Statement for the Record

J. Michael Hickey

Vice President - Government Affairs
National Security Policy
Verizon

Before the

Committee on Homeland Security
Subcommittee on Emerging Threats, Cyber Security
and
Science and Technology

United States House of Representatives

"The Communications Sector Coordinating Council and Cyber Security"

October 31, 2007

2:00 P.M.
311 Canon House Office Building

Overview:

Mr. Chairman and Members of the Subcommittee, my name is Mike Hickey and I thank you for the opportunity to testify before you on measures we have taken to address cybersecurity in the Communications Sector Specific Plan. I serve as Vice President of Government Affairs for National Security Policy at Verizon and as Chair of the Communications Sector Coordinating Council. I also serve as Vice Chair of the Internet Security Alliance and am an active member of the US Chamber of Commerce Homeland Security Task Force. Of these organizations, the Communications Sector Coordinating Council is uniquely chartered to represent the breadth of the communications sector on policy issues relating to the protection of critical communications infrastructure and key assets. Since 2005, it has emerged as an instrument for business engagement with government on policy matters relating to homeland security and emergency preparedness.

My comments will address the roles that have been established for industry and government in protecting the nation's critical physical and cyber communications assets, steps taken to protect these assets, what measures have worked effectively and what needs to be done to sharpen the collective focus as we move forward.

Tiered Approach to Critical Asset Protection:

Effective industry and government collaboration starts with the actions of individual organizations. The private sector owns and operates nearly 90% of this country's critical infrastructure. Because of industry's important role in national and homeland security, corporations like Verizon must dedicate the operations experience, resources and oversight necessary to be as self-aware and self-reliant as possible. Verizon is obligated to its shareowners and customers to take the steps necessary to secure its cyber, physical and human assets from disruption or attack. We cooperate with peer companies in order to support communications sector mutual aid obligations. We also proactively address our interdependencies with other sectors to ensure continuity of operations in time of crisis. Finally, we continue to work with government agencies at the Federal, State, regional and local levels to support appropriate security and emergency preparedness initiatives.

Strength from Within:

Verizon Communications Inc. is a Dow 30 company. It employs over 240,000 employees. In 2006, the company generated $88 billion in annual revenue and spent $17.1 billion on capital investments. Verizon's state-of-the-art voice, data and video networks are touched by over 100 million consumers and government and business customers daily.

Given its breadth of service and geographic coverage, Verizon's commitment to national security and emergency preparedness – grounded in corporate policy, sound business practice and hands-on experience – is long-standing and growing. In order to ensure the continuity of its own operations and to meet the requirements of its critical customers in time of crisis, Verizon has:

- Designed, built and managed network facilities that are robust and resilient;
- Embraced "best practice" business methods and security procedures;
- Created and tested business continuity and emergency preparedness programs that have served the corporation and its customers in times of stress;

- Responded successfully to a wide range of crises; and,
- Provided leadership strength to industry and government organizations dedicated to national security and emergency preparedness.

Verizon's Internal Security Councils: Verizon takes a holistic approach to addressing information security by coordinating business unit activity around network and information protection. This effort is led by the Verizon Executive Security Council (VESC), established in 1995 to oversee all aspects of information security within Verizon. Reporting to the VESC is the Verizon Information Security Council (VISC), an enterprise-wide, cross-organizational working committee comprised of lead security managers and information security teams. The VISC is charged with instituting a secure environment for company network, information management, processing, transport and delivery.

The Verizon business units that comprise the VISC are dedicated to providing coordinated information and network security services for Verizon. These services include firewall support, host (mainframe and distributed) management, virus protection, risk assurance, information security practices, information security awareness, Incident Response & Vulnerability scanning, and remote access security administration.

Computer Intrusion Response Team (CIRT): The Verizon CIRT provides 7x24 coverage for the entire enterprise, supporting all business units and organizational points of contact to assess intrusion impacts, contain and control further dissemination of problems across the company, and capture and preserve evidence for law enforcement/legal purposes. The CIRT also provides restoration options, identifies and closes security vulnerabilities (exploited or otherwise), and uses secure communication channels during response.

The CIRT's network of contacts and organizational breadth enable it to effectively work with the appropriate company personnel to coordinate incident response and resolution. A single point of contact is designated for all network or computer related security advisories to the enterprise, thus eliminating duplication of information and effort by quality checking all data prior to distribution. A historical repository of advisory data is also maintained for reference.

