there are no broad, sweeping policies or new approaches in the form of individual "magic bullets" that can hope to counter, much less defeat, a threat that is at once omnipresent and ceaseless. By the same token, we are neither powerless nor completely defenseless in the face of terrorism; and there are a number of practical steps that might usefully be taken that might effectively mitigate the threat.

First, ensuring that our intelligence resources and capabilities, especially with respect to human intelligence sources, are sufficiently funded, properly organized and continually oriented to actively identifying and countering the range of threats confronting American citizens and interests overseas.

Second, making certain that the security in and around the principal transportation nodes, both for air as well as maritime travel, most frequented by American tourists and business people overseas are of a uniform, high standard. In this respect, Federal Aviation Agency and Department of State inspection teams in the past have identified lax security in airports throughout the world, particularly in some African, East Asian and Latin American countries.

Third, working in concert with NGO's, further educate and inform the headquarters and staffs of these U.S.-based organizations of the importance of security and predeployment proactive measures that can be adopted to enhance the safety of Americans working overseas.

Finally, perhaps seeking to achieve further consistency and clarity in the travel advisories and other warnings and public announcements emanating from U.S. official government sources.

Finally, the threat of terrorism itself needs to be kept in perspective. In this respect, a prerequisite to ensuring that our formidable resources are focused where they can have the most effect is a sober and empirical understanding of the threat. Only in this manner can our efforts achieve the greatest likelihood of success and effectiveness.

Thank you very much.

Mr. PUTNAM. Thank you, Dr. Hoffman.

[The prepared statement of Mr. Hoffman follows:]

PROTECTING AMERICAN INTERESTS ABROAD: U.S. CITIZENS, BUSINESSES, AND NON-GOVERNMENTAL ORGANIZATIONS

Testimony of Dr. Bruce Hoffman

Vice President, External Affairs and Director, RAND Washington Office

Before the Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform

April 3, 2001

PROTECTING AMERICAN INTERESTS ABROAD: U.S. CITIZENS, BUSINESSES, AND NON-GOVERNMENTAL ORGANIZATIONS

Statement of Bruce Hoffman,*
Vice President, External Affairs and Director, RAND Washington Office

Thank you Mr. Chairman and distinguished Members of the Subcommittee, for the opportunity to testify before the Subcommittee on this important matter.

Nearly half a century ago the renowned British novelist and international traveler, Evelyn Waugh, presciently observed that, "In a few years' time the world will be divided into zones of insecurity which one can penetrate only at the risk of murder and tourist routes along which one will fly to chain hotels, hygienic, costly and second-rate."[1] Today, many Americans would likely agree with that assessment: simultaneously comforted by the monochromatic familiarity of restaurants and hotels that have become indistinguishable from one another whether located here or abroad; while increasingly leery of a world beyond our borders seen as populated by terrorists, kidnappers, brigands and bandits.

It is perhaps not surprising that such a world view of palpable threat and acute risk should exist given the seeming unrelenting litany of terrorist attacks, high-profile kidnappings, aircraft hijackings, extortions and robberies that have deliberately targeted or randomly entangled Americans either travelling or working abroad. To a large extent, this perception is grounded in an undeniable reality: for over three decades, terrorists have targeted the United States—and in turn its citizens—more often than any other country.[2] The report of the National Commission on Terrorism last year drew attention to precisely

---

*This testimony is derived from the author's cumulative knowledge derived from 25 years of studying terrorists and terrorism. Federal government grants or monies funded none of the work presented in this written testimony. **It should be emphasized that the opinions and conclusions expressed both in this testimony and the published work from which it is derived are entirely my own and therefore should not be interpreted as representing those of RAND or any of the sponsors of its research.**

[1]Evelyn Waugh, ""I See Nothing But Bordeom . . . Everywhere (London, *Daily Mail*, 28 December 1959)," in Donat Gallagher (ed.), *Evelyn Waugh: A Little Order——A Selection From His Journalism* (London: Eyre Methuen, 1977), pp. 47-48.

[2]Followed by Israel, France, Great Britain, Germany, the former Soviet Union and Russia, Turkey, Cuba, Spain, and Iran. The RAND Chronology of International Terrorism cited in Bruce Hoffman, "Terrorism Trends and Prospects," in Ian Lesser,et al., *Countering the New Terrorism* (Santa Monica, CA: RAND, MR-989-1999), p. 35.

this lamentable situation: "Terrorists attack American targets more often than those of any other country."[3] Recent testimony before a Senate Committee respectively by the Director, Central Intelligence, George Tenet and a senior State Department official further attested to this fact: with both men agreeing that "The United States remains a number one target of international terrorism. As in previous years, close to one-third of all incidents worldwide in 2000 were directed against Americans."[4]

That the world is perhaps a more dangerous place today for Americans than ever before is further evidenced by the U.S. State Department's list of "Current Travel Warnings and Public Announcements." As of this past Sunday (1 April 2001), for instance, more than a quarter of the world's countries were —for one reason or another— deemed unsafe for Americans to visit.[5] While one would doubtless expect to find Indonesia, Burundi, Israel (and the West Bank and Gaza), Colombia, etc. on the list of countries that Americans are recommended to avoid; the presence of the United Kingdom, for example, on an ancillary list of somewhat less dangerous places—but ones nonetheless with "terrorist threats and other relatively short-term conditions that pose significant risks or disruptions to Americans"---was slightly more bewildering. Admittedly, the 15 March 2001 advisory pertaining to the outbreak of foot-and-mouth disease in that country partially explains the UK's inclusion. But when one also consults the "public announcement" posted on 4 December 2000, which is still in force, a different picture presents itself of "numerous incidents of terrorism [in which] . . . some [Americans] have been injured when caught up in disturbances."[6] Those planning a holiday or embarking on a business trip might be forgiven for not knowing what to conclude from such messages: is it or is it not safe to travel to the United Kingdom? Am I at greater risk from terrorism by riding the London tube or from muggers while on the New York City subway? Is it more dangerous to visit the UK or to drive along one of American's highways to the nearest airport? The "Current Travel Warnings and Public

---

[3]Report from the National Commission on Terrorism, *Countering The Changing Treat Of International Terrorism* (Washington, DC, June 2000), p. iii.

[4]See Testimony of Thomas Fingar, Acting Assistant Secretary, Intelligence and Research, U.S. Department of State, Statement before the Senate Select Committee on Intelligence on "Worldwide Threat 2001: National Security in a Changing World," *Congressional Quarterly Abstract* (electronic version), 7 February 2001; and, Statement by Director of Central Intelligence George J. Tenet before the Senate Select Committee on Intelligence, "Worldwide Threat 2001: National Security in a Changing World," 7 February 2001 at:
http:www.cia.gov/cia/public_affairs/speeches/UNCLASWWT_02072001.html.

[5]See http://www.travel.state.gov/warnings_list.html accessed 1 April 2001.

[6]See http://www.travel.state.gov/warnings_list.html#u and http://www.travel.state.gov/warnings_list.uk.html, both accessed 1 April 2001.

Announcements" list of course makes no pretension whatsoever of being able to answer such questions, but at the same time it is difficult to disagree with the observation of these lists that was in Sunday's *Washington Post* travel:

> The warnings can be useful, but many travelers and travel professionals think the department often overreacts. Its current warning on Lebanon underlines the dangers of potential violence, but no travelers have reported problems there in years. During a two-week trip last summer, this reporter wandered the streets of Beirut without mishap. Even the southern parts of the country, which the [State] department described as particularly risky, seemed safe enough.[7]

At the same time, moreover, in a country like the United States where student-perpetrated homicides in our schools have become tragically uncommon, where national murder rates hover at around 16,000 deaths per year, and national violent crime figures annually exceed the one million incidents,[8] the risks to United States citizens traveling and working abroad need to be put in an admittedly discomforting perspective of just how safe we are in fact living and working and going to school within our own borders. Another *Washington Post* article this past weekend (on Saturday's front-page), for example, called attention to what is now sadly standard operating procedure in the metropolitan area's high schools: school safety drills "in which classrooms become protective bunkers . . . designed to show students, teachers and administrators how to survive should an intruder, or insider, suddenly appear with a weapon."[9] To put these two very different, equally tragic and heart-wrenching threats, in perspective: the 1999 Columbine, Colorado school shooting by two students killed 15 persons and wounded 23; that same year example (the most recent year for which published State Department statistics are available), according to the U.S. State Department's *authoritative Global Patterns of Terrorism*, a total of five Americans perished at the hands of terrorists and another 179 were injured as a result of some 169 terrorist attacks (a 52% increase from the previous year) directed against U.S. targets overseas.[10] It is perhaps worth noting that

---

[7]Gary Lee, "Deciphering State Department Warnings," *Washington Post*, 1 April 2001, p. E7.

[8]In 1999, a total of 15,533 persons were murdered in the U.S. (the 1998 figure was 16,973) among the 1,430,693 violente crimes that were recorded that year (1,533,887 in 1998). Source: Uniform Crime Reports, Federal Bureau of Investigation National Press Office, Washington, D.C., 18 December 2000.

[9]Michael E. Ruane, "School Safety Drills' New Mantra: Duck and Cover," Washington Post, 31 March 2001, pp. A1 & A13.

[10]Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism 1999* (Washington, D.C., U.S. Department of State Publication 10687, April 2000), p. 1.

on average, 26 Americans have been killed per year by terrorists since 1968:[11] in 1999, the year of the Columbine massacre, this figure was just two persons fewer than the 28 students killed nationwide in America's schools.[12]

In drawing this distinction, I should emphasize that I am by no means suggesting that terrorism does not pose a genuine and dangerous threat to Americans traveling or working abroad and indeed that whatever the number of persons killed and injured overseas it is incontestably tragic that any American should lose his or her life to violence or be wantonly harmed and injured simply because of the nationality of the passport they carry, the uniform they wear, or the job they perform. Rather, it is simply meant to point out that in assessing the terrorist threat posed to American interests and citizens abroad—as in the assessment of all types of terrorist threats—one needs to do so soberly and analytically lest we overreact, fail to place terrorism in the context of the many other risks and threats that exist and thereby inadvertently succumb to the fear and intimidation that is precisely the terrorists' timeless stock and trade.[13] As noted last week in my testimony before this same Subcommittee, we then risk making hard policy and security choices and attendant budgetary allocations based possibly on misperception and misunderstanding rather than on hard analysis built on empirical evidence.

With that caveat in mind, let me now turn to the first of the three subjects that I have been requested to address: that of, the general security environment for non-official Americans overseas. I will then turn to examining briefly the types of threats against non-governmental organizations abroad; and, finally will offer some general recommendations for protecting non-official American interests abroad.

THE GENERAL SECURITY ENVIRONMENT FOR NON-OFFICIAL AMERICANS OVERSEAS

Let me first point out that the above discussion of comparative threat assessment and relative risk analysis, drawing on cold statistics should not detract from the fact that the threat to Americans—including those travelling or living overseas in non-official capacities—is real, dangerous, and, I must note, arguably changing and growing in undesirable directions that could still more adversely affect U.S. citizens in the future. Whatever the , one point is incontrovertible: while the volume of worldwide terrorism

[11]Total deduced from published U.S. Department of State.

[12]Gregg Easterbrook, "Washington Diarist: Street Sign, *The New Republic*, 26 March 2001, p. 42.

[13]See "Combating Terrorism: In Search of A National Strategy," Testimony of Dr. Bruce Hoffman before Subcommittee on National Security, Veterans Affairs, and International Relations of the Committee on Government Reform, U.S. House of Representatives, 27 March 2001.

fluctuates from year to year, and the number of U.S. citizens killed or wounded rises and declines depending on the overall level of worldwide activity and the violent dimensions of each particular terrorist incident that affects Americans, one enduring feature is that the United States remains the favored target of terrorists abroad. As previously noted, since 1968, the United States has annually headed the list of countries whose nationals and property are most frequently attacked by terrorists. This phenomenon is attributable as much to the geographical scope and diversity of America's overseas commercial interests and the number of our military bases on foreign soil as to the United States' stature as the lone remaining superpower. Terrorists are attracted to American interests and citizens abroad precisely because of the plethora of readily available targets; the symbolic value inherent in any blow struck against perceived American "imperialism," "expansionism," or "economic exploitation"; and, not least, because of the unparalleled opportunities for exposure and publicity from the world's most extensive news media that any attack on an American target assures.

The reasons why the United States is so appealing a target to terrorists suggests no immediate reversal of this attraction. To a certain extent, as the French scholar, Gerard Chaliand has argued, it is a price that the West—and in particular the United States as leader of the free world—pays for its hegemony.[14] This has caused some analysts to argue that a less engaged U.S. foreign policy, exercising military restraint overseas and thereby eschewing the gamut of difficult and sometimes controversial missions involving peacekeeping and peace enforcement activities that in the past have invited attack, would have a salutary impact in reducing the incidence of terrorism directed against the U.S.[15] Whatever the logic of such proposals, however, even if such a policy of disengagement were desirable, much less, possible, it is by no means clear that the U.S. would be spared the opprobrium and violence that proponents of this option seek to nullify. Regardless of what the U.S. actually does, we are perhaps irrevocably perceived as a status quo power; a reactionary force upholding the prevailing order and thereby preserving our hegemonic dominance by tacitly inhibiting, if not actively suppressing, change.

Even those mostly parochial, local conflicts in places where the U.S. has traditionally had little if any active involvement, generate a somewhat surprisingly vehement degree of fear and loathing. In Sri Lanka, for example, the leadership of the

---

[14]Gerard Chaliand, "Preface' to Bruce Hoffman, *Le Mecanique terroriste* (Paris: Calmann-Levy, 1999), p. 9.

[15]See, for example, Ivan Eland, "Does U.S. Intervention Overseas Breed Terrorism? The Historical Record," *Foreign Policy Briefing, No. 50*, The CATO Institute (Washington, D.C.), 17 December 1998.

LTTE (the Liberation Tigers of Tamil Eelam), a militant and violent Tamil separatist movement,[16] reportedly decries the U.S. as an irredeemably "imperialist" power, arguing "wherever there is a revolution, America puts its hand in to interfere and to support the [ruling] government."[17] In other parts of south Asia, similar views are voiced with the same stridency. Recently in an interview with the *New York Times*, for example, Professor Mafiz Muhammed Saeed, the leader and founder of Lashkar-e-Taiba ("Army of the Pure"), one of several pro-Pakistani, militantly Islamic organizations fighting for the liberation of Kashmir from Indian rule, criticized the U.S. "Who is America to judge us?" he said. "We don't trust America, and we certainly do not see it as a champion of justice."[18] Indeed, these same acute feelings of anger towards and resentment of the U.S. were cited by Senator Warren Rudman and General Charles Boyd of the National Security Strategies Commission in testimony before this Subcommittee last week as auguring for continued—and perhaps even heightened—anti-American violence in the future.[19]

However, the main problem that we face in this critical area of protecting American citizens and interests abroad from both current and future threats rubs up against one of the fundamental axioms of terrorism: hardening one set of targets often displaces the threat onto another "softer" target.[20] In other words, security measures may successfully thwart planned or actual terrorist operations or even deter terrorists from attacking: but they do not eliminate the threat entirely, which may mutate into other, perhaps even more deadly forms. Determined terrorists, accordingly, will simply identify another range of vulnerabilities and hence potential targets; perhaps in turn adjusting or modifying their means and method of attack and executing a completely different kind of operation that still achieves their goal. The pattern of terrorist targeting of commercial aviation over the past three decades illustrates this point:

---

[16]That has been included on the State Department's Foreign Terrorist Organizations list since its inception in 1997 and is thereby proscribed from engaging in fundraising or any other political activities in the United States.

[17]Interview with a former high-ranking LTTE operative, Colombo, Sri Lanka, December 1997.

[18]Quoted in Barry Bearak, "Lahore Journal: A Jihad Leader Finds the U.S. Perplexingly Fickle," New York Times, 10 October 2000.

[19]See Prepared Statement of the Honorable Warren B. Rudman before the Subcommittee on National Security, Veterans Affairs, and International Relations of the Committee on Government Reform, U.S. House of Representatives, 27 March 2001.

[20]My RAND colleague, Brian Michael Jenkins, perhaps the world's foremost expert on terrorism, was the first to articulate this axiom of terrorist modus.

> During the late 1960s, for example, hijacking of passenger aircraft was among terrorists' favored tactics, accounting for 33 per cent of all incidents. However, as security at airports improved, as metal detectors and x-ray machines were installed at boarding areas, and as passenger profiling and other countermeasures were adopted, the incidence of airline hijackings declined appreciably to just seven per cent of all incidents in the 1970s and only four per cent in the 1980s. While these measures were successful in reducing airline hijackings, they did not stop terrorist attacks on commercial airlines altogether. Instead, prevented from smuggling weapons on board to hijack aircraft, terrorists merely continued to attack them by means of bombs hidden in carry-on or checked baggage.[21]

The 1988 in-flight bombing of Pan Am flight 103 being an especially notorious manifestation of this trend.

In the current context of heightened threats to U.S. diplomatic facilities and military forces overseas, as illustrated by such incidents as the 1996 bombing of the U.S. Air Force's Khobar Barracks in Saudi Arabia, the simultaneous bombings of the American embassies in Kenya and Tanzania two years later, and last November's suicide attack on the *U.S.S. Cole* in Yemen, the implication is clear. As we harden the range of American diplomatic and military targets long favored by terrorists—hardening existing embassies and consulates world-wide and building stronger, less vulnerable structures in particularly dangerous foreign posts while increasing the force protection afforded to our military personnel deployed overseas—we doubtless will not eliminate the terrorist threat completely, but risk displacing it onto "softer," more vulnerable and more accessible, unofficial, non-governmental targets—e.g., ordinary American tourists and travelers, business people and otherwise unwary citizens. [22]

The implications involving a potential increase in maritime terrorist attacks following the successful assault on the *Cole* are particularly chilling. For argument's sake, one might ask whether, as the defenses around and protective measures applied to U.S. warships increase in the aftermath of last November's devastating attack, does the threat posed by terrorism to a cruise ship heavily booked by American holiday-makers rise commensurately? It is horrifying to contemplate a *Cole*-type suicide attack on a

---

[21]Bruce Hoffman, "Terrorist Targeting: Tactics, Trends, and Potentialities," in Paul Wilkinson (ed.), *Technology and Terrorism* (London & Portland, OR: Frank Cass, 1993), p. 21.

[22]In my book, I make precisely this same argument: "success for the terrorist is dependent on their ability to keep one step ahead not only of the authorities but also of counterterrorist technology. The terrorist group's fundamental organizational imperative to act also drives this persistent search for new ways to overcome or circumvent or defeat governmental security and countermeasures." See Bruce Hoffman, *Inside Terrorism* (NY: Columbia Univ. Press, 1999), p. 180.

Princess or Renaissance cruise ship (to cite randomly two of the popular lines) steaming into a Caribbean, Mediterranean or U.S. port much less any other unprotected harbor. How serious this threat is currently taken and what steps are being enacted are not entirely clear.

This general pattern of terrorists attacking a wide variety of "soft' American targets is, however, already well established. For example, as previously noted, according to the State Department's annual Global Patterns of Terrorism for 1999, a total of 184 Americans were killed or injured by terrorists that year. Of this sum, seven were U.S. Government employees working overseas, nine were diplomats, nine were members of the U.S. armed forces, 26 were ordinary American travelers, tourists, journalists or expatriates and 133—or nearly three quarters of all America casualties—were business people. Viewed from another perspective, some 86 percent of Americans killed or harmed by terrorists in 1999 (the last year for which published statistics are available from the State Department) were neither government employees, nor diplomats nor military personnel.[23] This distribution, though is by no means atypical for the last five years of the decade, stands in stark contrast to the previous year when a total of 23 American fatalities overseas were recorded, with diplomats (19) leading the list—but as a result of the two East Africa embassy bombings—followed by other U.S. citizens overseas (3) and business people (one).[24] In 1997, business people, however, again headed the list of American victims (104 persons), other non-government/non-military U.S. citizens were next (14), followed by. government employees (four), diplomats (three) and military personnel (one). That year, 94 per cent of the casualties were in the business people/ordinary citizens' categories.[25] In 1996, this per cent was nearly identical, with business people and ordinary citizens accounting for 92 per cent of the total;[26] and, in 1995 it was similarly at the 90 per cent mark.[27] *Clearly, then, a variety of American citizens traveling, living and working overseas—but who have no ostensible or official connection with the U.S. government—are indeed already firmly in the terrorists' cross-hairs.*

---

[23]Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism1999*, p. 106.

[24]Idem., *Patterns of Global Terrorism 1998* (Washington, D.C., U.S. Department of State Publication 10610, April 1999), p. 96.

[25]Idem., *Patterns of Global Terrorism 1997* (Washington, D.C., U.S. Department of State Publication 10535, April 1998), p. 86.

[26]Idem., *Patterns of Global Terrorism 1996* (Washington, D.C., U.S. Department of State Publication 10321, April 1997), p. 1

[27]Idem., *Patterns of Global Terrorism 1998* (Washington, D.C., U.S. Department of State Publication 10610, April 1999), p. 73.

