Statement for the Record

John T. Sabo
Director, Global Government Relations, CA, Inc.
and
President, Information Technology-Information Sharing and Analysis Center (IT-ISAC)

Before the

Committee on Oversight and Government Reform
Subcommittee on Information Policy, Census, and National Archives
United States House of Representatives

Tuesday October 23, 2007
2:00 p.m.
Rayburn House Office Building, Room 2154

Mr. Chairman and Members of the Subcommittee

I am John Sabo, Director of Global Government Relations for CA, Inc., one of the world's largest software companies. I represent CA in a number of security and privacy-focused industry organizations including serving as the President of the Information Technology-Information Sharing and Analysis Center (IT-ISAC) and as a member of the IT-Sector Coordinating Council. I also serve as Chair of the ISAC Council, which addresses cross- sector information sharing issues.

I am here today in my capacity as the elected President of the IT-ISAC. On behalf of the IT-ISAC and its members, I want to thank you for the opportunity to share our thoughts on these critical issues.

Before I begin the substance of my testimony, I want to acknowledge and thank Assistant Secretary Garcia for his leadership. The Office of Cyber Security and Communications, specifically the National Cyber Security Division (NCSD), have been very supportive of our efforts. Indeed we have an excellent relationship with Greg and his team. Our challenge - and our goal - is to achieve similarly strong relationships with other parts of the Department of Homeland Security which also have operational responsibilities impacting the IT sector.

The Information Technology Sharing and Analysis Center (IT-ISAC)

An ISAC is an information sharing and analysis center. It provides a trusted, collaborative, information/intelligence sharing and analysis capability for critical infrastructure owners and operators. ISACs enable industry experts to establish working relationships, build trust, share sensitive vulnerability, threat, and mitigation information, conduct informed analysis, and collaborate with other sectors and government in an organized manner. The most advanced ISACs, such as the IT-ISAC, maintain operations centers, have multi-layered capabilities in terms of situational awareness and incident response, and have mechanisms in place to ensure the protection of sensitive information. If there is a single unifying vision across the ISAC community—and we do have a community and a Council—it is the continuing belief that, through our collaborative efforts and application of subject matter expertise, ISACs can prevent loss of life and economic value that would result from attacks against America's Critical Infrastructures.

The IT-ISAC was founded in 2001, after several years of development stemming from the discourse on Critical Infrastructure Protection (CIP) following the President's Commission and Report in 1998, the issuance of PDD-63 in June of 1998, and the accelerated interest in CIP during the Y2K era. The IT-ISAC is a non-profit organization which provides robust and trusted ISAC functionality for the IT sector. Our members include major IT corporations: BAE Systems IT; CA, Inc.; Cisco Systems Inc.; Computer Sciences Corp; eBay, Inc. Ernst & Young; EWA-IIT, Inc.; Harris Corporation; HP;

IBM; Intel Corporation; Juniper Networks; Microsoft Corporation; National Datacast, Inc.; Oracle USA, Inc.; Symantec Corporation; Unisys; USi, Inc.; and VeriSign, Inc.

Our central mission is to help protect the Information Technology infrastructure that propels today's global economy by identifying threats, vulnerabilities, and attacks on the infrastructure, and working in a trusted and collaborative environment to perform the analysis necessary to quickly and properly address them. The IT-ISAC shares information and intelligence with other sector-specific ISACs, U.S. CERT and with other government agencies.

The IT-ISAC also addresses physical threat issues affecting member company operational facilities and interdependencies, and has a growing capacity to share information associated with both physical and cyber issues enabling member companies to take appropriate action in response to threats and imminent attacks.

The IT-ISAC represents a significant, ongoing investment by the IT companies who are its members. IT-ISAC operations and operations center, security controls, Web site and communications protocols are entirely funded by member company dues. Additionally, the IT-ISAC relies on the dedicated commitment of member resources and expertise for analysis, collaboration, planning, and operational policy development.

