CIP PROJECT STAFF

John McCarthy, *Executive Director*

Emily Frye, *Associate Director, Law and Economics Programs*

Kevin "Kip" Thomas, *Associate Director, Research Programs / Research Associate Professor*

Dr. John Noftsinger, *Executive Director, JMU Institute for Infrastructure and Information Assurance*

Ken Newbold, *JMU Outreach Coordinator / JMU CIP Project Liaison*

Contact: cipp01@gmu.edu
703.993.4840

If you would like to subscribe to *The CIP Report* please click here.

Our focus this month on the Information and Communications sector reveals an extraordinary breadth of critical infrastructure. When Congress adopted the Communications Act over 70 years ago, few could have predicted the wide range of businesses, technologies, and partnerships that provide essential citizen services in the 21st century.

This month's edition captures many of the strategic plans for the next 70 years.

The National Communications System has proved to be one of the most successful infrastructure assurance organizations. Now entering its 41st year, the NCS, and its industry partners -- the National Communications Center and the Telecom ISAC, have created tried and true operational capabilities for national security & emergency preparedness communications.

The National Security Telecommunications Advisory Council, Network Reliability and Interoperability Council, and the National Infrastructure Assurance Council each guide the Administration in distinct areas of infrastructure complexity. The Media Security and Reliability Council is similarly generating insights into broadcast and media resilience - especially important for public trust in the event of a widespread disruption or terrorist attack. These advisory organizations are laying a foundation for supporting homeland security and critical infrastructure goals for both public and private sectors. The Sector Coordinators for Information and Communications similarly marshal resources to partner in meeting assurance objectives.

This month's newsletter also highlights multiple other institutions active in infrastructure protection. The Common Ground Alliance is typical of the unique and important insights professionals are developing to assure critical services and capture capabilities outside of communications that are part of the infrastructure nonetheless.

National Communications System: A Long History with National Security / Emergency Preparedness Telecommunications

The genesis of the National Communications System (NCS) began in 1962 after the Cuban missile crisis when communications problems among the United States, the Union of Soviet Socialist Republics, the North Atlantic Treaty Organization, and foreign heads of state threatened to complicate the crisis further. After the crisis, President John F. Kennedy ordered an investigation of national security communications, and the National Security Council (NSC) formed an interdepartmental committee to examine the communications networks and institute changes.
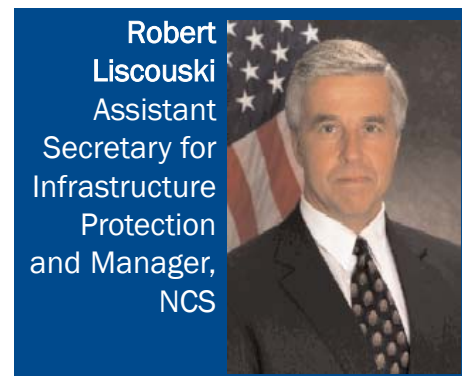
This interdepartmental committee recommended the formation of a single unified communications system to serve the President, Department of Defense, diplomatic and intelligence activities, and civilian leaders. Consequently, in order to provide better communications support to critical Government functions during emergencies, President Kennedy established the National Communications System by a Presidential Memorandum on August 21, 1963. The NCS mandate included linking, improving, and extending the communications facilities and components of various Federal agencies, focusing on interconnectivity and survivability.

On April 3, 1984, President Ronald Reagan signed Executive Order (E.O.) 12472 which broadened the NCS' national security and emergency preparedness (NS/EP) capabilities and superseded President Kennedy's original 1963 memorandum. The NCS expanded from its original six members to an interagency group of 23 Federal departments and agencies, and began coordinating and planning NS/EP telecommunications to support crises and disasters.

NCS Today

Robert Liscouski
Assistant Secretary for Infrastructure Protection and Manager, NCS

The National Communications System transferred from the Department of Defense to the Department of Homeland Security earlier this year, and on November 3, 2003 the Assistant Secretary for Infrastructure Protection was designated as the Manager of the National Communications System.

The Manager of NCS is responsible for the development of (1) Evolutionary telecommunications architecture; (2) Plans and procedures for the management of Federally owned or leased telecommunications assets; (3) Plans and procedures to eliminate technical impediments to interoperability of public and private telecom systems; (4) Test and exercise programs to evaluate the capability of national

The **Government Emergency Telecommunications Service** (GETS) is a telecommunications service that supports federal, state, and local government, industry, and non-profit organization personnel in performing their National Security and Emergency Preparedness (NS/EP) missions. GETS provides emergency access and priority processing in the local and long distance segments of the Public Switched Network (PSN). It is intended to be used in an emergency or crisis situation during which the probability of completing a call over normal or other alternate telecommunication means has significantly decreased. Using enhancements based on existing commercial technology, GETS allows the NS/EP community to communicate over existing PSN paths with a high likelihood of call completion during the most severe conditions of high-traffic congestion and disruption. The result is a cost-effective, easy-to-use telephone service that is accessed through a simple dialing plan and Personal Identification Number (PIN) card verification methodology. It is maintained in a constant state of readiness and provides a cost-effective means to overcome network outages through such methods as enhanced routing and priority treatment. Wireless Priority Service (WPS) is the wireless complement to the wireline Government Emergency Telecommunications Service.