TYPES OF THREATS AGAINST NON-OFFICIAL AMERICAN CITIZENS AND NON-GOVERNMENTAL ORGANIZATIONS ABROAD

A total of 778 Americans have been killed by terrorists overseas between 1968 and 1999 (again, the last year for which published Department of State statistics are available). Of this number, half (391) were private citizens, 319 were U.S. military personnel, and 63 were American diplomats. More significant is the fact that 83 percent of Americans killed by terrorists between 1968 and 1999 died in attacks where s were specifically targeted. By comparison, 14 per cent (106) perished as a result of simply being in the wrong place at the wrong time when a bomb went off, a rocket-propelled grenade was fired or shots rang out.[28]

In various other cases, however, individuals are targeted not necessarily because they are U.S. citizens, but because they are Westerners in general and hence opportunistically regarded by terrorists as desirable for their potential to bring large cash ransom payments from their employers and/or families. This appears to have been the case with the three Americans who were kidnapped—and subsequently murdered—by FARC guerrillas in northeastern Colombia in February 1999 (a fourth American, a helicopter technician employed by BP Amoco oil company was kidnapped by the ELN, the other principal left-wing Colombian guerrilla organization, and released in August 1999).[29] Similarly, the three aid workers, who were helping the U'Wa Indians, are thought by State Department officials to have also been in the wrong place at the wrong time and hence to have represented a serendipitous target of opportunity to the guerrillas. This was also the case with the two Americans who were among 14 foreigners kidnapped the following month by renegade Rwandan Hutus. All the victims were on a camping trip in Uganda's Bwindi Impenetrable National Park to observe gorillas. The two Americans were among eight of the foreigners whom the rebels murdered.[30]

All 12 of the Americans who died in 1998, however, were either employees of the U.S. embassy in Nairobi or dependents; while seven of the 11 U.S. citizens wounded that year by terrorists sustained their injuries either at Nairobi (six) or Dar-es-Salaam (one). Interestingly, three-fifths of all the terrorist attacks directed against U.S. targets that year were bombings: with American businesses the foremost target.[31] This pattern of

---

[28]In the case of 18 American victims the reason is impossible to determine. Total deduced from published U.S. Department of State.

[29] FBIS-LAT-2000-0810 "ELN Releases US Citizen Held for Year," Mexico City NOTIMEX, 31 August 2000

[30]Idem.,*Patterns of Global Terrorism1999*, pp. 1, 6 & 25.

[31]Ibid, p. 1.

targeting U.S. commercial interests and business people was evident during 1997 as well when four Americans, employed by Union Texas Petroleum, and their Pakistani driver, were specifically targeted in an attack on the van in which they were riding to work in Karachi. That same year, the body of Frank Pescatore, a U.S. geologist kidnapped by FARC in December 1996 was discovered in another incident where opportunism seemed to have played as much a part his abduction as his nationality.[32] In 1997, seven other Americans were also abducted. Four were seized in Latin America—an engineer and gold miner kidnapped by FARC in two separate incidents (both were released unharmed), a geologist seized by Ecuadoran Indians, and a geologist abducted by the ELN (both men were also freed)—and three in Yemen —two American businessmen and a tourist who were all later freed unharmed.[33]

By contrast, the 24 U.S. citizens who were killed by terrorists overseas in 1996 reflected the varying ways in which Americans are both deliberately targeted and killed or injured through sheer happenstance. For example, 19 of the fatalities were U.S. servicemen who died in the specific targeting of the U.S. Air Force Khobar barracks in Dhahran, Saudi Arabia. This figure, in fact, remains the highest number of US citizens killed in a single act of international terrorism since the 1988 in-flight bombing of Pan Am 103 (189 Americans perished in that incident).[34] However, the remaining five Americans who died that year were all killed in Israel. Each was unfortunate enough to have been riding a bus or standing in front of a shopping mall when a terrorist bomb exploded.[35]

1995 presented a similarly mixed picture of victimization by design or chance. Among the 12 U.S. citizens killed were two U.S. consulate employees who were deliberately gunned down by terrorists in Karachi; two missionaries who were executed by the FARC in Colombia; a tourist murdered by the Khmer Rouge in Cambodia; and two U.S. citizens killed in suicide bus bombings respectively in Jerusalem and the Gaza Strip[36] The latter victim was 20 year old Alisa Flatow, whose father filed suit in Federal District Court in Washington, D.C. and who in March 1998 won a landmark $247.5 million judgment against the Government of Iran for supporting Palestine Islamic Jihad, the group that had claimed responsibility for the bus bombing.[37]

---

[32]Idem., *Patterns of Global Terrorism 1998*, p. 1.

[33]Bureau of Diplomatic Security, *Significant Incidents of Political Violence Against Americans, 1997* (Washington, D.C., U.S. Department of State, 1998), p. 37.

[34]Idem., *Patterns of Global Terrorism 1997*, p. 1.

[35]Ibid., pp. 1 & 18.

[36]Idem., *Patterns of Global Terrorism 1996*, passim.

These basic patterns remain unchanged today. During the year 2000, for example, four American climbers were kidnapped by members of the Islamic Movement of Uzbekistan (IMU), who happened to come upon their encampment on a cliff face of Mount Zhioltaya Sten in Kyrgyzstan. They managed to escape captivity six days later, after killing a guard.[38] That same month, an American, Jeffrey Craig Schilling, was seized by the Abu Sayyaf organization, a radical Muslim group active in Mindanao in the Philippines. The organization had previously kidnapped two other U.S. citizens: a Protestant missionary named Charles Walton in November 1993 and a Roman Catholic priest, Father Clarence Bertellsman the following July—both were eventually released unharmed.[39] An American was among 26 biologists seized by the ELN who were released in August;[40] and, FARC hijacked a helicopter in Ecuador in October and kidnapped six US citizens, two Frenchmen, a Chilean and an Argentine.[41] In November, an American, who headed a program of the US Republican Institute in Azerbaijan, a non-governmental organization, was found murdered in Baku, apparently the victim of a robbery;[42] and in January 2001 a U.S. citizen in Chechnya there as part of a humanitarian aid mission organized by Action Against Hunger was kidnapped.[43]

As the latter incidents evidence, threats to Americans working for international humanitarian relief organizations and similar non-governmental organizations, present a special problem. NGO workers are increasingly under threat for a number of reasons. As Randolph Martin, senior director for operations at the New York-based International Rescue Committee explains, this is a reflection of a combination of developments and circumstances:

---

[37]David M. Herszenhorn, "Out of a Father's Grief, a Tool Against Terrorism," *New York Times*, 4 January 1999.

[38]See Michael Roberts, "Cliffhanger," and Greg Child, "Fear of Falling," *Outside Magazine*, November 2000 at http:www.outside.com; and, Pete Takeda, "Escape from Kyrgyzstan," *Climbing Magazine*, 15 December 2000, pp. 85-92.

[39]FBIS Transcribed Text, "Philippines: Abu Sayyaf Wants 4 Other States To Join in Talks To Free US National," FBIS-EAS-2000-0831, Manila Philippine Daily Inquirer, 31 August 2000.

[40]FBIS-LAT-2000-0812, "ELN Delivers Kidnapped Ecologists to Humanitarian Commission," Mexico City NOTIMEX, 12 August 2000.

[41] FBIS-LAT-2000-1012, "Ecuador Confirms Helicopter Hijacking, Kidnapping of Foreigners by FARC," Paris AFP, 12 October 2000.

[42]FBIS-SOV-2000-1130, "US NGO rep killed in Azeri capital," Baku Turan in Russian, 30 November 2000.

[43]FBIS-SOV-2001-0100, "US citizen abducted in Chechnya," Moscow ITAR_TASS in Russian, 10 January 2001.

- The overall increase over the past decade in the number and duration of conflicts to which aid workers are deployed;
- A general absence of rules of war or rules of conduct among the belligerents themselves, many of whom are irregular fighters and may also include criminals and bandits interested as much in plunder as in the realization of a particular political agenda;
- A prevailing perception of aid organizations as particularly "soft" targets that leads terrorists and other malefactors to conclude that such organizations and especially their employees can be "attacked with impunity"
- The erosion of the accepted neutrality of aid groups, who are seen by some belligerents as partisan, interventionist and generally an undesirable presence;
- A conspicuous lack of security among many NGO workers combined with a skeptical, if not averse attitude towards the need for security and other protective measures; and,
- The general rush to arrive on the scene of conflicts or humanitarian crises most needing help without adequate prior security preparation or thought. [44]

Martin's points dovetail with the views of another American citizen known to this author who works with a U.S.-based aid organization in a particularly conflict-plagued country in Africa. According to this person:

> The first threat we face is basic: threats against expatriates [by terrorists, guerrillas, paramilitaries and others] to gain publicity, or enhance panic and fear or to attempt to get aid agencies to withdraw. . . . The second threat is common banditry or theft that is common anywhere but enhanced in a country at war, facing severe economic difficulties . . . .The third threat that we face . . . is being caught in the cross fire- whether it be stray bullets hitting "expat" houses, rebel ambushes on the roads, hitting mines, or being caught in the field during a rebel attack. This third threat is often the most difficult to predict.

Based on the observations of this aid worker, the help provided by the local U.S. Embassy appears to be ingenuous, but limited. For example, when the security situation becomes especially tense or critical, the local U.S. embassy will sponsor a "Town Meeting" for all

[44]Randolph Martin, "FMR 4 April 1999: NGO field Security," New York: International Rescue Committee, accessed at http://www.irc.org.

American citizens. These meetings review the current security situation in the country, and discuss responses—that is, mostly going over evacuation procedures, addressing the effects of curfews, etc. In especially volatile countries or at times of heightened danger, local American embassies will organize a warden system for U.S. citizens and green-card holders resident in that country. The U.S. embassy will contact "wardens" (American citizens who are chosen to represent certain zones of a city or other defined geographic areas) in the event of a security incident. The wardens then alert or pass on any embassy communications to persons in their zone.[45]

In general, the problem with NGOs therefore appears to be two-fold. On the one hand, the NGOs themselves arguably pay too little attention to security and in the past have provided insufficient training and pre-deployment. While on the other hand, it often falls to the local American embassy to fill this void, whose efforts and activities in this respect can be limited as much by insufficient resources and too few personnel.

CONCLUSION: RECOMMENDATIONS FOR NON-OFFICIAL AMERICAN INTERESTS ABROAD

It should be recognized that terrorism is not a problem that can be solved, much less ever completely eradicated. No country with the breadth and magnitude of the overseas interests and presence that the United States has can reasonably expect to hermetically insulate or seal itself off completely from any and every manifestation of this threat. In this respect, there are no broad, sweeping policies or new approaches in the form of overarching bureaucratic fixes or individual "magic bullets" that can hope to counter, much less, defeat a threat that is at once omnipresent and ceaseless. By the same token, we are neither powerless nor defenseless in the face of terrorism and there are a number of practical steps that might usefully be taken that might effectively mitigate the threat. These could include:

- Ensuring that our intelligence resources and capabilities—especially with respect to HUMINT (human intelligence sources)—are sufficiently funded, properly organized, and continually oriented to actively identifying and countering the range of threats confronting American citizens and interests overseas;
- Making certain that the security in and around the principal transportation nodes—both for air as well as maritime travel—most frequented by American

[45]E-mail correspondence with an American working in Africa for a U.S.-based international humanitarian relief organization, 11 March 2001.

tourists and business people overseas are of a uniform, high standard. In this respect, Federal Aviation Agency and Department of State inspection teams have repeatedly in the past identified lax security in airports throughout the world—particularly in some African, East Asian, and Latin American countries;

- Further educating and informing the headquarters and staffs of United States-based NGOs and international humanitarian relief organizations of the importance of security and the pre-deployment and proactive measures that can be adopted to enhance the safety of Americans working overseas for these organizations in conflict-ridden countries of the world; and,
- Perhaps seeking to achieve further consistency and clarity in the travel advisories and other warnings and public announcements emanating from official U.S. government sources.

Finally, the threat of terrorism itself needs to be kept in perspective. There is a thin line between prudence and panic. Accordingly, a prerequisite to ensuring that our formidable resources are focused where they can have the most effect is a sober and empirical understanding of the threat. Only in this manner can our efforts achieve the greatest likelihood of success and effectiveness.

Thank you for your time. I will be happy to respond any questions that you might have.

Mr. PUTNAM. I thank all of our witnesses on the first panel.

Before we move into questions, I would say, pursuant to House rules and committee rules, I note for the record that the subcommittee requested and all witnesses appearing at this hearing in a nongovernmental capacity have provided a resume and disclosure of Federal grants and contracts received.

At this time, I would call on the gentleman from New York, Mr. Gilman.

Mr. GILMAN. Thank you, Mr. Chairman; and I want to thank our panelists again for focusing on the important aspects of what we're confronted with worldwide.

George Tenet, our agency head, CIA Director, stated, U.S. remains a No. 1 target of international terrorism. Close to one-third of all incidents worldwide in the year 2000 were directed against Americans.

I am going to address this to all of our panelists. Last week when we conducted our hearing we found that there was a proliferation of the responsibilities among 40 some agencies who had a little bit of their responsibility directed to terrorism; and I think then we focused on the need for a centralized agency, some central control at White House level. What I am going to ask all of our panelists, from your knowledge and your experience, and you all are experienced in this area, what improvements can we make that would have the greatest promise of improving the safety of Americans traveling abroad and Americans in business abroad?

Let's start with Mr. McCarthy.

Mr. MCCARTHY. I think that in order for people to protect themselves abroad, as they travel abroad they must have the information that exists in country at the time that they travel. The Office of Consular Affairs of the U.S. Department of State certainly provides a lot of information concerning the current economic—well, actually, the political situations in these areas. This information should—is very difficult sometimes to get. Of course, now with the Internet and several other means of mass communication, the public can get this information they need.

It's very difficult—it's very difficult for the U.S. Government to control activities in foreign countries, obviously, for sovereignty reasons. But I think some effort—much more effort must be made in order to try and help these countries. It's been my experience that the U.S. Government and the Western powers have exported democracy to some of these high-risk areas and emerging areas but did not export the handbook as to how democracy should be implemented, and I think the U.S. Government and its allies in the Western world should cooperate more with these countries to try and show them how democracy must be implemented and, in that way, possibly help safeguard not only the people within the country themselves but also the people who travel into these countries.

In many of the high-risk areas we see poverty—as Mr. Kucinich has pointed out, we see poverty and we see exploitation of the local populations by these new governments. Particular examples, of course, are Nigeria and Indonesia. And when you look at the way the money that's proliferating in these countries, the money that's available in these countries is unbelievable from the extraction—actually, from the extractive industry, from the extraction of oil

from these areas, and the tax dollars that the oil companies pay to the governments fails to trickle down to the populations themselves.

Yet if you look at the Far East—not the Far East but the Middle East and see the way the people in those countries live, they depend on the same source for their economy, namely the oil industry, but yet the governments treat them a lot better. Granted that they're not democratic governments, but here in the area of Nigeria and Indonesia, where they have exploited a democracy and the Presidents of those countries have more or less wrapped their arms around the democratic principles and trying to enforce them, yet the people remain fairly poor and poverty stricken.

The oil companies, of course, do take a beating in this regard; and they're blamed for everything. And the people in the communities look to the oil industry and the extractive industry and the companies there to supply them with the infrastructure and——

Mr. GILMAN. Mr. McCarthy, I am sorry to interrupt you. We've got four other panelists and my time is limited, if you could just wrap up.

Mr. MCCARTHY. What I am trying to say is that when we export democracy we have to export the handbook. We have to try and train the police and train the military to be responsible for their people there and for the people who come in there, and we have—and the U.S. Government I feel owes a responsibility to try and proliferate the problems.

Mr. GILMAN. Thank you. I see our time is running, Mr. McCarthy.

Mr. Littlejohn.

Mr. LITTLEJOHN. Thank you very much.

I agree with Jack. I think the first thing we need is good information, good intelligence information. As I made a statement in my opening remarks, often we get conflicting information. Presently, most of our members in the private sector working abroad work with OSAC, and we strongly believe that OSAC should be the organization that should be the clearinghouse. However, we question whether or not OSAC is getting all the information from Central Intelligence, etc., that could be sent out to U.S. companies to protect their people both traveling and living abroad.

Second, as Jack also mentioned, what goes on in a respective country. Now the FBI working with State had an excellent operation in National Academy of Budapest, which was very, very successful in training law enforcement in east bloc countries, and I understand that the DEA is looking at something in Thailand. There are also——

Mr. GILMAN. We have one in Thailand now. We've opened a similar one.

Mr. LITTLEJOHN. Is it open?

Mr. GILMAN. Yes, it's open and functioning. They're now exploring South Africa, but I am going to ask you to please wrap up.

Mr. LITTLEJOHN. OK. Finally, we have to do something to assist law enforcement communities in these communities who personally, A, are corrupt and, B, are not properly trained.

Mr. GILMAN. Thank you.

And Mr. Bishop.

Mr. BISHOP. Nongovernmental organizations engaged in humanitarian response in conflict situations are required by international humanitarian law to maintain their political independence. They do not represent the U.S. Government, and they cannot. As long as they're able to maintain this independence, they are at less risk of terrorist attack.

With great respect, Mr. Gilman, I do not think that, as their representative, it would be appropriate for me to comment on how the U.S. Government should organize itself to deal with terrorism. I have made several suggestions on what the U.S. Government might do to assist NGO's in enhancing their security overseas.

Mr. GILMAN. Thank you, Mr. Bishop.

Mr. Cilluffo.

Mr. CILLUFFO. Thank you, Mr. Gilman.

I personally don't think that there's a single fix, nor do I see this as a one-time fix. This is something that requires perseverance and continually reacting and keeping up with the state of the threat.

But on the macro side—and there are a number of micro issues that we obviously don't have time to discuss right now—but on the macro side I personally believe the first line of defense is intelligence. We should always get there before the bomb goes off. To date, signals intelligence and other technical means have provided the lion's share of actual counterterrorism operational intelligence, but the truth is that only a human source is going to tell you when and where a bomb is going to go off. So we need to enhance our human capabilities, and we need to make sure that there are no constraints prohibiting these capabilities from being able to flourish.

Obviously, we need oversight, and that's a responsibility that the Hill and others should take very seriously. But the point is that terrorists don't frequent the cocktail circuit, they are not Boy Scouts, and we need to be willing to recruit these sorts of individuals.

Second, I think improving the signal-to-noise ratio of indications in warning intelligence has been the biggest challenge. After a major event we're all at delta in terms of threatcon, but before you—basically, Embassies, military bases and even U.S. companies get bombarded with vague threat warnings. The challenge is going to be, how do you improve that from a vague warning to a very specific warning where you can take very specific actions to prevent, preempt or protect against a particular action?

Third, I think training, training cooperation. The ILEA is a good example. It's been a very successful model. We need to build on that. I think companies also need to be working with the indigenous security services; and I would note the millennium bombing, the Jordanians saved a lot of American lives during the millennium in Jordan. So I think we need to be working toward enhancing transnational cooperation.

Then, of course, there are a lot of prophylactic and antiterrorism as opposed to counterterrorism measures that should be taken.

Mr. GILMAN. Thank you very much.

Mr. Hoffman, our time has run, so we need——

Mr. HOFFMAN. I'll be very brief. I agree in improving intelligence, but I think also improving the accuracy and timeliness of open source information.

Mr. GILMAN. Could you put the mic a little closer, please? I can't hear you.

Mr. HOFFMAN. Sure. Improving the accuracy and timeliness of open source information as well as intelligence and its dissemination.

Second, increasing, I think, the overseas resources available to Americans. It is my understanding—I may be incorrect—that OSAC is oriented primarily toward the American business community, but increasing the resources available to ordinary American citizens. Regional security officers, for example, at our Embassies and consulates, already overworked, I think do a superb job. Their responsibilities have increased as the number of surveillances reported against their Embassies has grown, but their focus is diplomatic security, not necessarily that of ordinary Americans.

And, finally, I think strength in programs such as the Anti-Terrorism Assistance Program run by the Department of State, which trains law enforcement personnel in other countries, that helps them improve their own security and, in turn, affects the safety of Americans but also fosters an atmosphere of invaluable cooperation and liaison.

Mr. PUTNAM. Thank you, Dr. Hoffman.

Mr. GILMAN. Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you, sir.

At this time, I will recognize the ranking member, Mr. Kucinich, for 10 minutes as well, after which we're going to try to go back and hold firm on the 5-minute rule, alternating between sides. Mr. Kucinich.

Mr. KUCINICH. I thank the gentleman, and I again want to thank the witnesses for their participation.

Mr. McCarthy, I have a detailed summary of questions that I have for you as the director of corporate security for Texaco, and rather than make this entire meeting the focus of Texaco, what I'd like to do is to—I am going to submit these questions for the record, but I'd like to give those questions to you and perhaps you could respond in writing. That way we can facilitate this.

I am not here to embarrass anyone, but I do have some concerns about Texaco's practice in Ecuador. I know you're working right now on trying to settle a case for $500 million on the pollution in Ecuador and the Amazon region, and I have questions that relate to human rights abuses with Texaco and Chevron in Nigeria and questions that relate to Texaco and Unocal in Burma and questions that relate to Texaco in Indonesia.

But as I review all the questions, what it comes down to is this. I think this hearing can help solve some real concerns that people have in the world about business. Dr. Hoffman was the only panelist who had a—what I think is some degree of political analysis as to what our dilemma is here, and I speak as someone who has had some background in international business as a marketing director for a software company. I had the chance to go around and visit many countries and saw Fiumicino airport protected by people with machine guns, understand the climate some of you are working in.

These hearings have a way of communicating the fear that's out there. None of us wants to see any of our citizens hurt abroad, that's for sure. We want to be able to see American business go abroad and be successful and help other countries grow as well. I think all of us would agree with those principles.

But there's another level here that we have an opportunity to get to beyond this litany of questions which, Mr. McCarthy, I assume you would be willing to respond to them, rather than us drag it out here, but I want to go beyond that.

