Problem Solvers to the Telecommunications Industry

ATIS SECURITY SUMMIT REPORT

A Report from the Summit --

Security of Service Provider Infrastructure in an Era of Convergence, February 4-5, 2003

ABOUT ATIS

The Alliance for Telecommunications Industry Solutions (ATIS) is a member company organization that is the leader for standards and operating procedures for the communications industry. More than 400 communications companies participate in ATIS' 16 committees, forums, and Incubator Solutions programs, where work focus includes wireline and wireless network interconnection standards, number portability, improved data transmission, Internet telephony, toll-free access, telecom fraud, and order and billing issues, among others. ATIS is accredited by the American National Standards Institute (ANSI). Visit the ATIS web site at < http://www.atis.org >.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Printed in the United States of America.

ATIS Security Summit --

Security of Service Provider Infrastructure in an Era of Convergence, February 4-5, 2003

Abstract

Security threats and related protection concerns have been on the rise since the terrorist events of September 11, 2001. The critical role that enterprise, access, and core infrastructure networks play in supporting user, commercial, and government needs have turned our communication networks into terrorist targets. For these reasons, ATIS hosted a Security Summit on February 4-5, 2003, in Washington, DC. The Summit's objective was to focus on the security requirements of service provider networks, address key questions of security readiness, availability, and tactical planning to ensure the protection of our telecommunications infrastructure, and to coordinate the technical standardization processes to ensure that the right interoperable and scalable security standards can be implemented quickly and efficiently. This comprehensive approach to security is also needed to ensure the rollout of next-generation technologies that are vital to the industry: a key area of interest for ATIS.

The two-day summit gathered more than 140 leaders from all sectors of the telecommunications industry. Carriers, service providers, government officials, and standards development organizations presented their requirements and perspectives to work toward building new industry-wide standards for network, IP, and wireless security.

Table of Contents

Security of Service Provider Infrastructure in an Era of Convergence, February 4-5, 2003

1 EXECUTIVE SUMMARY

On February 4-5, 2003, the Alliance for Telecommunications Industry Solutions (ATIS) held a two-day Security Summit entitled "Security of Service Provider Infrastructure in the Era of Convergence," to bring together senior executives from wireline and wireless service providers and equipment manufacturers -- as well as high-ranking officials from government agencies -- to thoroughly assess the security aspects of the nation's communications infrastructure.

As a secondary -- but also important -- objective, the Security Summit was convened to address the findings of the ATIS "Signaling for Voice over Internet Protocol Summit (SVoIP Summit)" held August 13-14, 2002. During that Summit, wireline and wireless service providers identified IP security shortfalls as a showstopper for the national rollout of VoIP services.

Along with the assessment of today's communications system by service providers, equipment manufacturers, and government, and their estimations of where future efforts should be focused, equally important is the identification of current or future standards and "Best Practices" to determine if any unmet requirements exist. To meet this demand, leaders from an assortment of relevant Standards Development Organizations (SDOs) provided an overview of their existing and future standards work efforts, as they continue their initiatives in creating standards that meet the needs of the communications industry.

As a result of the two-day Security Summit, ten (10) common statements or themes surfaced. Of those, ensuring that industry undertakes a "holistic" approach to security, as well as the concept that security should be built into standards and not retrofitted, seemed to be reiterated numerous times by all participants and attendees. Use of the Network Reliability and Interoperability Council's (NRIC) "Best Practices" (both past and future) were also deemed of importance, while SDOs consistently stated that critical security standards and "Best Practices" must be coordinated among appropriate standards developers to ensure that necessary standards and "Best Practices" can be developed in a timely manner.

The Security Summit's findings of common themes and focus areas surrounding security (including industry standards for security being prioritized and coordinated across the industry), will be submitted to the ATIS Technical and Operations Council (TOPS Council), as they commence work-efforts to address industry's security needs, among other relevant technical and operational industry initiatives of strategic importance.

Under the TOPS Council's direction, a focus group of mid-to-senior-level management experts will be formed to thoroughly examine and comprehensively define all the themes and focus areas identified during the Security Summit; as well as other issues (not raised specifically during the summit) relevant to the industry's security needs. The focus group is expected to define a coordinated standards development program for network security, a timeline for completion of standards activities, and other work-plans that fulfill the requirements of service providers and the US Government.

2 OPENING REMARKS

ATIS President and CEO Susan Miller opened the ATIS Security Summit and offered brief remarks on the purpose and objectives of the summit program.

Ms. Miller identified three reasons for holding the ATIS Security Summit:

- *Reason One*: The nation's communications networks are terrorist targets. She noted that the terrorist acts on September 11, 2001 have raised enormous concern among leaders in industry and government over the vulnerability of the nation's critical infrastructure to terrorism. These concerns have resulted in the recent formation of the US Department of Homeland Security, in order to bring together a coordinated approach among numerous federal agencies to combat terrorism. This new department merges, under one roof, the capability to identify and assess current and future threats, map those threats against the nation's vulnerabilities, issue timely warnings, and take preventative and protective action.

  Specific to the communications industry, Ms Miller also noted that various government agencies and advisory bodies are active in efforts to identify terrorist vulnerabilities in the nation's communications networks. She noted that the FCC launched its sixth Network Reliability and Interoperability Council (NRIC VI), which is leading efforts to identify best practices designed to support network security and reliability in both existing and future network technologies and through the delivery of services.

  In addition to NRIC VI, Ms. Miller noted that the White House's National Security in Telecommunications Advisory Committee (NSTAC), as well as the President's Critical Infrastructure Protection Board, are evaluating the issues of emergency preparedness and emergency communications.

- *Reason Two:* Without resolving the issues around security and lacking the right standards for security being developed and implemented, the industry is delaying the deployment of next-generation services desired by consumers. Ms. Miller noted that ATIS and ATIS Committee T1 hosted a summit on Voice over IP (VoIP) in August 2002. Wireline and wireless service provider requirements for the successful rollout of VoIP were identified by the industry's leading service provider executives, and specifically, security was identified as a "showstopper" for the rollout of VoIP. She noted that as VoIP becomes a fundamental architecture of our networks, it also becomes a back door that makes national and international infrastructures unavailable in an emergency. It was recommended at the VoIP summit that the industry develop a comprehensive approach to security, including standards to protect networks from denial of service attacks. Ms. Miller further offered that the existing reliability of the network has been due in large part to cooperative industry efforts and standardization of frameworks for service and performance requirements, interfaces, and physical characteristics for technologies, systems, and business processes. She noted that both NRIC VI and NSTAC view industry standardization as a critical component in securing the networks of today and the packet-based services of the future. VoIP, mobile services, data services, data exchange, and other next-generation technology deployments will rely on industry-wide standards that ensure security and thwart acts of terrorism.

- *Reason Three*: ATIS has identified the need to address network security issues, whether it be for the rollout of new technologies and services, or the need to protect our networks and the networks of the future from significant security threats, in a prioritized and coordinated approach across the industry, with all the stakeholders involved. The stakeholders include service providers, the standards groups, the equipment and software vendors and -- with respect to security -- the government. She emphasized the need to address these issues and get the right standards developed, all in a prioritized, coordinated way that will realize greater efficiencies and greater effectiveness both in costs and process for the entire industry. She added that the challenges of developing such standards are quite significant when one considers the large number of groups working on

industry standards and the need to coordinate such work. A rough count has shown there are nearly 300 such groups.

In conclusion, Ms. Miller identified the objective of the summit: to identify where there is a need for interoperable and scalable security standards within and among multi-service provider networks.

Ms. Miller then introduced the next introductory speaker, ATIS Board Chairman Ross Ireland of SBC Communications.

3 ATIS PLAN FOR CHANGE

Ross Ireland is Senior Executive Vice President for Services at SBC Communications and Chairman of the ATIS Board of Directors.