The **Telecommunications Service Priority** (TSP) Program provides national security and emergency preparedness (NS/EP) users priority authorization of telecommunications services that are vital to coordinating and responding to crises. Telecommunications services are defined as the transmission, emission, or reception of intelligence of any nature, by wire, cable, satellite, fiber optics, laser, radio visual or other electronic, electric, electromagnetic, or acoustically coupled means, or any combination thereof. As a result of hurricanes, floods, earthquakes, and other natural or man-made disasters, telecommunications service vendors may become overwhelmed with requests for new telecommunications services and requirements to restore existing telecommunications services. The TSP Program provides service vendors with a Federal Communications Commission (FCC) mandate for prioritizing service requests by identifying those services critical to NS/EP. A telecommunications service with a TSP assignment is assured of receiving full attention by the service vendor before a non-TSP service.

NCC Members

Federal: Departments of Commerce, Defense, Energy, Justice, State, FEMA, and General Services Administration.

Industry: AT&T, Cisco, Lockheed Martin Global Telecom, Computer Sciences Corporation, EDS, GTE, ITT, Lucent, Nortel, SAIC, Sprint, and US Telecom Association.

NCS *(Cont. from Page 2)* security or emergency preparedness telecommunications requirements; and (5) Alternative funding mechanisms.

The Manger of NCS is also charged with -
● Implementing and administering approved related telecommunications programs and plans;
● Chairing the NCS Committee of Principals;
● Serving as the hub for industry-government planning and information sharing;
● Conducting technical studies and examining research and development programs;
● Managing the Federal Telecommunications Standards Program to ensure that industry, national, and international standards are used as the basis for Federal telecommunications standards; and
● Providing reports and other duties as required by the President or the NCS Committee of Principals. ❖

Brent Greene is the 10th Deputy Manager of the National Communications System and is responsible for the day-to-day policy, technical, and programmatic oversight in coordination of all Federal government-wide activities in national security and emergency preparedness communications. He became the Deputy Manager in April 2001.

Telecommunications Sector ISAC: National Coordinating Center

In 1982, telecommunications industry and Federal government officials identified the need for a joint mechanism to coordinate initiation and restoration of national security and emergency preparedness (NS/EP) telecommunication services. In 1983, the group recommended to the National Security Telecommunications Advisory Committee (NSTAC) and to President Reagan that a joint industry and government-staffed National Coordinating Center (NCC) be created as a central organization to handle emergency telecommunication requests. On January 3, 1984, the NCC opened for business.

In January 2000, the National Coordinating Center was designated as the ISAC for telecommunications. On March 1, 2000, the NCC-ISAC commenced operations. The NCC-ISAC membership is based on NCC membership, which is evolving to reflect a broader base of technologies comprising the telecommunications infrastructure. The NCC-ISAC supports the mission assigned by Executive Order 12472 and the national critical infrastructure protection goals of government and industry. The NCC-ISAC facilitates voluntary collaboration and information sharing among its participants, gathering information on

Information Security: The Long Campaign

Harris Miller, President
Information Technology Association of America

Stakeholders from critical infrastructure industries will gather in Santa Clara shortly. Broadly defined, their mandate is to move from plan to action on cyber security. The Bush Administration issued its long-awaited National Strategy to Secure Cyberspace last September. The Summit will be the first forum of its kind since the release of the President's Strategy. By seeking the perspectives and commitments from public and private sector leaders on priorities, metrics, and milestones, ITAA and the industry alliance coordinating this Summit will help government strengthen the security of cyberspace, and cultivate and sustain the public private partnership for cyber security.

As the Information and Communications Sector Coordinator under Presidential Decision Directive 63, ITAA was the single IT Association invited by the White House to participate in the official unveiling of the Strategy. Do we agree with everything in the government report? No. But we do believe that this is the most comprehensive and serious attempt to address these issues to date, and we look forward to continuing to work with all levels of government to make this plan a success.

The National Cyber Security Summit takes the Strategy sever-

al steps forward. Conducted in partnership with the Department of Homeland Security and three other leading trade associations: the Business Software Alliance, TechNet and the U.S. Chamber of

Harris Miller

Commerce, the Summit will organize around 5 task forces, each addressing key challenges identified in the National Strategy: 1) Awareness for Home Users and Small Business; 2) Cyber Security Early Warning systems; 3) Corporate Governance; 4) Technical Standards and Common Criteria; and 5) Security Across the Software Development Life Cycle. These task forces will be responsible for developing recommendations with tangible deliverables by March 1, 2004, and a work plan for accomplishing those recommendations.

