STATEMENT

OF

FRANK J. CILLUFFO
CO-CHAIRMAN, CYBER THREATS TASK FORCE HOMELAND DEFENSE INITIATIVE
CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

BEFORE

THE U.S. SENATE

COMMITTEE ON GOVERNMENT REFORM

"CRITICAL INFRASTRUCTURE PROTECTION: WHO'S IN CHARGE"

OCTOBER 4, 2001

Chairman Lieberman, Senator Thompson, and distinguished committee members, it is a privilege to appear before you today to discuss this important matter. I would like to commend you for squarely facing this complex challenge.

In the wake of the terrorist attacks on the World Trade Center and the Pentagon, the United States is confronted by harsh realities: Our homeland is vulnerable to physical attack, gone is the sense that two oceans provide protection. But this is not only a US problem. In many ways it was a blast heard round the world, the reverberations of which will be felt for years to come.

It is widely accepted that unmatched U.S. power (economic, cultural, diplomatic, and military) is likely to cause America's adversaries to favor "asymmetric" attacks over direct conventional military confrontations. These strategies and tactics aim to offset our strengths and exploit our weaknesses.

The terrorists attacked highly visible symbols not only of our military strength, but also of our economic prowess. Though exceedingly well planned, coordinated, and executed, the comparatively low-tech means employed by the terrorists raises the possibility of a well placed bomb, a cyber strike, or worse yet a more inclusive, more sophisticated, assault combining both physical and virtual means on one, or several, critical infrastructures. The window of opportunity for implementing a comprehensive course of action that will remedy existing shortcomings is rapidly closing.

As we will never be able to protect everything everywhere all the time from every enemy – at least not in a democracy such as our own – now is the time for clearheaded prioritization of policies and resources. Unless we examine the problem in its totality, we may simply be displacing risk from one infrastructure to another. We need to approach the problem holistically, examining the dangers posed to our critical infrastructure in both the physical and virtual worlds and where they converge.

Infrastructures have long provided popular terrorist targets: telecommunications, electric power systems, oil and gas, banking and finance, transportation, water supply systems, government services, and emergency services. Destruction or incapacitation of these systems could have a debilitating effect on US national and/or economic security. This is a brief sampling of terrorist attacks on critical infrastructures intended to frame an historical context for the discussion.

Telecommunications

In 1987, the LTTE attacked a telecommunications complex north of the Jaffna tower, severely damaging or destroying the sophisticated computer systems housed there.

This was part of an overall campaign to deprive the residents of Jaffna of basic amenities, including public libraries and telephone services.

Electric Power Systems

In 1997 IRA terrorists sought to bomb 6 National Grid Group sub-stations, which would have cut off all power to the city of London and the south-east. Had this plot succeeded, it would have crippled hospitals, transportation, emergency services, and vital computer links and would have taken months to return full service. A joint operation by MI5, Special Branch, and the Anti-Terrorist squad thwarted the plan and resulted in the arrest of top IRA conspirators.

Oil and Gas

In July 1996, Scotland Yard foiled an attack by the IRA directed against gas and water plants in London. The police arrived "in the nick of time," arresting seven people and confiscating 180 pounds of semtex.

Over a year and a half period between 1997 and 1998, there were more than 160 attacks on Canadian gas wells, pipelines, and businesses. Terrorists have struck with various sorts of artillery, bullets, and bombs.

In 1999 there were 132 terrorist attacks against transportation, 16 more then the year before. Of these pipelines lead the list, accounting for 78% of the total.

The FARC and the ELN have had great "success" in targeting Colombia's oil and gas pipelines. According to the most recent State Department study, Patterns of Global Terrorism, in 2000 the ELN carried out the majority of the 152 attacks against the Cano Limon, Columbia's second largest crude oil pipeline. As a result, Occidental Petroleum had to halt exports through most of August and September.

The retarded growth of the Russian pipeline illustrates how these security concerns can severely impact not only established structures but also the development of new ones.