Do you see that there is a role for human rights principles, such as we had with the Sullivan principles in Ireland, human rights principles to guide the work of U.S. multinational corporations and those principles incorporating workers' rights, environmental quality principles? Mr. McCarthy, do you think that if Texaco had or could enunciate principles of doing business that it would enable Texaco not only to be less of a target but for Texaco to lead the way in terms of a new era in global business? I'd like your response.

Mr. MCCARTHY. Texaco at the present time is part of an initiative which has been developed by the British Foreign Office and the U.S. State Department where for the past year—actually began in November 1999 and completed with a press release in December 2000, where it supported and welcomed a number of human rights principles that were developed with the cooperation of the extractive industry and the NGO's. It's about a 10-page document and has been released to the public. And just recently we came from a meeting in London where we're in the process of determining how these human rights principles can be incorporated into the business plans of various industries, not only from the extractive industries but also from other American business industries, these principles.

Mr. KUCINICH. See, I think Texaco and your business partner Chevron, because of your presence in so many countries, can help to lead the way internationally for setting new standards for human rights. I mean, it would be very easy, frankly, to spend this time in this committee to go over the litany of human rights challenges which are faced, and I can also understand that in the extractive industry you enter into a climate which you're going to receive resistance anyhow, and I can also understand in talking to people in your industry the challenges that you face from people who don't want to be fair. I know that, too, but I think with the tremendous financial power which Texaco has, with the scope and the reach of your industry, that there might be an opportunity here to create some new possibilities.

Now, we can—you know, again, I understand the past. I know the record, believe me. I have spent a lot of time studying the record of Texaco and Chevron and other people in your industry. But we can't change that past. We can change the future, and so I would like you to submit to this committee, and I'd like to see it personally, and I'd like to work with you in crafting some human rights principles and principles that protect workers and the environment because we might be able to have an opportunity here for a new dialog. Then, if we take that direction, it may be that some of these security risks which we find ourselves having with our citi-

zens abroad would not take the shape that they have taken today. And, again, that's not to in any way soft pedal what I think is a disturbing record of human rights violations, but we're all accountable, not just you. I am accountable, too. We're all accountable.

So to try to go above this debate, yes, we should do something about making sure our citizens are safe abroad. Whether we want to use the intelligence apparatus of the United States of America to do that, I'll let some of my other colleagues get into that, but I would like to work with you to do something about creating new possibilities in this new millennium for human rights. I think we could do it, and I think Texaco has the understanding to do it. I don't think there's any industry in this country that has the kind of power and scope that your industry has, but we need to find a way to go into a new millennium with some new possibilities.

So we have a short time for a response, but I just wanted to refocus this a little bit. Mr. McCarthy.

Mr. MCCARTHY. Well, I think I—for Texaco, Texaco's always been interested in human rights and as part of its values—and its vision and values certainly has incorporated the basic human rights and operates in a perfectly legitimate and ethical manner around the world. That's been our policy. And again, as I say, we are part of the most recent initiative as far as developing human rights principles to be used not only in the extractive industry but all other industries that happen to operate in high-risk areas.

Mr. KUCINICH. And I would like to again work with you to facilitate the delineation and enunciation of those principles. So it goes beyond talking. I am just openly offering that. I mean, I could take another position here at this committee table, as you well know, but I am not doing that. I am submitting questions for the record, but I am letting you know, let's go beyond where we are at because I don't think where we're at is satisfactory, to be charitable about it.

Mr. MCCARTHY. Well, as I said, that Texaco with the Department of State and the British Foreign Office is working very diligently and has crafted over the past year and has worked very hard with NGO's, Human Rights Watch, Amnesty International and several other NGO's as well as the top companies from the extractive industry in formulating these principles that have already been promulgated. And we are working now in phase two to try and find some way that we can implement these principles around the world.

So we're already doing that. In fact, we've taken a leadership role. I was one of the first ones to sit on this board and take a leadership role in establishing these human rights principles. So Texaco and the extractive industry is certainly out in front when it comes to trying to put together human rights principles that protect people and protect their property.

Mr. KUCINICH. I'd like to have some followup meeting with your company about these things. I just see this as the opening of a dialog. Thank you.

Mr. PUTNAM. Thank you, Mr. Kucinich. Gentleman's time has expired.

Mr. Otter, you're recognized for 5 minutes.

Mr. OTTER. Thank you very much, Mr. Chairman; and I think this is probably a pretty timely hearing that we're having.

I, like the previous member of the committee, have had a lot of experience in the international marketplace. I was the president of a company called Simplot International, which was a company that sort of followed McDonalds, if you will, around the world; and we supplied the French fries. I am from Idaho, if that surprises you.

Anyway, I found that in order to be successful internationally the first two mistakes that most companies make when they go into a foreign country, into a foreign value system is—No. 1 is failure to recognize their traditions and to respect those traditions; and the second thing is failure to recognize their practices and their beliefs and then respect those.

And, you know, I can think of many, many cases where I would no more put up with the way women are treated in certain areas of the world, especially the Middle East, than I believe any person in this room would, yet depending upon the value that we place on those goods and/or services that we get from that area of the country we are willing to look beyond that. So I think part of our whole attitude toward what we want to happen in the rest of the world has got to conform to what the rest of the world wants as well. Because I know I was not going to be successful.

I have been to 82 foreign countries and, for the most part, everybody in those countries—and there isn't a country I can believe or that I was part of that I was in that didn't have a little bit different value system than what I as a farm boy from Idaho had. And so I had to respect that if I was going to be successful.

The second thing that I found out is that almost anyplace I went, anyplace I went, not only my company but any other American country had elevated the value of life, had elevated the style of living, had elevated the purpose of the individual in society. It was maybe slow, and it may be, to some who wanted perhaps a little more, a little faster response in human rights, in other areas, it may well be slow, but I can tell you, from the time that I first arrived in a country until maybe I went back several times to view how the operation was going, things had improved, understandings had come together.

So laying that as a format for all the panelists, I want to ask you a couple of things. It's been my experience that the types of, quote, unquote, terrorism basically came in two areas. One was economic terrorism. They were after me or one of my people in order to hold us for ransom so that they could get some money to advance some more of their efforts which in many cases, believe it or not, the world believed was an advancement of human rights, oddly enough.

The second thing was for philosophical purpose, and philosophical purpose is broke down into two veins. One is religious, and the other was political. I never went to a U.S. office in a foreign area without making sure that everybody, everybody that I knew knew why I was going there. I did not want to be part of the information gathering system of the U.S. Government because that immediately left me suspect in my community, in the business community, and it immediately left me vulnerable to some of these folks who were, quote, unquote, working for democracy in their country.

I'd just like you to respond all but briefly, now that I've made my speech, all but briefly as to whether or not I am right or wrong. No. 1, do you believe that Texaco, any country you went into, are those people worse off now that you're there or better off? And with the experiences that the rest of you have and including the humane efforts of Mr. Bishop's outfit. Mr. McCarthy first.

Mr. MCCARTHY. Well, I think in many of the undeveloped areas that the extractive industry has gone into that the people are better off than they were before. The reason that's true is because, just as we practice humanitarian and philanthropic aid here in the United States, we also do it overseas in these poor areas. And so we build roads for them, we build hospitals for them, we furnish them with light sources and medical equipment and medical training and medical facilities that they normally would not have. This has, in effect, lengthened their life and increased their standard of living.

Mr. OTTER. Thank you.

Mr. Littlejohn.

Mr. LITTLEJOHN. First of all, I agree with the traditional belief. Clearly, a business is not going to be successful unless it's molded around the local traditions and beliefs. But, second, the area of terrorism, I've experienced—I've had kidnappings in the Philippines, Colombia, Russia and Mexico which I have managed.

Mr. PUTNAM. The gentleman's time has expired. If we could finish out this panel with a yes or no, if people are better as a result of these.

Mr. LITTLEJOHN. Yes.

Mr. OTTER. Thank you.

Mr. Bishop.

Mr. BISHOP. Sometimes. In Sierra Leone, there was a conflict. It was ended. We needed, with the U.S. Government and other donors, to provide development assistance to consolidate that peace. They walked away from it.

Mr. PUTNAM. Thank you, Mr. Bishop. We'll put you down as a sometimes.

Mr. Cilluffo.

Mr. CILLUFFO. Well, I sit here in the city of northern charm and southern efficiency. I don't have business interests abroad, so I can't answer the first question.

The second question, however, you are seeing a shift from—I mean, terrorism has always been both political and economic, but you are seeing a shift toward less political terrorism, toward more nationalist and radical fundamentalist religious terrorism.

Mr. OTTER. Thank you.

Dr. Hoffman.

Mr. HOFFMAN. Well, with all due respect I would say that's not the right question because it's not so much important what I think but what they think. And I think a problem is what we regard as benevolence and munificence they see as interference, as propping up the establishment and as preserving the status quo, and that's the problem.

Mr. PUTNAM. I am sorry, we're going to catch you the next round.

The chair recognizes Mr. Tierney for 5 minutes, plus a Washington version of a yes or no.

Mr. TIERNEY. Thank you, Mr. Chairman, and thank you for your fair way of handling this hearing. Is there going to be another round of questioning after the first panel?

Mr. PUTNAM. I have got time, if you've got time.

Mr. TIERNEY. I am hard pressed to let pass some of the comments that were made, because I am dying to find out just how much mistreatment of women would equal the price of commodities or what we get out of commodities in some of these countries. I don't think we should let that go unexplored at some point, and perhaps we'll ask all of you the question along that line.

But let me start with the question for perhaps Mr. Cilluffo initially. What is your opinion what the United States should do beyond providing information and communication networks and electronic data bases, newsletters and other publications in order to increase security for corporate interests worldwide?

Mr. CILLUFFO. I do think that when we do look at information sharing and intelligence cooperation, that is absolutely crucial. And we are not talking about a Kumbayah kind of fest where we sit at the campfire——

Mr. TIERNEY. I understand. I am talking about beyond that.

Mr. CILLUFFO. I also think that we can be working toward common standards, common procedures to benchmark what is OK and what is not. I am not saying—I don't know if we want to go down that path too far, because then you're accountable based on certain standards, but I think we can work toward that. And I also think that working with our foreign counterparts is absolutely essential and not just in terms of investigations and techniques and capabilities but also understanding the rule of law, the way we at least—maybe it's blinded, but the American version of the rule of law.

Mr. TIERNEY. Thank you.

Mr. Littlejohn, what do you say to that? How much more should the United States through its official agencies do to protect corporate interests beyond information and communications?

Mr. LITTLEJOHN. Well, I think we need help in the field. I think when companies are starting a startup operation they should be aware of what they're getting into. And, as I pointed out in my initial recommendations, I believe that agencies, particularly FBI leadouts in the country, should be introducing the security people to the local law enforcement agencies, people that they can trust that can help. But I do believe also that OSAC has been providing us a lot and should continue on to provide both training and information; and the RSOs, of course, have to get into that.

Mr. TIERNEY. To the extent that the United States provides that kind of assistance to corporations, do you believe that there's any right for the public, the tax-paying public, to expect backing and quid pro quo from businesses such as a commitment to certain environmental standards and perhaps treatment of employees?

Mr. LITTLEJOHN. Oh, absolutely. How to define it, I couldn't say, but, yes, I believe that.

Mr. TIERNEY. How about you, Mr. McCarthy? Do you believe that there's a right for us to require some standard of environmental standard and employee protection in return for what the U.S. taxpayers' money does in security interests?

Mr. MCCARTHY. Well, I think that these companies in the extractive industry are already providing that to a certain extent. The division of values of American companies embody the American spirit which incorporates environmental protection and human rights, and most companies that I am aware of anyway have incorporated that division of values.

Mr. TIERNEY. You don't want to rely on what Texaco has done for protection of environmental rights in making that statement, do you?

Mr. MCCARTHY. Well, Texaco has done pretty good in protecting environmental rights.

Mr. TIERNEY. Well, I have got to go there then.

I've got to ask you. You've been sued in New York, your company, for dumping tens of millions of gallons of toxic waste into the Amazon over a period of 20 years. Is that your idea of a good environmental policy for indigenous people?

Mr. MCCARTHY. I am really not fully familiar with the problems in Ecuador at this particular point in time. For me to answer these questions would be pure speculation on my part.

Mr. TIERNEY. You're basically answering my question. Without the knowledge of what your company has been at least charged with doing and which they settled at the cost of $500 million for doing—you're aware of the settlement?

Mr. MCCARTHY. I am aware of that——

Mr. TIERNEY. But you don't rely on that for the statement that your company has a great record of protecting environmental interests?

Mr. MCCARTHY. I don't really represent Texaco at this particular meeting. I represent OSAC, and I was under the impression that my presence here was to deal with terrorism, not with the policies and programs of Texaco. If we had——

Mr. TIERNEY. Well, you're talking about security for our nationals, right?

Mr. MCCARTHY. If I knew that the questions would deal on human rights and on problems in Ecuador certainly somebody would be here to answer those questions for you.

Mr. TIERNEY. Well, I just have to tell you that I hope all the witnesses are prepared to answer what responsibilities people that are protected at the cost of taxpayers' money owe back to the taxpayers in terms of corporations. My question was really designed toward, could we rely on some expectation that if we're going to spend taxpayer money for security measures abroad, could we expect that those corporations would be asked to adhere to certain environmental standards and labor standards?

Mr. MCCARTHY. Well, as I mentioned to you, Texaco, as well as other companies in the extractive industry, are already engaged in issues with foreign—with not only the U.S. Government but foreign governments in trying to put together human rights policies and other policies that will address those situations.

Mr. TIERNEY. Thank you.

Mr. PUTNAM. Gentleman's time has expired.

The Chair would note that the role of human rights advocacy in reducing resentments and easing the terrorist threat may indeed be a very appropriate topic for a future hearing. The subject of to-

day's hearing is the potential—excuse me, the protection of the U.S. interests against the immediate threat of terrorism.

Mr. TIERNEY. Point of order on that, please.

Mr. PUTNAM. You're recognized.

Mr. TIERNEY. Is that to say that you're limiting the hearing, there will be no questions about what we might expect back in return for the provision of those security measures?

Mr. PUTNAM. No. The gentleman is incorrect. It was simply to remind all members and the audience that the topic of today's hearing is protecting of U.S. interests against the immediate threat of terrorism. You can direct your questions in whatever way you see fit. You're an elected Member of Congress.

We will do one more round for this panel and then bring in panel two. Mr. Gilman, you are recognized.

Mr. GILMAN. Thank you, Mr. Chairman; and I'll be brief.

Mr. McCarthy, as co-chairman of the OSAC organization I note that OSAC is supposed to be a clearinghouse for exchange of information among everyone in the private sector, businesses and executives and NGO's, etc. The panelists have all highlighted the fact that we need better intelligence, more accurate intelligence, better exchange. Tell me what OSAC does to improve that intelligence dissemination.

Mr. MCCARTHY. OSAC is a—they have a council of approximately 30 security professionals which actually operate the OSAC facility—the OSAC organization. One of the major things that OSAC has done is put together the electronic bulletin board, the electronic data base; and this data base contains not only anecdotal information but professional analyst information concerning political and criminal situations abroad.

Mr. GILMAN. And security threats as well?

Mr. MCCARTHY. Security threats abroad, and it's available on a Web site. A part of it is password protected because it's—some of it is very specific and would be considered proprietary, and a lot of it is only of interest to the security professionals, but the majority——

Mr. GILMAN. Let me interrupt a moment. How do you protect your password security for OSAC information?

Mr. MCCARTHY. When you're an American company and sign up for OSAC, you are given a password. The senior security officer is given a password which he can proliferate throughout the company at his discretion.

Mr. GILMAN. Can NGO's find that access?

Mr. MCCARTHY. There are some NGO's that are included in OSAC. The Church for Latter Day Saints, for instance, is a very, very active member of OSAC.

Mr. GILMAN. And tell me about your country councils. I understand OSAC has country councils.

Mr. MCCARTHY. They have about 30 councils that have been started around the world, and the purpose of these councils is to try and give to the nonprofessional security-type information that would help him fulfill his responsibilities. In many companies, maybe a person who's assigned to the human resources would also have a security responsibility and he is not very proficient in many

of the best practices of security, and through the country council these practices are passed down from the other companies to them.

Mr. GILMAN. And what's your relationship with the government agencies in providing the information you have available?

Mr. MCCARTHY. There are government agencies who are technical advisers as part of OSAC also, the FBI, for instance, and the Department of Commerce and several other agencies.

Mr. GILMAN. Diplomatic Security Agency?

Mr. MCCARTHY. Diplomatic security actually runs those, yes, sir.

Mr. GILMAN. Thank you very much.

Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you, Mr. Gilman.

The Chair recognizes Mr. Kucinich for 5 minutes.

Mr. KUCINICH. Thank you, sir.

To Mr. Bishop, continuing the discussion I started with Mr. McCarthy, what would be the value if major American corporations or American corporations doing business in the—you know, generally anywhere around the world would have in advance of their business activities fully enunciated human rights principles, including workers rights, environmental quality principles? And, of course, that would also mean, you know, if we are talking human rights we are talking about the rights of women, children. What if that was the motif that was put out there for everyone to understand this is what we stand for and it was backed up by business practices that were consistent with the enunciation of those principles? What would be the effect on improving America's image abroad and America's position?

Mr. BISHOP. The organization that I represent hasn't taken a position on that issue.

Mr. KUCINICH. I am asking you personally. What do you think?

Mr. BISHOP. I think that, speaking generally, that the adoption of such a practice would improve the image of international business, many of these have lost their American identity abroad, and be a calming influence.

Mr. KUCINICH. Mr. Cilluffo, what do you think about that?

Mr. CILLUFFO. I believe that it actually does make bottom-line sense. To win the hearts and the minds of any indigenous or local population has been crucial in time of war, in time of crisis. So I do think that it would be something valuable.

The devil's in the details, and I have no idea——

Mr. KUCINICH. What you just said, though, impressed me, because you talked about the bottom line. Because it would occur to me that business may actually lose money with practices that are adverse to human rights. I mean, is that——

Mr. CILLUFFO. Initially, but the long-term benefits could outweigh the short-term costs and just in terms of support of a local indigenous population. That is—it's been—I mean, militarily, even in traditional national security terms, I think that should be underscored, and it's very important.

Mr. KUCINICH. Yeah, I think—and, Dr. Hoffman, would you respond to that? Because then I just want to make a comment on this. Go ahead.

Mr. HOFFMAN. I think it would be extremely useful. It would certainly, at minimum, deprive the terrorists of the propaganda that

they generate and market against the United States to drill up hostility to our country and also to increase their own recruits.

Mr. KUCINICH. It seems to me that human rights should be consistent with people making money. I mean, why not? Just as environmental quality principles—you know, we are in a new millennium where there's new ways of dealing with environmental challenges that can also save money. Sometimes that smoke going up the stack is profits lost, for example.

It seems to me that when we're looking at the possibility of a new millennium we could go one or two ways. We could end up with more violence, which requires a greater presence and security networks, etc., or we could take the world in a different direction. And I think that our corporations are in the position where they can help make it happen, even—may have even more influence than U.S. Government itself when we're talking about activities abroad, which is why I raised this. Because, look, we're all heirs of traditions that we may not always agree with and sometimes question, which is why I am a little bit uneasy about asking any individual to be singularly accountable for what his organization or corporation does, but we all have a role in where we go from here.

So, as you said, Mr. Cilluffo, you know, the devil is in the detail. I think it would be useful to convene U.S. corporate leaders on this issue and gather observations about what might be a common set of human rights principles covering workers and environment. And, you know, if you do that we might make some progress on some of our trade issues because, as you know, one of the major sticking points in a number of our trade agreements is the sense that corporations will not support human rights, workers rights, environment. If we can get corporations to do that voluntarily, then perhaps we can start a new era of human progress. That's where I am coming from.

So I thank the witnesses and look forward to further exchange on these matters. Thank you.

Mr. PUTNAM. Thank you, Mr. Kucinich.

The Chair and the subcommittee thanks the panel for their testimony and their thoughts on these issues.

At this time we will excuse the first panel, take about a 2-minute recess and bring up the second panel. Thank you.

[Recess.]

Mr. PUTNAM. The hearing will return to order.

Are all witnesses present?

The Committee on National Security, Veterans Affairs and International Relations is pleased to welcome our second panel of witnesses for the hearing on Protecting American Interests Abroad: U.S. Citizens, Businesses, and Nongovernmental Organizations.

As you are aware, you will be giving sworn testimony. At this time, please stand and raise your right hands.

[Witnesses sworn.]

Mr. PUTNAM. Note for record that the witnesses responded in the affirmative.

At this time, we will take the witnesses' opening statements. I ask that you please adhere to our 5-minute rule.

We will begin with Mr. Peter Bergin, Director of Diplomatic Security Service and Co-Chairman of Overseas Security Advisory Council, U.S. Department of State. Welcome.

STATEMENT OF PETER BERGIN, DIRECTOR, DIPLOMATIC SECURITY SERVICE, CO-CHAIRMAN, OVERSEAS SECURITY ADVISORY COUNCIL, U.S. DEPARTMENT OF STATE; MICHAEL WAGUESPACK, DEPUTY ASSISTANT DIRECTOR, COUNTERINTELLIGENCE OPERATION SUPPORT, FEDERAL BUREAU OF INVESTIGATIONS; DIANNE ANDRUCH, MANAGING DIRECTOR, OVERSEAS CITIZENS SERVICES, BUREAU OF CONSULAR AFFAIRS, U.S. DEPARTMENT OF STATE; AND LEONARD ROGERS, ACTING ASSISTANT ADMINISTRATOR, HUMANITARIAN RESPONSE, U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT

Mr. BERGIN. Thank you very much, Mr. Chairman. I am pleased to be with you today to address this important matter with you.