The IT industry, as creators of the information infrastructure, is wholly committed to achieving the most secure computing environment possible. Security is not achieved overnight, and just as

new products are developed to improve security, so are new ways to undermine it. We -- along with our partners and customers in the public and private sector -- are fighting a long campaign.

Our industry has consistently demonstrated, through our words and our actions, the seriousness of our resolve. Over two years ago, the nation's leading IT vendors began talks to establish an IT-ISAC, and in August 2001, we were able to stand up the ISAC through the leadership of founding member companies like AT&T, Cisco, HP, IBM, Intel, Oracle, and Microsoft. The National Cyber Security Alliance, which our Association and companies played a major role in forming, is a public-private partnership that reaches out to home users and small businesses to promote information security awareness and to recommend practical steps to harden computer systems against cyber attacks. This important initiative is led by companies like AOL, Akamai, EDS, Internet Security Systems, Network Associates and Symantec. ITAA, along with its partner, Brainbench, also introduced a cyber security awareness certification program, I-ACERT, in 2003, designed to be the cyber security program for the rest of us. I-ACERT assesses the level of cyber security awareness of non-technical computer *(Continued, Page 14)*

NSTAC at 20: Providing National Security Telecommunications Policy Expertise for Two Decades

Earlier this year, the President's National Security Telecommunications Advisory Committee (NSTAC) celebrated its twentieth anniversary, marking a milestone achievement in the history of industry and Government collaboration. Established in 1982 by Executive Order 12382, President's National Security Telecommunications Advisory Committee, the NSTAC continues to be at the forefront of emerging national security and emergency preparedness (NS/EP) communications issues.

Dr. Vance D. Hoffman, Chairman and CEO of Lockheed Martin, serves as the current chair of the NSTAC.

Composed of up to 30 industry leaders, NSTAC members are presidentially appointed chief executives from the telecommunications, aerospace, hardware, software, and other relevant industries. The committee works in partnership with the Federal Government through the National Communications System (NCS), an interagency consortium of 23 Federal departments and agencies that serves as the focal point for industry/Government NS/EP communications planning and response. Since its inception, the NSTAC has advised four

Presidents and six Administrations and has proven itself adept at responding to new challenges related to changes in technology and national priorities. The NSTAC, in keeping with its long, supportive history, will continue to provide essential guidance through its new Executive Agent - the Secretary of Homeland Security.

NSTAC: THE PAST AND PRESENT

Several factors during the early 1980s provided the impetus for the NSTAC's establishment. First, comprehensive command, control, and communications capabilities became ever more important in executing military and disaster-response operations, and the Government became increasingly reliant upon privately owned commercial communication systems to conduct its business. In addition, the telecommunications industry rapidly evolved and changed as competition and new services were introduced into the marketplace, and the Government needed a forum through which to remain abreast of new advances and to assess the impact of those new technologies on NS/EP activities. Finally, with the divestiture of AT&T, the Government lost its single point of contact within the telecommunications industry to coordinate NS/EP efforts. Consequently, the establishment

of the NSTAC provided the necessary formal mechanism to continue to effectively facilitate industry/Government cooperation in the post-divestiture environment.

During its early years, the NSTAC focused its efforts on concerns over the Government's growing reliance on commercial telecommunications services. As the telecommunications network continued to evolve, however, NS/EP communications planning and response also became increasingly complex and critically dependent on information infrastructures, demanding an innovative means of protecting the Nation's public and private communications assets. In response, the NSTAC amended its task force attention to include planning and response issues. In the years since its inception, NSTAC activities have led to the development of technical reports with recommendations to the President and operational programs that provide essential telecommunications capabilities to the nation's Government personnel and first responders during times of crisis.

To gain a wide range of perspectives for its recommendations, NSTAC and its various task forces work with numerous industry and Federal bodies, including the

NSTAC *(Cont. from Page 5)* Federal Communication Commission's Network Reliability and Interoperability Council (NRIC), the National Telecommunications and Information Administration (NTIA), the National Infrastructure Assurance Council (NIAC), the White House Office of Science and Technology Policy (OSTP), and the National Institute of Standards and Technology (NIST). NSTAC task forces have worked with these organizations to examine such issues as the network security implications of Internet technologies, "last mile" bandwidth availability, intrusion detection, information sharing, network convergence, and research and development activities.

In 1982, when President Ronald Reagan established the NSTAC he sought advice on the implementation of the country's national security policy from the perspective of the telecommunications industry. Twenty years later, the NSTAC continues to provide valuable advice to the President in five critical mission areas: critical infrastructure protection, information assurance, network convergence, information sharing, and outreach.