Banking and Finance

In 1992, the IRA bombing of London's Baltic Exchange cost three lives and caused over $1 billion in damage.

Building off of this model, they struck again in 1993, bombing London's "Square Mile, England's financial center, again inflicting over $1 billion worth of damage. This bomb, detonated over the weekend when casualties would be low, targeted British economic strength.

In April 1996, the LTTE drove a truck laden with explosives into the Central Bank in Colombo, the capital of Sri Lanka, killing 91 people.

Transportation

Air

In July 22, 1968 the Popular Front for the Liberation of Palestine (PLFP) highjacked an El Al flight. With the 1972 attack on Ben-Gurion airport, terrorists graduated from attacking airplanes to indiscriminate bombings.

With focused efforts and diligence, the number of attacks 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-terrorist operations, terrorists changed tactics, moving away from hijacking aircraft to bombing them.

Railroads and Trains

In 1995, an unknown group calling themselves the "Sons of Gestapo" derailed an Amtrak train, causing it to plunge off a 30-foot high bridge and crash into a dry streambed 50-60 miles from Phoenix, Arizona, by removing 29 spikes from the track.

Also in 1995, Aum Shinrikyo carried out their sarin gas attack in the Tokyo subway system. Not only is this attack significant because of it was an attack on the transportation but also because it was the first indiscriminate use by a terrorist organization using a chemical nerve agent.

Even threats can have a substantially disruptive effect. In April, 1997 IRA bomb threats alone shut the city of London down. The IRA detonated a real bomb at the Leeds station, without injury. They then made a series of calls using the code words designed to inform the police that it really was an IRA member on the line, and shut down the King's Cross, St. Pancras, Paddington, and Charing Cross rail stations, the Jubilee subway line, numerous streets around Trafalgar Square, Gatwick and Luton Airports were entirely closed, and Terminal Three at Heathrow was closed temporarily. In essence, the IRA managed to shut London down by the mere threat of violence.

Just last week, a bomb aboard the North East Express, traveling between New Delhi and Gauhati, India derailed seven cars and injured 100 people. Though no group had claimed responsibility, authorities believe it to have been the work of the National Democratic Front of Boroland.

Maritime

In October 1985, four Palestinian terrorists hijacked the cruise ship Achille Lauro and her 750 plus passengers. They killed American Leon Klinghoffer, and then violently threw his body and his wheelchair overboard. Egyptian and PLO officials managed to negotiate a deal with the terrorists in which they would be granted safe passage from Egypt if they surrendered the ship and her passengers. While en route, US fighter planes intercepted the plane, forcing it to land.

Piracy accounts for 28% of the worldwide violent attacks carried out against transportation in 1999, up 36% from the year before. Considering that 85% of the world's good travel by ship, those figure add up to substantial losses in a hurry.

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. The bombing of the USS Cole continues to serve as another grim reminder that terrorists will continue to probe and will strike where they can.

Also in October 2000, the LTTE mounted a well-organized attack on Trincamalee harbor, injuring 40 people and destroying two crafts by guns and a large passenger craft by explosion. These attacks are part of the overall attack and looting campaign carried out by the Sea Tigers, the LTTE's naval branch.

The fall 2000 report of the Intertagency Commission on Crime and Security in U.S. Seaports highlighted that in terms of the threat posed by terrorism "their vulnerability to attack is high" and "such an attack has the potential to cause significant damage."

Water Supply

In October 1987, a teenager threatened to blow up the Bonneville Dam on Washington state's Columbia River unless he received $15,000. An FBI agent shot and killed him. The "detonator" turned out to be a cell phone.

Emergency Services

In 1996, a Swedish man disabled portions of the US emergency 911 system in Southern Florida from his home in Goteburg.