Management Structure: Verizon has sharpened its focus in addressing its evolving challenges in network technology and security. Key internal organizations have been realigned to apply consistent, best practice solutions to IT and network technology across business units. Verizon's Executive Vice President and Chief Information Officer has oversight over a range of technical support organizations serving the company's major business units. Meanwhile, a newly created position of Executive Vice President and Chief Technology Officer has responsibility for establishing and managing the overall direction, technology and planning of all Verizon networks. The CTO in each of Verizon's business groups remains responsible for the day-to-day execution of their network deployment strategies.

Technical Support: A full array of internal technical, consulting and R&D services are available to guide decision making and strengthen best practice within all major business units. For instance, the Verizon Information and Network Security organization advances security strategies that integrate people, process and technology (such as firewalls, intrusion detection systems, virus protection, and remote access) with full adherence to information security policies and practices; while also providing technical and consulting services to business units - all with a primary focus on information asset protection.

Verizon Information Security Focus is Crucial: In today's evolving threat environment, malicious insiders are the greatest threat to our critical national infrastructures. Today's geo-political climate will result in cyber attacks against national communications and control systems of economic, safety, or political significance. And politically (ideologically) motivated cyber attacks are increasing in volume, sophistication, and coordination. Verizon is addressing today's very real threats. Standards organizations must address carrier class security issues and architectures. The vendor community needs to produce equipment & software that meet Verizon's security objectives. And our customers and peer carriers need to work with us to mitigate security risks.

Sector Leadership and Collaboration:

Verizon, and its peer companies within the Communications Sector, have a long history of cooperation in national security and emergency preparedness. This history distinguishes the Communications Sector from most other critical sectors identified in the National Infrastructure Protection Plan. The sector personifies cooperation and trusted relationships that have resulted in the delivery of critical services when emergencies and disasters occur. A strong bond between the private and public sectors exists today in large part because of several organizations that were created in response to earlier threats to the nation's critical infrastructure.

National Communications System: The Sector Specific Agency for the Communications Sector is the National Communications System (NCS), currently housed within the Department of Homeland Security's National Cyber Security and Communications Division.

The NCS was established by President Kennedy in the aftermath of the Cuban missile crisis when communications problems between the United States and key international players threatened to further complicate the crisis. Since 1963, the NCS has worked to strengthen the communications facilities and components of various Federal agencies, focusing on interconnectivity and survivability.

National Coordinating Center for Telecommunications: In 1982, telecommunications industry and Federal Government officials identified the need for a joint mechanism to coordinate the initiation and restoration of national security and emergency preparedness telecommunications services. In 1984, Executive Order 12472 broadened the NS/EP role of the National Communications System and created the National Coordinating Center for Telecommunications as a central public-private sector organization to coordinate response to emergency communications situations.

In January 2000, the NCC was designated an Information Sharing and Analysis Center for Telecommunications in accordance with PDD-63. The NCC-ISAC facilitates information sharing among government and industry participants regarding vulnerability, threat, intrusion, and anomaly information affecting the telecommunications infrastructure.

The National Security Telecommunications Advisory Committee (NSTAC): The NSTAC was created 25 years ago, in 1982, by Executive Order 12382. NSTAC provides another highly successful example of how the private sector helps direct government decisions around national security and emergency preparedness communications (NS/EP). This advisory committee to the President brings together 30 industry chief executives representing major telecommunications companies, network providers, information technology companies, finance and aerospace businesses. NSTAC provides industry-based advice and expertise to the President on a wide range of telecommunications problems related to implementing NS/EP communications policy issues. These include, but are not limited to, information security, information assurance, and critical infrastructure protection.

NS/EP communications enable the government to make an immediate and coordinated response to all emergencies, including cyber attacks. NS/EP communications allow the President and other senior Administration officials to be continually accessible, even under stressed conditions. The impact of today's dynamic technological and regulatory environment is profound with new technologies and increasing competition bringing both new opportunities and new vulnerabilities to the information infrastructure. The NSTAC is strongly positioned to offer advice to the President on how to leverage this dynamic environment to enrich NS/EP communications capabilities and ensure that new architectures fulfill requirements to support NS/EP operations; and to avoid introducing vulnerabilities into the information infrastructure that could adversely affect NS/EP communications services. The NSTAC's current work plan includes issues ranging from information sharing and the security and reliability of converged networks to research and development (R&D) issues related to converged networks.