CRITICAL INFRASTRUCTURE PROTECTION

The well being of the Nation and its ability to sustain national security missions depends on secure and reliable infrastructures. The exploitation of vital services, such as telecommunications, energy, transportation,

and banking and finance, would be detrimental to the welfare of the United States. During the mid-1990s, the President acknowledged such interdependencies and encouraged the private sector to actively participate in the protection of critical infrastructures from both physical and cyber attacks.

Following the September 11, 2001, terrorist attacks, the NSTAC played a leading role in helping the Government understand potential vulnerabilities and in developing policy recommendations to mitigate associated risks. Building on previous infrastructure specific assessments, the NSTAC analyzed physical security threats and possible remedies to critical telecommunications infrastructure sites, focusing, in particular, on trusted access issues, concentration of critical telecommunications assets in telecom hotels, and the resiliency of Internet peering points.

The NSTAC is also fostering cooperation and information sharing initiatives across all critical infrastructures, including the electrical power, transportation, and financial services industries.

INFORMATION ASSURANCE

The Nation relies on the information and communications infrastructure to function successfully, and the NSTAC is actively involved in efforts to address cyber-related vulnerabilities, network security issues, and wireless technology vulnerabilities

that threaten this infrastructure. The launch of several distributed denial of service attacks and the propagation of malicious worms in the last few years have demonstrated how easy it is for nefarious actors to exploit cyber vulnerabilities. In addition, the growing reliance on mobile e-services and applications has rendered security of wireless protocols and systems an issue of concern, especially when related to NS/EP communications transiting wire-

Mr. Duane Ackerman, Chairman, and CEO of BellSouth Corporation, serves as the Vice Chairman of the NSTAC.

less networks and technologies.

NETWORK CONVERGENCE

The late 1990s saw a fundamental shift in the overall architecture of the telecommunications network as many telecommunications carriers chose to leverage components of both the circuit-switched and packet-based network infrastructures resulting in a period of network convergence before the full transition to the next generation network. Over the past several years, the NSTAC has focused much attention on the NS/EP consequences of the converged environment, especially as it relates to such NS/EP communications programs as the Government Emergency Telecommunications Service and the Telecommunications Service Priority (TSP) system. Acting on

LEGAL INSIGHTS

by Emily Frye

Redefining Efficiency

Voice transmission over the Internet - fondly called VoIP - is big, and growing bigger.

According to Vijay K. Bhagavath, telecom analyst at Forrester Research, nearly 10% of businesses have replaced their traditional telephone systems with a form of VoIP. At first blush, switching to VoIP looks to be the sensible business decision: the bills are generally cheaper. The goal of business is to maximize profits; cutting the overhead of telephone bills contributes to that goal. Indeed, in the capitalist school of thought, it's every man for himself, and lower phone bills could be just the advantage that tips a business into the winning sphere.

Traditionally, immediate cost reductions have been equated with efficiency, and efficiency is equated with profitability. But VoIP presents a dilemma. If all businesses eventually migrate to a telephone system that moves over the Internet, society at large will have lost one of its chief weapons in the war on vulnerability: communications diversity.

Our critical business and national security communications increasingly move over the nation's digital backbone. The traditional phone system moves over copper wire. Attacks on one do not of necessity result in damage to both. By contrast, mass migra-

tion to VoIP could result in a world where a cyberattack takes down both Internet communications and the telephone system.

The members of my church had a small taste of this experience during Hurricane Isabel, when the church office - which relies on purely digital communications - effectively was incapacitated for three weeks. After three short days, the 900 members began to lose patience. Consider how much worse it would have been if 900 unhappy customers of a previously well-oiled business could not contact their representatives for an indefinite period of time, even to get a status update. If that business could at least keep in touch with its customers to explain delays and make alternative arrangements, it would be able to maintain some semblance of order and mitigate damage until its Internet connectivity was restored.

The damage from total communications incapacitation is exponentially greater than the damage from significant communications disability. In short, the traditional calculus of business efficiency changes in the face of current threats. The short-term benefit to business from adopting a superficially cheaper technology may lead to an unmanageable long-term social consequence. The business calculus looks like this:

Operating Cost - Reduction in Overhead = Increased Efficiency

The national security calculus looks like this:

Operating Cost - Reduction in Overhead + Increase in Risk = ?

Different constituencies would replace that question mark with "Increased National Security Costs" or "Net Efficiency Loss." Business people might even say - in all good faith - "Why should I care? National security is not my responsibility." While government's responsibility is to the people, business' responsibility is to its owners and shareholders: turn a profit. Societal externalities have always posed a problem for policymakers, because it is difficult to make the argument that, instead of focusing on individual interests and profits, business should focus on the collective social effects of decisions made by large numbers of businesses. Yet in some arenas - such as the environmental arena or the telecommunications arena - similar questions have been posed before and have resulted in a range of interventions. Is it possible to meld the efficiency equation and the risk equation into a workable solution for both business and national security interests?
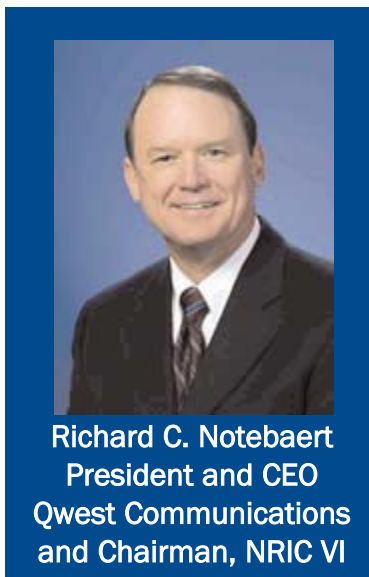
We have a little bit of time left to intervene: the technology that