And the list goes on. These examples only begin to plumb the depth of what we have already seen and intimate what is possible. What if the terrorists had decided to crash

one of the planes into a nuclear power plant, a liquefied natural gas plant, or an oil refinery? There would be many more potential casualties as well as the dangers posed by environmental concerns. The Nuclear Regulatory Commission stated that America's nuclear reactors would not be able to sustain an impact from an airplane used of the kind used in the September 11th attacks. Thirty-one states have nuclear power plants that supply about 20 percent of the nation's electricity supply. If one of these was hit not only would we need to deal with the interruptions of electric power, but also with the cleanup and pollution from the damaged reactor.

Bits, bytes, bugs, and gas will never replace bullets and bombs as the terrorist weapon of choice. Al Qaeda in particular chooses vulnerable targets and varies its modus operandi accordingly. They become more lethal and innovative with every attack – the first attempt on the World Trade Center, the Khobar Tower, the U.S. embassies in Africa, the USS Cole. In light of this demonstrated escalation and flexibility, we must shore up our vulnerabilities, and cyber threats are a gaping hole. While bin Laden may have his finger on the trigger, his grandson may have his finger on the mouse. Moreover, cyber attacks need not originate directly from al Qaeda, but from those with sympathetic views.

For too long our cyber security efforts have focused on the "beep and squeak" issues, and have been attracted to the individual virus or hacker in the news, often to the neglect of the bigger picture, incorporating the economy and beyond. It is time to identify gaps and shortfalls in our current policies, programs, and procedures, begin to take significant steps forward, and pave the way for the future by laying down the outlines of a solid course of action that will remedy existing shortcomings. Along these lines, there have already been a series of actions taken, some prior to September 11 and some post.

In particular, I applaud the creation of the new cabinet level Office of Homeland Security, directed by Pennsylvania Governor Tom Ridge. It is my understanding that a comprehensive review will be completed by next week, which will set out the office's roles, missions, and responsibilities. We will then have a better sense of the explicit roles and responsibilities pertaining to homeland security and how they pertain to critical infrastructure protection – perhaps most notably continuity of operations and continuity of government missions.

This attack was a transforming event. We cannot examine past precedent as to what had and had not worked before because we now have a new frame of reference, one that requires a new outlook. Because this is a top priority issue, organizational charts, titles, and line items, historic emblems of bureaucratic power, fade into the background. Governor Ridge will have the ammunition required to carry out his mission because it has the full confidence and backing of the President. But even an undertaking of this importance takes some time to move from concept to capability.

Once the immediacy of the problem has settled into routine, several months hence, we should consider codifying and institutionalizing its mission with congressional legislation and additional statutory authority if needed.

Prior to the events of 11 September, the executive branch was drafting a new National Plan and Strategy to provide guidance and direction for cyber security, scheduled for release by year's end. Likewise, an Executive Order (EO) on the same subject, entitled "Critical Infrastructure Protection in the Information Age," was near completion and efforts are underway to ensure that it jibes with the other initiatives. And, in his first National Security Presidential Decision (NSPD 1), promulgated on March 5, 2001, President Bush emphasized that national security also depends on America's opportunity to prosper in the world economy. Indeed, cyber security lies at the core of our economic prosperity, which is our "nerve center" – and President Bush and his team should be congratulated for having taking new steps on this front.

As both the Executive branch and Congress consider how best to proceed in this area, we should not be afraid to wipe the slate clean and review the matter with fresh eyes. We need to be willing to press fundamental assumptions of national security. Cyber threats and information assurance are cross-cutting issues, but government is organized along vertical lines. Though it is crucial to conduct our review with a critical eye, it is equally important to adopt a balanced viewpoint – one that appreciates both how far we have come and how far we have to go.

Fortunately, centers of excellence do exist – both in government and the private sector - and we should leverage and build on them. Only now, with the requisite amount of water under the proverbial bridge, have we amassed sufficient knowledge and experience to formulate the contours of a comprehensive cyber security strategy. It is essential that any strategy encompass prevention, preparedness and incident response, vis-à-vis the public and private sectors, as well as the interface between them.