OSAC, which was created by Secretary of State George Shultz in 1985, is a partnership, a one-of-a-kind partnership between the private sector and the government to address the security concerns of the U.S. private sector around the world. The Bureau of Diplomatic Security is entrusted to carry out the U.S. Government responsibilities in this partnership.

This afternoon I will explain how the Bureau of Diplomatic Security, through OSAC, exchanges security information with U.S. companies, nongovernmental organizations, educational institutions and private entities so they can make informed decisions about how best to protect their people, their facilities and their investments overseas.

What makes the Council most effective is the breadth of its membership. The Council is comprised of 30 representatives from all sectors of business—financial, airlines, pharmaceuticals, consumables and high-tech, among others—as well as government representatives from the Departments of State, Commerce and Treasury and the Agency for International Development. In addition, there are seven government technical advisers from the Federal Bureau of Investigation, the National Security Agency, the National Counterintelligence Center, the U.S. Secret Service, the Federal Aviation Administration, the Financial Crimes Enforcement Network and U.S. Customs.

The Maritime Security Council, an organization of ocean carriers, cruise lines, and related industries, also serves the Council as a technical adviser.

Four committees serve as the engine for OSAC.

The Transnational Crime Committee provides information and case studies on transnational criminals and organizations. The Transnational Crime Committee is currently chaired by Motorola.

The Protection of Information and Technology Committee deals with intellectual property issues. It is currently chaired by American International Group Inc.

The Security awareness and Education Committee reviews and updates the OSAC Web site and publications. It is currently chaired by Cargill.

Our fourth committee is Country Council Support. This committee, which is chaired by Kellogg, promotes communications between OSAC and Washington and the field.

Overseas, OSAC is represented by its country councils. They serve in the front lines where private sector problems are addressed in cities around the globe. An American private sector representative and the Embassy regional security officer [RSO], chair these councils. Currently, there are OSAC country councils in 35 cities around the world.

The exchange of information is the reason OSAC exists. OSAC has an interactive Internet site of security information. This Web site contains press reporting from around the world, unclassified Embassy reporting, information on overseas contacts, groups prone to violence, upcoming global events, cybercrimes and other special topics. This user-friendly site, which is managed by Diplomatic Security, receives over 50,000 hits per week.

The operational element of OSAC is Diplomatic Security's Research and Information Support Center [RISC]. RISC is staffed by six analysts who are regional security experts. The RISC staff is dedicated exclusively to the U.S. private sector with interests overseas. This staff is the person-to-person focal point for the exchange of overseas security information with the private sector. RISC analysts do over 150 consultations per month. RISC has also supported the U.S. private sector overseas at major events such as the Sydney Olympics, the World Bank/IMF meetings in Prague and the World Economic Forum in Davos.

Every November OSAC holds its annual briefing. This event regularly attracts over 700 private sector executives to the State Department. At this session, OSAC presents a worldwide threat overview specifically tailored to the private sector.

OSAC publishes material on topics such as emergency planning for American families and businesses abroad, protecting U.S. business information overseas and responding to a biological or chemical threat. These publications are all available on the OSAC Web site or on hard copy.

All of our information services—the Web site, the consultation with the RISC analyst, the annual briefing and the security publications—are free.

We have a number of initiatives designed to keep OSAC relevant in today's ever-changing security environment. OSAC, joined by the State Department's Bureau of Consular Affairs, has formed the University Working Group. This working group is developing safety programs and establishing best practice guidelines to increase security awareness for students and faculties traveling and studying abroad. The schools now represented on the University Working Group are Pepperdine, Louisville, Ohio State, Arcadia, University of Southern California and Michigan State.

Another initiative involves training. The State Department now makes available to the private sector a 2-day personal security program to prepare their employees to live and work overseas. This program offers much the same training that State Department and other U.S. Government employees receive before they are assigned abroad.

In the last year we've done four sessions for over 100 private sector participants. The feedback has been positive. The Congress has had a lot to do in legislating our authority to train the private sector, and we thank you.

The future holds many challenges for OSAC. As more American companies travel and conduct business abroad, we are expanding—we are working to expand our constituent base. We also have an effort under way to increase the number of country councils.

Just as U.S. Government officials represent American values and interests around the world, every American abroad is a partner in our diplomacy. Any threat to their security is a threat to U.S. national interests. OSAC is U.S. foreign policy at its best. OSAC provides security information to the U.S. private sector so that it can travel, operate and invest safely in a world that is constantly changing. OSAC is government that works.

Mr. Chairman, thank you.

Mr. PUTNAM. Thank you very much. We appreciate your testimony.

[The prepared statement of Mr. Bergin follows:]

TESTIMONY OF PETER E. BERGIN
PRINCIPAL DEPUTY ASSISTANT SECRETARY
FOR DIPLOMATIC SECURITY AND
DIRECTOR OF THE DIPLOMATIC SECURITY SERVICE

BEFORE THE HOUSE COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS AND INTERNATIONAL RELATIONS

APRIL 3, 2001

I am pleased to participate in this hearing on the important subject of protecting American private sector interests abroad.

As Director of the Diplomatic Security Service, I am Co-Chairman of the Overseas Security Advisory Council (OSAC), with Jack McCarthy who was before you earlier this morning. OSAC is truly an example of a mutually supportive private sector/government partnership, established to address the global security concerns of the U.S. private sector. I want to explain the efforts of the Bureau of Diplomatic Security, through OSAC, to provide security information to U.S. companies, non-governmental organizations, educational institutions and other private entities, so they can make

informed decisions about how to best protect their people, facilities, investments and intellectual property overseas.

DIPLOMATIC SECURITY

The Bureau of Diplomatic Security (DS) has a broad mission but its primary function is to provide a secure environment for the safe conduct of foreign affairs. In addition, we provide protection for the Secretary of State and other senior government officials, for resident and visiting foreign dignitaries, and for foreign missions in the United States.

We have statutory authority to investigate passport and visa fraud, crimes that can facilitate terrorist and other criminal attacks against our national interests. Our Protective Intelligence Investigations Division (PII) is responsible for investigations involving terrorist threats and activities directed at personnel and facilities that we are responsible for protecting.

In close cooperation with the FBI and other agencies, our counterintelligence program is designed to deter foreign

intelligence efforts directed against our personnel and facilities worldwide.

Working with other Department bureaus and federal agencies, DS is the operational component for the Counterterrorism Rewards Program, the Antiterrorism Assistance (ATA) Program, and the program for the Protection of Foreign Missions and Officials (PFMO) here in the United States - the latter two are vital to securing effective security assistance from host governments abroad for our operations in their countries.

Finally, DS administers and co-chairs the Overseas Security Advisory Council (OSAC). We believe OSAC is the preeminent private sector/U.S. government partnership for global security concerns of U.S. private sector interests.

OSAC

Around the world today, there is much violence and disruption which has the potential to cause loss to U.S. companies, or to threaten the safety of Americans abroad.

We have seen attempted extortion and violent attacks against facilities, vehicles and personnel, cause a major U.S. oil company to suspend operations in a country in the Far East; U.S. pharmaceutical companies and their employees targeted by extreme animal activists in a European country and an explosion at a U.S business in Latin America. All U.S. citizens and interests are currently the subject of a worldwide security caution.

With the increasingly global competitive economy, the protection of intellectual property and preventing cybercrime/cyber terrorism are issues of paramount concern to corporate America. According to a survey conducted by the American Society for Industrial Security and PriceWaterhouseCoopers, "....in 1999, Fortune 1000 companies sustained losses of more than $45 billion from thefts of their proprietary information." Results of the sixth annual survey by the Computer Security Institute (CSI) released three weeks ago showed that 85% of 538 respondents (primarily large corporations and government agencies) "....detected computer security breaches within the last twelve months." One hundred and eighty six of those respondents were willing and/or able to quantify their financial losses at over $377 million.

Threats and incidents of all types are increasing and they are not going away.

The Overseas Security Advisory Council exists to foster U.S. investment abroad--not discourage it. We help U.S. companies doing business abroad to safely conduct business and remain competitive in the global economy despite everything going on around the world.

It would be worthwhile to spend a moment telling you how OSAC came to be.

In the early 80's, global terrorism and international violent crime were increasing. Special Agents of the Diplomatic Security Service serving as Regional Security Officers (RSO) at our Embassies around the world and responsible for the security of all official Americans and U.S. facilities overseas, were increasingly being approached by the U.S. private sector with concerns about their personnel and facilities.

Secretary of State George Shultz instructed DS to formalize this ad hoc exchange of information. The result was the

establishment of the Overseas Security Advisory Council under the Federal Advisory Committee Act (5 U.S.C.A. App. 2, ss1-14 et seq., and 22 U.S.C.A. s2656, Management of Foreign Affairs). The Omnibus Diplomatic Security and Antiterrorism Act of 1986 (P.L. 99-399) provides that the Assistant Secretary for Diplomatic Security be responsible for "liaison with American overseas private sector security interests." Sixteen years later, OSAC is comprised of over 1,800 private sector constituents.

OSAC's goals are to: maintain close liaison between the USG (State Department and other agencies) and the private sector; to exchange security information; provide guidance to U.S. businesses for security programs and plans; and protect the global competitiveness of American business.

I want to emphasize the exchange component, as this is a true partnership. This is a program that provides information from the U.S. Government, and access to the knowledge and experiences of private security professionals in the U.S. and around the world.

The thousands of employees or representatives of U.S. international businesses or organizations abroad, U.S.

citizens, host or third country nationals, represent a vast pool of information which may be pertinent to the security of the personnel and facilities of other U.S. organizations. OSAC acts as a clearing house for the exchange of information among the private sector.

Information is the perfect tool to fight the threat of terrorism and all forms of criminal activity. Issues that are of concern to the Council and our constituents include but are not limited to: transnational, organized, and cyber crime; terrorism; corruption; product tampering and counterfeiting; crisis management; disaster preparation and evacuation planning; protection of intellectual property and cargo hijacking.

The Council is comprised of 30 private sector representatives from all sectors of business -- financial, airlines, pharmaceuticals, consumables, high tech etc. -- as well as government representatives from the Departments of State, Commerce and Treasury and the Agency for International Development. In addition, there are seven government Technical Advisors from: the Federal Bureau of Investigation, the National Security Agency, the National Counterintelligence Center, the U.S. Secret Service, the

Federal Aviation Administration, the Financial Crimes Enforcement Network and U.S. Customs. The Maritime Security Council, an organization of ocean carriers, cruise lines and related industries, is also a Technical Advisor in an effort to address maritime security issues including the protection of cargo and the thousands of U.S. citizens who travel on cruise ships. In this remarkable coalition, with broad representation across the government and the private sector, security transcends competition.

Council members normally serve for two to four years and in the last decade, over 60 firms have served on the Council at the invitation of the Secretary of State.

An Executive Group provides leadership and strategic direction for the Council and the Committees. The Council formally meets three times a year to identify priorities and benchmark progress on programs and issues, with committees meeting more often as necessary.

The four committees are: Transnational Crime, which provides information and case studies on transnational criminals and organizations, currently chaired by Motorola; Protection of Information & Technology, which deals with

intellectual property issues, currently chaired by American International Group, Inc.; Security Awareness and Education, which reviews and updates the OSAC web site and publications, currently chaired by Cargill; and Country Councils Support, which promotes communication between OSAC and the field, currently chaired by Kellogg.

COUNTRY COUNCILS

In its early days, OSAC saw a need to create a forum in which problems of concern to the private sector could be addressed in the region affected. Country Councils began in 1988 to replicate the OSAC organization on a local level. Currently there are OSAC Country Councils in 35 cities around the world.

Country Councils are composed of host country, third country or U.S. executives with security responsibilities for U.S. firms. The Embassy Regional Security Officer (RSO) co-chairs the group with a private sector representative. Embassy support from the Ambassador, the Foreign Commercial Service, Consular American Citizen Services, and the economic or political sections as

appropriate, greatly enhances a Country Council's effectiveness.

A Country Council routinely provides an organized conduit for the exchange of information between the U.S. Embassy and the private sector representatives in country. In an emergency, information is exchanged quickly and efficiently among colleagues accustomed to working together.

A Country Council is also a forum for American private sector and Embassy representatives to focus on security issues of mutual concern. If necessary, an approach can be made to the host government in a cohesive manner as opposed to an individual basis which may yield only one time or short term solutions. This sort of approach was effective when a government representative in a South American country issued arrest warrants for managers of U.S. companies that did not discount their prices when the country dollarized.

Councils organize themselves to allow for differences in the security and cultural environment. They meet regularly - some quarterly, some annually, some once a month. Often, they have outside speakers on security topics of interest,

such as aviation security, environmental/animal rights activism, cargo hijacking and kidnapping.

In some cases, the Country Council falls under the umbrella of, or is the security committee of, the American Chamber of Commerce. In other cases, the OSAC Country Council chooses to operate separately from the Chamber. The important thing is that they do what works in a given environment.

OSAC's Country Councils Support Committee acts as a conduit between Country Councils in the field and OSAC in Washington, D.C. Members of the committee contact Country Councils regularly to exchange information, offer assistance and promote communication among Country Councils around the world.

OSAC Services To Constituents

OSAC Web Site

The OSAC INTERNET site (http://www.ds-osac.org) of security information contains press reporting from around the world, unclassified embassy reporting, information on overseas

contacts, groups prone to violence, upcoming global events (anniversaries) and other special topics.

There is information from our constituents to assist their colleagues such as a sample crisis plan that could be used as a model. There is a new section on cyber crime and cyber terrorism which has news stories and articles, a dictionary of jargon and links to other sites. An average of 80 to 100 new entries are made each day. This Diplomatic Security - managed site is user friendly, has a high speed search engine, an interactive component and receives over 50,000 hits per week.

RESEARCH AND INFORMATION SUPPORT CENTER

The operational element of OSAC is Diplomatic Security's Research and Information Support Center or RISC. RISC is staffed by six Security Specialists who are experts in their respective regions and dedicated exclusively to the U.S. private sector with interests overseas. This staff of analysts is the focal point for the exchange of information on security related incidents overseas between the Department of State and the private sector in the United States. The RISC is able to provide "any enterprise

incorporated in the United States doing business abroad" with timely security-related information of an unclassified nature.

Analysts search the world media every day and post relevant information on the OSAC web site of security or business interest to our constituency, including material they translate from foreign language dailies. They also review unclassified State Department cables from embassies around the world and abstract and post items of interest. They are looking not just at events but at the political, economic and social atmospherics which may impact U.S. business decisions. They take the next step with the information and distill the implications for U.S. companies and their assets abroad.

The analysts do over 150 consultations per month, mostly by telephone; some by e-mail. Examples of the kinds of inquiries they field are on civil unrest such as strikes or demonstrations, crime/safety issues, foreign election results and their implications or expansion into a new country or region.

In late February, while on official travel in South Africa, RISC's Africa specialist received word of demonstrations planned against certain American pharmaceutical companies in New York, Cape Town and Pretoria. OSAC promptly notified security executives at the targeted companies. This is but one instance of many where RISC provided the private sector timely, relevant information concerning threats to disrupt their operations.

RISC has also supported the U.S. private sector overseas at major events such as the Sydney Olympics, the World Bank/IMF meetings in Prague and the World Economic Forum in Davos. After the conference in Prague which brought out protesters from anti-globalization and anarchist groups similar to those experienced in Seattle and Washington, D.C., one of our constituents from a Fortune 100 financial institution wrote to us: "We had real concerns for the safety of our personnel while attending the Prague IMF meetings. Due in part to this excellent sharing of safety related information, no injuries were suffered by any of our visiting personnel. There was a real need for this [safety] information and OSAC filled this need and provided a service of tremendous benefit to the personnel from the

American financial institutions who attended the Prague conference."

ANNUAL BRIEFING

Every November, OSAC holds its Annual Briefing which brings over 700 private sector security executives to the State Department. OSAC presents a world threat overview, specifically tailored to the private sector, as well as speakers from government and the private sector. The Secretary of State is routinely the keynote speaker. Country Councils from around the world are also represented.

SPECIAL BRIEFINGS

OSAC makes presentations to business audiences (professional associations, Country Councils) both domestically and abroad on various aspects of the global security environment.

PUBLICATIONS

OSAC publishes and distributes material prepared by security practitioners in business and government to the private sector. Publications such as: Emergency Planning Guidelines for American Businesses Abroad, Security Guidelines for Families and Children, Protecting U.S. Business Information Overseas and A Practical Guide to Responding to a Biological or Chemical Threat are all available on the web site or in hard copy.

All of the services -- the web site, consultations with RISC analysts, the Annual Briefing and publications -- are free. We often tell our constituents that the OSAC program represents their "tax dollars at work."

CURRENT INITIATIVES

OSAC is continually working, not just to maintain a hallmark program, but to move forward with responsive and innovative initiatives to assist the private sector in confronting new security concerns as they arise.

University Working Group

One current initiative is directed toward educational institutions. OSAC, joined by the Bureau of Consular Affairs, has formed the University Working Group to coordinate to develop safety programs and establish "best practices" guidelines to increase security awareness for students and faculty traveling and studying abroad. The University Working Group will share their results with colleges and universities throughout the country.

The schools represented on the University Working Group are: Pepperdine University, University of Louisville, Ohio State University, Arcadia University, University of Southern California and Michigan State University.

Security Overseas Seminar

Another current initiative involves training. OSAC has worked with the Department of State's Overseas Briefing Center to make available to the private sector a two-day program to prepare employees from the private sector to live and work overseas.

It is much the same training that State Department and other USG employees receive, although it was customized for a private sector audience. The Overseas Briefing Center nominally charges companies $250 per private sector participant - which is the same amount the USG pays for employees who are not from the State Department.

The course covers topics such as personal security, cross cultural issues and security, specific tactics and trends and what the U.S. Embassy can - and can not - do for members of the private sector.

It is beneficial for the employee and their family members and good for their organization. We have done four sessions for over 100 private sector participants to date and the feedback has been overwhelmingly positive. We would like to thank the Congress for passing the legislation allowing the Foreign Service Institute to train the private sector. (In October 1998, the Foreign Service Act of 1980 was amended to provide the Foreign Service Institute the authority to train the private sector on a reimbursable basis.)

THE FUTURE

As more American companies and their employees travel and conduct business abroad, we are working to significantly expand our constituent base, particularly targeting small and mid size companies. Additionally, we have a focused effort underway to increase the number of country councils. OSAC will only remain relevant if the private sector is committed and the government remains sensitive to the private sector's growing requirements.

CONCLUSION

I have explained what OSAC is, what its goals are, how it is set up to serve our private sector constituency and the specific services we provide. Just as U.S. Government officials represent American values and interests around the world, every American abroad is a partner in our diplomacy; any threat to their security is a threat to U.S. national interests.

OSAC is U.S. foreign policy at its best. It provides a forward-leaning opportunity to address security issues which impact our country's role and citizens working

abroad. It provides security information to the U.S. private sector so that it can travel and invest safely in a world that is constantly changing. OSAC is government that works!

Mr. Chairman, thank you for the opportunity to speak to the Subcommittee today. I would be happy to answer any questions you or other Members may have.

Mr. PUTNAM. The Chair now recognizes Mr. Michael Waguespack, Deputy Assistant Director of Counterterrorist Operation Support Section, Federal Bureau of Investigations. Did I pronounce your name correctly?

Mr. WAGUESPACK. You pronounced it correctly, Waguespack. Just for the record, I am the Deputy Assistant Director for Counterintelligence Operation Support.

Mr. PUTNAM. The record will note the change. You're recognized.

Mr. WAGUESPACK. Thank you, Mr. Chairman. I also thank members of the committee for inviting the FBI to testify about the ANSIR program as the committee examines the topic of "Protecting American Interests Abroad."

While other agencies in the government have primary responsibility for protecting U.S. interests overseas, the FBI participates with them as appropriate and contributes to the overall government effort.

The acronym ANSIR stands for "Awareness of National Security Issues and Response." As part of its national security mission, the FBI has been providing awareness information in order to reduce the vulnerabilities of U.S. citizens, corporations, and institutions to intelligence and terrorist activities since the early 1970's. By knowing what intelligence services and terrorists do and how to frustrate their plans, American interests are better protected.

The initial focus of this program in the 1970's was the protection of classified government information, property and personnel. At that time, the program was known as DECA, Developing Espionage and Counterintelligence Awareness.

In the 1990's, several challenges occurred which led the FBI to decide that a larger audience should be receiving its national security message. First, foreign intelligence services expanded their targeting to include unclassified private sector proprietary economic information.

Second, the threat of terrorist attack on American interests here in the United States and abroad escalated. Additionally, the serious problem of computer intrusion and the costly menace of the computer virus dictated the FBI awareness message should reach a broader audience in a timely fashion to protect harm.

The FBI's ANSIR program's message is principally aimed at U.S. corporations, although other government agencies and law enforcement also benefit from it. The principal method of disseminating FBI information is through ANSIR e-mail which I will describe later. The ease of replicating e-mail communication accounts for the global nature of its dissemination.

American interests abroad receive ANSIR communications primarily from their headquarters in the United States, which relay ANSIR e-mail to them, though on occasion the awareness message is delivered directly to those overseas.

In addition to making potential targets of intelligence and terrorist activities less vulnerable through awareness, the FBI also has a unique capability to respond when these activities are identified in the United States. This response capability is a key part of the awareness message. The FBI does more than simply identify problems, it does something about them.

Let me just talk briefly to the organizational structure of ANSIR. The ANSIR program is by any measurement of government programs a very small one. Currently, there is one supervisory special agent assigned as the national ANSIR program manager in the National Security Division at FBI headquarters.

