STATEMENT

OF

FRANK J. CILLUFFO
DEPUTY DIRECTOR, GLOBAL ORGANIZED CRIME PROGRAM
CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

BEFORE

THE U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS

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

APRIL 3, 2001

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 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 "¼threatened 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.