Such a strategy would generate synergies and result in the whole amounting to more than simply the sum of the parts (which is not presently the case). Such an approach would also offer enhanced protection for the "nerve center" that is the U.S. economy.

A Brief Snapshot

Information technology's impact on society has been profound and touches everyone, whether we examine our economy, our quality of life, or our national security. Along with the clear rewards come new risks and a litany of unintended consequences that need to be better understood and managed by our industry and government leaders.

Unfortunately, our ability to network has far outpaced our ability to protect networks. The events of September 11 are a marked counterpoint to the daily

invasion through cyberspace. There is no shortage of examples of our vulnerability, based on past red team exercises. Likewise, demonstrated capabilities – fortunately, without truly nefarious intent – are also in evidence. Already, we have seen a young man in Sweden disable portions of the emergency 911 system in Southern Florida and a Massachusetts teenager disable communications to an aviation control tower.

Fortunately, however, we have yet to see the coupling of capabilities and intent (aside from foreign intelligence collection and surveillance), where the really bad guys exploit the real good stuff and become more techno-savvy. It is only a matter of time before the convergence of bad guys and good stuff occurs. We must develop the means to mitigate risk in an electronic environment that knows no borders.

Against this background, we need a true national debate on infrastructure assurance, and we need to re-think national security strategy – and, by extension, economic security and our nation's security – accordingly. It can no longer be a case of the government leading and the private sector following. In other words, Silicon Valley and the Beltway, where the sandal meets the wingtip, must stand side by side and on equal footing in addressing these issues and formulating responses.

As to the specific question of "who's in charge", this is a shared responsibility between the public and private sectors.

Building a Business Case

Government, industry, and individuals all have leadership roles to play. Cyber security and its implications for economic security represent twenty-first century challenges. Twentieth century approaches and institutions simply will not work. Instead, we need new organizations, novel management practices, and an array of new tools. Though this is not an area where government can go it alone, it can – and must – set a good example. In fact, only through leading by example can the government realistically hope for the private sector to commit the sort of effort – in time and resources – expected of them. And we need to be sure and set the bar high.

But, while government is eminently well suited to do certain things, others are best left to industry to do. Put another way, just as important as identifying what government should do is identifying what it should not do. What follows below is an attempt to put flesh on these skeletal statements in so far as they relate to cyber security and its implications for economic security.

Before proceeding to focus on sector-specific (that is, public and private) strategies, however, I would like to briefly lay out a few general guiding principles. In particular, a solid approach to critical infrastructure protection and information assurance (CIPIA) must, in my view, be centered on three "prongs," namely: policy, technology and people. Underpinning this triadic structure must be education and

awareness, and superseding it must be leadership. Without leadership, the entire structure crumbles because policy priorities are only sustained if political will and the necessary resources support them.

Improving the Public Sector's CIPIA Readiness

The starting point for the discussion here must surely be Presidential Decision Directive 63, the May 1998 directive that established the framework for tackling the critical infrastructure/cyber security issue. Among other things, PDD-63 established the National Infrastructure Protection Center (NIPC), the Critical Infrastructure Assurance Office (CIAO) and the National Infrastructure Assurance Council (NIAC), as well as identifying the "National Coordinator" (at the NSC) as the central coordinating figure for the federal government. The PDD laid out aggressive goals for improving federal systems, incident warning and analysis, research and development efforts, IT security worker skills, and cooperation among federal agencies and with the private sector. Unfortunately, this directive has proved to be long on nouns and short on verbs. Put another way, planning is everything – plans are nothing. The time has come for implementation and execution.

But planning, implementation and execution are all complicated by the fact that the government is presently organized along vertical lines – even though cyber security constitutes a cross-cutting mission. Among other things, this makes it difficult to assure accountability. Against this background, we need to streamline and re-adjust the workings of our public sector, and coordinate its constituent components so as to increase efficiency, clarify responsibilities and heighten accountability – all the while bearing in mind that outreach to the private sector is equally critical.