The IT-ISAC extends its resources to support other sectors on cyber security issues, for example by initiating daily cyber security calls with as many as nine other ISACs (such as water, surface transportation, public transit, multi-state and financial services) and US CERT. We also work collaboratively as a member of the IT-Sector Coordinating Council (IT-SCC), where the IT-ISAC is formally represented on the Executive Committee. This in turn provides access to the valuable cross-sector policy work of the Partnership for Critical Infrastructure Security (PCIS), which is the umbrella policy organization across all SCC’s. The IT-ISAC is also a member of the ISAC Council, which currently includes 13 ISACs, enabling us to address operational issues of common concern and value across critical infrastructure sectors.

All together, the trusted relationship among our members; the routine collaboration among them, our operations center, and other sectors; the expertise that resides within our member companies; and our mission of protecting the Internet Infrastructure provide the motivation and the capability to collectively address our sector’s operational responsibilities on cyber security. We take this responsibility seriously, and have been recognized by both the IT Sector Coordinating Council and the Department of Homeland Security’s National Cyber Security Division, our IT Sector Specific Agency, as the operational arm of the sector.

The Embedded Internet

The United States has always recognized the unique role communications plays in ensuring the national security and emergency preparedness posture of the country and protecting its citizenry. Telecommunications systems are also very robust – but for more than a century they have planned, practiced, and prepared for recovering and reconstituting operations. In the aftermath of the Cuban Missile crisis and during the height of the cold war America took steps to bolster its plans and programs to support the recovery and reconstitutions vital to it economy, security, and defense.

Likewise, the criticality of the Internet must receive equivalent attention. The Internet has become part of the DNA of the modern economy. It is vital to communications, commerce, and defense of every developed nation. Internet "true believers" are sometimes dismissive of catastrophic scenarios that could result in serious degradation or Internet interruption. Despite the fact that the Internet has proven resilient in the face of both physical and cyber incidents, we should not ignore the imperative to plan for events that exceed our current understanding of threats. History often proves us wrong and surprises us with the "unthinkable."

However, unlike in the Telecommunications sector where there is a long history of collaboration, cooperation and coordination within industry and government on emergency preparedness, response, and national security issues, there is a growing concern that the U.S. lacks key capabilities for recovering and reconstituting Internet functions in the event of a catastrophic disruption. The Government Accountability Office (GAO) and the Business Roundtable have both released reports expressing significant concerns about the ability of the nation and its largest corporations to respond to and recover from a significant Internet failure in an effective and efficient manner. The table below summarizes some of the significant and systemic challenges to recovering or reconstituting key internet functions in a crisis.

Table 1: Report Summaries on Internet Recovery Challenges

RECENT REPORTS	INTERNET RECOVERY CHALLENGES
Government Accountability Office: *INTERNET INFRASTRUCTURE: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan (GA0-06-672 and GAO-06-1100T)* June/September 2006 http://www.gao.gov/new.items/d06672.pdf and http://www.gao.gov/new.items/d061100t.pdf	Key challenges to establishing a plan for recovering from an Internet disruption include (1) innate characteristics of the Internet (such as the diffuse control of the many networks that make up the Internet and the private-sector ownership of core components) that make planning for and responding to disruptions difficult, (2) lack of consensus on DHS's role and when the department should get involved in responding to a disruption, (3) legal issues affecting DHS's ability to provide assistance to entities working to restore Internet service, (4) reluctance of many in the private sector to share information on Internet disruptions with DHS, and(5) leadership and organizational uncertainties within DHS.