Mr. Ireland opened his remarks by noting the economic difficulties of the communications industry in general. While technology change continues its rapid pace, industry companies are experiencing a time of scarce capital, reduced investment, and bankruptcies, with slow response from the regulatory community. Mr. Ireland further explained that companies have been forced to ask themselves "where's the value?" and are interested in channeling what resources they do have towards priorities.

He further expressed that a new approach is required for standards, one that removes inefficiencies and promotes cost effectiveness to standardization activities and their outputs. Mr. Ireland noted that there are over 300-plus standards groups in existence today: many were born during a boom economy period, but are now a significant drain on business resources. He shared that a lack of coordination exists between these groups, and in effect, there is an industry failure to work on standardization activities that address the industry's most urgent priorities. This results in competing standards, standards that do not support interoperability, and standards that are not implementable. In short, the standards process in today's environment is not an efficient model for doing business.

Mr. Ireland elaborated on efforts now underway at ATIS to execute a "Plan for Change" for the industry's standardization activities that identifies the priority issues of the industry and coordinates efforts of standards organizations and forums. He shared that ATIS has 1,400 participants from more than 400 companies active in its 16 industry standards committees and forums. He further mentioned that, while it is a membership organization of communications companies, it is not a trade or advocacy association and has no restrictions on membership. ATIS membership includes local service providers, interexchange carriers, manufacturers, software developers, resellers, and other companies. The ATIS membership offers a broad perspective and the ATIS Board of Directors governing the organization is comprised of the most senior representatives from within the industry. He mentioned that ATIS is an organization accredited by the American National Standards Institute (ANSI). Furthermore, he elaborated that these attributes uniquely position ATIS to prioritize the industry's technical and operational issues, and to coordinate needed standards work among standards organizations.

Mr. Ireland then shared with the audience the basics of the ATIS "Plan for Change." He remarked that the ATIS Board of Directors launched the TOPS Council, which has identified sixteen key industry priorities. These priorities -- with the five most urgent priorities (those that Mr. Ireland indicated are keeping the industry's chief technical executives "up at night") identified at the top of the list -- are as follows:

1. VoIP
2. Wide Area Ethernet
3. Mobile Wireless Service
4. Security Issues
5. Data Interchange (Billing)
6. Optical Networks
7. DSL Evolution
8. Wireless Evolution
9. IP Telecom Network Management
10. Reliability Measurements
11. Wide Area Storage
12. Numbering
13. Emergency Communications Services for IP
14. Communications Assistance for Law Enforcement Act (CALEA)
15. E911 Evolution
16. Priority Access

Mr. Ireland said that the ATIS TOPS Council is identifying, on behalf of the industry, the necessary steps for moving forward on standards activities for these 16 priorities. Furthermore, Mr. Ireland shared that the council will identify what standards work has been completed, what gaps in standards work exists under each priority, and the most appropriate standards organizations for completing necessary standards work, so that the industry can effectively "fill the gaps." He emphasized that the effort will require close partnership among SDOs, in order to achieve a cohesive, coordinated approach that thoroughly addresses these industry priorities.

Mr. Ireland explained that the summits hosted by ATIS -- specifically the VoIP Summit held in August 2002 and now the ATIS Security Summit -- are identifying the "standards gaps" among the 16 industry priorities, and noted that the TOPS Council has additionally identified sub-elements under each of the priorities. He shared that the successful implementation of the ATIS Plan for Change would lead to the elimination of duplicative standards efforts, achieve cost and process efficiencies, optimize investment and resources allocated by companies towards standards development, move "stuck" technologies forward (i.e., technologies that cannot advance because no standards or solutions exist to support them in networks), and bring products and services to market faster. In closing, he indicated that achieving these efforts would position the industry to achieve one unified voice for US standards.

4 GOVERNMENT PERSPECTIVES ON SECURITY

Moderator Susan Miller introduced the goal of this session as the need to access information securely and reliably as the foundation of human and economic commerce. She then introduced the Government Perspectives on Security session speakers: Mr. Brent Greene of the National Communications System, Mr. William Ruhl, USTA Member on NSTAC, and Mr. Howard Schmidt, Chair of the President's Critical Infrastructure Protection Board.

4.1 NCS Perspective

Brent Greene is Deputy Manager of the National Communications System (NCS).

Mr. Greene's message was succinct and very clear: "the security of the [national telecommunications] backbone is critical."

He prefaced his remarks by introducing the National Communication System (NCS), a government entity that coordinates national security and emergency preparedness (NS/EP) using the telecommunications backbone. Its accomplishes its goals by partnering closely with the telecommunications industry. He stated that ATIS has been and will continue to play a major role in building partnership relationships between the industry and government regarding national standards, and agreed with Ross Ireland that the coordination of standards is key. The challenge now, as a nation, is to bring those national standards into the global standards arena.

Mr. Greene emphasized that it is through a strong industry/government partnership that a national telecommunications security direction is designed. He characterized NCS' industry partnering with four key elements, which together establish the security direction of the nation:

- *Industry CEO to NSTAC*: An executive level partnering organization was established in 1982 with the establishment of the National Security Telecommunications Advisory Council (NSTAC). It is here that owners/operators of the telecommunications infrastructure can partner with NCS on Critical Infrastructure Protection (CIP) strategic level issues
- *Operational Arm*: The process of actually coordinating telecommunications in response to emergency events in the direct support of "first responders." Mr. Green elaborated on the development of the Government Emergency Telecommunications Service (GETS). This is a good example of how industry and government can work together to support critical infrastructure needs. He went on to say that prior to "9/11" only 70,000 GETS cards were in distribution to government employees. Its use, allowing priority access to telecommunications networks through the 710 access code, proved vital during "9/11" and the critical period that followed. Since that time, NCS has doubled the amount of cards issued. His next issue dealt with the need to develop a similar procedure using the wireless telecommunications infrastructure. NCS has, to date, been working closely with T-Mobile, a GSM service provider, in deploying wireless priority access service (PAS) at the base-station level. NCS will soon work with AT&T Wireless and Cingular, who are also deploying GSM networks. Budget restraints at this point preclude NCS from working with CDMA carriers, but NCS realizes the need to deploy PAS in all networks to increase access, lower stress on the networks, and spread the burden of national security.
- *Cyber Warning Infrastructure Network (CWIN)*: Mr. Greene introduced the CWIN, describing how the structure is designed and how it connects NCS to the Department of Transportation, Department of Energy, the Natural Resources Information Council (NRIC), and other agencies in a time of emergency. This network is different from and not connected to the common Signaling System 7 (SS7) network in use today, and that the core or "inner-ring" to this spoke-wheel architecture is nationally classified information. The initial plan calls for about 70 nodes (spokes) or network coordination centers, but may be increased to as many as 150 or more.
- *IP based early warning system*: Mr. Greene's final key element dealt with a program that is not yet piloted but explained that it is designed to be a national level, early warning system via the Internet. He stressed that the design of such a system remains to be determined until the lack of security on the Internet is mastered.

Mr. Green concluded by saying that underlying everything he has mentioned are technical and operational standards. Getting industry concurrence on what the standards are and being able to act with speed and urgency is paramount. He sees the NCS participating by identifying which standards can truly advance national and global security, leading to protection of the telecommunications backbone.

4.2 NSTAC Perspective

William Ruhl is CEO of D&E Communications Inc., an ATIS Board Member and USTA Member of NSTAC.

The National Security Telecommunications Advisory Committee (NSTAC) was formed in 1982 to advise the President on national security and critical infrastructure preparedness issues. It represents a marriage between government and industry. Mr. Ruhl reported that in its 20-year history, NSTAC has greatly facilitated an increased dialogue between industry and government, successfully defending critical infrastructures.

NSTAC is comprised of 30 executive level (CEO) industry leaders (suppliers, service providers, hardware manufacturers, software providers, and system integrators) appointed by the President. The principal working group of NSTAC is the Industry Executive Sub-committee (IES), whose focus has been on the convergence of technologies: this is deemed essential to the success of the telecommunications industry. Mr. Ruhl identified the converging technologies to be voice, data, and video.