Successes enjoyed to date were often in areas without significant budgetary implications or where the need for change was so compelling that some work had to be accomplished. Without strong budgetary authority residing in the National Coordinator, many important items could not be accomplished and, among other things, this made it very difficult to assess responsibility or accountability when CIPIA readiness failed.

On a positive note, the Department of Defense (DOD) and Intelligence Community have established a level of information assurance readiness that is typically much more mature then their civilian agency counterparts. This is to be expected, as they have experienced the impact of cyber attacks over the past decade and experienced many of their own vulnerabilities. The rest of the federal government will continue to benefit from these DOD experiences and the solutions that DOD has crafted for itself. These provide building blocks for the government to develop its cyber security strategy.

The government must lead by example. Without first having its own house in order, it cannot provide the private sector with the necessary support or encouragement essential to promoting strong CIPIA. Seven recommendations for action in the federal government follow. [1]

(1) Leadership. Critical to the federal government effort is having at its apex a single individual or group endowed with the requisite powers and responsibilities to make the system work. To this end we need to appoint a senior government official with clout or "teeth" - that is an Assistant to the President for Information Security – whose efforts are supported by the White House. This senior official would have a small staff and use an interagency working group to coordinate federal agency efforts and programs. This position should be confirmed by Congress and among other things would be empowered to issue directives regulating the security of federal agencies IT systems; would hold budget review authority on those portions of a federal agencies budget concerning information technology or critical infrastructure to ensure sufficient security funds are requested; and would conduct audits/assessments to ensure federal agency accountability and adherence to IT security standards. This senior official would be responsible for reporting to the President, and to the Congress, on the performance of individual agencies.

In addition, this senior official would be responsible for developing an annual plan to identify crosscutting issues, have a limited budget to begin to develop crosscutting government-wide solutions, and ensure sufficient research and development efforts are undertaken.

The foregoing proposal, with its centralizing features, is intended to streamline and replace the myriad of structures that currently exist. Notably, a similar motive apparently underlies the Executive Order that is currently being formulated. There is a good chance that the EO will establish some sort of a board, including a number of federal agencies and organizations, with a chair and a vice chair from the private sector, with an eye towards clarifying and delineating responsibilities in the area of cyber security, and heightening accountability. This may have two chains of command – one through the National Security Advisor and the other through the Director of the Office of Homeland Security.

(2) Risk Mitigation. A key element in improving the computer security of federal agencies is the need to rapidly respond to incidents or threats and repair known software faults. The federal government must implement a system to provide real time information assurance vulnerability alerts to system administrators, identifying possible attack techniques or targets and known threat ISP addresses. This system, which could leverage the less robust FEDCIRC system already in-place at GSA, must be fully connected to the defense department, intelligence, and law enforcement

warning systems and must also maintain good communications with private sector operated warning centers.

An equally important risk mitigation effort in the federal government is the efforts to rapidly identify, distribute, and install software "patches" which are developed by vendors to correct known flaws in operating system codes. The time period between the distribution of the patch by the vendor and the installation of the patch by the system administrator is the most vulnerable time for an operating system, and the pace of this installation must be increased. Additionally, the federal government must work hard on the development of automated tools to help with both vulnerability alert distribution and automated pact identification and installation.

Finally, to evaluate the effectiveness of the security management and risk mitigation efforts at federal agencies, the central office or board could have an "expert review team" at its disposal. This "red team" of 20-25 personnel with the requisite technical skills, could be used to evaluate the cyber security over federal agencies and provide feedback (government-wide) on the "best practices" and common vulnerabilities they encountered.

In fact, I would go so far as to suggest that there ought to be required, by law, an annual test of each agency's vulnerabilities and capabilities (with the latter assessing their ability to respond to events). Further, based on the results of the annual testing process, we could derive baselines that would be applicable across the board, so as to hold all agencies subject to the same standard of account.