Network Reliability and Interoperability Council VI: Enhancing Telecom Security

The Network Reliability and Interoperability Council is the successor to the Network Reliability Council that was first organized by the Federal Communications Commission in January of 1992. The Council was initially established following a series of major service outages in various local exchange and interexchange wireline telephone networks. The Commission established the Council to study the causes of service outages and to develop recommendations to reduce their number and their effects on consumers. Since then, the NRIC has been rechartered five more times in order to commission studies in the areas where the Council believes reliability concerns to be greatest.

The Council is composed of CEO-level representatives of over 50 carriers, equipment manufacturers, state regulators, and large and small consumers. The pur-

poses of the NRIC are to give telecommunications industry leaders the opportunity to provide recommendations to the

Richard C. Notebaert
President and CEO
Qwest Communications
and Chairman, NRIC VI

FCC and to the industry that, if implemented, would under all reasonably foreseeable circumstances assure optimal reliability and interoperability of wireless, wireline, satellite, and cable public telecommunications networks. This includes facilitat-

ing the reliability, robustness, security, and interoperability of public telecommunications networks. The scope encompasses recommendations that would ensure the security and sustainability of public telecommunications networks throughout the United States; ensure the availability of adequate public telecommunications capacity during events or periods of exceptional stress due to natural disaster, terrorist attacks or similar occurrences; and facilitating the rapid restoration of telecommunications services in the event of widespread or major disruptions in the provision of telecommunications services. NRIC VI is addressing topics in the areas of homeland security, network reliability, network interoperability, and broadband deployment. A listing of NRIC-VI deliverables can be found at http://www.nric.org /pubs/nric6/category.html. ❖

E911 Services

In early November, the House passed the E911 Implementation Act of 2003 (H.R. 2898) which will provide grants, planning and coordination to local 911 call centers, also known as Public Safety Answering Points (PSAPs). The legislation addresses the problem of accurately locating wireless 911 callers, which constitute more than half of the 200 million 911 calls placed each year.

Currently, only 18% of the nation's PSAPs can accurately display a wireless phone's location. The bill provides federal matching grants to state, tribal and local governments in the amount of $100 million a year for the next five years. In June the Senate Commerce Committee approved similar legislation (S. 1250) which could come to a full Senate vote before the end of this year.

Meanwhile, the General Accounting Office has issued a report that says enhanced 911 services are still years away for many states. Lack of funding is one of the key hindrances according to the report. Deployment of E911 services is estimated at more than $8 billion over the next five years. ❖

Critical Infrastructure Risk Assessment Tool Development at James Madison University

Introduction

The current state of world affairs necessitates that critical infrastructure service providers in all sectors evaluate where their systems are vulnerable and the costs associated with system down time. Even in a world free of extremist activities, this information would be exceedingly useful to predict damages and costs resulting from natural disasters or human error.

Because critical infrastructure facilities and systems tend to be functionally complex, they do not have obvious system-wide failure probabilities, modes, and consequences. Therefore, seemingly minor problems may propagate and result in complete mission failure. Particularly concerning are "single point failure" locations in many known facilities and sys-

tems. Which failure points or point combinations would lead to the most serious and "most-to-be-avoided" consequences? To analyze and quantify operability under adverse conditions, probabilistic risk assessment tools may provide a "snapshot" of failure modes at a single point of time for certain initiating conditions. Likewise, elaborate physics models developed to treat weapon's effects on systems implicitly compute effects at a single point in time.

The Tool

The Network Security Risk Assessment Model (NSRAM) is a tool that improves upon these computational models by explicitly adding the time dimension to the evaluation of functional mission susceptibility to the failure addressing interdependent sub-

systems of complex facilities and systems. The tool is designed to compute the evolution of overall mission failure probability over time by evaluating initial failure probabilities, effects of onset times and system repair/reconstitution times for single or combinations of critical infrastructure systems.

Understanding the Concept

To better understand the modeling capability of NSRAM, it is important to explain key words and concepts of NSRAM:

- Model-a group of things we call elements.
- Elements-are the things you want to model. Elements have attributes and ports.
- Attributes-are name, color, size, etc.
- Ports-connect two elements; ports are not multi-purpose.
- Parts-lead to different parts inside an element.
- Flows-elements communicate via flows, which are also made up of elements.