The ANSIR program also has at least one special agent in each of its 56 field offices assigned as the ANSIR program coordinator. This is actually a collateral duty assigned to take no more than 10 percent of the coordinator's time. The coordinator acts as the point of contact for request of assistance and inquiries generated by ANSIR.

A special agent is assigned this duty because decades of experience with the ANSIR program has shown that the private sector prefers discussing national security issues with an individual who has operational experience.

The ANSIR program has no membership. Rather, individuals, corporations, government agencies and organizations which request FBI national security awareness information may receive unclassified awareness information via ANSIR e-mail or through presentations conducted by ANSIR coordinators and other knowledgeable individuals that are arranged through the program. Presentations are given both at the classified and unclassified level.

What is today the ANSIR e-mail program began as the ANSIR fax program in 1995. After the private sector shifted its principal means of communication to the Internet in 1996, ANSIR fax became ANSIR e-mail. The program uses the FBI's Law Enforcement On-Line [LEO], as its Internet service provider to ensure the security and integrity of ANSIR e-mail. This program was initiated to greatly improve the efficiency of disseminating the FBI's awareness message.

While personal presentations, videotapes and mail all have their value, nothing is as efficient as Internet e-mail for quickly distributing an advisory whose value diminishes with every passing hour.

Recently, the number of ANSIR e-mail subscribers was reported to be over 30,000. Each ANSIR e-mail advisory eventually reaches substantially well over this number depending on the content of its message. Key messages which members of Fortune 500 and large government agencies wish to pass on to their personnel have the largest international dissemination.

The number of ANSIR e-mails disseminated annually vary depending upon the threat environment. In the calendar year 2000, a total of 63 advisories were disseminated. Because the ANSIR e-mail has asked its subscribers which advisories within 17 infrastructures they desire to receive, not all advisories are received by every subscriber. However, the majority of subscribers ask to receive advisories from all 17 infrastructures.

Let me talk briefly about the ANSIR program with regard to the counterterrorism effort. The role of the FBI's ANSIR program in the U.S. counterterrorism effort overseas is within the FBI's primary mission of preventing, deterring, and defeating terrorism activities in the United States. To this end, the ANSIR program provides terrorism awareness information valuable to public and private sector organizations.

ANSIR e-mail is a component of the government's National Threat Warning System. The National Threat Warning System has established a protocol for the rapid dissemination of terrorism threat and warning information throughout the Federal Government, law enforcement, and the private sector. The protocols established by the NTWS provide uniformity in defining what constitutes a threat advisory which should be disseminated and the language used to describe it.

Mr. PUTNAM. Sir, if you could conclude your remarks.

Mr. WAGUESPACK. Yes, sir.

Mr. PUTNAM. We have a copy of your written testimony. We'll be able to derive our questions from that.

Mr. WAGUESPACK. In conclusion, then, I would just like to say that you can talk about the cooperation that exists between government programs concerning the protection of American interests abroad. The FBI's ANSIR program coordinates all overseas activity in which it is requested to engage with the Department of State. In fact, the FBI Deputy Director Thomas Pickard is a member of the Overseas Security Advisory Council Executive Board. As noted—would be noted in the written testimony, we have also been sponsored to present various programs through the Defense Security Service and other government agencies internationally.

We think that the ANSIR program is a "good news" program, and I hope that this information is helpful. I look forward to answering any questions.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Mr. Waguespack follows:]

Statement for the Record of
Michael J. Waguespack,
Deputy Assistant Director, National Security Division
Federal Bureau of Investigation

on the
FBI's ANSIR Program

before the
House Committee on Government Reform
Subcommittee on National Security, Veterans Affairs,
and International Relations

April 3, 2001

Mr. Chairman, I would like to thank the members of the committee for inviting the FBI to testify about the ANSIR Program as the committee examines the topic of *"Protecting American Interests Abroad: U.S. Citizens, Businesses, and Non-governmental Organizations."* While other agencies in the government have primary responsibility for protecting United States interests overseas, the FBI participates with them as appropriate and contributes to the overall government effort.

The acronym ANSIR stands for "Awareness of National Security Issues and Response." As part of its national security mission, the FBI has been providing awareness information in order to reduce the vulnerabilities of U.S. citizens, corporations and institutions to intelligence and terrorist activities since the early 1970's. By knowing what intelligence services and terrorist do and how to frustrate their plans, American interests are better protected. The initial focus of this program in the 1970's was the protection of classified government information, property and personnel. At that time, the program was known as "DECA" (Developing Espionage and Counterintelligence Awareness). In

the 1990's, several changes occurred which led the FBI to decide a larger audience should be receiving its national security message. First, foreign intelligence services expanded their targeting to include unclassified private sector proprietary economic information. Second, the threat of terrorist attack on American interests here in the United States and abroad escalated. Additionally, the serious problem of computer intrusion and the costly menace of the computer virus dictated the FBI awareness message should reach a broader audience in a timely fashion to prevent harm.

The FBI's ANSIR Program's awareness message is principally aimed at U.S. corporations, although other government agencies and law enforcement also benefit from it. The principal method of disseminating FBI awareness information is through ANSIR Email described in the following section. The ease of replicating email communication accounts for the global nature of the dissemination. American interests abroad receive ANSIR awareness communications primarily from their headquarters in the United States which relays ANSIR Email to them, though on occasion the awareness message is delivered directly to those overseas. In addition to making potential targets of intelligence and terrorist activities less vulnerable through awareness, the FBI also has a unique capability to respond when these activities are identified in the United States. This response capability is a key part of the awareness message. The FBI does more than simply identify problems; it does something about them.

ANSIR Organizational Structure, Membership and Programs

The ANSIR Program is by any measurement of government programs a very small one. Currently, there is one Supervisory Special Agent (SSA) assigned as the National ANSIR Program Manager in the National Security Division at FBIHQ. The ANSIR Program also has at least one Special Agent in each of the 56 FBI Field Offices assigned as the ANSIR Program Coordinator. This is a collateral duty designed to take no more than 10% of the Coordinator's time. The Coordinator acts as the point of contact for requests for assistance and inquiries generated by ANSIR. A Special Agent is assigned this duty because decades of experience with the ANSIR audience has shown that the private sector prefers discussing national security issues with an individual who has operational experience.

The ANSIR Program has no membership; rather, individuals, corporations, government agencies and organizations which request FBI national security awareness information may receive unclassified awareness information via ANSIR Email or through presentations conducted by ANSIR Coordinators and other knowledgeable individuals arranged through the program. Presentations are given to both classified and unclassified audiences.

What is today the ANSIR Email Program began as the ANSIR Fax Program in 1995. After the private sector shifted its principal means of communication to Internet email in 1996, ANSIR Fax became ANSIR Email. The program uses the FBI's Law Enforcement On-Line (LEO) as its Internet

Service Provider (ISP) to ensure the security and integrity of ANSIR Email. This program was initiated to greatly improve the efficiency of disseminating the FBI's awareness message. While personal presentations, video tapes and mail all have their value, nothing is as efficient as Internet email for quickly distributing an advisory whose value diminishes with every passing hour. Recently, the number of ANSIR Email subscribers was reported to be over 30,000. Each ANSIR Email advisory eventually reaches substantially well over this number depending upon the content of the message. Key messages which members of the Fortune 500 and large government agencies wish to pass to all their personnel have the largest international dissemination.

The number of ANSIR Emails disseminated annually vary depending upon the threat environment. In calendar year 2000, a total of 63 advisories were disseminated. Because ANSIR Email has asked its subscribers what advisories within 17 infrastructures they desire to receive, not all advisories are received by every subscriber; however, the majority of subscribers ask to receive advisories from all 17 infrastructure categories. All ANSIR Email communications are unclassified.

The Role of ANSIR in USG Counterterrorism Efforts Overseas

The role of the FBI's ANSIR Program in USG Counterterrorism efforts overseas is within the FBI's primary mission of preventing, deterring and defeating terrorism activities in the United States. To this end, the ANSIR Program provides terrorism awareness information valuable to public and

private sector organizations, many which have overseas facilities and/or personnel who travel overseas.

ANSIR Email is a component of the government's National Threat Warning System (NTWS). The NTWS has established a protocol for the rapid dissemination of terrorist threat and warning information throughout the federal government, law enforcement, and the private sector. The protocols established by the NTWS provide uniformity in defining what constitutes a threat advisory which should be disseminated and the language used to describe it.

As the committee is aware, U.S. Government agencies with facilities and personnel overseas have been hardening those facilities and routinely provide their personnel with awareness information to make them safer. After government targets, well known U.S. Businesses and non-government organizations are likely terrorist targets due to their close association with American culture and values. Upon request, headquarters elements of these private sector organizations receive threat and warning information via ANSIR Email which they email in turn to their overseas operations.

Occasionally, ANSIR Program personnel travel overseas to give presentations at the invitation of other U.S. Government agencies or private sector organizations. In the last several years, ANSIR presentations have been given to U.S. Corporations and/or U.S. Government agencies in the following overseas locations:

United Kingdom

Republic of Ireland

Czech Republic

Austria

Hungry

Slovakia

Australia

Japan

Republic of Korea

Argentina

Republic of Panama

These overseas ANSIR presentations were sponsored in part by the U.S. Department of State (Bureau of Diplomatic Security/Overseas Security Advisory Council), Defense Security Service, American Society for Industrial Security, American Chamber of Commerce, as well as U.S. Corporations such as IBM and Coca-Cola.

Attending these overseas unclassified ANSIR presentations are both U.S. Citizens and host country citizens, as both are potential targets due to their association with their U.S. employer. It is also the practice to invite host country government officials from law enforcement agencies or ministries with which the FBI routinely deals to be present during unclassified briefings. Classified ANSIR presentations are provided in appropriately secure locations to U.S. Citizens with the necessary security

clearances.

The Role of ANSIR in Countering Economic Espionage Overseas

After the Cold War, the FBI determined that while espionage against U.S. defense contractors continued unabated by some traditional Cold War adversaries, there was a broader effort underway by a surprising number of Cold War allies to use their intelligence services to clandestinely collect unclassified proprietary information from U.S. corporations. These non-traditional adversaries understood that economic information was as much a vital part of their national security as political or military information. It also became evident that traditional Cold War adversaries had also expanded their collection targets to proprietary economic information to a degree greater than previously observed. These developments were recognized by the Congress, as evidenced by the passage of the Economic Espionage Act of 1996, which gave the FBI primary jurisdiction in such matters.

Anyone can be vulnerable to intelligence collection activities. The proprietary secrets of the American economy are attractive targets of foreign intelligence services because conducting economic espionage is cheaper than research and development. Intelligence services are extraordinarily sophisticated and have substantial resources to carry out their missions. They train their personnel to acquire information clandestinely so their targets do not know it has been compromised.

A key to reducing vulnerability to intelligence collection activity is knowing and countering

common techniques used by foreign intelligence services which can minimize or even eliminate their opportunity for success. If foreign intelligence services believe the effort is too great or the risk is too high, they will look for another target. The FBI's ANSIR Program attempts to reduce American vulnerability by providing awareness information on the techniques used by foreign intelligence services to collect proprietary economic information.

The threat to computer and telecommunication systems has also increased dramatically in recent years. This threat takes on a variety of forms and ranges from foreign intelligence services, to disgruntled employees, to teenage hackers. Timely notification of the latest intrusion techniques and the latest virus detected "in the wild" can provide an edge in protecting systems. In concert with the Department of Justice and FBI's National Infrastructure Protection Center (NIPC), ANSIR Email also provides advisories on the latest computer intrusion threats as well as timely notification on the latest virus. For private and public sector organizations which desire to share information about cyber intrusion incidents, computer system vulnerabilities and physical infrastructure threats, the NIPC's InfraGard initiative provides such a mechanism. There are currently 518 members in the 56 InfraGard Chapters nationwide.

Procedures for Providing Assistance to American Businesses with Security Concerns

Business security concerns can take a variety of forms. The FBI is not resourced to conduct physical, personnel or information evaluations for the private sector. There are ample sources within

the federal government which provide information and requirements for protecting classified facilities, personnel and information and there are reputable firms in the private sector which provide able counsel on how to protect unclassified facilities, personnel and information.

Notification that a business may be the target of foreign intelligence collection or terrorist activity allows the FBI to respond with appropriate investigative and operational activities to resolve the matter. The procedure is simply to notify any FBI office in the United States or the FBI Legal Attache or U.S. State Department Regional Security Officer in American Embassies overseas.

Conclusion

Mr. Chairman, I would like to conclude my opening statement by advising the committee of the cooperation that exists between government programs concerned with the issue of "Protecting American Interests Abroad" especially those in the awareness community. The FBI's ANSIR Program coordinates all overseas activity in which it is requested to engage with the U.S. Department of State. In fact, FBI Deputy Director Thomas Pickard is a member of the Overseas Security Advisory Council Executive Board. As noted above, ANSIR has been sponsored by the Defense Security Service and has conducted joint presentations both in the United States and overseas.

We think the ANSIR Program is a "good news" program. I hope this information has been helpful and I look forward to answering any questions you have.

Mr. PUTNAM. At this time, the Chair recognizes Ms. Diane Andruch, Managing Director, Overseas Citizens Services, Bureau of Consular Affairs, U.S. Department of State. Welcome.

Ms. ANDRUCH. Thank you, Mr. Chairman and members of the subcommittee. I have submitted my full statement for the record, which I will now summarize.

The Bureau of Consular Affairs [CA], is charged with exercising the Secretary of State's responsibility to provide consular protection and services to U.S. citizens abroad. The Department has no higher priority.

I will be speaking today about the work of my office, Overseas Citizens Services [OCS], to provide vital emergency and non-emergency assistance to U.S. citizens abroad on a daily basis. We help Americans in dire circumstances, including deaths, arrests, missing persons, medical evacuation and financial emergencies.

In times of crisis, such as natural disaster, civil unrest, political instability or transportation disasters, OCS coordinates the consular response in Washington and at our posts abroad, and provides a vital point of contact for Americans in the United States concerned about their relatives overseas.

We try to make it easy for Americans to reach us. Our phone number is in every U.S. passport. Machine readable photo digitized U.S. passports issued since November 16, 1998 also include our Web site for our home page. We are available 24 hours a day, 7 days a week, worldwide throughout our Embassy duty officer program.

One of our primary objectives is to alert citizens to situations that may adversely impact their safety and security. The cornerstone of this effort is our consular information program. OCS prepares a consular information sheet for every country in the world, which includes basic information about local conditions. When the Department determines that it is unsafe for Americans to travel to a particular country, we issue a travel warning. We issue also public announcements which will cover short-term events, such as the potential for violent demonstrations. In 2000, we prepared 40 travel warnings and 138 public announcements.

In addition, we issue worldwide caution public announcements on terrorism and threats against American interests abroad, such as the announcement issued on January 1st of this year which remains in effect.

American communities abroad are also alerted to threats through our Embassies' warning systems. These are through telephone, multi-fax and e-mail trees designed to share information quickly when there is imminent danger to Americans overseas.

We get the word out about our consular information sheets and that program by disseminating them to our missions abroad, the media, the travel industry and other U.S. Government agencies and to e-mail list subscribers. We also place them on our Consular Affairs home page at www.travel.state.gov. Our home page has seen as many as 600,000 hits a day or 13 million hits in a month. In the year 2000, our home page received 96 million hits. And we anticipate our first million hit day won't be too far in the future.

For those without computers, our materials are also readily available by telephone recording, fax on demand, and by mail. Our

home page also includes pamphlets and other detailed information on a wide variety of topics.

Now I would like to talk a minute about the information contained in these documents that we've been discussing, how we obtain it; in particular, crime, safety and security information. For the most part, the information is provided by our Embassies and consulates abroad. Information on local crime, areas of instability and the overall political climate are provided with the input of various offices within the Embassy. If a threat applies equally to private and official Americans alike, it must be shared with both. This we referred to as our "no double standard" policy.

Information about terrorist threats is obtained from a variety of sources: from the U.S. intelligence community, those of our allies, friendly sources, open threats and other sources. No matter what the source, though, all the information is taken seriously and put through a comprehensive evaluation process.

Threats are evaluated based on evidence—on threat evidence alone, not on political or policy issues. Before the information is shared with the public, however, it must be specific, credible and noncounterable. This threshold precludes us from publishing unsubstantiating information and suffering the consequences of "crying wolf."

The Department's Bureau of Diplomatic Security [DS], reviews this information pertaining to private Americans. Information obtained and analyzed by DS, in concert with another office of the Department, the Office of Counterterrorism, the Bureau of Intelligence and Research, and other sources in Washington is also shared and evaluated by our missions in the affected country or region.

In addition to daily interaction among OCS in these offices, OCS chairs a weekly meeting with representatives from DS, INR and S/CT to review all outstanding threatening information. Our posts abroad also evaluate the threat information through their emergency action committees. These are usually chaired by the Ambassador and made up of the deputy chief of mission, the security officer, consular and other representatives of U.S. agencies at the post as necessary.

If a threat is determined to be specific, credible and noncounterable, DS shares the information with our Bureau in Washington, and we evaluate whether it is adequately addressed in our consular information program or whether something else needs to be done.

When the political situation in a country begins to deteriorate or other threats to the security of American interests are evident, the Department convenes the Washington Liaison Group [WLG], to alert the interagency community to the situation and coordinate interagency planning. This WLG typically includes representatives of other agencies throughout Washington.

Mr. Chairman, the dangers that crime, security threats, kidnapping and terrorism pose for U.S. citizens abroad are of great concern to the Department of State. When an American citizen is taken hostage, for example, the Department and the Embassy in the host country work closely with the host government and with other U.S. Government agencies and family members of the victim

as well to develop a strategy for the expeditious resolution of the hostage situation. Consular officers abroad serve as the key point of contact for family members and remains in regular contact.

The State Department's Office of the Coordinator for Counterterrorism works closely with law enforcement agencies, including the FBI and military, to develop resolution strategies and may lead to an interagency foreign emergency support team known as FEST to support the chief of mission at that Embassy concerned.

The FBI may dispatch hostage negotiation experts at the request of the host country government, and the FBI has responsibility for post-incident investigation and prosecution of those who kidnap American citizens.

While the U.S. Government has a clear policy on the issue of hostage taking, we will make no concessions to terrorists holding American citizens hostages. We will use every and all opportunities and appropriate resources to gain the safe return of those American citizens being held hostage.

In June 2000——

Mr. PUTNAM. Ms. Andruch, I would also ask if you would summarize.

Ms. ANDRUCH. OK. If I may then just conclude by saying that I believe that we in the Department, and specifically the Bureau of Consular Affairs, are doing a good job in working with other agencies to recognize the needs—the needs of Americans traveling overseas. And I look forward to working with you and others to see if we can do an even better job. Thank you.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Ms. Andruch follows:]

STATEMENT OF

DIANNE M. ANDRUCH
MANAGING DIRECTOR, OVERSEAS CITIZENS SERVICES
BUREAU OF CONSULAR AFFAIRS

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS

COMMITTEE ON GOVERNMENT REFORM

UNITED STATES HOUSE OF REPRESENTATIVES

April 3, 2001

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to testify on behalf of the Bureau of Consular Affairs of the Department of State regarding "security threats, particularly terrorist threats, posed to private American interests abroad: U.S. citizens, businesses and non-governmental organizations, and what the U.S. Government is doing to address those threats."

The Bureau of Consular Affairs (CA) is charged with exercising the Secretary of State's responsibility to provide consular protection and services to United States

citizens abroad. There is no higher priority of the Department of State than the protection and welfare of Americans overseas.

The Bureau of Consular Affairs is comprised of three directorates. Our Visa Services Directorate facilitates the legitimate travel of foreigners to the United States for business and tourism. It is estimated this travel remitted 100 billion dollars of commerce for the United States last year. Our Passport Services Directorate, with 16 Passport Agencies and over 4000 acceptance facilities throughout the United States, issued over 7 million passports in FY-2000. The third directorate, which I will be speaking about today, is Overseas Citizens Services, commonly referred to as OCS.

Before I discuss the collection, evaluation and dissemination of threat information, I would like to give you a brief overview of the broader function of OCS.

OCS provides a full range of emergency and non-emergency consular services to Americans residing and traveling abroad. We exercise this responsibility through a staff in Washington and our consular colleagues in our Embassies and Consulates throughout the world. Consular

Duty Personnel are available 24 hours a day, 7 days a week in Washington and overseas.

We try to make it easy for Americans to reach us. Our phone number is in every U.S. passport. Machine-readable photo-digitized U.S. passports issued since November 16, 1998 also include the web site for our home page. Moreover, we are initiating a project to insert into every passport mailed to U.S. citizens in the United States a card that includes our telephone number, our internet address, and a short statement of our mission to facilitate the safe travel of Americans overseas and to assist them in their time of need. It also notes the importance of having adequate medical insurance when traveling abroad. In times of crisis, we publicize our emergency telephone numbers through the media.

OCS provides vital assistance to U.S. citizens abroad on a daily basis and during periods of crisis.

On the non-emergency side, our embassies and consulates provide notarial and judicial assistance services in connection with travelers' personal and business dealings, issue Consular Reports of Birth to document the birth and United States citizenship of children born abroad to United

States citizen parents, issue replacement passports to Americans who have had their documents lost or stolen, assist in Selective Service registration, provide guidance to Americans seeking to register and vote absentee, and assist in the distribution of Federal Benefits checks to beneficiaries overseas, among other services.