Business Roundtable, Two Reports: *Essential Steps to Strengthen America's Cyber Terrorism Preparedness* June 2006 http://www.businessroundtable.org/pdf/20060622002CyberReconFinal6106.pdf **-----------------------** *Growing Business Dependence on the Internet: New Risks Require CEO Action* September 2007 http://www.businessroundtable.org/pdf/Security/BR_Internet_Business_Dependence_Report_09252007.pdf	* Inadequate early warning system – The US lacks an early warning system to identify potential Internet attacks or determine if the disruptions are spreading rapidly. * Unclear and overlapping responsibilities – Public and private organizations that would oversee recovery of the Internet have unclear or overlapping responsibilities, resulting in too many institutions with too little interaction and coordination. * Insufficient resources – Existing organizations and institutions charged with Internet recovery should have sufficient resources and support. For example, little of the National Cyber Security Division's funding is targeted for support of cyber recovery. -- * Internet dependence – CEO's need to address this as a major risk. Recommendations include making cyber security a CEO-level issue, addressing it in more complete business continuity plans, improving communications with industry partners and government, and participating in ISACs in sectors where ISACs are operational.

Industry-Government Planning Process – Operational Goals

The cautionary findings of those reports are largely correct. However, we have already started working to address them, in most cases in collaboration with the government and those who depend on the Internet.

The IT Sector's strategy is outlined in the IT Sector Specific Plan (IT SSP), which many of my colleagues in both the IT-ISAC and the IT-SCC collaborated with NCSD during the drafting process. The IT SSP is designed to provide a framework on how to enhance the security of the IT Sector. At the heart of this plan is the need to protect key IT sector operational functions (as opposed to specific physical assets). The plan focuses on enhancing national capabilities for

(1) Prevention and protection through risk management
(2) Situational awareness, and

(3) Response, recovery and reconstitution of America's information technology infrastructure.

It is appropriate to point out at this point that many of the individuals who are Board members or other leaders in the IT-ISAC also hold positions of trust in our Sector Coordinating Council. While participating in many IT-SCC policy efforts, they bring the views and expertise of the IT-ISAC to the table. These interlocking relationships help provide consistency in vision across the policy and operational components of cyber security issues and enhance the visibility of these issues with our government colleagues.

During the development of the IT SSP, government and industry participants, including many experts from the IT-ISAC membership, identified key challenges that need to be strengthened to achieve the sector's goals. Four of these challenges impacting response and reconstitution are shown in the following table.

Table 2: Critical Challenges and Needed Capabilities (source IT SSP)

Critical Challenges	Needed Capabilities
Robust Coordinated Response Capabilities	The capability to respond to and recover from a nationally significant event is critical to promoting the resilience of the IT Sector and other CI/KR sectors. An all-hazards operational response and recovery capability is needed to bring public and private sector security partners together to coordinate activities. Emergency communications, collaboration, and analytical tools could enhance effective response; this may include bolstering existing public and private sector resources and capabilities.
Reconstitution of Communications Services and Networks	A protective program initiative may be developed to assist with implementation of Federal Government authorities under Section 706 of the Communications Act applicable to key Internet functions. This program should also include developing the plans, programs, and mechanisms for identifying and refining requirements and developing reconstitution capabilities.
Reconstitution of Data	Data reconstitution tools and techniques are needed to ensure the integrity and availability of data. Development of a protective program should be linked closely to R&D activities designed to develop and pilot capabilities that enable key public and private sector systems to reconstitute rapidly data that could be corrupted, either intentionally or unintentionally.
Out-of-Band Data Delivery Capability	A protective program initiative is needed to provide mechanisms for delivering patches and other software to critical users if key Internet/network functions are not available. Such programs could include procuring space on satellites or unused television spectrum for moving software (e.g., critical patches or software) to key sites during a crisis or network congestion/failure.

I will briefly discuss some of the issues associated with these challenges and needed capabilities.

Strengthening Response Organizations

A key element of responding to attacks on the Internet Infrastructure is ensuring that we have organizations within industry and government with the collective expertise to organize a response to and effectively manage an incident. Development of this response capability is concomitant to the IT-SSP planning process, but is a distinct component. However, a recurring frustration for many of us in the operational space is the disproportionate amount of resources and energy DHS expends, and to which industry contributes, in a continuous planning cycle compared with the quite limited focus and resources allotted to implementing the plans and supporting operational capabilities. We recognize the value of participation in the policy and planning process, and have made significant contributions working via the IT-SCC, but we strongly believe there must be an equivalent commitment to implementation. As President Eisenhower once said as a General, “In preparing for battle I have always found that plans are useless, but planning is indispensable.”