So, why does all of this matter? And why did we create NSRAM? So NSRAM can simulate systems after they've broken down. For instance, if a computer breaks, it needs to be replaced. A repairman can actually be a conduit to flows. We want the flow and elements to be the same so
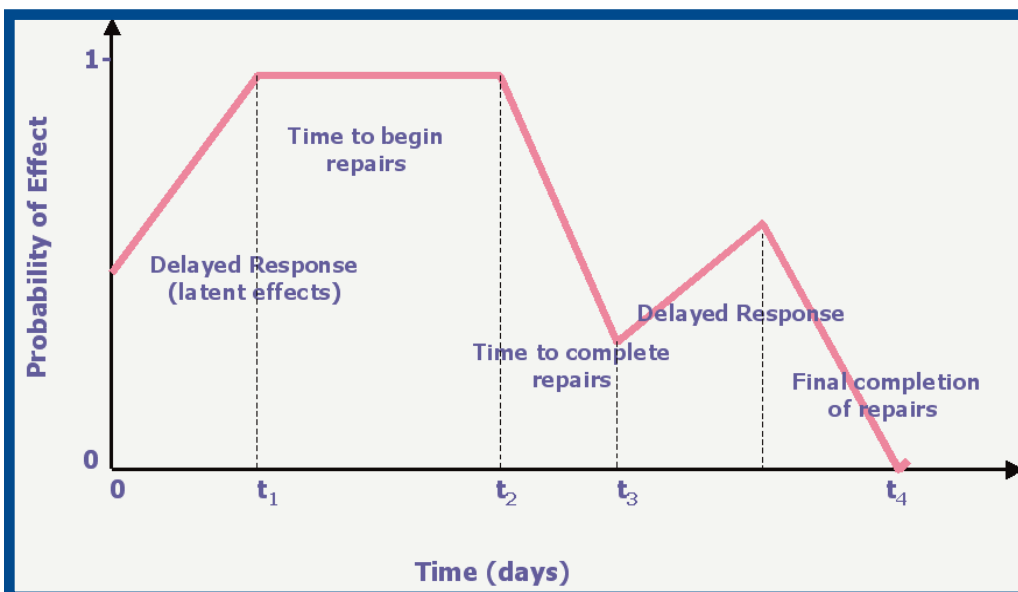
Figure 1. *The chart above indicates a notional output plot.*

Protecting Utility Infrastructures at the Common Ground Alliance

Damages to underground facilities are usually preventable and most frequently occur due to a breakdown in the damage prevention process. The responsibility for preventing excavation damage is shared by all stakeholders, and includes elements such as planning, effective use of one-call systems, accurate location and marking of underground facilities, adherence to safe digging practices, proper placement of facilities, and strong public education and awareness. Damage to underground facilities can affect the vital services and products delivered through those facilities. Underground facility damage can result in injury and death, as well as severe property damage and loss of vital services and products, such as telecommunications, water and sewer, electric power, cable television, and the flow and supply of liquid petroleum and natural gas. Damage can cause vital facility outages for homes, businesses, hospitals, air traffic control operations, and emergency service providers.

At the heart of damage prevention is improved information accuracy and consistency in communication between excavators and operators of underground facilities. One-call systems provide a reliable and efficient process for excavators to notify facility owners/operators of planned excavations. The one-call process allows operators with facilities in the vicinity of a proposed excavation site to mark the

location of their equipment and facilities in advance of the excavation. This gives excavators knowledge by which to excavate safely.

Damage prevention practices vary significantly among states, one-call centers, excavators, facility owners/operators, regulatory agencies, designers, and other stakeholders associated with or impacted by underground facilities. States have a variety of unique laws and regulations governing the practices, enforcement, and performance analysis data related to underground facilities' damage prevention.

In August of 1999 a report titled *Common Ground: Study of One-Call Systems and Damage Prevention Best Practices*, was prepared in accordance with, and at the direction and authorization of the Transportation Equity Act for the 21st Century (TEA 21), Public Law 105-178, signed into law on June 9, 1998. The Common Ground Study was performed and written through the efforts of a joint government/industry quality team. The purpose of the Study was to gather and assess information to determine the best of existing one-call notification system and underground facility damage prevention practices. The Best Practices are recognized by experts in damage prevention to be most effective in preventing damage to underground facilities and protecting the public, excavators, and the environment.