Under more dire circumstances, we help Americans who have become destitute obtain funds from family and friends or through our loan programs; provide Americans arrested or detained with information about local procedures and due process, protest any mistreatment, provide a list of attorneys and liaise with family and friends back home; help locate missing Americans; assist the victims of kidnappings and their families; notify next-of-kin when an American dies overseas, and serve as provisional conservator of the estate of a deceased American, as necessary.

A substantial and ever-increasing aspect of the Department's consular work involves the provision of services in connection with children. OCS provides advice and guidance to U.S. citizens, and leadership in the international community on parental child abduction, international adoption, child support enforcement and child

abuse and neglect. Our Office of Children's Issues in OCS serves as the U.S. Central Authority for the Hague Convention on the Civil Aspects of International Child Abduction, and will serve as U.S. Central Authority for the Hague Convention on Inter-Country Adoption.

In times of crisis, when Americans are affected by events such as natural disasters, civil unrest, political instability or transportation disasters, OCS coordinates the Consular response in Washington and at our posts abroad. We immediately alert Americans to the existing danger. We oversee the operations of our consular personnel in the affected country and establish and maintain the consular segment of the Washington-based task force. In addition, we provide a vital point of contact for Americans in the U.S. concerned about relatives overseas. We also serve as a focal point for our involved missions to seek guidance and instruction on consular assistance and we collect information on the status of Americans overseas and share it with concerned family members and friends.

Another important aspect of our consular crisis work is assuring that there is adequate consular staffing and resources to manage the problem. We supplement consular

staff overseas with temporary help from the U.S. or neighboring posts, maintain crisis teams ready to provide the first response to an emergency, and liaise with other offices in the Department and in the U.S. Government to bring all appropriate resources to bear and to ensure a concerted, coordinated response. Recent crises have included the earthquakes in Taiwan and Turkey, the Singapore Air disaster in Taiwan and the terrorist bombings of our embassies in Nairobi and Dar es Salaam. We have assisted in the evacuation of Americans from foreign countries on average 10 times a year over the past decade.

Of course, rather than react to problems, one of our primary objectives is to prepare Americans for their travel abroad by giving them some basic information alerting them to situations that may adversely impact their safety and security. The cornerstone of this effort is our Consular Information Program. The basic document in this Program is the Consular Information Sheet (CIS). OCS prepares and issues a Consular Information Sheet for each country in the world. The Consular Information Sheet provides basic information about conditions in the country. This includes the location and phone number for the U.S. embassy, entry/exit requirements, crime and security issues, road

safety, medical facilities and other information as appropriate.

In certain instances, when the Department determines that it is unsafe for Americans to travel to a particular country, we issue a Travel Warning. Generally, we have Travel Warnings in place for about 20-25 countries of the world at any given time. Most would be readily recognizable by the public -- Iraq, Libya, Somalia, etc. Unfortunately, others less recognizable fall into this category on occasion.

To supplement these documents, we issue Public Announcements, which generally cover short-term events, such as the potential for violent demonstrations during elections in a particular country. In the Year 2000, we issued 40 Travel Warnings and 138 Public Announcements. We currently have Public Announcements in place on Macedonia because of the conflict in the northern part of the country between ethnic Albanians and the government and on Peru in the lead up to elections.

Since the bombings of our Embassies in Nairobi and Dar es Salaam in 1998, we have found it useful to issue Worldwide Caution Public Announcements, to alert Americans

generally to the fact that terrorists have threatened action against Americans and American interests abroad. The latest such Announcement was issued on January 1, 2001, and remains in effect.

In addition to the Consular Information Program, the American communities abroad are alerted to threats through warden systems, which are designed and maintained by our Embassies and Consulates. This system provides a quick mechanism for sharing information when there is imminent danger to the American community. Because Embassies now communicate with hundreds or even thousands of citizens, the traditional warden system has evolved into a combination of telephone, multi-fax, e-mail, high frequency radio, media and home page mechanisms. The best method of communication is determined on a country-specific basis within the context of local circumstances. In addition to routine exercising of the warden systems by each of our individual posts for readiness, in the Year 2000, we expanded and conducted a global test of the consular warden systems we use to contact our citizens during a crisis.

In seeking broad distribution of our Consular Information Program documents, we disseminate them to our missions abroad, the media, the travel industry, other U.S.

Government agencies, and to e-mail list subscribers. We also place them on our Consular Affairs home page at www.travel.state.gov. Our home page has seen as many as 600,000 hits a day, or 13 million or more hits a month. We are currently averaging about 300,000 hits a day. In the Year 2000, our home page received 96 million hits, and we anticipate our first "million-hit day" will not be too far in the future. To put this growth into perspective, our home page received only 30,000 hits a year five years ago. Our materials are also available by telephone recording, fax-on-demand and by mail.

In addition to these key materials, our home page includes pamphlets and other detailed information on a wide variety of topics of interest and importance to the American traveler.

Now, I would like to talk about the information contained in these documents we have been discussing and how we obtain it.

For the most part, the information is provided by our Embassies and Consulates in the subject country. Information on local crime, areas of instability and the overall political climate are provided with the input of

various offices within the Embassy. Every effort is made to keep this information current as it applies equally to the American public and the official American community. We have an obligation to both groups and to share all information which may equally, adversely affect them. We call this our no double standard policy. If a threat applies equally to private and official Americans alike it must be shared with both.

Other information, particularly that which may pertain to terrorist threats, is obtained from a variety of sources -- from the U.S. intelligence community, those of our allies, friendly sources, open threats, etc. No matter what the source all information is taken seriously and put through a comprehensive evaluation process.

The Aviation Security Improvement Act of 1990 provided specific criteria to be used in evaluating aviation threats and the tenets for dissemination of threat information. The Department subsequently adopted this standard for assessment and dissemination of all threats to Americans abroad. Threats are evaluated based on threat evidence alone, not on political or policy factors.

Before the information is shared with the public, it must meet the three criteria I have just mentioned. It must be specific and credible and non-counterable. This threshold precludes us from publishing unsubstantiated information and suffering the consequences of "crying wolf."

Since the Department's Bureau of Diplomatic Security (DS) reviews threat information with regard to our official personnel and facilities abroad, it also performs this function for threats pertaining to private Americans. Information obtained and analyzed by DS, in concert with the Department's Office of Counter-Terrorism (S/CT), the Bureau of Intelligence and Research (INR), and other sources in Washington, is also shared and evaluated by our missions in the affected country or region. In addition to daily interaction among OCS and these Offices, OCS chairs a weekly meeting with representatives from DS, INR and S/CT to review all outstanding threat information.

Our posts abroad also evaluate the threat information through their Embassy Emergency Action Committees, usually made up of the Ambassador, Deputy Chief of Mission, Regional Security Officer, Consul, representatives of other U.S. Government agencies at the post, the Peace Corps and other officers at post as appropriate.

If a threat is determined to be specific, credible and non-counterable, DS shares the information with CA and we determine whether it is adequately addressed in our Consular Information Program documents or whether something more needs to be done. In some instances, we may have general information in our CIS, but believe the severity of the threat is such that it needs to be highlighted in a Public Announcement.

When the political situation in a country begins to deteriorate, the Department convenes the Washington Liaison Group (WLG) to alert the inter-agency community to the situation and coordinate interagency planning. The WLG typically includes representatives of other concerned agencies and offices (e.g., DOD, AID, HHS, INS, Peace Corps, and various State Department Bureaus including International Organizations (IO) which coordinates with the U.N., and Public Diplomacy which coordinates the Fulbright Program. At the overseas post affected by the threat, the Ambassador convenes the Emergency Action Committee to determine what steps the Embassy should take to safeguard the welfare of American citizens in country. The official U.S. Government community generally is informed about a threat through formal Embassy channels. Direct-hire AID

personnel and Peace Corps volunteers, for example, are alerted by their respective country directors. The AID director would also contact AID contract employees, who are considered unofficial Americans but who fall under the authority of the AID director. Private Americans, including employees of non-governmental organizations and the United Nations, are told of a threat through the normal Embassy warden system.

Mr. Chairman, the dangers that crime, security threats, kidnapping and terrorism pose for U.S. citizens abroad are of great concern to the Department of State. When an American citizen is taken hostage, for example, the Department and the U.S. Embassy in the host country work closely with host government authorities, other U.S. Government agencies, and family members of the victims to develop a strategy for the expeditious resolution of the hostage situation. Consular officers serve as a point of contact for family members in the United States, providing support and updates as new information is received. The State Department's Office of the Coordinator for Counter-Terrorism (S/CT) works closely with law enforcement agencies and the military to develop resolution strategies, and may lead an interagency Foreign Emergency Support Team

(FEST) to support the Chief of Mission at the U.S. Embassy involved in the event. The FBI may dispatch hostage negotiation experts at the request of the host country government, and the FBI has responsibility for post-incident investigation and prosecution of those who kidnap American citizens. While the U.S. Government has a clear policy on the issue of hostage taking - we will make no concessions to terrorists holding American citizens hostages - we will use every appropriate resource to gain the safe return of American citizens who are held hostage by terrorists.

In the event a U.S. citizen hostage is murdered, consular officers assist the victim's family with the return of the victim's remains to the United States, issuance of the Consular Report of Death and other necessary documents, and other logistical matters. Consular officers overseas and in Washington also provide support services to families of victims.

In June 2000, we established a new program in OCS, in coordination with the Victims of Crime Office of the Department of Justice, to attempt to ensure that American victims of crime abroad and their families receive the same services given to crime victims in the U.S. As a result,

we have been able to provide more timely consular assistance and direct referral services to state and federal victim compensation and counseling programs for Americans who are victims of serious crime abroad, including hostage-taking and other terrorist acts. In addition, we are exploring ways to capture information on the nature and location of crimes being committed against Americans abroad. Since crime can affect any U.S. citizen traveling or residing abroad, this data, when available, will be reflected in the crime segments of our Consular Information Sheets where appropriate.

Approximately 3.2 million Americans reside abroad and Americans make more than 60 million trips outside the U.S. each year. Most Americans have positive, memorable experiences. While unforeseen events can occur anywhere, we believe that safe, informed travel is best achieved by learning everything possible about conditions in the country you are visiting. All U.S. citizens traveling or residing abroad, and their families should review carefully the Consular Information Sheet, and applicable Travel Warnings and Public Announcements before they make a decision to go to a particular country or region. It is also important to review our general safety and security

publications, and to register with the U.S. embassy or consulate. We are now engaged in a project to explore methods to establish an on-line registration system.

In the event of an emergency confronting Americans abroad or their families in the United States, the Bureau of Consular Affairs is available 24 hours a day, 7 days a week at (202) 647-5225. As I said previously, this phone number is on pages 2 and 5 of every U.S. passport. Our embassies and consulates abroad are also available at any time through our duty officer program.

To respond to the concerns of Americans traveling or residing abroad, we hold many outreach briefings in the United States to key stakeholders in tourism, travel, education, and other organizations. This year we are launching an expansion of our outreach program. For example, between March 23 - June 1, 2001 we will speak to hundreds of Congressional staff, business and community leaders, schools and other key stakeholders in Washington, D.C., Miami, Phoenix, Los Angeles, Charleston, Chicago and Philadelphia. We will resume our outreach sessions in the Fall with visits to additional cities around the country. Our embassies abroad and our Passport Agencies in the United States are also engaged in extensive outreach to the

American community. Moreover, Consular Affairs is about to launch a new initiative in our Public Affairs Office (CA/P) to expand the consular outreach program.

We are also partnered with DS's Overseas Security Advisory Council (OSAC) and participate in their outreach activities with American business security experts and other private organizations.

In summary, I believe we are doing a good job, but recognize the ever-increasing need to do an even better job in raising security awareness among Americans traveling or residing abroad to prepare our citizens for safe, informed travel. We must continue to have a zero tolerance for those who would harm our citizens working or traveling abroad. While every such incident cannot be controlled, we are committed to both reducing the potential for and mitigating the effects of such acts. We believe this strategy will continue to be effective.

The Department's efforts to protect Americans traveling abroad have been facilitated by our ongoing dialogue with Congress, and we look forward to working with you to seek opportunities for improvements in international travel information and services.

Mr. Chairman, this concludes my testimony. Thank you for the opportunity to speak to the Subcommittee today. I will be happy to answer questions that Members may have.

Mr. PUTNAM. At this time, the Chair recognizes Mr. Leonard Rogers, Acting Assistant Administrator, Humanitarian Response, U.S. Agency for International Development. Welcome.

Mr. ROGERS. Thank you, Mr. Chairman. It's an honor to appear before the subcommittee today.

At the beginning of this new century, there are many places in the world where Americans are in constant danger, and there is no place where we can consider ourselves completely safe.

Protection of Americans abroad is a challenge; however, it's a challenge we must meet. Our work overseas is important to our own interests and values and to all those who seek peace, prosperity and security. We cannot allow ourselves to be thwarted by terrorism and random violence.

At this Agency for International Development, we are increasingly concerned about the risk to our own employees and to our private partners, the nongovernmental organizations which are so critical to implementation of our development and humanitarian assistance programs overseas, organizations like CARE, Catholic Relief Services, Mercy Corps, and Samaritan's Purse.

In 1970, there were 81 U.S. private voluntary organizations registered with AID. Now there are 446. Together, with the key U.N. organizations, such as the World Food Program and UNHCR, they are the backbone of our work in the field. We simply could not be as effective without them.

Yet, the nature of our humanitarian assistance has changed radically. Once we concentrated on natural disasters such as hurricanes and earthquakes. Now our work is heavily weighted toward complex emergencies in places like Kosovo, Sudan, Afghanistan and Somalia. So our challenge is to balance the need for field presence in dangerous places against the need to do everything we can to assure our NGO partners are as secure as possible.

There are several steps we at USAID are taking to strike the right balance. First, working with InterAction, we are developing and funding security training programs for both NGO, staff and executives. This will help ensure our people in the field are as prepared as possible.

Second, we finance security equipment such as radios and appropriate security staff as part of all our grants. And in approving new grants, we attempt to ensure that each NGO has fully considered the security needs of all of its staff.

Third, we are reaching for consistency in security operations across the entire community working in these dangerous countries, including the U.N. and other donors. This helps ensure a common approach and backstops support in an emergency. USAID and State Department's Refugee Bureau also directly fund U.N. security operations in select separation situations.

Fourth, we finance research and studies on current security issues as they affect NGO's. For example, we help determine how best to provide appropriate insurance for NGO staff in dangerous settings.

Finally, we provide our humanitarian assistance based on principles of neutrality and impartiality. This means our NGO's are not seen as favoring one side or another in a conflict, and there is no basis for retaliation against them by partisans.

Nevertheless, there are limits to what we can do. We must recognize there is an inherent risk in working in developing countries. To illustrate the dangers of this environment, since 1992 the United Nations has lost 189 civilian personnel to accidents and to random targeted violence. U.S. and international NGO's face this same violence and suffer similar losses.

The countries our NGO and U.N. colleagues work in must be held accountable for protecting humanitarian workers. We must insist that governments bring to justice those who commit crimes against humanitarian workers. Otherwise, we can expect these risks to continue to escalate.

Mr. Chairman, the American people give high priority to our development and humanitarian aid programs. U.S. NGO's are critical to our successful delivery of assistance in the field. We will continue to take their security needs seriously. We will continue to work through the USAID security director with OSAC to improve security for all Americans overseas.

Thank you, Mr. Chairman. I would be happy to answer questions.

Mr. PUTNAM. Thank you, Mr. Rogers.

[The prepared statement of Mr. Rogers follows:]

Statement of

Leonard Rogers
Acting Assistant Administrator
Bureau for Humanitarian Response
U.S. Agency for International Development

Before the

Committee on Government Reform
Subcommittee on National Security,
Veterans Affairs and International Relations
U.S. House of Representatives
Washington, D.C.

on

"Protecting American Interests Abroad:
U.S. Citizens, Businesses, and
Non-governmental Organizations"

April 3, 2001

Thank you, Mr. Chairman and members of the Subcommittee, for the opportunity to testify today. The potential threat to Americans overseas, and the measures we can take to reduce the risks our people face, are very important and timely subjects.

The U.S. Agency for International Development has the legislative mandate to carry out development and humanitarian assistance programs abroad. As USAID Acting Assistant Administrator for Humanitarian Response, I have the responsibility for emergency relief for natural and manmade disasters, crisis transitions, food aid and USAID's relations with U.S. private voluntary organizations.

USAID is increasingly concerned about the risks to our own employees and to our private partners in many of the countries in which we work. We have taken a number of steps to address the problem. Nevertheless, it is important to continue to be vigilant and to work to improve security operations for all Americans overseas.

Today, I would like to focus on the non-governmental organizations which play such a critical role in implementing U.S. development and humanitarian assistance – organizations like CARE, Catholic Relief Services, Mercy Corps and Samaritan's Purse.

Since the end of the Cold War, the world seems confronted with a rising number of vicious internal conflicts, many spurred by ethnic and religious hatred. Many innocent people, especially women and children, become caught up in fighting or are intentionally driven from their homes. The American people give a high priority to assisting the victims of this sort of conflict, and private citizens as well as the U.S. Government contribute resources to U.S. non-governmental organizations in order to help. Unfortunately, this means staff from these organizations must put themselves at risk. In addition, we seem to be in a period where terrorism is an ever-present concern. So the security environment for American non-governmental organizations overseas is dangerous.

The Security Environment for American NGOs

Since the U.S. Government's involvement in Bosnia starting in 1992, Somalia in 1993 and Rwanda in 1994, USAID has become increasingly aware that the relief environment within which our partners and our own staff work has fundamentally changed. More relief agencies are going where only the International Committee of the Red Cross (ICRC) had previously dared to go. Non-governmental organizations (NGOs) are now working in increasingly complex, militarily charged areas and are often ill equipped to deal with the delicate operational, political and moral decisions they are being barraged with on a daily basis. There is a dearth of experience, policy and consistency with respect to how closely humanitarian workers coordinate with military personnel or if they choose to use armed guards to protect relief supplies.

Both the U.S. Government and the NGOs we work with are finding it more important than ever to uphold the basic humanitarian principles of neutrality and impartiality. When these principles are breached, the lives of those working in the field are put at risk. The mere perception that humanitarian workers favor one side over another puts their lives at risk. Even so, the neutrality that once sheltered humanitarian workers is no longer sufficient protection in environments where civilians are increasingly the direct targets of combatants.

In terms of our funding of NGOs, in 1970 there were 81 U.S. private voluntary organizations (PVOs) registered with USAID. I would like to note that a PVO is the term given to an NGO with registration status at USAID. There are now 446 registered PVOs, of which 234 have received USAID funding. This growth demonstrates how important these organizations have become as implementing partners. USAID's registration process allows us to ensure that a significant share of the PVOs' funding comes from private sources and that the organization has the management capacity to handle U.S. Government resources. Once registered, PVOs can apply for grants from USAID in Washington, or our field missions can provide assistance directly to PVOs operating overseas. (This does not, however, preclude unregistered NGOs from receiving USAID funding.) Most of our disaster relief is allocated directly to PVOs working abroad. This proliferation of PVO activity demands that we take a closer look at how the U.S. Government can further support protection of its citizens in the field.

While the U.S. Government can assist with resources, information and diplomacy, protection is largely the responsibility of host governments and institutions, and they need to be held accountable. We must insist these governments bring to justice those who commit crimes against humanitarian workers. Otherwise, we can expect these acts of violence will continue to escalate.

The signs of this more dangerous security environment have been manifested in many ways, from mundane topics like insurance rates to gruesome headlines. As early as 1992, one of our smaller NGO partners reported that its insurance agency was about to charge $2,500 for each of its personnel that the organization wished to insure in Bosnia. In 1993, a larger NGO partner stated it might have to recall all of its personnel in danger zones worldwide when the organization found out that, after a land mine accident in Somalia, the standard worker's compensation insurance did not cover its staff for this type of accident and that it needed specific war-risk insurance.

Evidence has mounted steadily that heading to the field on a mission of mercy is no longer sufficient protection against random or targeted violence. Incidents include: the 1995 abduction and ultimately declared murder of a U.S. citizen and well known relief worker, Fred Cuny; the murders of six International Committee for the Red Cross delegates in Chechnya in 1996; the murders of a high-level UN Children's Fund (UNICEF) representative and a World Food Program (WFP) logistics officer in Burundi on October 12, 1999; the murder of three UN High Commissioner for Refugees staff, including an American citizen, Carlos Caceres, in West Timor in 2000; and the killings of UN Mission staff in Kosovo in November of 1999 and May of 2000. Just last week, over

20 relief workers were under siege in the Medecins Sans Frontieres (Doctors without Borders) compound in Mogadishu, Somalia.

The increased threat of violence is not something U.S. NGOs are experiencing in a vacuum, or in numbers disproportionate to their representation in the field. Since 1992, the United Nations (UN) has lost 184 civilian personnel to accidents and to random and targeted violence. In addition to the steps USAID has taken to address this issue, UN specialized agencies, the UN Security Coordinator, the Inter-Agency Standing Committee and NGOs are all working to minimize their vulnerability to security threats while simultaneously not compromising the importance of their presence in insecure environments. In February, the UN Security Coordinator's office, representatives from the UN Office for the Coordination of Humanitarian Affairs (OCHA), and all of the major UN operational agencies gathered in Rome to systematically review and, in some cases, redraft the architecture, mechanisms and procedures of UN security practices. The United Kingdom's Department for International Development's Complex Humanitarian Affairs Division and the European Commission's Humanitarian Office are working directly with their partners and in consultation with USAID in support of community-wide initiatives and increased funding for operational security of individual implementing partners.