Mr. Ruhl presented some of the critical issues with which NSTAC is involved but did not elaborate extensively on any particular issue. They are:

- *Critical Infrastructure Protection (CIP)*.
- *Information Sharing and Analysis*: Mr. Ruhl noted that the Freedom of Information Act (FOIA) tended to inhibit sharing of information. However, due to the efforts of NSTAC, the new Homeland Security Act grants exemptions believed necessary for security protection.
- *Priority Access*: With the Government Emergency Telecommunications Service (GETS).
- *Cyber-security and Crime*.
- *Network Security*: Dealing with SS7, Internet, and the primary telephone network.

Mr. Ruhl went on to list NSTAC success stories, emphasizing the special importance of NSTAC's work on last mile bandwidth and the IEEE 802.11 wireless LANs. The NSTAC successes are as follows:

- National Coordinating Center;
- Special Routing Arrangement Service;
- Wireless Priority Service;
- Telecommunications Service Priority;
- Telecom vulnerability and survivability assessments;
- Telecom industry engagement in critical infrastructure protection issues;
- Network Security Information Exchange;
- Network convergence studies;

- Critical Telecom Facility Protection;
- Telecommunications interdependencies;
- Last mile bandwidth vulnerabilities;
- International cooperation on cyber attacks;
- Wireless security studies (802.11, etc.); and
- Input to national strategy to secure cyberspace.

Mr. Ruhl identified some of the current issues the NSTAC IES is currently involved in, which include:

- *Cyber crime penalties*;
- *Access requirements* at telecom central offices;
- *Redundancy issues* in the financial sector; and
- *Wireless security (private and commercial networks)*: Mr. Ruhl noted that the IES has just released, for ballot, a recommendation for the President based on their recent study on Wireless Security.

In conclusion, Mr. Ruhl emphasized that NSTAC brings an unique strategic focus to both physical and cyber issues of national security, deals with complex problems, and brings technical depth to security matters. In addition to developing Presidential recommendations, NSTAC established the National Coordinating Center (NCC), an organization where industry representatives work side-by-side on a daily basis with members of the NCS staff. The NCC facilitates information sharing between industry and government to lessen the impact of threat, intrusion, and vulnerability via early notification. The NCC was responsible for coordinating restoration of the telecommunication infrastructure following "9/11."

4.3 Critical Infrastructure Protection Board Perspective (CIP)

Howard Schmidt was recently named Chair of the President's Critical Infrastructure Protection Board.

In response to "9/11" and the President's call for a national strategy to defend cyberspace, the Critical Infrastructure Protection Board -- or Cyberboard as it is commonly known -- was created in October 2001. The concept is to get senior governmental leadership involved and secure cyberspace and protect our nation's growing dependency on it.

Cyberspace is the central nervous system for the nation's critical infrastructure, which is composed of the private sector and public institutions. The CIP Board has identified the critical infrastructure areas as: agriculture, food & water, public health, emergency services, government, defense industrial base, energy, transportation, chemical, banking, Information Technology (IT) & telecommunications, and shipping. These critical areas affect the nation as a whole and are all IT-based. The obvious downside to being all IT-based is that there are vulnerabilities in cyberspace. There are malicious forces (people) wishing to exploit these vulnerabilities to do damage to national security, public safety, and the economic wealth of our nation.

In response, the Cyberboard released a draft National Strategy – the first draft strategy ever – to encourage the public and industry to secure their portion of cyberspace. This strategy,

complemented with the National Strategy of Physical Infrastructure and Key Assets will comprise the HomeLand Security (HLS) Strategy. With valuable input from NCS, NSTAC, the National Infrastructure Advisory Committee (NIAC), FCC, and the public, the Cyberboard is revising the draft National Security Strategy and focusing in on five, clearly identified cyberspace security priorities. These priorities are:

1. The need to develop a robust national cyber-security response system.
2. National Cyberspace Security Threat and Vulnerability Reduction Program. (Accelerating patch management issues where vulnerabilities exist – write more secure code.)
3. National Cyberspace Security and Training Program. (Creating more IT security professionals, adding to current certification programs, and educating home users. Firewalls and boundaries are no longer sufficient, but must be made secure out to the end-points -- end-to-end security.)
4. The need to do more to secure our government systems.
5. National Security and International Cyberspace Security Cooperation. (Including international cooperation of law enforcement to take stringent measures for security.)

Mr. Schmidt closed by saying the Cyberboard uncovered a vital statistic: 80-85% of what is deemed as critical infrastructure is owned and operated by the private sector. Mr. Schmidt encouraged everyone present to take action in response to this statistic, consistent with meeting the five national priorities while simultaneously making decisions that are good for their business models, customers, and cost-effective risk analyses.

To close this session on Government Perspectives, Susan Miller summarized each speaker's presentation on the current state of national security issues, and provided an historical view of their organizations, current activities, and future goals. Most importantly, Susan Miller noted that each executive highlighted the importance of partnerships between government and industry to build a national concurrence to protect the security backbone on a national and international basis.

5 SERVICE PROVIDER PERPSECTIVES ON SECURITY

Moderator Ross Ireland introduced the Service Provider session by introducing a large panel of presenters drawn from different segments of the service provider industry who addressed security issues from the perspective of the carrier, SS7 provider, and the wireless space. Mr. Bill Smith of BellSouth, Mr. Mark Wegleitner of Verizon, Mr. John Erickson of SBC Communications, and Mr. Arthur Deacon of AT&T presented wireline perspectives; Mr. Bruce Johnson of VeriSign and Mr. Ken Hunter of Agilent Technologies presented SS7 network perspectives; and Mr. Ramu Potarazu of Intelsat and Mr. David Wachter of T-Mobile concluded with wireless perspectives.

5.1 WIRELINE PERSPECTIVES

5.1.1 BellSouth Perspective

Bill Smith is Chief Product Development and Technology Officer at BellSouth, an ATIS Board Member and Chairman of the ATIS Board's new TOPS Council.

Mr. Smith started by noting that the newest and greatest challenge facing the industry is to think outside the box of traditional threats and risks – where industry has experience in protecting its networks -- and to visualize, understand, and prepare for those threats that are unimaginable.

To assist in mitigating attacks and risks, Mr. Smith commented that BellSouth, first and foremost, follows the "Best Practices" established by the NRIC VI, and particularly finds the guidelines created through the NRIC groups on Network Reliability, Network Interoperability, and Broadband a true value-add. The addition of NRIC VI's "Homeland Security," and its focus groups on Physical Security and Cyber Security, has also been valuable as a focus of BellSouth.

In regards to physical security, BellSouth is keen on the focus group's efforts to establish guidelines to address vulnerabilities such as design & constructions, infrastructure, and physical access control. Due to this work, BellSouth has had to rethink several of its fundamental operating approaches (e.g., publicly advertising building locations). Further, BellSouth believes that nearly all major network outages could have been prevented if *NRIC VI: Physical Security Best Practices* had been followed.

Mr. Smith noted that BellSouth's focus in the physical security space is to "protect the network's critical payload" from three (3) major attacks: 1) Interception; 2) Modification; and 3) Interruption. Today, the acknowledge-base and experience exist to protect the "payload" against disasters already seen. It is the malicious attacks that haven't been experienced or observed that cause the greatest concern and, hence, the need for industry to prepare for the unthinkable.

As to cyber-security, BellSouth follows the NRIC focus group's efforts to establish guidelines to address issues such as user validation/authentication, software release/control, administrative procedures, and background checks on critical personnel. Standardization efforts in the area of "Management Plan" -- such as the initiatives undertaken by ATIS/T1M1 -- are also of importance, and BellSouth will rely on existing activities under ATIS, and other SDOs, to continue this critical work.