The study and subsequent initiatives led to the development of the nonprofit organization recognized as the Common Ground Alliance (CGA). The CGA focuses and supports industry efforts to continue the implementation and development of the Damage Prevention Best Practices. Through the CGA, individuals and organizations that design install, operate, repair, and regulate underground facilities will reap the benefits of building on the Best Practices identified by America's damage prevention professionals in the Common Ground Study. ❖
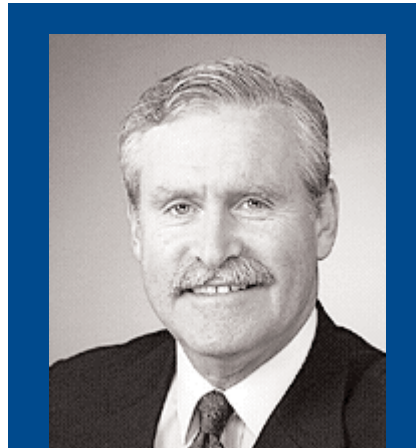
Media Security and Reliability Council:
Emergency Communications and Public Warning System

Leaders from the broadcast, cable and satellite industries began consideration of best practices recommendations to ensure effective delivery of emergency information through public warning systems. The recommendations were presented to members of the Media Security and Reliability Council (MSRC) at its biannual meeting this summer at the Federal Communications Commission.

FCC Chairman Michael Powell said, "The most important responsibility the government and media share during times of crisis is to ensure the safety and well-being of our citizens. Making sure that people receive urgent information that is timely and accurate is truly a life-saving service that warrants our utmost attention and support. The recommendations we have seen today address some of the biggest challenges we must face regarding the delivery of a reliable public warning system."

Dennis J. FitzSimons, MSRC chairman and president and chief executive officer of Tribune Company said, "September 11 was a wake-up call for all concerned–media, interest groups, government. We have to review what works and what doesn't. We simply have to communicate in a timely and accurate fashion. The public depends on us and we must come through." The Public Communications and Safety working group presented to the Council its interim report and offered for consideration twenty-six best practices recommenda-

tions aimed at ensuring the effective delivery of emergency information and warnings to the public.

Dennis FitzSimons
President and CEO
Tribune Company
and Chairman,
Media Security and
Reliabiity Council

Public Communications and Safety best practices recommendations include:

● A single federal entity should be responsible for public warning and all-hazard risk communication.
● Effective emergency communications should be achieved through a public/private partnership.
● Local and state governments should coordinate with media to create, review and update emergency communications procedures.
● Local media should form emergency jurisdiction/market cooperatives to assure coordinated delivery of local

emergency messages to all constituencies.
● The Emergency Alert System should be periodically tested, upgraded as necessary and implemented and maintained at local, state and national levels.
● Research into development of alternative, redundant and/or supplemental means of communicating emergency information to the public should be accelerated.
● Local jurisdiction/market cooperatives should share their locally developed best practices for coordination, delivering risk communications and continuity planning under crisis conditions.

MSRC is a Federal Advisory Committee that reports to FCC Chairman Powell. Chairman Powell formed MSRC following the events of September 11, 2001, in order to study, develop and report on best practices designed to assure the optimal reliability, robustness and security of the broadcast and multichannel video programming distribution industries. ❖

Emergency Communications are being addressed in the United Kingdom as well. As part of the UK government's efforts to improve the nation's resilience, industry stakeholders recently formed the UK Media Emergency Forum. The forum recently published findings from an exercise to test the media's effectiveness during a simulated chemical/biological attack. Similar to the Media Security and Reliability Council in the US, the UK Media Emergency Forum has published best practice guidelines for enhancing the media's ability to perform critical functions in the aftermath of a widespread outage or terrorist event

NSRAM *(Cont. from Page 9)* they can go back and forth (interchangeable). This matters because elements have behaviors that depend on back and forth flow and their attributes.

For instance, when malicious software flows into a computer, the computer will react in different ways. If the computer has no virus protection software, the computer is corrupted and will go down; however, if it has virus protection software, the software can kill the virus. Thus, elements should be able to look at what's flowing inside, back and forth, and react. The result is a matter of reliability.

Required System Inputs

The tool will require the following inputs:
1) scenario-dependent environmental stresses, or system "insults"
2) system's network of relationships
3) individual functional components' failure probability distributions
4) timing of effects onset and reconstitution/repair system repair sequencing

The tool will enable a comparative evaluation of potential functional debilitation modes

using realistically available system information augmented by reasonable engineering assumptions. The software is designed to quantify both the probability of mission outage (Pe) and outage time. Among the outputs it will provide to the user is a simple plot of Pe versus time. A notional output plot (Figure 1, page 9) is shown in the figure. The tool will be useful for determining the most critical failure points and the most cost-effective protection/upgrade approaches. ❖

NCC / ISAC *(Cont. from Page 3)* vulnerabilities, threats, intrusions, and anomalies from telecommunications industry, government, and other sources. The NCC-ISAC analyzes the data with the goal of averting or mitigating impact upon the telecommunications infrastructure. Additionally, data is used

to establish baseline statistics and patterns and is maintained to provide a library of historical data. Results are sanitized and disseminated in accordance with sharing agreements established for that purpose by the NCC-ISAC participants.