USAID Approach to Enhancing NGO Security

The realities and lessons learned from the above snapshot of the past eight years have informed the methods which USAID uses to address the security needs of relief personnel in the field. These lessons are: symbiosis, management, awareness, accountability, context and capacity. In shorthand, they may be referred to as the SMAACC principles:

1. Symbiosis. U.S. NGOs cannot be safe without the entire humanitarian relief community observing and practicing good security management. A misjudgment or carelessness by one organization can easily compromise the security of another. To this end, USAID, through its Office of US Foreign Disaster Assistance in the Bureau of Humanitarian Response (BHR/OFDA), has endeavored to reach the widest possible audience when supporting security training and operational security coordination, and in funding equipment and personnel that support individual NGO programs. This thinking also underpins our attempts to promote universally accepted standards with respect to security planning and practices and in supporting the Security Coordination functions of the UN.

2. Management. In order for security to exist, the leadership of each and every NGO, UN agency and donor office must see security as a top priority and as an intrinsic aspect of program design and personnel deployment. In September 2000, USAID through OFDA funded a "Security Seminar for NGO CEOs" course, including the research and development in preparation for the course.

3. Awareness. OFDA has supported research that has demonstrated that risk can be minimized without foregoing presence. Our approach to increasing awareness has included research on appropriate models of security management. This research has in turn informed the curriculum of various security courses and has been published as stand-alone documents to help individual field administrators and agency managers. The training funded by USAID has probably done the most to date to increase knowledge and demand for better security practices.

4. Accountability. Accountability must be comprehensive. NGOs that engage in good security practices, when conducted sensitively and responsibly, will promote not only their own security but also the security of their intended beneficiaries. USAID has attempted to educate NGOs on this point through OFDA proposal guidelines. In these guidelines, OFDA requires information on how security factors are reflected in the design of each intervention and asks if each agency's board of directors is aware of the InterAction Security Planning Guidelines and if the agency adheres to them.

5. Context. NGOs and other relief personnel need to understand clearly they are not corporate representatives nor are they diplomats nor military personnel. The security practices and thinking that are suitable to these professions are often inappropriate to relief personnel. Many of the skills and abilities of these other communities, however, can be useful to NGO workers if their application accounts for the "context" of NGO work, that is, to work in solidarity with people in need. It is impossible and inadvisable to mandate or train for a specific response to all security threats; a response that may save a person's life at a roadblock in one country could get that person shot in another. Context is also useful in determining which security concept, or combination thereof, to employ: acceptance, protection or deterrence.

6. Capacity. OFDA provides capacity-building opportunities for NGOs that are committed to improving the security of their international and national staff and protecting their intended beneficiaries. This capacity building is done through funding of training at the community-wide level, subsidizing the costs of equipment and systems, and funding research and writing that demonstrate how NGOs are incorporating security as a value into their agencies,

USAID Support of NGO Security

It must be emphasized that NGOs are independent of governments, of the UN, and of one another. U.S. citizens work for NGOs based in Britain, France and other countries. Thousands of Irish, Australian, British, Kenyan and Indonesian nationals are employed by U.S.-based NGOs. As an influential donor, we can promote best practices, we can encourage NGOs to create policies and to manage and plan for security, and we can provide funding to help ensure they have sufficient resources to ensure their security. However, we cannot force NGOs to do what they will not, and we cannot assume

responsibility for their actions, nor can the U.S. Government be held directly accountable for the decisions of individual NGOs and their staffs.

Currently, USAID, through OFDA, is contributing over $1.4 million to UN operational security coordination in Angola, Southern Sudan and Burundi. Additionally, OFDA regularly funds coordination structures in other disaster situations that serve as the locus for the exchange of security information for the entire relief community. On an on-going basis, OFDA funds the hardware (radios, satellite phones) and personnel costs (guards, increased employee benefits) required. Moreover, OFDA funds increased insurance premiums and more secure housing required in each USAID-supported NGO program in order to ensure that our partners have adequate resources available to meet their technical security requirements.

OFDA has decided that its security-specific initiatives, as distinct from operational requirements, are most useful when they are targeted to the community rather than to individual NGOs. This practice promotes community standards and a common language for discussing security. The practice also demands that NGOs demonstrate their own commitment to improved security management. In 1995, OFDA solely funded InterAction's development of a curriculum and two pilot security training courses that continue to inform training and thinking on the subject around the globe. OFDA continues to fund field security management training through RedR, an NGO that provides a variety of training for humanitarian personnel. To date, RedR has offered security management workshops in Kosovo, Sierra Leone, Indonesia, Liberia, United Kingdom and Angola to over 160 NGO managers and staff and also has offered one "training-of-trainers" course to 20 persons in the United Kingdom. The next offering of the field security management course will take place in Nairobi, Kenya targeting NGOs working in Sudan, Burundi, Rwanda, and Somalia.

Another way that OFDA promotes security, maximizes impact and reinforces the need for humanitarian community-wide solutions to security needs of NGOs is by working formally and informally in consort with other donors. USAID's OFDA, State Department's Bureau of Population, Refugees and Migration (PRM), and the European Community Humanitarian Office have signed a joint statement supporting further security initiatives. State/PRM has pursued its own security initiatives as well, such as in providing $500,000 to the United Nations to help establish a country-wide field security mechanism in the Democratic Republic of Congo to include the deployment of UN field security officers and to provide for some of the security needs of NGOs. The United Kingdom's Department for International Development and a private company, Cable and Wireless, co-fund, along with OFDA, the RedR security course program.

As I said earlier, last September, in an effort to increase NGO top management's commitment to and realization of improved security practices, USAID, through OFDA, sponsored InterAction's two-day seminar targeting the chief executive officers (CEOs) of U.S. and European NGOs. As a follow-on to the NGO CEO program, OFDA is funding research into an area that the CEOs identified as one requiring more answers: how to better address the security of their local staff. OFDA has also sought more directly

persuasive ways to promote NGO security via the requirement instituted in the 1998 "Guidelines for Grant Proposals and Reporting" that NGO proposals submitted for OFDA funding include information on how the security context of a given situation has informed program design and by including NGO security in the programs of the past three biennial conferences of OFDA's NGO partners. OFDA also reinforced the "InterAction Security Planning Guidelines" by reference in its own guidelines and by including the entire text as an annex.

Through OFDA, USAID contributed to the research and writing of the book, Operational Security Management in Violent Environments, Van Brabant, K., 2000 and directly and indirectly completely funded the subsequent publication, Mainstreaming the Organizational Management of Safety and Security, Van Brabant, K., March 2001. These works build on many of the initiatives described above and offer not only theoretical models and practical advice, but provide a roadmap for the institutional change required for the integration of security into the management of NGOs.

In the future, in addition to direct programmatic and coordination costs, OFDA intends to continue funding security training. In early summer, OFDA intends to issue an annual program statement soliciting new ideas for the promotion of NGO security. USAID will also continue to coordinate its activities with other donors and leverage its funding to ensure the greatest impact on NGO security.

USG Support of Expatriate Community

Mr. Bergin has just spoken about the Overseas Security Advisory Counsel (OSAC). The USAID Director of Security represents our Agency to OSAC and, with the complete encouragement and support of OSAC and the Director of the Diplomatic Security Service, has worked to have the interests of U.S. non-governmental organizations represented. OSAC has opened its electronic bulletin board to NGOs. The USAID Security Director has made an effort to reach out to NGOs to share awareness of the availability of security support through OSAC, in meetings with the Advisory Committee on Voluntary Foreign Aid, the Overseas Cooperative Development Council, and constituent NGOs of USAID's Office of Private and Voluntary Cooperation. This is an ongoing initiative. The Security Officer has advised USAID senior staff to be cognizant of the security of NGOs and has given specific guidance on how to accomplish this.

In conclusion, USAID takes seriously the security threats to its private sector partners working in difficult environments abroad. The Agency has taken and will continue to take action to make others aware of security needs and to give these needs serious consideration.

Mr. PUTNAM. At this time, the Chair recognizes the chairman, Mr. Shays.

Mr. SHAYS. Given my not being present for all the testimony, I'm happy to follow at the end. I thank the chairman and would yield to Mr. Gilman.

Mr. PUTNAM. Mr. Gilman from New York.

Mr. GILMAN. Thank you, Mr. Chairman. I thank Chairman Shays for yielding his time.

I would first like to especially welcome Peter Bergin, Director of Diplomatic Security Service. Mr. Bergin's agents around the world have provided highly professional protection details for Members in Congress whenever our colleagues are out traveling abroad. We thank you for allowing one of your personnel to be assigned to our International Relations Committee, Pat Durkin, who has done an outstanding job. And your former members have been of great asset and service to us. I hope you will continue in that direction.

I want to thank our panelists all for their instructive information. A number of—Peter Bergin, a number of the investigative personnel at-risk analysts provide good information to us. How many do you have working in that area?

Mr. BERGIN. We have six.

Mr. GILMAN. Six in the whole world.

Mr. BERGIN. They cover all areas of the whole world.

Mr. GILMAN. I think you need a lot more.

Mr. BERGIN. Well, our budget for the OSAC program is about $1 million. If you look at the number of constituents that we have in OSAC, a number close to 2,000, that's really about $500 a constituent. And $500 goes a long way in terms—if we can provide people information which will save someone's life or save from being injured, I think it's money well spent.

One of the problems that we have is that, for example, if we send a risk analyst to South Africa to deal with an issue of the private sector community there, there's no backup. So we would be looking to increase it probably by putting an additional analyst for each region of the world.

Mr. GILMAN. I hope you'll let us know about your request for that additional personnel.

Mr. BERGIN. We will, sir. Thank you.

Mr. GILMAN. You mentioned in November an annual briefing at the U.N. for security purposes where you invite private organizations and security people. Is there any congressional involvement in that meeting? If not, I would urge you to——

Mr. BERGIN. I don't believe so.

Mr. GILMAN. I would urge you to expand it and include them, and particularly in this committee. I think we would all be interested in some involvement.

Mr. BERGIN. We would be delighted, sir.

Mr. GILMAN. Your publications, how available are they to the public?

Mr. BERGIN. Well, sir, they are available on the Web site. They're available to all the public. They're free. And if using the Web site, they call into the OSAC office, we can send them hard copies. So they're readily available.

Mr. GILMAN. I would hope that your bulletin—I don't know how regularly you put out an OSAC bulletin.

Mr. BERGIN. It's every day.

Mr. GILMAN. Would you make that available to this committee?

Mr. BERGIN. We would be happy to, sir.

Mr. GILMAN. Thank you very much. Now, with regard to training, which it has been emphasized there's need for greater training, what do you do with regard to training? I know you have some training sessions.

Mr. BERGIN. Yes. As I mentioned, sir, we have held four sessions in the past year. These are actually provided by the State Department's Overseas Briefing Center. The Overseas Briefing Center for the State Department provides training to State Department employees and other agency employees who are assigned overseas. This is an opportunity to provide employees of NGO's, corporations, universities, an opportunity to get the same training that U.S. Government employees get prior to their assignment overseas. And the subjects are personal security, cultural security, awareness of those kind of issues.

Mr. GILMAN. Is that done here at the UN?

Mr. BERGIN. No, sir. It is done here in Arlington at the National Foreign Affairs Training Center.

Mr. GILMAN. Mr. Waguespack, we welcome the FBI being here. How many ILEAs are there, the international training programs, around the world today?

Mr. WAGUESPACK. I'm sorry, sir.

Mr. GILMAN. How many ILEAs are there in place today.

Mr. WAGUESPACK. One ILEA in place in Budapest.

Mr. GILMAN. What about the one in Thailand? I visited that when they opened it.

Mr. WAGUESPACK. Sorry, sir.

Mr. GILMAN. You're not familiar with that one?

Mr. WAGUESPACK. I am not involved in that part of our program, so I don't have all the specifics on the numbers out there.

Mr. GILMAN. And I understand you're exploring one for South Africa; is that correct.

Mr. WAGUESPACK. Sir, again, that is not an area of my expertise. I haven't been involved in those. I can't answer that question for you.

Mr. GILMAN. Well, training has been emphasized in this hearing, and it would seem to me that the FBI can provide a great service by encouraging more ILEAs around the world. I know your Director, Mr. Freeh, has been very cooperative and very supportive of doing that. And I would hope you could tell us of any others that are being considered.

Mr. WAGUESPACK. Yes, sir, I will be glad to take that for the record.

Mr. GILMAN. Ms. Andruch, your Overseas Citizens Services, what is the public's access to your bulletins where you talk about a travel warning?

Ms. ANDRUCH. We have those. Those are published on our Web site as well as being made available through travel agencies and through the media. We also, for people who may not have access to an Internet, we provide them by mail if they call us. We have

an officer—someone available to the public 24 hours a day if they should wish specific information about a country.

Mr. GILMAN. What about the media? Do your travel warnings go out to the media?

Ms. ANDRUCH. Yes, sir, immediately. As soon as they are issued, they go out. At the time they go on the Web, they go to the media, and they go to the travel agencies.

Mr. GILMAN. How about to your Congress people?

Ms. ANDRUCH. Would you like to get special copies on them?

Mr. GILMAN. I think it would be important for you to circulate that to all of the Members of the Congress and the Senate, since we're always in touch with our constituents. I know my office has continual requests for is it safe for me to travel to this part of the world.

Ms. ANDRUCH. Yes, sir.

Mr. GILMAN. So we would welcome if you could make those travel warnings available to us.

Ms. ANDRUCH. We would be happy to. We might be able to—I'm not very technical, but we might be able to look at something like a hot link to our Web page if that would be helpful.

Mr. GILMAN. Well, whatever could help us in disseminating that information.

And, Mr. Rogers, we welcome you from AID. What are you doing about training the NGO's about security? I notice you indicate there are hundreds of NGO's out there working with your agency. What do you do to train them for security?

Mr. ROGERS. Well, we do two things, Mr. Chairman. First we work with InterAction, which is the umbrella group for NGO's, provide resources to them for their security training program. And then in the field, we work with the international community onsite. Normally, we have a disaster assistance response team that's in the field that will work with the NGO's in the field, work with the U.N. and their security officers, work with the Embassy and the regional security officer to provide information and alert the NGO's to current conditions in the country.

Mr. GILMAN. Well, thank you, Mr. Rogers. I want to thank our panelists. I know my time is up. Thank you, Mr. Chairman.

Mr. PUTNAM. You're welcome, Mr. Gilman.

Mr. Otter, I apologize for having to cut you short on the last panel, but feel free to fire away at this one.

Mr. OTTER. Does that mean I have a whole bunch of extra time on this one?

Mr. PUTNAM. Sure. Why not?

Mr. OTTER. The victims. Thank you very much, Mr. Chairman.

In my previous life, prior to coming back here to D.C., Mr. Rogers, I was—1983, I guess it was, President Reagan then appointed me to a task force. It was the Task Force on International Private Enterprise. There were 17 of us, as I recall, and we traveled to different parts of the world.

As a result of that 18-month experience, I ended up on the World Bank's advisory committee for agricultural loans. You know, all the testimony that I heard today, not only from this panel but the first panel, never once in consideration of a loan to a foreign participant

was the environment, was human rights, were any of those things ever brought up.

Is it the practice of the IMF or the World Bank or any other agency that AID has a participatory program with, is it their practice now to assess these environmental and human rights factors in the international marketplace?

Mr. ROGERS. Yes. Certainly. The—it's actually the Treasury Department that has the representative that works with the World Bank. But each one of the World Bank's loans, in fact, the loans of each one of the multilateral banks, is reviewed against a variety of criteria. And certainly the U.S. Government's view about the environmental practices of the recipient country, about the environmental impact of the loan itself, are all factors that are considered, and the human rights performance of the country is also considered.

Now, we are one among many countries that sit on the executive board of the World Bank. So there are other voices to be heard as well. And occasionally there's controversy over individual loans.

Mr. OTTER. Are these decisions made in a democratic process? The 50 percent, the 51-plus—or 50 percent plus 1 wins?

Mr. ROGERS. I'm not sure what the voting rules are for the Bank itself, but there is some process that people go through to assure that the views of the executive directors are heard.

Mr. OTTER. Let's just say for a moment, Mr. Rogers, that I'm back in the international marketplace, and I'm trying to develop products and plants overseas in order to develop markets, mostly because of proximity. It's closer to my market than my plant in Idaho. Maybe it's the natural resources. I can duplicate the quality and the nature of the natural resources, renewable resources, farm resources in that foreign country that I can in Idaho. And, you know, maybe the energy is a little cheaper in this day and age because California is not stealing their electricity like they are from Idaho. You know, maybe it's any one of these factors.

When I make this decision, the thing that I do or did is, I would go to one of these agencies that AID obviously has a working relationship with, and I say I want to invest $30 million—I want to invest $30 million in Ishmir, Turkey. We built a plant in Ishmir, Turkey to supply french fries for the McDonald's in Europe.

I want to know what the process is now then that this agency, whether it's the World Bank or the IMF or whoever, would make funds available to me now. Do I have to comply with OSHA in Ishmir? Do I have to comply with EPA? Do I have to comply with affirmative action? Do I have to comply with all the rules and regulations we have in the United States in order to put this site in Ishmir, Turkey?

Mr. ROGERS. I believe that you would be obliged to comply with the local regulations, and then the Bank would have its own standards if it were financing this program. But basically the local standards would apply, plus whatever standards the multilateral lending institution would have.

Mr. OTTER. So the rule of law, then, that Mr. Cilluffo talked about in panel one, the rule of law certainly then entertains the rule of law of the host country, right?

Mr. ROGERS. Absolutely.

Mr. OTTER. Thank you. That's all I have, Mr. Chairman.

Mr. PUTNAM. Thank you, Mr. Otter.

I have a couple of questions. First of all, to build on what Mr. Otter's point was with the first panel, in your opinion, are Americans, both governmental employees and American tourists abroad, safer today overseas than they were 20 years ago?

We'll start with Mr. Rogers and work on down. All right.

Mr. ROGERS. My opinion is definitely that they are not. I'm not 100 percent sure what the reason is, but since the end of the cold war, we seem to have this proliferation of very vicious political and ethnic conflicts, and they seem to be affecting our interests more widely than they did in the past.

The United States is interested still in being engaged in those countries. We provide humanitarian assistance to those countries. Americans want sometimes to travel to those countries. So, all in all, I would say we are at much greater risk, even setting aside the apparent rise in terrorism. So I would say the answer is the environment is much more dangerous than it was 20 years ago.

Mr. PUTNAM. Ms. Andruch.

Ms. ANDRUCH. Yes. I think I would have to bow to the experts on security as to actually if we're safer now than we were 20 years ago. But I think just the availability of travel and the increasing number of Americans both residing and traveling overseas makes it more likely that Americans would be the victims of some sort of disaster overseas.

Having said that, however, I also think that technology being what it is, and the availability of information to everyone, that we do have the opportunity now to get out information so that the travelers, if they avail themselves of that information, can make a much better informed decision on where and when they travel. Thank you.

Mr. WAGUESPACK. I think Americans abroad are at greater risk today than they were 10 years ago, 20 years ago, primarily because of the increased terrorism threat, but also because of the increased risk to collection activities on the part of intelligence services for proprietary economic information as well, and that's something that we should not lose sight of, as well as from a criminal element. So I think, across the board, Americans in various parts of the world are at greater risk than previously.

Mr. PUTNAM. Mr. Bergin.

Mr. BERGIN. Yes. Since the East African bombings, Mr. Chairman, I have never seen as much information about threats in my 28-year career in diplomatic security. There is considerable amount of ground noise regarding threats. The specificity is certainly questionable. That's one of our big jobs during the day is to—when that threat window is opened, we've got to close it. We've got to make sure that we've covered all the bases there.

I would second what Ms. Andruch said about information. I think information today in terms of what we provide the public and to our diplomats is much more accessible than it was 20 years ago. I will recount for you, when I was in Cairo as the RSO, we spent a considerable amount of time during the Gulf crisis briefing not only diplomats and their families, but also engaging the private sector.

Our philosophy and that of the American ambassador was that the American public in Cairo, in Egypt, needed to know what the Embassy knew with respect to threats that entire community faced. That's basically what we've evolved to in OSAC, and with the assistance of the Bureau of Consular Affairs, that the American public know what we know in terms of American threats abroad.

Mr. PUTNAM. Well, addressing that point, and it was raised in the first panel as well, separating the wheat from the chaff and determining what is noise and what is valuable information, are our various information gathering agencies integrated and coordinated enough to make those determinations, and are the bulletins that are then posted or the information that is then passed on, is it as accurate and valid as it should be or could be?

Ms. Andruch and then Mr. Bergin.

Ms. ANDRUCH. Yes, sir. I think our—the cooperation among the various agencies in Washington and certainly the bureaus within the Department is excellent. I think, you know, on a daily basis, we talk to DS probably at least three or four times. And whenever there is any information that they've heard, they've gotten from a source, whether it be in Washington or at the post abroad, that information is shared. And we have contacts on—you know, in other agencies, including the intelligence community. So I think, yes, it is.

Mr. PUTNAM. Do you coordinate with ANSIR?

Ms. ANDRUCH. Yes, we do. We talk to FBI. We talk to the agency. We talk to everyone, you know, who might have some input on it.

One of the—on the first panel, someone mentioned something about the classification of information and sort of alluded that was sometimes a problem. I, in fact, don't think it is, because when there is something that's out there and it's determined to be credible information, we find a way of working together to get that information to the public. And having the security officers and other people, other agencies represented at Embassies abroad makes it—it's so much easier in a way because there's a little bit of built-in redundancy. That same information that DS and other agencies overseas are gathering for possible use by the Embassy and the official community overseas is always shared with the private community.

Mr. PUTNAM. Mr. Bergin.