The ongoing rollout of Voice over IP (VoIP) is also a focus area for BellSouth. Areas of interest include user authentication, signaling issues (as discovered during the ATIS Signaling Over IP Summit), VoIP's support of CALEA, and other security issues.

Mr. Smith believes there are opportunities for improvement in addressing security including collection tools (associated with cyber-security), software development tools, and background checks for critical personnel. Additional analysis between IPv6 and IPv4 migration, interoperability testing, and other network interactions should also be further explored.

Mr. Smith summarized his perspective by saying that there is a great deal of experience in addressing traditional security issues, but malicious intent raises new concerns and demands a new approach: that NRIC VI Best Practices should be followed when appropriate, that industry should rethink its approach to its network architecture, and that standards groups play a critical role that should be relied upon by industry. In closing, Mr. Smith commented that security is an industry challenge – not a company challenge – that demands an industry solution.

5.1.2 Verizon Perspective

Mark Wegleitner is Senior Vice President of Technology, CTO for Verizon Communications, and an ATIS Board member.

Mr. Wegleitner opened by noting that as industry migrates to the packet-based network paradigm, it now faces fresh challenges in securing its networks, as end-users have access to networks like

never before. As such, new approaches to security are critical. Today, logical and physical security elements of the network must be designed in (from the beginning) and not retrofitted.

Verizon's top security concerns are providing protection to the customer, protection of the systems, maintaining service availability (regardless of network technology), and ensuring confidentiality and integrity of their information. Verizon seeks to ensure there is no malicious action between the customer and the system, or between the operations force and the system, or even between the system elements in the case of an indirect attack. With 80-85% of the communications critical infrastructure residing in the private sector, responsibility for ensuring network integrity falls on private industry.

Mr. Wegleitner's philosophy for implementing 21st Century cyber-security is:

- Perimeter hardening, with physical measures being just a first step;
- Security must be layered (i.e. defense-in-depth);
- All network elements must be hardened as "Defensive Strong Points" in their own right;
- Deploy multiple security technologies, both internally and externally;
- Deployed assets must have integrated security capabilities that support end-to-end protection; and
- No networking link is trustable.

Verizon is focused on network protocol protection, application protocol protection, and management protocol protection. To this end, Verizon has several major internal initiatives underway. First, Verizon is proactively improving internal infrastructure by securing logins, blocking network "sniffing," and testing security measures. Secondly, Verizon is developing service offerings for customers to include network and applications monitoring, firewall management, and web/email scanning. Lastly, Verizon is sharing their findings and (current and future) requirements with industry and standards groups globally, such as ATIS/T1M1, for standards development and coordination.

Mr. Wegleitner believes industry's challenges are:

- Service providers must collaborate on accumulating security related actuarial information to measure progress;
- Standards bodies must follow ANSI/ITU-developed security frameworks and leverage existing standard technologies recognizing today's reality; and
- The vendor community must implement current Best Practices, adhere to standards, support future needs, and adjust Product Plans to Today's Security Realities.

In conclusion, Mr. Wegleitner challenged the standards bodies to address carrier class security issues and architecture, the vendors to produce equipment and software that meet security needs, and the customers and carriers to work together to mitigate security threats.

5.1.3 SBC Communications Perspective

John Erickson is Vice President for Information Technology at SBC Technology Resources, Inc.

Mr. Erickson opened by describing the current state of the Internet. The number of Internet hosts has been increasing, despite the decline in the economy and the NASDAQ. The number of threats to the Internet is continuing to rise and fixing them has significant cost.

At the same time, broadband adoption is growing and expected to continue to do so. We have reached the point where we cannot live without data communications. Networks are everywhere, always on, and average bandwidth per user is increasing. These trends mean that the window of opportunity for cyber-attacks has grown. Attacks are more frequent, more sophisticated, and easier to launch than previously, and cyber-terrorism has begun. In this atmosphere of "perfect storm" for cyber-security, there is a potential for data corruption or loss, revenue losses, and critical infrastructure damage. To address the threats, we must consider the many different aspects of the problem and look for multi-contributor solutions.

Carriers have two fundamental roles in this situation: 1) protecting their networks; and 2) protecting the customer. Accomplishing these two things is vastly complicated for the carriers because of the huge scale of their data networks, which are comprised of millions of ports and terrabytes of data; the scope of their customer base, which ranges from residential subscribers to multinational corporations; and the broad penetration of their services, which means that it is literally impossible to screen every individual. In addition, carrier networks themselves are complex and evolving: operation support systems are being changed out, the voice network is moving from TDM to packet-based, and protocols are becoming more complicated.

Mr. Erickson stated that it is also important to remember that carriers are also system integrators. As a result, the vulnerability of the interconnected system increases significantly as more components, each with inherent vulnerabilities, are interconnected. A single compromised system can be used to launch an attack on other parts of the network. Carriers cannot afford to look at every detail of every box integrated into the network. Their plea is that vendors provide them components that are secure, with vulnerabilities shut down before they reach the carriers.

Mr. Erickson divided possible solutions to cyber-threats into three categories:

1. The worst responses are denial of the problem, physical isolation, or reconstructing the network after a problem has been encountered.
2. Attempting to hide your presence on the network, surgical removal of a problem once it has been found, and building a perimeter defense are better responses, but far from adequate.
3. The three best alternatives are network-based security; systemic isolation, which adds security agents within the network; and organic growth, which builds security into the network from the ground up.

Network-based security has some nice aspects, for it allows carriers to provide some protection to their customers' networks and allows aggregation of data on threats, which may result in earlier detection. Designing-in security from the beginning, down to the processor level, is extremely important.

Mr. Erickson next addressed what carriers are doing, addressing both telephony and data, since the two networks are both important in solutions to this problem. On the telephony side, he stated

that carriers are using some traditional approaches for security: fault tolerance, dual homing to ensure there is a link left in service if one fails, ring redundancy for central office interconnection, and large network operations centers that continually track the health of telephony and private line networks.

On the data side, the picture is more complex. Carriers are addressing viruses, trojans, and worms via scanning and cleaning. Integrity checking and diligent backups are being used to address potential data corruption. Unwanted content can be filtered, although it is sometimes hard to know what content is wanted and what is not. Firewalls can knock some denial of service attacks down. Authentication can prevent break-ins. Data interception and theft can be addressed by encryption, in VPNs, for example.

Thus, the carrier data space consists of backbone routers and switches and routers interconnected in redundant ways, with wide data security added to this mix across the data enterprise. In addition, carriers have corporate information security groups who administer security policies and practices, business continuity groups who contemplate disasters and how to recover from them, national coordination, and very restricted access to management and signaling networks. Although very serious damage can be done by compromising a host-to-host network or networks, much more serious damage can be done by compromising the signaling or management networks.

So what should the industry do? Denial is obviously not a good approach. Everyone needs security, down to the individual user. The industry needs to close the vulnerabilities in the existing systems and create the secure black box. More needs to be done in the areas of network-based security and developing software that can serve as a systemic immune system for the network. Security should be built into systems from the beginning, as they are being designed. Lastly, the industry should continue collaboration to share what works and what does not.

Mr. Erickson closed by reporting that SBC has created the Internet Assurance and Security Center in the SBC TRI labs. This Center will focus on protecting customer networks and critical infrastructure. It is intended to promote partnership between industry, government, and academia to look at the deeper aspects of security and how it might be improved.

5.1.4 AT&T Perspective

Arthur Deacon is Vice President of Network Operations, Service Assurance and CCO at AT&T.

Mr. Deacon described how Network Management intersects security in three fundamental ways:

- As a mechanism to initiate the security policy on the devices that constitute the network,
- As a mechanism to collect and process information that may indicate violations, or attempted violations, of the policy; and
- As a component of the network's infrastructure that must also be protected and monitored.

Also, to ensure network security, industry needs to consider three critical elements: people, process, and system.