There are specific actions government can take, consistent with existing plans, to leverage and enhance the value of the operational capabilities of industry’s and government’s information sharing and response capabilities.

- **Leverage the expertise within the ISACs on a more consistent basis**. The ISACs work on operational issues on a daily basis. For operational purposes, DHS should leverage the expertise within these organizations, instead of consistently turning to policy councils. When there is a fire in your town, you don’t call the city council – you call the local fire department or 911 emergency number. Unfortunately, some DHS components routinely bypass sector-designated ISACs and do not make use of their information sharing capabilities or work with them on operational matters. These practices must change in order to reflect sector decisions.

- **Stabilize US CERT:** The US CERT cannot play its intended role if it lacks the necessary resources – people, expertise and budget to do the job outlined in both the Cyber strategy and HSPD 7. The US CERT’s effectiveness is first and foremost dependent upon its people. The loss of the US CERT director and other departures of key staff concern industry and create uncertainty about the stability of the partnership planning and operational understandings we have reached.

- **Increase Funding for US CERT:** The US CERT budget should be examined to see if it is actually in scale with its overall mission. Congress may want to consider fencing off the US-CERT budget – which supports a national mission -- so that it cannot be taxed by other parts of DHS for non cyber related activities.

- **Define and Clarify the Role and Relationship Among the US CERT and other DHS Analytical Entities:** We question use of the Homeland Infrastructure Threat and Risk and Analysis Center (HITRAC) - which has minimal cyber expertise – to develop threat cyber-focused reports that, unlike HITRAC physical threat reports and analysis, have limited value. Although the cyber threat analysis and reporting are vital, that responsibility would appear to be more appropriately undertaken by the US CERT working with their industry partners. At a minimum, the relationship among US CERT, HITRAC and other DHS analytical entities needs to be evaluated, defined and improved.

- **Actively Encourage Companies to Join the IT-ISAC.** The Business Roundtable released a report last month that listed joining and participating in industry specific ISACs as one of five key recommendations for the business community.

The government should recognize this as a best practice, and, as such, encourage IT Sector companies to actively participate in the IT-ISAC as well as follow in its spirit by using functioning ISACs such as the IT-ISAC for operational matters.

- **Support the Cross Sector Operationally-Focused ISAC Council in the Same Manner that it Supports the Cross- Sector Policy Entity (PCIS).** Much as the PCIS provides a forum for the sector coordinating councils to collaborate on cross-sector policy issues, the ISAC council, with 13 ISACs as active participants, provides a forum for sector specific operational entities to collaborate, share information and best practices, and develop and coordinate operational policy issues. This work is critical in fostering increased, effective sharing of information and intelligence across sectors and enhancing our ability to improve situational awareness and incident response.

  Although DHS support enables a contractor to host four meetings a year at their facility, for which the Council is appreciative, we believe that some DHS resources should be directed to support the substantive information sharing initiatives fostered by the Council which are carried out by ISACs. As an example, the ISAC Council has initiated a set of tangible projects involving improved emergency communications contact lists and information sharing product inventories which can have great benefit for the sectors and government, but are being done as volunteer efforts. DHS support for these as well as for the Council's "Framework for Information/Intelligence Sharing," formally provided to DHS in October 2006 and endorsed by the PCIS, would have great utility for our operational partnership.

- **Provide More Detailed and Frequent Briefings to Owners and Operators, Through the ISACs**. The ISACs include members who have employees with security clearances at all classification levels. In fact members of the IT-ISAC have taken advantage of a DHS program to support clearances at the Secret level for industry cyber experts. This makes sense, because under the NIPP, the ISACs and other sector designated operational arms are responsible for analyzing and sharing information about threats to specific sectors. Given the clearances held by many of our industry experts, DHS should have in place a regulararized program to brief operational staff. However, DHS typically organizes such briefings for policy representatives, and not ISAC members - operational experts who are positioned to address the specific operational threat or security issue that was discussed. As one example, in August DHS hosted a classified briefing on the National Intelligence Estimate. The ISACs were not invited to that meeting. Although we requested the same briefing for the ISACs and our members, neither the briefing nor a plan for regular ISAC briefings has yet been made available.