Mr. BERGIN. Yeah. I would say, Mr. Chairman, that one of the most powerful lessons that we've learned out of the East African bombings is that no agency can do it by itself in terms of protecting Americans abroad. Diplomatic Security can't do it by itself. The intelligence community can't do it by itself. DOD can't do it. But if we work together—and I have seen an improvement, a terrific improvement in the last 2 years—if we work together, we stand a better chance at deterring and preventing terrorism against official Americans as well as private American citizens. But you've got to work together, and there has to be wise integration of all of our national assets to this end.

And I believe, for example, I can pick up the phone and call J34 over at DOD and get assistance, both logistical and people assistance, to augment what we're trying to do overseas when a threat is identified. So I'm comfortable that externally, you know, beyond

the State Department, we're working closely with the agency, the FBI, DOD to protect all Americans abroad.

And I would say one of the things that was mentioned in the first segment was that we needed to introduce the private sector to the host country security police officials. We do that on a regular daily basis. RSOs are doing that all the time so as to advance the interests of the private sector abroad, because we feel we're obligated to do that.

Mr. PUTNAM. Did anyone else want to answer that on the panel?

Mr. WAGUESPACK. I would just say from the perspective of the FBI, certainly within the terrorism threat warning arena, our focus—if I leave the committee with nothing else but this point, is that our focus is, when we get a credible threat, our focus is to get that information out as quickly as possible and to share it with the community.

Mr. PUTNAM. Thank you. Mr. Shays.

Mr. SHAYS. Thank you very much, Mr. Chairman. First, let me thank you for chairing this hearing. You were supposed to do a good job, not a great job. And I appreciate that you are very capable, and thank you very much for doing that.

I also, before concluding this hearing, want to recognize Alex Moore, career Foreign Service officer who is currently working with the subcommittee under the auspices of the Pierson Fellowship Program. At the State Department, Mr. Moore has served as a special agent in the Bureau of Diplomatic Security since 1985. As part of his yearlong fellowship, Alex was responsible for all the research and preparation for this hearing. We appreciate his help on previous hearings as well. We're grateful for his very good work and trust he will return to the State Department with a deeper understanding of the legislative oversight process. Alex, thank you very much.

I also want to welcome our witnesses. I'm sorry I didn't get to personally greet you, but you have been in very good hands.

I would like to know, how does the U.S. Government differentiate between terrorists and criminal incidents? Maybe we can just run straight down.

Mr. BERGIN. I think that's something that's quite blurred. I think when you——

Mr. SHAYS. I'm going to ask you to talk a little louder, too.

Mr. BERGIN. I would say that's something that's quite blurred in terms of whether an incident is terrorism or whether it's criminal. For example, the incident down in Ecuador where these folks held Americans and foreigners in the last—since November and released them in March—is that crime? Is it terrorism? It's a difficult thing because perhaps some of them have relationships with known terrorist groups. But maybe they are—you know, they've separated. It is a very, very difficult thing.

But one of the things that we try to do in, at least in the State Department, is we provide antiterrorism assistance training to governments all over the world. In the last year, we've trained about 20,000 police and security officials. And the multiplier effect of that is significant, because the Embassy—it's difficult beyond the walls of the Embassy to provide security. But if you can engage the host government, if you can train them to standards of the United

States, Americans who travel and invest abroad benefit significantly.

Mr. SHAYS. Thank you.

Mr. WAGUESPACK. Again——

Mr. SHAYS. Do me a favor. I'm just curious. My ears must be—just tap your mic a second. It's not picking up all that great. But talk a little louder, if you would, sir.

Mr. WAGUESPACK. Again, I would agree with Mr. Bergin. I think there is very definitely a blurred line between pure terrorism and criminal activity. The two go hand in hand. Terrorist groups commit criminal activity. They commit crimes. And certainly from the FBI's perspective, as we go after terrorist groups, much of what we look at is what is their criminal activity as opposed to just, you know, setting off bombs, whatever. Many of these groups are engaged in all sorts of criminal activity to further whatever their objectives and goals are. So the two are very much intertwined, and you can't really segregate counterterrorism or terrorism purely from criminal activity.

Ms. ANDRUCH. Yes, I agree. And I would like to add, though, that from the consular perspective, our concerns for and response to victims of crime or terrorism are the same. And one of the things that we've been very fortunate in working with the Department of Justice, we now in the Office of Overseas Citizens Services, have a crime victims specialist.

What we're trying to do is ensure that victims of crime receive the same sort of counseling and have the same sort of resources available to them overseas that they would have if a similar thing happened to them in the United States.

So we don't make that distinction, although we recognize that there is a difference from what we see. The effect on the person is the same, and so we react to that in the same way. Thank you.

Mr. ROGERS. We would rely on the State Department to draw the line in terms of a definition. But I would say that it seems somewhat more likely that Americans would be the victims of terrorists, whereas common criminal activity would tend to be more random and perhaps a bit easier to prepare for than terrorism.

Mr. SHAYS. You kind of answered this, so I'm not asking for a redundant answer, but if you have something you want to amplify—how does the U.S. Government respond to terrorist threats differently than criminal threats?

Mr. BERGIN. Well I think, given the political dimension of terrorism, I think there is a tendency in the U.S. Government to react considerably to a terrorism threat. If it's crime, I think that crime is endemic. And having served in places where crime is a critical problem for us, I mean, we spend—the Embassy, the RSO, spends a lot of time with country councils and the private sector to ensure that they have the commonsense general awareness of crime.

But in terms of a criminal threat, for example in Ecuador, the United States engaged the FBI and a number of Defense Department assets to resolve that issue, which could be either viewed as a criminal act against the United States or a terrorist act.

Mr. SHAYS. OK. Thank you.

Mr. WAGUESPACK. Again, from an FBI perspective, the terrorism program is part of our tier one strategic program. And so much of

our resources in the FBI are focused first and foremost on the national security aspects, the terrorism/counterterrorism part of what we do.

In addition to that, obviously on the international criminal side, international organized crime, those kinds of issues, while we worked in the international scene, we're looking primarily at what the impact is in the United States, on the United States, but realizing that you can't work solely within the United States; we do have to work on the international scene.

But from a strategic standpoint in the FBI, terrorism and what we're looking at from a national security standpoint is our priority tier one program along with the national foreign intelligence program.

Ms. ANDRUCH. Our consular information program, which I mentioned briefly in my testimony, has information. The consular information sheets that we have available on each country has specific information devoted both to crimes, trends in crime, and in terrorism when that is known. The public announcement and travel warnings that we will put out on an individual country are more often for terrorism threats because those are the ones that we will hear about through the intelligence community.

Mr. ROGERS. I don't have anything to add.

Mr. SHAYS. I have another round of questions, but I'm happy to defer to the gentleman.

Mr. PUTNAM. You can just continue.

Mr. SHAYS. Let me just ask you, what countries do the best job of protecting American interests overseas and which do the poorest job? I don't want to create a national incident here, but——

Mr. BERGIN. It is definitely uneven, sir. I mean, I don't have a list of the most prominent in terms of countries that provide us protection, but certainly our aim is to ensure a baseline of service.

Mr. SHAYS. Right. I understand. But let's try to get to the question, though, I mean with all due respect. There are some countries that you have a better relationship than others, and who would those be?

Ms. ANDRUCH. On an individual basis, I would have a hard time answering that as well, but I think in countries where we have a very small presence, I think our—we're hampered then to the extent of, you know, having fewer people to get the information out.

And someone on the first panel also mentioned NGO's, of course, tend to go to the countries where there is perhaps a primitive infrastructure, if any at all. In those countries, then, our work will then be that much more difficult.

Mr. SHAYS. See, I have a theory that the only one who tops the State Department in terms of responding to a question as carefully as Alan Greenspan, that he talks—he talked—in fact, I fear that his training came from the State Department.

But maybe you could answer the question this way: What are the factors that affect a foreign government's responsiveness to American security concerns the most? What—when are they most—what are the issues of the—the factors where they may be more responsive to our concerns? When they may get drawn in? When they may be embarrassed? I mean, what would that be? Is it that we

have worked out better relations with those countries or we've had longer contacts? What tends to make a country more responsive?

Mr. BERGIN. I think it definitely comes down, sir, to the strength of a relationship between the United States and a particular country. For example, in Egypt, there was definitely a concern about their ability to provide security to Americans because of the number of incidents there stemming from the Achille Lauro. And what we did was the Congress created the Antiterrorism Assistance Program. Basically what this did is it gave the State Department a tool——

Mr. SHAYS. To reach out.

Mr. BERGIN [continuing]. To which they could engage the Egyptians and train them on how to protect. For example, in Luxor, we had an incident in 1997 where you had a number of western tourists killed as a result of terrorist incidents. The security forces——

Mr. SHAYS. It wasn't too good for the tourist trade, was it?

Mr. BERGIN. Absolutely not. And clearly that is something vital—it's a $2 billion industry in Egypt. But clearly that's not in the interest of Egypt to do that. Nor is it in the U.S.' interest. So what we did is flux the ATA program to provide training to police officers in upper Egypt, and we haven't had an incident yet. And they're much more vigilant today than they were 2 years ago.

Mr. SHAYS. OK. Anyone else want to respond?

Ms. ANDRUCH. I wish I—I would like to say that I wish I was as good at predictions as Alan Greenspan, because then we wouldn't have as many problems as we do.

Mr. SHAYS. No, no, no. The thing with Alan Greenspan is that when you're done, everybody thinks that he agrees with them. So both sides leave content. It's quite a skill.

Ms. ANDRUCH. I'll do my best. One of the things—I just—you know, in individual countries with consular officers overseas, I think one of their main responsibilities is to do the outreach and sort of the public diplomacy with the law enforcement people in that particular country.

So I think that responses from those people are generally good. I think when they—when they are less good is if there's something in the political situation at the time that makes them sort of want to use a particular case as a hammer.

Mr. SHAYS. OK. Mr. Chairman, I just have three more questions.

I want to know these two. I'll ask them the same. What is the U.S. Government's policy in kidnapping, and what is the FBI's role in cases of kidnapping overseas? Start with the FBI.

Mr. WAGUESPACK. Normally, in kidnapping situations overseas involving an American person, the normal procedure would be for a coordinating subgroup at the NSC to——

Mr. SHAYS. I really am sorry. I'm having trouble hearing you.

Mr. WAGUESPACK [continuing]. A coordinating subgroup at the NSC to bring together all the components of the U.S. Government to look at the U.S. Government response. Depending on what comes out of that interagency forum in terms of how we as the U.S. Government should best respond to that particular situation, the FBI may be brought in to provide advice, to provide assistance. But, again, it depends. It's on a case-by-case situation. And in many cases, in most cases, we normally will send agents to assist.

But, again, it's done on a case-by-case basis in an interagency forum.

Mr. SHAYS. Does the FBI define the U.S. Government's response to kidnapping? Can the State Department provide me any difference or——

Mr. WAGUESPACK. Well, again, it's an NSC-led forum. So it brings together the various components of the government, and a collective view of that forum decides what is the best government response.

Mr. ROGERS. In the case of nongovernmental organizations, we would consider strongly their preferences as well. There's an incident now in Sudan where four ADRA staffer members, the Adventist Relief Agency, which is a U.S. private voluntary organization, were kidnapped. The preference there was the United States not step in, that they allow the U.N. and the NGO to see if we could negotiate the release of these individuals.

Mr. SHAYS. When I was in the Peace Corps, I always felt that I had kind of the government behind me. When I think of the volunteers who serve in nongovernment organizations, but in the same capacities as teachers and so on, working in nursing care, health care, would the response for someone in a nongovernment agency be treated the same as a government—someone who is not a government employee be treated the same way as a government employee?

Mr. WAGUESPACK. To the best of my knowledge, there would be no differentiation.

Mr. ROGERS. Except to the extent that the NGO wanted to express a preference. If they felt they could handle it better if the U.S. Government was not involved, then normally we would stand back and allow them to take that course.

Mr. SHAYS. Thank you, Mr. Chairman, for being so generous with the time, and I thank the panel.

Mr. PUTNAM. Thank you, Mr. Chairman.

Mr. Otter, do you have any further questions?

Mr. OTTER. No. No.

Mr. PUTNAM. I'm curious what the U.S. Government's role, security role, will be in the upcoming Olympics in Athens in 2004.

Mr. BERGIN. Well, I know the Ambassador in Athens is engaged with the Greeks on this matter. I know that, for example, we sent a couple of agents to Athens in February to discuss with the Greeks what sort of security arrangements they were planning for the Olympics and how the Embassy would interface with the Greeks in terms of providing security, not only for the teams and the USOC, but also private American citizens who would be visiting Athens during that time period.

Mr. WAGUESPACK. Again, I can only speak limited to that particular area, since I am not engaged in the counterterrorism division, but I know that our counterterrorism personnel were certainly engaged in looking at the issues and working with their counterparts abroad on that issue. But in terms of the specific details, I'm not familiar with the specifics.

Ms. ANDRUCH. The Bureau of Consular Affairs will be sending out additional consular staff for that, as they do with any time there is a large gathering of Americans, hopefully there will not be

any large terrorism events or anything of a major crime, but just for the usual kind of problems that arise with Americans traveling in large numbers.

Mr. PUTNAM. Are there current bulletins on Greece as we speak?

Ms. ANDRUCH. No, sir, I don't believe so.

Mr. PUTNAM. Mr. Rogers.

Mr. ROGERS. I'm not aware of any.

Mr. PUTNAM. The previous panel in written testimony had indicated that perhaps we are too quick to issue bulletins and travel advisories, in essence getting back to this differentiation between noise and sound or the difference between information and real positive data.

I'm curious. If you were evaluating the United States, would you issue a travel bulletin?

Mr. WAGUESPACK. It depends on what city.

Ms. ANDRUCH. I guess that's me. I think there are countries, in fact, who do warn their travelers, their tourists, against certain areas in the United States. I know, for example, when there were—people were being murdered after they rented cars in Miami because the cars were sort of—you know, pointed out tourists. That became a problem for many countries. So I think the answer would probably have to be yes.

Mr. PUTNAM. There's a big problem in my State.

Ms. ANDRUCH. You know, one thing, though, if I could turn that back not to your initial question about, you know, our sort of issuing perhaps too many warnings or travel warnings or public announcements. We take our responsibility concerning the safety and welfare of Americans very seriously, and it is the State Department's No. 1 priority.

Fortunately for us, that is our primary concern. So while it is unfortunate that in some—you know, there may be countries who suffer a loss of tourism, or travel agencies who aren't selling quite enough tickets or quite as many tickets as they had, and we're sorry for that. But at the end of the day, you know, if we have information that we believe is credible and there is a threat out there, it's our responsibility to get the word out.

Mr. PUTNAM. Thank you. Mr. Otter.

Mr. OTTER. Mr. Chairman, I do have a couple of questions that I would like to ask.

First, of the FBI. Do you rate foreign law enforcement agencies?

Mr. WAGUESPACK. Do we rate them?

Mr. OTTER. Do you rate them? The gentlemen was—geez, we want to introduce these NGO's to the foreign law enforcement agency when we get in there, and we want them to know that they're there. How do I know whether they're the good guys or the bad guys if you don't rate them? Would you know? Is there any reason that you or the CIA would know?

Mr. WAGUESPACK. Do you know in terms of rating like 1, 2, 3, 5, 5, A, B, C, D, E? Is that——

Mr. OTTER. No. Like these are good guys or these are bad guys.

Mr. WAGUESPACK. Well, certainly. I mean, again, as we look at, as we have expanded our "leg atts," for example, around the world, our legal attaches, our whole purpose in doing so is to be able to

work with the local and national police authorities in those countries and to build relationships with those entities.

Another aspect of what we have done in terms of our National Academy, we have brought more and more foreign nationals into the National Academy for training as we normally train our U.S. police officials. Director Freeh has taken this on as one of his priorities, is to bring foreign national police officers in for this training.

So from that perspective, absolutely. I mean, we would have a much better sense of who we can work with because of the relationships that have been developed as a result of the National Academy training, as a result of our interaction through our legal attache program.

Certainly from that perspective, sure, we know that certain individuals, certain governments, certain organizations, are more inclined to work with us than others. So, in that sense, yes.

To be able to give you a rating, say this one is better than that one, much better, less, I am not prepared to do that right now. But certainly in our interaction with these individuals, with the organizations and these environments, absolutely.

Mr. OTTER. Let me give you an example, and maybe this—that's what I should have done in the first place. In the late 1970's, we had an operation down in Colombia in a little town called Tumaco. And Tumaco is right out on the West Coast. It was a lumbering operation. We actually bought it from another outfit, Potlatch Corp. I don't know if you can do commercials here or not. But, anyway, we bought it from Potlach, and we were operating it for a while. In fact, we were doing so well with it we decided to put in another lathe. It was a plywood manufactory, so we decided to put in another lathe.

Fortunately for us, we went to the Colombian Government, through the World Bank or IMF or some other agency. We got about $300,000 to buy this lathe. We got it down to Tumaco, which is tough to get to, and we had it on the dock. And one more $25,000 payment to the local police would have gotten it off the dock, but my boss said no. He said, once you start that, that's just a down payment. He said, we got the money borrowed there. We ended up, in fact, walking away from the entire asset, which is about an $18 million asset.

What could I have done? Now, admittedly, this is 30, almost—well, 25 years ago. What could I do today to ensure my capital sources that are willing to loan me the money for this capital, what could I do today to ensure that—anybody—what could I do today to ensure them that says my government agency, one of you folks, tells me it's going to be safe if we put it down there?

Mr. WAGUESPACK. In that particular environment, I don't know that anybody could assure you that your capital would be absolutely 100 percent safe.

Mr. OTTER. Well, let me just tell you that one of the first things I always did, if I could not borrow the money in that country, I didn't go to it.

Mr. PUTNAM. Mr. Shays.

Mr. SHAYS [presiding]. It helps to have real-world experiences.

This is a question that I would like to throw out. What is the fundamental difference between the FBI's awareness of National Security Issues and Responses—is that called ANSIR.

Mr. WAGUESPACK. ANSIR.

Mr. SHAYS. The ANSIR program and OSAC, the Overseas Security Advisory Council Program. And I specifically am interested to know, are we not duplicating efforts with these two programs?

Mr. WAGUESPACK. Let me just say from the ANSIR program, our program, as I indicated in my opening statement, is a small program. We are focused with ANSIR to provide threat and warning information through e-mail to——

Mr. SHAYS. I'm really sorry. I'm having trouble hearing you. You've got to pull the mic closer to you. I really want to hear what you're saying here.

Mr. WAGUESPACK. Our main focus is to provide threat warning information through e-mail, because we have found that is the most efficient way of getting information that needs to be gotten out in a timely manner to as many customers, subscribers, as possible. It is only a small part of the overall outreach program that the U.S. Government has. Within the U.S. Government, there are any number of outreach programs. OSAC is one of them. OSAC is a much bigger program in terms of the outreach to the private sector, especially overseas.

Our primary constituency is in the United States with the ANSIR e-mail. But it does get out internationally as we get this information out to the headquarters components of U.S. corporations here in the United States. If they have a presence abroad and they feel that the information is relevant to their international presence, then they can get the information out through their headquarters. On occasion, we will send it out directly if we have more specific information that relates to an international component of a U.S. corporation or U.S. entity.

So ANSIR e-mail is simply that, getting threat warning information out to as many subscribers who want the information and the individuals who come into us indicating that they are interested in getting this information. And we have about 30,000 subscribers currently that we send this information out to.

In addition to the e-mail, we also provide threat briefings, both classified and unclassified, to individuals, companies, corporations, that are interested in more specific, more focused briefings relative to their specific areas of concern.

So it really isn't outreach for us specifically in the United States, but it does have an international dimension as we work with these corporations that have outlets internationally, as well as working with OSAC and other entities of the U.S. Government such as the Defense Security Service, working specifically with other private sector entities like the American Society for Industrial Security. We work with them. We've gone out at the request of specific corporations, for example, giving threat briefings to companies abroad as well. So that's really our focus of our program in ANSIR.

Mr. BERGIN. OSAC, sir, is—it's international. It's a council created by then-Secretary George Shultz who recognized that there was a potential for displacing the risk back in 1985 when we had the bombings in the Embassies in Beirut and Kuwait and the Ma-

rine Barracks, that there was a potential for diverting that risk to softer targets and the American business overseas.

So when it was created, the focus was the American business abroad. And it has evolved over the years to include nongovernmental institutions, universities and educational institutions. But the focus is clearly overseas. And it's infrastructure, which consists of two diplomatic security special agents, six regional security experts who provide threat assessments to the private sector, is—which has about a $1 million budget—is centered on how can we as a government respond to the needs of the American private sector around the world?

And as a component of that is a membership which consists of 30 entities, and they range from AOL to Cargill to the Church of Latter Day Saints. But 30 of these members really are the workers. It's their council. The government is basically the steward of a council run by the American private sector, if you will. And its design is to make it safe for Americans to travel and invest abroad.

It's that simple. There is no competition. It's cooperation and collaboration. And in the 2 years that I've been the chairman of this thing, it's really—it's unbelievable, I don't like the word "synergy," but there is a multiplier effect there where people are actually networking so—and transcending competition between them all to make it safe for all of them to work overseas. But it's an overseas program, sir. It's not domestic.

Mr. SHAYS. Thank you, Mr. Chairman.

Mr. OTTER. You're the chairman.

Mr. SHAYS. I am the chairman. I had the gavel. See, if I had the gavel, I would have asked you to speak louder, and I would have gotten you to do that. I guess with the power invested in me, I can adjourn. With the power invested in me, thank you all very much, this is adjourned.

[Whereupon, at 1:10 p.m., the subcommittee was adjourned.]

○