Mr. Deacon cautioned that in the course of devising and deploying networks, industry must protect the various network planes, such as the End-User, Control, and Management, against vulnerabilities and threats such as interruption, interception, modification, and fabrication. Additionally, eight security dimensions including Access Management, Authentication, Non-

repudiation, Data Security, Communication Security, Integrity, Availability, and Privacy must be understood internally as well as externally.

Mr. Deacon cited, as a case to point, the importance of knowing precisely where critical network software is being written, where it gets coded, and how it gets tested before deployment in the network. The trend toward "off shoring" this mission-critical software is disconcerting and a major hurdle for the service providers desiring to ensure solid end-to-end security (i.e, from a product's deployment to its removal from service).

Mr. Deacon noted that as industry migrates to packet-based services, Network Management tools must also evolve. To this end:

- Capabilities are required to monitor, detect, and react to traffic conditions in networks whether the conditions are day-to-day events or anomalies;
- Development is needed for packet-based services where comprehensive capabilities have been developed and implemented for circuit-switched networks;
- Management and support structure must evolve proportionally with technology;
- A holistic approach to packet network management is essential, as router networks and security concerns become more complex.

In today's communications environment, capability authentication is handled via proxy (often human) and requirements vary significantly from customer-to-customer, vendor-to-vendor, and ISP-to-ISP. The tasks in the operations environment are also predominantly manual (with high risk for errors), and monitoring and detection schemes lag the equipment design and development.

Mr. Deacon commented that for the future environment, enhanced network management capabilities should be based on consistent policy-based network management tools. Additionally, security should be considered a subset of the total management system where alerts can be detected quickly and dealt with efficiency. (In the example of “the worm,” the detection was outstanding, but appropriate response was less than clear.)

Mr. Deacon's recommendations for the industry:

- Vendors should continue to develop policy-based network management capabilities/systems/tools for use by the service providers. All vendors and service providers should be champions within the industry and standards community to lead advancement toward this long-term goal.
- Standard bodies (such as the IETF) should be specifically charged to develop requirements and standards to ensure the systems are interoperable across all platforms.
- Industry forums (such as the NRIC) should develop best practices that build upon existing standards and capabilities.
- Long-term IP address accountability is essential and must be assured.
- Vendors should build protections into their hardware and software that reduce the ability of intruders to hide their identity (“spoofing”).
- Incident disclosure in the current NCS/NCC model should be improved.
- Vendors should develop products that install with unnecessary features turned-off and security that must be configured by policy before operation.
- Vendors should implement industry standards for OAM&P security in software, network elements, and management systems (NRIC VI Best Practice).

Mr. Deacon summarized industry's next steps as:

1. *In the near term*: Codify and filter access control, to enable people to do the tasks manually;
2. *In the medium term*: Automate repetitive tasks for consistency; and
3. *In the long term*: Create automation that supersedes human intervention in the separation of the End User Plane, Control Plane, and Management Plane against threats (i.e., development of "Automated Intelligence").

Mr. Deacon closed urging industry to be preventive, proactive, and predictive to secure the nation's networks.

5.2 SS7 NETWORK PERSPECTIVES

5.2.1 VeriSign Perspective

Bruce Johnson is Senior Vice President of Operations and Engineering at VeriSign Telecommunication Services, an ATIS Board Member, and Treasurer of ATIS.

Mr. Johnson opened his remarks by pointing out that SS7 is both a protocol and an architecture. He emphasized that the SS7 network itself is rather simple, though the services that run over it are complicated.

The four components of the SS7 architecture are telephone switches or signaling points (SPs), links, signaling transfer points (STPs), and databases or signaling control points (SCPs). SPs are connected via A-links to STPs, which are specialized packet switches for routing SS7 messages. The fourth element of the SS7 architecture is the SCPs or databases themselves, such as a local number portability database or an 800 database. Both A links and STPs are deployed as mated pairs, so that if one element of the pair goes out, the other can pick up the load. In addition, the two elements of a mated pair of STPs are generally geographically separated so that the different switches in a pair are on different power grids and served by different network infrastructure.

Mr. Johnson discussed five potential threats to the SS7 network:

1. Unauthorized access;
2. Masquerading;
3. Threats to data integrity;
4. Threats to data confidentiality; and
5. Denial of Service (DoS).

In evaluating the risk of unauthorized physical access to the network, Mr. Johnson stated that it is important to remember that SS7 is a packet network used to communicate between telecom switches, databases, and STPs. The SS7 network is therefore a closed network that end users cannot access. The heart of the SS7 network, the STPs, have what is known as a gateway screening function, which allows control of messages both in entering the network as well as where they are routed. These controls are set up and maintained by the SS7 network operators. Messages from the Internet cannot get into the SS7, further reducing external threats.

Laxness in managing STP gateway screening tables is probably the major risk to maintaining secure SS7 networks. Although historically, local exchange carriers were quite stringent in managing gateway screening controls, there is a trend away from this among some new network operators with the introduction of many new SS7-based services.

In some cases, IP is being used as an SS7 transport protocol to get beyond the bandwidth limitations of earlier SS7 network architectures. This also can introduce the risk of unauthorized access, depending on the architecture used. Mr. Johnson's company continues to use a point-to-point architecture for their SS7 over IP deployment. Other possibilities are IP clouds or, undesirably, sending SS7 messages directly over the Internet.

Unauthorized personnel gaining physical access to an STP or switch site can also cause physical damage to the SS7 network. Although providers have secure access to their buildings and hopefully do thorough background checks of personnel with SS7 network access, colocation makes the network more accessible.

Masquerading refers to introducing fraudulent originating or terminating SS7 messages into SPs, STPs, or databases. SS7 protocol analyzers are used by many network operators for conformance and service testing, and in the hands of the wrong person can be used for masquerading. For example, database inquiry or TCAP messages could be used to obtain data from databases, or network management messages could be used to shut down network nodes, trunk groups, or services. The risk of successful masquerading and shutting down nodes is reduced significantly by safeguards built into the protocol itself, since the protocol will automatically reactivate parts of the network removed from service unless continually instructed not to do so.

In considering threats to integrity, or manipulation of system configuration or system data files, Mr. Johnson noted that problems of this type are most likely to result from unauthorized access to the systems used to administer STP translation and screening tables. Because of the secure environment in which the administration systems are operated, security breaches of this type are most likely to be internal (i.e., carried out by personnel internal to the company itself).

Threats to confidentiality -- such as eavesdropping -- can also result from breaches of SS7 network security, as SS7 messages carry sensitive information. For example, messages to calling card validation databases contain the calling card numbers and PINS of the card holder. This information, if obtained by the wrong party, can be used in fraud.

The possibility of breaches in SS7 network security resulting in denial of service (DoS) is reduced by the fact that the SS7 protocol itself is very robust, designed to minimize congestion and route around failures. (However, it is not eliminated.) Loops in message routing have recently been a problem, resulting in increased network congestion. It is possible that such loops could be introduced intentionally, causing enough congestion to result in isolating interconnected networks from one another.

Mr. Johnson concluded by saying that the 3 major threats to the SS7 network are:

1. Bugs in SSP or STP software, such as those which caused major outages in the past;
2. Security breaches or network failures caused by internal personnel, which will hopefully be recognized and correctly quickly; and
3. SS7 over IP, if insecure architectures are deployed.

Improving the quality of software in the switches, reducing internal personnel threats, and implementing SS7 over IP in a point-to-point method will all work to minimize these threats.

5.2.2 Agilent Technologies Perspective

Ken Hunter is Senior Solutions Architect with Agilent Technologies.

Agilent has brought forth an SS7 security practice to detect and remedy security breaches in the SS7. Mr. Hunter noted that when SS7 fails, call and service handling becomes impossible. Also, while detection of security breaches are fine, recovery is not that good, and reports may not reveal internal problems such as operational errors or insider abuse. This problem is exemplified where larger service providers grant access to 2nd and 3rd tier providers, causing many times more entries into the SS7 network. These additional entries must be securely protected.