The NCC's industry and government representatives use the NCC's unique organization to work together during day-to-day operations, coordinate NS/EP responses during crises, and produce emergency response plans and procedures as a result of lessons learned during actual events. ❖

Websites:

Cellular Telecommunications & Internet Association: http://www.wow-com.com/

Telecommunications Industry Association: http://www.tiaonline.org/

U.S. Telecom Association: http://www.usta.org/

I&C Sector Input to the National Strategy: http://www.wow-com.com/pdf/may2002_national_strategy.pdf

NSTAC *(Cont. from Page 6)* the advice of the NSTAC, the NCS increased its participation in standards bodies and the Executive Office of the President formed an interagency Convergence Working Group to address issues associated with network convergence.

INFORMATION SHARING

In the late 1990s, the NSTAC set out to better understand existing and proposed channels with which the telecommunications industry shares information. The NSTAC observed that information sharing depends on receiving a benefit when voluntarily shared, is based on trusted relationships, and may be affected by legal barriers. Through its Network Security Information Exchange and its task forces, the NSTAC continues to examine information sharing, especially as it relates to critical infrastructure protection and legislative and regulatory activities.

OUTREACH

Through outreach efforts such as symposia, published reports, and interaction with public and private sector leaders, the NSTAC fosters the exchange of information between NS/EP stakeholders. The NSTAC provides technical analyses and develops risk assessments with other commercial industries to heighten the awareness of cross-sector information assurance and infrastructure protection issues. The NSTAC also actively encourages the exchange of ideas among representatives from industry, Government, and academia through research and development (R&D) Exchanges. Since 1991, the NSTAC has sponsored five R&D Exchanges.

NSTAC: THE FUTURE

During the past 20 years, the NSTAC has been an integral member in one of the most successful public-private partnerships. As the NCS transitions to the DHS and the Government continues to explore new ways to protect its home front and critical infrastructures-physical and virtual-the NSTAC will continue to play an important role in furthering NS/EP priorities.

The NSTAC continually re-evaluates its relevance to the changes in technology and in the geopolitical landscape-adapting its priorities appropriately. During the next few years, it will study and provide recommendations to the President and the Administration on issues related to network and cyber security, critical infrastructure protection, infrastructure interdependencies, physical security, and information sharing.

The NSTAC members and the entities they represent are committed to the partnership in support of national security and emergency preparedness on behalf of the United States and look forward to serving the President for another 20 years. ❖

Legal Insights *(Cont. from Page 7)* enables VoIP is still buggy. The rate of call-dropping and other inconveniences is slowing adoption somewhat.

At the moment, however, there is a difficult legal obstacle to intervention. A federal judge has ruled that state public utility commissions cannot regulate VoIP because it is an "information service" rather than a regulated telecommunications service. The Federal Communications Commission appears poised to consider the issue, as there is broad dissent on the question of whether VoIP can or cannot be regulated. As Carl Wood of California's Public Utilities Commission has observed, "If it looks like a duck and walks like a duck and quacks like a duck, that's what it is."

This duck is about to take off. We need to hold on to it long enough to figure out what flight path it's on. ❖

Info Security *(Cont. from Page 4)* users-people who do not necessarily program computers, but must know how use them responsibly.

Our companies are looking within, with more Boardroom-level attention being paid to security needs and concerns than ever before. And this means investments to ensure excellence. We strongly believe that the government must also look within, and ensure security of its own systems. A September 2002 ITAA-Meta Group survey of IT management found that 77% of respondents felt the private sector was more advanced in hardening information systems than the public sector. The same percentage termed the vulnerability of the public sector to cyber attack either "high" or "extremely high."

Information security is a lynchpin of homeland and economic security. Incentives to strengthen homeland cyber defense are driving industry efforts to continue building partnerships with government organizations at all levels. At a minimum, ITAA is committed to the recognition of the following facts and principles:

● Industry owns and operates most of this infrastructure and, therefore, is its natural steward for safety and security issues;

● Government and industry share an interest in the health and growth of the Internet and e-Commerce and must find common ground on which to coordinate on critical information infrastructure protection issues;

● Government entities at the federal, state, and local levels need to better coordinate their national security activities in order to improve coordination and cooperation with the private sector;

● "Cyber ethics" must become a regular and understandable part of the Internet lexicon. Ethical online behavior must be taught at home, in school and in the workplace; and

● Government and industry share an interest in addressing critical infrastructure assurance issues on a global basis.

ITAA believes a multi-faceted approach is needed to manage risks and improve U.S. cooperation on issues of information infrastructure assurance. Cooperation must extend across industries and borders and bring together industry with government. Protecting our infrastructure is a collective responsibility.

Ours is a risk management and risk mitigation approach. There is no perfect plan to assure absolute information security, just as there is no strategy short of grounding the nation's air fleet to assure absolute airport security. We must wage a long campaign in which we constantly identify risks, weigh vulnerabilities, and adopt reasonable, rational fixes to each. ❖