(3) Warning. A critical step towards coordinating federal agency readiness and preparedness efforts is the construction of a centralized intrusion detection and warning center. Again, the FEDCIRC system could serve as a basis for this system, but would require significant increases in personnel, and budgetary and policy authority. This center would serve a number of critical functions; it would provide indications and warning of an impending attack for all federal agencies; it would employ a federal agency "infocon" system to establish readiness and preparedness levels on federal agency information systems; it would house a cyber incident response team to assist agencies in incident management; and finally the center could play a crucial role in the implementation of information assurance vulnerability alerts and software patch alerts mentioned previously. This center would serve non-DOD federal agencies, and would work with and parallel the efforts of the Joint Task Force Computer Network Operations that DOD has successfully employed for the past three years.

(4) Standards. The federal government needs to improve its standards in both the management of information security systems and the procurement of information technology systems. In the area of security standards management, federal agencies have requirements established in numerous documents including OMB Circular A-

130 and several laws. The missing ingredient has been a strict auditing and assessment system to enforce these standards. Specifically, OMB has never been properly manned to implement and enforce such an assessment system. Frequent audits by GAO have demonstrated that, in the absence of a tool to hold them accountable, federal agencies have routinely failed to meet the standards laid out in A-130. If the senior official called for above is given some budgetary review over agencies IT programs, he will have the tool to enforce audit and assessment findings, which would be conducted by the "red team" mentioned above. It would also be beneficial if the results of the audits were provided to the President and Congress as a "report card" to help keep the pressure on federal agencies senior leadership. In the absence of this pressure, many agencies do not treat information security as a critical or core agency mission.

Information technology system procurement standards are another key public sector shortfall. The government needs to have (or work with) a laboratory in which IT products undergo a review and validation process, from which GSA will then provide a list of acceptable products for federal agencies to procure. In the absence of such a procurement standard many federal agencies continue to install information technology equipment with little or no security components installed.

(5) Training and Education. There are numerous components of information assurance training and education that the federal government must continue to push.

First, the public sector needs to raise IT security awareness among the general federal workforce. This includes the use of effective security techniques (i.e. passwords) and the need to limit access to IT systems without proper clearance. This awareness training needs to be conducted on a recurring basis, and be tied to an employee's computer access.

Second, we need to continue to train and certify our federal IT security workforce, and to the extent that this mission is out-sourced, ensure that the contractor workforce meets the proper training and certification standards for operating federal systems. Fortunately these training and certification programs are easily available in the private sector, and require very little tailoring for federal government use.

Third, we need to continue to recruit and develop a skilled and "current" IT security management workforce. While IT security managers compose only a small percentage of our federal workforce, these specialists are a rare group of worker and one in great demand in the private sector as well. The Clinton Administration's "Cyber Corps" program was a step in the right direction, identifying and developing university information assurance programs, and recruiting students directly from those few existing programs with scholarships for federal service. An unexpected challenge has been the small number of existing information assurance programs, and the even smaller number of students who were U.S. nationals and thus available for security

clearances and federal service. Efforts to develop academic programs, and grow a generation of faculty, need to be closely coordinated between the government, universities, and the private sector, as all three will ultimately benefit from it's success.

From the government's perspective in particular, the aim would be to attract the best and the brightest to public service for at least a portion of their careers. Unless we succeed in doing so, in the long run, our national security will suffer. Put another way, recruitment and retention are, for the public sector, issues as pressing as education and training.

To retain a trained and educated IT security workforce the federal government will have to evaluate its retention and pay packages, for these workers are in heavy demand outside the government as well. We need to introduce reward programs that would not only lay out a promotion path but also establish recognition mechanisms separate from promotion (as was done in Y2K), and we need to revisit the pay scales for these relatively rare but highly prized information security experts.

(6) Reconstitution. One area where little headway has been made is the effort to identify public sector information systems, and determine how they will be rapidly reconstituted following a successful cyber attack. This involves not just the federal systems that support our core agency missions, but also the private sector communication and power systems on which the federal systems depend as well. This reconstitution effort raises challenging questions of public – private sector cooperation and coordination that may involve the Defense Production Act and similar legislation. This effort may also identify single points of failure and needed remedies that could have significant budget implications; as such more aggressive attempts to tackle the challenges of reconstitution problem are warranted.