Mr. Hunter went on to list SS7 vulnerabilities and potential methods of attack:

- *Insider Network Abuse* is possible both unintentionally by not keeping tables updated for the gateway screening, and intentionally by such methods as L&P fraud, billing, credit card fraud, changing data, injecting messages, or even modifying code running at the card level.
- *Outside Attacks* focus on denial of services (DoSs) and network (message) flooding. Also problematic is the numerous international network access points, which may result in interference and degradation, and the individual hackers that attempt to access the network for consumer fraud.

Mr. Hunter offered the sharp increase in network traffic during the 9/11 terrorist attacks as an example of the network's vulnerability to flooding and saturation, and encouraged everyone to imagine the implications of an orchestrated, concurrent rogue message attack aimed at crippling the national network, similar to the geographic nature of the attacks on 9/11.

He reiterated that the inherent SS7 security capabilities are not robust because the original SS7 network was designed for use in a closed network, and therefore wasn't designed to combat security breaches. Subsequently, there have been very few changes in standards to upgrade the entire SS7 capability, though Technical Subcommittee T1S1 has created important recommendations for the evolving environment.

Mr. Hunter noted the prevention of attacks on three SS7 particular targets is of importance -- especially in regards to LNP. They are:

1. *SSP* – Perimeter gateway for attack;
2. *STP* – Routing attack target; and
3. *SCP* – Database attack target.

Mr. Hunter stated that there is no end-to-end protection for all of these components. Agilent's response has been to put together 24 potential scenarios for insider and outsider attacks, in order to detect and mediate security attacks, while better understanding and identifying the sources.

Mr. Hunter concluded by stating that the resulting costs of security breaches are enormous. He argued that security solutions are further compounded by the desire of security officers not to reveal the flaws in their networks. However, upgrading the SS7 security infrastructure would be invaluable.

5.3 WIRELESS PERSPECTIVES

5.3.1 Intelsat Perspective

Ramu Potarazu is President and COO at Intelsat, Ltd.

Mr. Potarazu summarized the mission of Intelsat, describing it as the premier satellite provider interconnecting 200 countries and territories and 99% of the world. Since "privatizing" in 2001, Intelsat has made a number of changes in its operating procedures to expand its service offerings, apply security protocols more broadly, and established a government unit to concentrate on serving its government customers.

Intelsat relies on many of the carriers present for its infrastructure, and therefore, its security. Whereas originally Intelsat had its own, very tight security with its own space segment capacity, with expanded operations into "hybrid solutions," it now relies heavily on colleague providers and their ability to make sure their infrastructure is intact. Intelsat prides itself on its Quality of Service (QoS) record spanning 30 years of operation, during which no customer has ever been unable to use its ground or satellite network.

System security is extremely important, as 50 ground stations access the satellite network worldwide for a wide range of government, enterprise, and corporate customers, which achieves a "four-nines" level of quality of service similar to the "five-nines" expected by wireline carriers. All access to the ground and satellite network, whether via carrier partners for the ground segment or ground stations for the satellite segment, follows the Intelsat "Security Pack" process that protects the network from external intrusions. Satellite assets represent a $300 million investment per platform, which must be protected with command encryption, physical security, and secure access via the Command Center.

Internal security at Intelsat includes some basic but vital tactics such as redundant antennas, restricted access to ITAR-cleared staff, quarterly backup operations to validate sky security, and -- post 9/11 -- moving central control back to Intelsat headquarters. In conclusion, it is most important for Intelsat that all communication links are secure via partners, because of the level of sensitive data that Intelsat transmits.

5.3.2 T-Mobile Perspective

David E. Wachter is Director of Business Development at T-Mobile.

Mr. Wachter described T-Mobile as committed to pushing the edge of the wireless services: GSM is deployed across the entire network, GPRS has rolled out throughout the US, wireless LAN "T-mobile hotspots" are being enabled coast-to-coast, EDGE will be deployed later this year, and -- in Europe -- UMTS.

T-Mobile's focus is therefore ensuring customer security. To give customers what they are looking for -- namely the ability to roam from one wireless LAN to another -- and the ability to move from wireless "hotspots" to GSM networks, T-Mobile's main concern is making these networks interoperable.

Mr. Wachter sites an opportunity for T-Mobile to improve wireless LAN security by interworking it with the GSM network. He identifies the biggest security issue for wireless being the minimal physical barriers to intercepting a wireless signal. This is complicated by the evolving hacker technologies, making for easy hacks.

GSM operates under a very “standards-driven” network with built in authentication practices for mobile wireless using the SIM card, which ties back into authentication at the network level. It includes encryption for user identity protection, and T-Mobile substitutes the IMSI (or mobile identifier) for a temporary one that further masks users from eavesdropping. He notes that in some cases, particularly overseas, fellow carriers are requiring that a GSM approach be taken to improve wireless LAN security.

Further security activities include currently supporting SSL, user-name and password. Starting next year, T-Mobile will enhance to 802.1x to enable network-based authentication, and will be rolling out software that allows customers to automatically launch VPN, to enhance the level of secure authentication sign-on.

Finally, Mr. Wachter stated that GSM has a good track record and ability to provide user security. Wireless LAN represents both a challenge and an opportunity to bring those same capabilities and secure principles. As a final note, T-Mobile currently provides secure phones for NSA government officials that can be used worldwide within the GSM network.

5.4 Questions and Discussion from the Audience

Concerns were raised about how security and network management work together. Panelists conceded the need for improvement, and reemphasized that changes are needed in our way of thinking, to include addressing malicious intent in order to protect ourselves at the front end.

Another key question addressed assessment of Abstract Syntax Notation (ASN.1) vulnerability within networks. The risk is that successful lab testing of 100 nodes often does not translate into scaled environments when software is rolled out into the live network of 1000-2000 nodes. Some security entities have issued Best Practices, but total coverage has yet to be reached.

Interoperability emerged as a key issue to ensure security across the industry. It was stated that summits such as this help the industry understand common best interests, the need to communicate, and to determine how best to work together. This cooperation must increase as new technologies emerge.

There was expressed concern in the lack of reporting coming out of packet wireless networks. Respondents concurred that an increase in reporting is necessary to drive implementation of solutions, and noted that there has been some voluntary reporting on wireless and ISP through NRIC.

Moderator Ross Ireland concluded that it is important not to become complacent that other or older application security measures meet the security requirements for new applications, such as taking a packet system and using it for voice or video. Current applications and network security policies must be revised and updated to acknowledge real-time current threats. Otherwise the vulnerability of the telecom network will continue to be at high risk.

6 NETWORK ACCESS SECURITY STANDARDS

Ed Hall, Vice President of Technology Development at ATIS, began the afternoon session by introducing moderator Ray Hapeman, Chair of ATIS Committee T1 and Director, Standards Analysis and Consulting, at Telcordia Technologies.

Mr. Hapeman introduced this session overview of standards work currently underway in the access network. ATIS Committee T1 representatives described standards for wireline and wireless networks, and Telecom Industry Association (TIA) representatives presented security initiatives in user terminals and in enterprise networks such as Intranets and PBXs. The session concluded with a discussion of the critical security issues facing IEEE 802.11 access.

6.1 Committee T1 Overview

Ray Hapeman, Chair of ATIS Committee T1 and Director, Standards Analysis and Consulting, at Telcordia Technologies, presented an overview of Committee T1

Mr. Hapeman introduced the work of Committee T1 and defined its mission to provide communications standards for implementation across global, end-to-end communication, and related services and applications.

He summarized the activities of T1's six technical subcommittees:

- Performance and reliability in T1A1.
- Interfaces, power and protection of networks in T1E1.
- Internetwork operations administration, maintenance, and provisioning in T1M1.
- Wireless mobile services and systems in T1P1.
- Services architecture and signaling in T1S1.
- Digital synchronization in T1X1.