Information Technology and Telecommunications Convergence

The *National Strategy to Secure Cyberspace* – Which was recently reaffirmed by the by the White House in its *2007 Homeland Security Strategy* – stressed the need for a

National Cyberspace Security Response System. We believe that with convergence between traditional "IT" and "Telecommunications," it is important to build a joint, robust response capability that enables government and industry to work cohesively to monitor the integrity of and protect our cyber infrastructure.

As an initial first step, we welcome the physical collocation of the U.S. government's cyber and telecommunications watch-and-warning centers, the US CERT and NCC watch, on a common floor in a common building. Assistant Secretary Garcia has invited the IT-ISAC to have representation in this facility, and we look forward to working with his staff to make this happen as quickly as possible and to move beyond collocation toward a truly merged and integrated watch, including enhanced industry participation.

This initiative, directed by Assistant Secretary Garcia in collaboration with industry, represents precisely the kind of leadership that DHS is capable of bringing to address new operational requirements while leveraging ISAC capabilities.

Infrastructure Reconstitution

The IT-SSP highlights a critical need to develop capabilities to reconstitute data. We are not just dependent on access to the Internet to communicate, conduct commerce or defend ourselves – we are dependent upon data. Experts conceive of attacks that would seek to disrupt critical national functions by corrupting select sets of data in a particular sector or in critical points of the economy. The large scale disruption of data may not be a sudden event but may unfold slowly over a period of days and result in economic dislocations or service degradations that could rival more traditional cyber or physical attacks. The U.S. currently has no unclassified programs or efforts that have been shared with the IT-ISAC about how they are prepared to assist the private sector in the event that such an attack were to occur.

The reconstitution of the physical and logical elements essential to the Internet is, also critical. The current National Response Framework (NRF) attempts to address this with the Emergency Support Function 2 and the Cyber Annex. ESF 2 is largely concerned with the roles and responsibilities of the U.S. government's agencies in dealing with restoration of National Security/Emergency Preparedness (NS/EP) critical services provided by regulated wireline carriers and identifies the process they will use to prioritize service requirements. However, it is not clear that same processes would adequately support the IT networks' packet-based communications environment.

The NRF's Cyber Annex appropriately recognizes challenges that response entities will have to deal with when managing complex incidents. However, the cyber annex does not fully address key response challenges such as:

- Designating which public sector agency the private sector would turn to if it needed specialized equipment to be prioritized. Would they go to the Department of Commerce and ask the National Telecommunications and Information Administration (NTIA) to sponsor it through the Defense Priority Allocation

Service process that executes Defense Production Act authorities? Or would the sector turn to its Sector Specific Agency, the NCSD?

- Describing how industry and government would come together in response to a crisis. As with other ESFs and sector annexes, the Cyber Annex should outline procedures and protocols for response actions necessary to maintain connectivity, analogous to the proscriptions to agencies in the ESFs. The annex should define a high level organizational model that the private sector can use as a basis for an operational plan, including a robust communications protocol. For example, if the Critical Warning Information Network (CWIN) or some other means is deemed to be the key mode of communications in response to an event, then it should be stated explicitly and a Concept of Operations developed in concert with the IT and Communications sectors.

- Detailing how government agencies will support and work with the private sector in the event of a catastrophic cyber incident.

- Responding to cyber events that cause substantial national disruption, but still not meet the threshold for a Stafford Act declaration.