The Network Reliability and Interoperability Council (NRIC): Government-imposed solutions may hinder the ability of business to adapt and respond effectively to the changing threat environment. So it becomes critical for business and government to work collaboratively towards solutions that are meaningful, adaptable and sustainable. The voluntary development of and compliance with "best/sound practice" approaches to physical and cyber security is a model that is time tested. It is illustrated through the work of the Federal Communications Commission's Network Reliability and Interoperability Council. The NRIC is a successor to the National Reliability Council, first established in 1992. Through the work of seven successive councils, subject matter experts from business and government have come together to address network reliability and interoperability issues of concern, develop best/sound practices and encourage voluntary adoption. The NRIC will soon merge with the Media Security and Reliability Council (MSRC) to create a new organization, the Communications Security, Reliability, and Interoperability Council (CSRIC).

National Security Information Exchange (NSIE): In April 1990, the Chairman of the National Security Council's Policy Coordinating Committee requested the NCS Manager identify what actions industry and Government should pursue to protect critical NS/EP telecommunications from the growing "hacker" threat. The NCS Manager subsequently requested that the NSTAC provide industry's perspective on the network security issue. Ultimately NSTAC created a mechanism for security information exchange and produce a corresponding implementation plan. The NSTAC and NCS Manager also established separate, but closely coordinated, Network Security Information Exchanges (NSIEs). In May 1991, the NSIE charters were finalized, and

NSTAC companies and government departments and agencies designated their NSIE representatives, chairmen, and vice-chairmen. The NSTAC and government NSIEs held their first joint meeting in June 1991.

Industry and government coordinate through their respective NSIEs to voluntarily share sensitive information on threats to operations, administration, maintenance, and provisioning systems supporting the telecommunications infrastructure. Government NSIE members include departments and agencies that use national security and emergency preparedness (NS/EP) telecommunications services, represent law enforcement, or have information relating to network security threats and vulnerabilities. NSTAC NSIE representatives include subject matter experts who are engaged in prevention, detection, and/or investigation of telecommunications software penetrations or have security and investigative responsibilities.

The Communications Sector Coordinating Council (CSCC) and its Sector Specific Plan (SSP):

Verizon recognizes its critical operational dependence on other sectors and has established the necessary vendor relationships to meet both normal and extraordinary continuity of business requirements. In turn, all critical sectors are heavily reliant on the Communications Sector to support their own continuity of operations.

The Homeland Security Act of 2002 provided the basis for DHS' role in the protection of the nation's critical infrastructure and key resources (CI/KR.) The Act assigned DHS responsibility for developing a comprehensive national plan for securing CI/KR in conjunction with other Federal agencies, State and local agencies and authorities, the private sector and other entities.

The complexity of cross sector independencies was recognized in the 2006 National Infrastructure Protection Plan, resulting from Homeland Security Presidential Directive 7. HSPD-7 focused on the identification, prioritization and protection of the nation's critical assets. It prescribed the development of the National Infrastructure Protection Plan (NIPP) and corresponding Sector Specific Plans. Perhaps most significantly, the NIPP encouraged the establishment of sector coordinating councils. In so doing, it brought greater sector diversity to the table and significantly advanced the institutional capacity of sectors to formally and proactively address cross-sector dependencies.

Communications Sector Coordinating Council (CSCC): The Communications Sector Coordinating Council (CSCC) became operational in calendar year 2006. It was chartered to foster the coordination of policy initiatives to improve the physical and cyber security of sector assets, and ease the flow of information within the sector, across sectors and with designated Federal agencies. Through the CSCC, private-sector owners, operators and suppliers can engage Federal government entities to: identify and coordinate policy issues related to the protection of critical infrastructure and key resources; facilitate the sharing of information related to physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices; and, address policy issues related to response and recovery activity and communication following an incident or event. The CSCC now embraces 35 member companies and has become more representative of the diversity of the Communications sector. Members include wireline, wireless, cable, satellite, information service providers, as well as commercial and public broadcasters, service integrators, and equipment vendors. Small and medium size companies are represented through CTIA, USTelecom, ITA and NCTA. Verizon currently chairs the CSCC.