Committee T1 recently created a security program to provide standards necessary to secure the nation's telecommunications infrastructure, with a coordinating document available to Summit attendees, both on the CD-ROM and at the T1 website, < http://www.t1.org >.

6.1.1 T1A1 Standards Work

Bob Hall, T1S1 Chair from SBC Communications, presented the work of T1A1 under the leadership of Randy Wohlert, T1A1 Chair.

Mr. Hall began by restating that next generation networks are truly at risk in terms of security. This means that there has to be consistent levels of security across the networks on an end-to-end basis, a key work area for T1A1. It has evolved its scope and mission to focus on the security aspects of network performance and reliability.

The security initiatives are now being defined in conjunction with T1S1. Predominantly, T1A1 is looking at two key issues relative to end-user security:

1. *A framework document*, to look at security issues and itemize them.
2. *Defining the security performance metrics on end-to-end basics*. Needing to define what security means, and how to measure whether security is "on" in a given service compounds this simpler goal.

Mr. Hall went on to say that T1A1 intends to direct this security work to the ITU. He concluded by stating T1A1 has risen to the challenge by emphasizing security aspects of performance and reliability, including control and end user plane requirements and performance metrics.

6.1.2 T1E1 Standards Work

Rick Townsend, T1E1 Chair from Lucent Technologies Bell Labs, presented the work of T1E1.

Mr. Townsend discussed the scope of T1E1's work to protect security at the physical layer, specifically how it addresses protection in both an electrical and physical sense.

T1E1 has produced two standards that specifically address electrical protection to keep the network free from harm while minimizing damage should an incident occur:

1. T1.320-1999, *Above-Baseline Electrical Protection for Designated Telecommunications Central Offices and Similar-Type Facilities Against High-Altitude Electromagnetic Pulse (HEMP)*. (HEMP is the result of a nuclear explosion.) This standard discusses baseline design considerations when building the facilities, namely shielding and grounding, to mitigate electromagnetic pulse effects.
2. T1.331-1999, *Description of Above-Baseline Physical Threats to Telecommunications Links*, which describes and defines the various abnormal physical threats that might affect telecommunication links.

He continued by offering a list of T1E1's standards for electrical equipment:

– T1.308-2002, *Central Office Equipment - Electrostatic Discharge Immunity Requirements.*

– T1.313-2002, *Electrical Protection for Telecommunications Central Offices and Similar Type Facilities*.

– T1.316-2002, *Electrical protection of Telecommunications Outside plant*.

– T1.318-2000, *Electrical Protection Applied to Telecommunications Network Plant at Entrances to Customer Structures or Buildings*.

– T1.328-2001, *Protection of Telecommunications Links from Physical Stress and Radiation Effects and Associated Requirements for DC Power Systems*.

– T1.333-2001, *Grounding and Bonding of Telecommunications Equipment*.

– T1.334-2002, *Electrical Protection of Communications Towers and Associated Structures*.

He went on to list standards that militate against physical damages:

– T1.329-2002, *Network Equipment Earthquake Resistance Standard*.

– T1.307-2002, *Fire Resistance Criteria – Ignitability Requirements for Equipment Assemblies, and Fire Spread Requirements for Wire and Cable*.

– T1.319-2002, *Equipment Assemblies – Fire Propagation Risk Assessment Criteria*.

Mr. Townsend concluded by offering that there is significant experience in T1E1, and offered it as a place to look at existing standards and translate them from addressing not only natural threats but also new intentional threats.

6.1.3(A) T1M1 Standards Work

Mike Fargano, T1M1 Chair and Standards Program Coordinator at Qwest Communications, presented the work of T1M1.

Mr. Fargano emphasized the common aspects of network management standards as they apply to access, transport, packet, circuit switch, wireless, and wireline networks. He argued that network management is vital because an incursion into it can cause a major disruption or outage in the network.

He described T1M1's history in security work, and emphasized its most recent work with the Management Plane Security Standard, a collaboration with government, NSTAC, NSIE, and liaisons such as OIF, TIA, etc., as critical work to secure the telecom network.

He mentioned that Rod Wallace would follow his presentation with more specific information, so instead emphasized that his group specifically and consistently looks for business drivers in their work, and he highlighted two such drivers associated with the Management Plane Security Standard:

1. *Efficiency*, in reduced costs via commonalties and economies of scale.
2. *Effectiveness*, by regionally managing risks.

He summarized by saying the compelling business rationale to implement the T1M1 Management Plane Security Standard [i.e., dpANS T1.276-200x] is that it: (1) raises the baseline OAM&P security requirements to meet the current (new) realized security risks; and (2) provides for the new "sweet spot" (i.e., new minimum [risk adjusted] cost zone) between no/low security and too much security (with the relative high costs that come with these two extremes).

6.1.3(B) T1M1 Management Plane Security

Rod Wallace, Subject Matter Expert, gave a perspective on Management Plane Security.

Mr. Wallace summarized T1M1's work on Management Plane Security. He began by noting that providers specify different but similar security requirements and vendors offer similar but different security features, making systems that are expensive and complicated to integrate and secure. In addition, infrastructure security is not considered a revenue generator for service providers or vendors. In response, the objective of this standard was to establish a common baseline to solve the integration and security challenges and to manage costs to both providers and vendors.

A short history of the standard shows that it was started confidentially, in the NSIE, but was made public to facilitate sharing between providers and vendors. The document contains 59 mandatory security requirements, it has been recommended for inclusion into the OAM Best Practices of NRIC VI under cyber-security, and T1M1 intends to submit it to the ITU as a global standard.

Mr. Wallace concluded that the remaining challenge is to have service providers adopt the standard and put it into their RFPs.

6.1.4(A) T1P1/3GPP Standards Work

Asok Chatterjee, T1P1 Chair, 3GPP PCG Chair, and First Vice Chairman of the ATIS Board of Directors, summarized the work of T1P1.

T1P1 is involved in wireless systems, and is specifically interested in involving itself with what happens in second-and third generation technologies. Simply stated, T1P1 does this by developing wireless access standards and working closely with the international Third Generation Partnership Project (3GPP).

3GPP partnership brings together six participating standards organizations from around the world to create solutions and avoid duplication. As Mr. Chatterjee summarized, the goal of 3GPP is to "get it done, get it done well around the globe, and do it once." T1P1 takes specific North American requirements into that discussion.

Mr. Chatterjee then introduced Steven Hayes who chairs 3GPP to discuss the work between T1P1 and 3PPP more thoroughly.

6.1.4(B) 3GPP Additional Perspective

Stephen Hayes, 3GPP Core Network Chair, presented the activities of 3GPP.

Mr. Hayes described the overall security of GSM: the most widespread technology in the world, especially overseas. It is a family of technologies, divided into GPRS or packet support. EDGE and wideband CDMA are the related 3G access technologies. Core network technologies supporting this are circuit-switch subsystems, packet-switched subsystems, and IP multimedia systems – this last being a source of most recent security developments.

Mr. Hayes argued that second generation GSM has fair security overall, and that its imperfections are now being addressed in the third generation:

- Authentication data (e.g., cipher keys) sent protected inside one network and between networks.
- Cryptographic keys (e.g,. cipher keys) increased from 64 to 128 bits long.
- Cryptographic algorithms were made public for third party review for outside validation.
- Made active attacks impossible (e.g., "false base station").

He discussed network domain security, noting that one major objective has been to protect integrity and confidentiality of signaling data inside core networks and between core networks by priorities:

- *First priority*: To protect authentication vectors carried in MAP messages – MAP (Mobile Application Part) on top of SS7.
- *Second priority*: To include GTP (GPRS Tunneling Protocol) protected by IPSec mandatory in control plane; optional in user plane.
- IPSec used to protect IP-based interfaces.
- *Main issues for 3GPP release 6*: Use of PKI for key management is under development.

– Extending protection to Radio Network Controller.