(7) Research and Development. The federal government is only a small player in the development of next generation information technology systems. However, in the area of information security systems the work at the DOE Labs and DARPA is still the cutting edge effort. As such, the public sector's R&D efforts are crucial to developing the "next generation" of IT system security, and we must continue to ensure that the DOE and DOD budgets provide a healthy environment for the labs to work in. Additionally, the NSF funds much of the university-based IT research that is looking at the "generation after next" and can therefore impact the consideration of security in those systems.

But the Government is not alone in this endeavor. The private sector is an indispensable partner in protecting critical infrastructures.

The Private Sector: A Crucial New Partner

The benefits from improving the CIPIA readiness of the Private sector are two-fold. First we improve the resilience of our economic infrastructure to cyber attacks and second, we improve our federal government's readiness, because so many critical government functions are conducted on privately owned and operated telecommunication, information and power systems.

Several important steps can be made by the government to support the private sector's CIPIA efforts.

(1) Encouraging Standards. Government can – and should – also provide specific incentives to the private sector to better protect its own systems. For instance, government could act as the catalyst for the establishment of industry-wide standards for information assurance in different business sectors, and could establish liability limits against disruption of service for companies using security "best practices." Equally, tax breaks or equivalent "credits" could be accorded to companies that use certified safety products and enforce specific types of security procedures. (The mechanism for certifying the safety and effectiveness of security products should be the consensus product of a private-sector dialogue that government should facilitate).

(2) Information Sharing. Government could also grant relief from specific provisions of antitrust laws to companies that share information related specifically to vulnerabilities or threats. Notably, the Freedom of Information Act (FOIA) has been a significant obstacle to public-private information sharing to date because companies run the risk of having sensitive or proprietary data compromised if it is revealed to the public, and fear damage to shareholder confidence if vulnerabilities are publicly acknowledged. Fortunately, FOIA-related obstacles are now being recognized and addressed. Senator Bennett in particular, should be commended for his leadership in this area.

(3) Liability Relief. Furthermore, government could provide extraordinary liability relief to the private sector in the case of cyberwarfare (similar to the indemnification authorities set up in the case of destruction of commercial assets through conventional warfare). Financial relief for digital disasters would have insurance companies insuring to a certain level, with government intervening in cases of massive outages or shutdowns. Likewise, a consortium of insurance, software and hardware companies could create a pool for reinsurance purposes.

Although quantifying risk in the cyber area is difficult because of the lack of experience and actuarial data, insurance companies should be encouraged to include in their portfolios limited liability indemnification policies against cyber disruption. Here, government should be the catalyst, not the enforcer, for the creation of parameters and standards.

(4) Partnering with Federal Government. In addition to "incentivizing" the private sector in the ways outlined above, government should seek to solidify partnerships between the public and private sectors. Already, under the auspices of the CIAO, the Partnership for Critical Infrastructure Security has brought together hundreds of leading corporations and various federal agencies to address the problems of infrastructure assurance. This is a good example of a step in the right direction – but we need to do more.

By way of illustration, we should try to improve public-private cooperation through information sharing on: vulnerabilities, warnings of ongoing attacks or threats, hacker modus operandi, and solutions and defenses to established threats and attacks. In doing so, we should try to learn from our experience with the National Infrastructure Protection Center (NIPC), which was not always successfully viewed as the entry point for private sector cooperation with the government. Looking to the future, we should aim to leverage the NIPC's strengths, its ability to conduct complex cyber incident investigations and enforcement. At the end of the day, the NIPC, as an initiative, represents a good start – as a central focus for law enforcement and incident analysis, but not the central point for all forms of private sector cooperation.