CSCC members meet quarterly to review industry and government actions on critical infrastructure protection priorities, confer with Federal agency representatives, review cross sector CIP issues, and coordinate with industry participants in NSTAC and the NCC ISAC to ensure industry coordination. Council work groups meet frequently to engage industry and government SME's on task force initiatives. Top 2007 CSCC priorities include the sector's risk assessment of critical assets, cross sector pandemic planning and implementation of access and credentialing and emergency wireless protocols.

The CSCC and IT Sector Coordinating Councils maintain close coordination on a range of policy and operational initiatives. Both sectors participate in a recently formed cross sector cyber security work group. Both have worked to heighten industry's role in NS/EP exercises such as last summer's ESF2 exercise in New Orleans and in TopOff 4. In the aftermath of Katrina, the Councils met to discuss ways of strengthening industry preparation and response to major events. Both participate in ongoing sector risk assessment activity. Both organizations have elected sector liaisons to attend each other's coordinating council meetings and they meet annually to confer, with government counterparts, on ongoing sector activity.

Partnership for Critical Infrastructure Protection (PCIS): The Communications Sector Coordinating Council is a member of the Partnership for Critical Infrastructure Security (PCIS.), a private sector organization. PCIS is comprised of the leadership from each of the Sector Coordinating Councils, which represent the owners and operators of the critical infrastructure and key resources sectors identified by the government in HSPD-7. The mission of PCIS is to coordinate cross-sector initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services. This mission encompasses physical, cyber, and human security that rely on strong infrastructure integrity and resilience. Accordingly, the PCIS mission spans the full spectrum of critical infrastructure matters from prevention, planning, and preparedness to business continuity, mitigation, response, and recovery.

The PCIS has worked to encourage a productive industry partnership with the Federal government over the past six years. It was formally recognized as the Private Sector Cross-Sector Council in the National Infrastructure protection Plan when it was released in 2006. The NIPP states that the "cross-sector issues and interdependencies are addressed among the sector coordinating councils through PCIS. PCIS members, including the CSCC, continue to work with designated Federal agencies on implementation of their sector specific plans.

Communications Sector Specific Plan (CSSP): The CSCC completed work on the CSSP for critical infrastructure and key resource (CI/KR) protection, as recommended by the NIPP, in December 2006 the plan was subsequently released in May 2007. It was developed jointly by industry and the National Communications System, with input from Federal government agencies ranging from the US Department of Commerce to the Federal Communications Commission.

The CSSP provides a framework for protecting the Nation's critical communications assets and key resources. It addresses asset identification, risk assessment and mitigation, protective programs and government measurements.

The goals of the CSSP include the need to:

- Protect the overall health of the national communications backbone;
- Rapidly reconstitute critical communications services after national and regional emergencies;
- Plan for emergencies and crises by participating in exercises and updating response and continuity of operations plans;
- Develop protocols to manage the exponential surge in utilization during an emergency situation and ensure the integrity of sector networks during and after an emergency event;
- Educate stakeholders on communications infrastructure resiliency and risk management practices in the Communications Sector;
- Ensure timely, relevant, and accurate threat information sharing between the law enforcement and intelligence communities and key decision makers in the sector;
- Establish effective cross-sector coordination mechanisms to address critical interdependencies, including incident situational awareness, and cross-sector incident management.

The CSSP acknowledges the lead role played by private sector owners and operators in protecting critical assets. The communications companies that own, operate and supply the Nation's communications infrastructure have historically factored natural disasters and accidental disruptions into network resiliency architecture, business continuity plans, and disaster recovery strategies. The interconnected and interdependent nature of these service provider networks has fostered crucial information sharing and cooperative response and recovery relationships for decades. The CSSP also articulates the role of the Federal government in providing the support and resources necessary to identify threats and help mitigate risk.

The Communications Sector's strategy is to ensure the nation's communications networks and systems are secure, resilient, and rapidly restored after an incident. The approach outlined in the CSSP includes:

- Defining industry and government roles in protecting communications infrastructure by leveraging corporate capabilities and government programs;
- Adopting an architectural approach to infrastructure identification and risk assessment processes;
- Coordinating with other sectors and customers on critical infrastructure dependencies and solutions for mitigating risk; and
- Working closely with DHS to advance sector protection and mitigation measures.