Out-of-Band Data Delivery to Ensure Internet Recovery Capabilities

In the event that there were a serious event that degraded key Internet functions and prevented critical infrastructures and critical government agencies from receiving patches or emergency software updates/programs through the Internet, the options for distributing the critical software updates as well as accompanying information are not attractive. Putting people in cars with boxes of compact disks and physically distributing software may be the ultimate fall-back distribution method, but it has obvious disadvantages. While such a solution might work for an individual enterprise or a small set of customers located in close proximity, it is not an acceptable solution for an Internet dependent nation.

Government's role is to ensure that an appropriate operational environment exists to support the recovery of the Internet. The government has done this for voice communications. Through the National Communications System, the government has maintained various programs designed to ensure wireline and some wireless communications in crisis situations and reconstitution of capabilities in the event of the loss of service or infrastructure. There is no tool that will facilitate the recovery of critical Internet functions. CWIN has been rolled out to some operations centers in the private sector, but its deployment is limited, there is no current operational Concept of Operations (CONOPS) for its use in the context of the ISAC community, and there is currently little confidence that this system would be usable in a real crisis, although we understand that work is underway to evaluate CWIN and its operational utility.

The IT SSP identified high level needs for a system that would allow the dissemination of software and recovery information when the network was disrupted or un-trusted. From the IT-ISAC perspective, I would like to provide some thoughts on the key attributes that a successful out-of-band solution should:

- Be identified and tested by both government and the private sector;
- Be technology neutral, long-lasting and supported by the private sector.
- Leverage existing infrastructure that can reach both densely populated urban centers as well as remote critical infrastructure facilities.
- Have a CONOPS developed by government and industry, integrated with ISAC CONOPS, and be tested regularly.
- Enable industry, which will be providing the software patches and programs, to have authenticated and trusted access to the system.
- Have a clear and easily understood set of protocols.

If designed properly, such a system would be utilized in response to a widespread internet disruption, but could also be useful for other types of challenges stemming from concerns such as pandemic flu, or catastrophic physical events such as Katrina. A well-designed internet recovery backup communications system could assist public-private interests by providing flexible response options that could be valuable for response in many types of incidents.

With respect to all of these initiatives, a key responsibility is operational readiness and measurable performance. Tests, drills, and exercises are critical to readiness. The Cyber Storm series of exercises has proven to be very valuable for the IT-ISAC, and other organizations that participated in them. Planning for Cyber Storm II is well underway, and I encourage other elements within DHS that conduct exercises to use the Cyber Storm II planning processes as a model. However, we should not wait for major annual or bi-annual exercises before testing our response capabilities. We should train and conduct drills on a routine basis to test our capabilities and update our procedures. In fact this is one of the areas where the ISAC Council has focused.

Bring Balance to Operational Priorities

Finally, I want to re-emphasize that the gap needs to be closed between DHS' resource commitments to writing policy documents and its resource commitments for operational capabilities. We have a very mature policy development capability, in part because DHS makes large resource and funding commitments to develop plans, update plans, create annexes to plans, and evaluate plans. However, relatively few resources are made available for implementing plans and building the operational capabilities that we will need to adequately respond to incidents. Clearly a rebalancing is necessary.

Now that the various sector specific plans are in place, we have had a perfect opportunity to shift our priorities from “planning” to “implementing”-- building incident response and other capabilities that we called out in those plans. Nevertheless, we continue to see attention and resources devoted almost exclusively to policy development rather than to government-industry operational implementation. Although planning is clearly necessary, unless attention is paid to building, testing and measuring the effectiveness of operational components, the plans have very little value.

To help address this, we believe that a DHS top priority must be to support and leverage the significant operational investments made by the IT-ISAC and other ISACs, to strengthen the operational, information sharing and response capabilities of ISACs and government organizations, and to develop an out of band backup capability to distribute data to support Internet recovery, should a serious disruption take place. An obvious starting point would be for all DHS components to integrate the IT-ISAC and other sector-endorsed ISACs into their day to day operational processes.

Thank you again for the opportunity to be with you today on behalf of the IT-ISAC. I will be happy to answer any questions you may have.