Cross-sector cooperation on information sharing is especially important because each sector has its own comparative advantage: whereas government possesses the core insights on CIP from a national security perspective, the private sector possesses the core insights on information security management. With this in mind, government should continue to assist the private sector by interacting constructively with information sharing and analysis centers (ISACs), which are sector-specific associations on the industry side, and by continuing to facilitate cyber security discussions within these various sectors (including banking and finance, telecommunications, and information technology).

Key Issues and Challenges

The suggestions above are not exhaustive, of course. And, even if it were possible to cover the field, it must be conceded that no matter how concerted our efforts are, there will be failures, whether in the public or the private realm. For this reason, reconstitution and business continuity (that is, the restoration of essential systems and services) is a matter that we cannot afford to ignore. Indeed, continuity of operations and government may be the key to deterrence: if we can restore our systems and provide business continuity in relatively short order following an attack, the incentive to engage in further attacks of the same sort in future should be diminished. Now more than ever, the public and private sectors need to work together to ensure our nation's continued health and vitality. The private sector needs to appreciate its role in protecting our nation and visa versa.

The Internet truly became an invaluable tool during and after the 11 September terrorist attacks. It proved a valuable tool for the government to disseminate vital information and for businesses to continue functioning. FirstGov.gov fashioned a special section to provide information to the public in the form of links to relief services, status updates, and federal and private organizations providing public response and recovery services. The FBI established channels to receive information regarding their investigations on their website. Concerned citizens created a website where people could post and people one could check on the status their loved ones. Numerous charities are able to receive and disseminate funds to those who need them. The media reported that more than a third of the money received by the American Red Cross, or pledged to it by donors, came over the Internet. The Internet did what it was designed to do – facilitate communication – and in so doing clearly demonstrated its significance. In the midst of the physical turmoil, the virtual world continued to function. However, there may be a dark side.

Stories abound about al Qaeda's use of the Internet – the full extent of which is not yet known. Reports claim their cyber tradecraft ranged from the highly sophisticated, like steganography, to the comparatively innocuous, like code words or phrases. An email reminding someone to "walk the dog" could have been a covert signal to proceed with an attack. No amount of computing power or code breaking could have tumbled that clue. We do know that in the past their techniques have involved a combination of both high-tech and low-tech means of tradecraft and communication.

Our policies in response to threats of any kind, moreover, must not stifle the engines of innovation that drive our economy and enhance our lives. Unfortunately, we have been trying to prosecute 21st century crimes armed only with 19th century laws. This must change and I applaud Congress efforts to empower our federal agencies with the needed statutory authorities.

Now more than ever, we cannot afford to overreact or put up too many virtual or physical walls or the bad guys win by default because we have lost our way of life. The cure must never be worse than the disease – undoubtedly the benefits outweigh the risks.

In particular, some seem to think that privacy, security and electronic commerce are mutually exclusive. This is just not so. The "game" is not zero-sum: we can – and should – ensure privacy, security and e-commerce. Indeed, it would be fair to state that you cannot have privacy without security, and without security, e-commerce will never flourish.

At the end of the day, it all comes down to leadership -not only in government, but in the private sector and on the part of individuals, too. President Bush, and his team, deserves much credit for piloting the ship of state through these roiling waters.

America rests easier knowing that he is at the helm and is charting our course. And we are grateful to the other world leaders who stand with us. But make no mistake, we are in the eye of the storm. Fighting terrorism will take not only new strategies and new tools, but also the old grit and determination that have been America's historical reactions to unjust aggression and war.

In political terms, some of the difficult battles are still to come. Combating terrorism - in all its forms - requires a sustained campaign. This campaign will continue to demand united support for years. While I hope that the intense focus of the spotlight shifts away from the issue soon, I urge Congress to continue its unified efforts on this front.

That said, while the president and Congress have already demonstrated political will on this matter - and I say this will all sincerity - that alone will not be enough. We all share responsibility for this issue and we must all muster the will, and be prepared to contribute the resources, to deal with it. Plainly, the challenges that we face are great. But we, as a nation, are up to the task.