The CSSP defines the three major arenas where risk assessments are conducted: industry self-assessments; government-sponsored assessments and government-sponsored cross sector dependency analyses. Industry self-assessments of risk are ongoing. Such assessments are conducted to verify compliance with company policies, industry standards, contract agreements and regulatory requirements.

Throughout 2007, industry has turned its attention to working with government to define relevant government sponsored assessments through a National Sector Risk Assessment (NSRA) process. Through this process, industry and government have undertaken a qualitative risk analysis of Communications Sector infrastructure and have narrowed the scope of risk assessments to nationally critical network elements. This process will result in a draft government assessment by December 2007, with a final report to be completed by March 2008. Based on the outcomes of this government assessment process, government may conduct more quantitative assessments of selected architecture elements in conjunction with industry.

The third and final element of the CSSP risk assessment process is the analysis that government will undertake with industry on cross-sector dependencies. Work will commence in 2008, the process will identify high-level critical sector communications dependencies and will leverage NCS risk assessment methodologies to identify communications dependencies specific to a facility or function. The goal will be to assist other sectors in the assessment of communications dependencies for high-risk assets.

The Communications and IT Sector Coordinating Councils have worked to ensure that respective risk assessment efforts, although distinct, are complementary where the sectors overlap. This cross-sector participation increases information sharing, including lessons learned. In each sector, cyber threats associated with the sector's functional or network elements will be identified and vulnerabilities and consequences associated with such threats will be assessed to determine risk.

Whatever success the CSCC has achieved in the development of the CSSP has resulted from industry's singular focus on developing a critical asset protection plan that is designed by industry for implementation by industry. In order to accomplish this, the NCS stepped forward to advocate industry positions within the Department of Homeland Security and with DHS project contractors. A strong element of social capital exists among industry representatives and Federal agency personnel within the Communications Sector. This trusted relationship helped to produce a practical, meaningful asset protection framework that can now be used by industry and government partners to better meet the country's security requirements. The CSSP is realistic and well-grounded.

Critical Asset Protection Over the Long Term: What cannot be underestimated by policymakers is the enormous amount of private sector resources that are being devoted to finding solutions – with government partners – to achieve greater effectiveness in our country's security and response programs. The Communications Sector continues to commit significant financial resources and subject matter expertise to strengthen critical business practices. It will continue to dedicate time and expertise to its work with the NCS and other Federal, state and local government partners to address emerging operational and policy issues.

To ensure even greater effectiveness in protecting the Nation's critical communications infrastructure – both physical and cyber - industry and government partners must be clear about their respective roles in getting the job done. Industry is the first line of defense in protecting assets and mitigating risks, and aggressive business continuity and security practice will remain critically important as the Nation's risk environment continues to evolve. Although the

Communications Sector’s long history of coordination will change as industry restructuring continues, close planning and coordination within the sector will continue to be a mainstay of efforts to fortify physical and cyber security programs.

Government must continue to ensure clarity of roles and responsibilities among all levels of government and the private sector. It should continue to advocate for strong sector and cross sector collaboration on operational and policy issues and in providing the necessary intelligence and operational support to ensure effective industry preparedness and response, in particular by refining and improving roles and responsibilities in the National Response Framework.

Although industry and government have made progress on long standing issues pertaining to protection of critical assets and key resources, much work lies ahead. There must be an even greater Federal government focus on effective engagement and integration of state and local authorities in all aspects of critical infrastructure protection and emergency response, including the rollout and coordination of initiatives “on the ground”. For instance, practical steps on access and credentialing and emergency wireless protocols for shutdown and restoration of service must be taken to facilitate industry response to natural or man-made disasters. Myriad jurisdictional laws and requirements may be complex, but real world execution is overdue. Government must also continue to integrate industry more fully on operational planning, coordination and joint policy initiatives. Effective partnerships require early involvement of industry and direct engagement in government programs, including protection and response plans, which impact the private sector’s critical industry assets. Although government has recognized the importance of sharing timely threat intelligence with industry, more needs to be done in this area to advance NS/EP interests. Finally, recent Congressionally mandated changes in organization and functions within DHS need to be fully implemented and understood by all stakeholders in the critical infrastructure protection and emergency response domain. In sum, Industry and the Federal government have much to do on the full array of critical infrastructure protection initiatives, while advancing transition plans for the upcoming change in Administration.

Mr. Chairman, this concludes my testimony. I would be happy to answer any questions you or the subcommittee might have about Verizon or the Communications Sector.