Finally, T1P1 has added security improvements in IP Multimedia Systems via the following:

– Mutual authentication and message protection;
– Secure negotiation of security mechanism;
– Minimum roundtrips;
– Authentication performed in advance of session establishment;
– Message protection started at earliest possible opportunity;
– Compatible with use of both TCP and UDP;
– Terminal does not need to support public key operations; and
– Smart card based security.

These final four are in the works and expected to be completed by December 2003:

1. No longer relying on bearer network security to provide IMS user plane security (e.g., UMTS/GPRS packet domain ciphering in 3GPP Release 5);
2. Ciphering of IMS access signalling;
3. Opportunities in future releases to integrate end-to-end key agreement with SIP (e.g., MIKEY); and
4. End-to-end encryption options.

6.1.5 T1S1 Standards Work

Bob Hall, T1S1 Chair, presented the work being done by T1S1.

Mr. Hall concisely outlined six responses that T1S1 will be working on in terms of security, namely:

1. Development of an Architecture, to define what is meant by security.
2. Joint Work with T1A1, who will look at end-to-end and performance while T1S1 looks at control plane aspects.
3. Key Involvement in T1 Security Project.
4. Review of SS7 Security to look at models and expose vulnerabilities. Some recent outages point to trusted networks flooding the network and causing problems.
5. Review of Security in IP Gateways, leading to VoIP.
6. Continued Work with ITU-T Study Group 11.

6.2 TELECOMMUNICATIONS INDUSTRY ASSOCIATION (TIA)

Dan Bart, Senior VP of Standards and Special Projects at TIA, presented the work of TIA.

In a brief overview of TIA, Mr. Bart divided its role into three key parts: as a trade association representing suppliers to the industry, as an SDO, and providing secretariat services to other organizations. Written into the mission of TIA is work on standards, advocacy, and marketing products to the industry.

In regards to standards development, TIA has more than 600 standard documents in print. TIA dates back to the 1920s with the Radio Manufacturer's Association in Chicago. Now based in Washington, TIA includes eight Product-Oriented engineering committees (TR-/FO-) and 70 working committees of 1,300 members drawn from academia, manufacturers, providers, and end-users, including the government.

Mr. Bart charted TIA's participation with Homeland Security- and CIP-related activities:

- TIA and TIA members have been involved for over 20 years in the activities of NSTAC, with recent focus in the Wireless Task Force.
- TIA closely monitored the work of the President's Commission on Critical Infrastructure Protection.
- TIA was on the Steering Committee of the Information Security Exploratory Committee (ISEC); NSTAC proposed the creation of an Information Security Standards Board (ISSB).
- TIA and its members have participated on the FCC's Network Reliability Council (NRC) and Network Reliability and Interoperability Council (NRIC).
- With Presidential Decision Directive 63 (PDD-63) TIA was chosen as one of the Sector Coordinators for the Information and Communications Sector by the Department of Commerce.
- As a Sector Coordinator, TIA also holds a board seat on the Partnership for Critical Infrastructure Protection (PCIS); PCIS addresses cross-sector and interdependency issues.
- TIA is active in the planning of ANSI's Homeland Security Standards Panel (HSSP), another cross-sector activity.
- TIA shares information with other international groups like the ITU and Global Standards Collaboration (GSC) in these high interest subject areas.

Following Mr. Bart's overview of TIA were reports from three TIA subcommittees, with Mr. Bart himself presenting the work of TR-41, Cheryl Blum presenting TR-45, and Chris Carroll introducing the TR-45 Ad Hoc Authentication Group.

6.2.1 TR-41

Dan Bart summarized the work of TR-41.

Mr. Bart presented the threats against IP Telephony and overlays that are native to the IP environment. Since many threats have been previously articulated, he instead emphasized that 70-80% at the enterprise level are internal, not external, though these are rarely published.

A group within TR-41 looks at the following threats against IP:

- *Threats against the application*, including toll fraud, unauthorized access to resources, unauthorized access to voice mail and other private information.
- *Threats against the infrastructure*, including threats against proxies/call agents, routers and switches, authentication resources, conference bridges.
- *Threats against the endpoints*, IP phones, gateways, "soft phones."
- *Threats against the signaling streams*, monitoring to determine call patterns, instituting "man in the middle" attacks, and enabling phones to act as bugging devices.
- *Threats against the media streams*, including eavesdropping and recording, and on-the-fly modification of phone conversations.

He re-emphasized that following threats are not new, but in an IP world there is greater exposure. These threats are therefore addressable.

6.2.2 TR-45 – Mobile and Personal Communications Systems Engineering Committee

Cheryl Blum, Chair of TR-45, from Lucent Technologies, presented the activities of TR-45.

TR-45 develops performance, compatibility, interoperability, and service for mobile and personal communication systems for TDMA, CDMA, and AMPS-based systems. It's comprised of six subcommittees and several ad hoc groups, most notably TR-45 Ad Hoc on authentication, and Ad Hoc group LAES, whose work is detailed below.

Ms. Blum said that TR-45 has been developing security service since the early 90's. Current activity includes developing standards for WPS (Wireless Priority Service) for CDMA systems, primarily for voice and circuit-switched data.

Security services include authentication, message encryption, and voice privacy, and in the interest of ongoing security, developing enhancements to these in terms of encryption and privacy.

In particular, she outlined ad hoc group TR-45.2's active development of emergency services:

- *1996*: FCC released Enhanced-911 (E911) requirements.
- *1997*: Joint Standards Work with TIA and Committee T1 resulted in publication of J-STD-034, Enhanced Emergency Services Phase 1.
- *2000*: Joint Standard document, J-STD-036, Enhanced Wireless-911 Phase 2 was published. Standard supports both network-based and handset-based solutions.
- *2002*: Joint Standard J-STD-036-A was published with enhancements to the original version.
- *2002*: An addendum to J-STD-036-A was balloted. Publication is expected during 2Q/2003.

In support of this ad hoc group, all subcommittees have been called to provide end-to-end solutions for emergency services, particularly for obtaining position determination. Some groups have developed standards to support global emergency services.

Ms. Blum gave a brief introduction and timeline to the work of the ad hoc committee TR-45 LAES, responsible for developing standards to support the CALEA work:

- *1994*: CALEA legislation introduced to Subcommittee TR-45.2 by law enforcement.
- *1997*: A joint standards work with TIA and Committee T1 resulted in publication of TIA/T1 J-STD-025 as safe harbor standard for CALEA. The standard was challenged at FCC over nine features not included, and was challenged over two features that were included.
- *1999*: FCC released the Third Report and Order validating six of the nine punch list items and indicating that further work needed to be done on the packet data solution in the standard. FCC supported the level-of-location information provided.
- *2000*: J-STD-025-A published in April containing six punch list items.
- *2000*: Industry held two joint experts meetings during 2Q/2000 to explore packet data issues.

The ongoing work for security of IP networks and wireless LANs is being focused by 3GPP2, but Blum envisioned that TR-45 may have to provide support for CDMA and wireless LAN interoperability in the areas of electronic surveillance and emergency services.

6.2.3 TR-45 LAES Ad Hoc Group

Chris Carroll, Chair of TR-45 Ad Hoc Authentication Group, presented its work.

TR-45 works closely with both third generation partnership projects – it has a joint working relationship with 3GPP for coordination and harmonization, and works closely with 3GPP2 (the second partnership project).

Carroll focused on the cryptographic development aspects of the ad hoc group's work.

TR-45 has developed 3G security, with the following capabilities:

- 128-bit root secret k.
- 128-bit Entity Authentication (SHA-1 Algorithm).
- 128-bit Message Authorization (ENMAC).
- 128-bit AES Encryption (Rijndael Algorithm).
- 3GPP AKA protocol (Global Roaming), with mutual authentication between mobile and network.
- Backwards compatibility.
- R-UIM support.
- Air interface and network algorithm negotiation.
- Mobile IP, Radius/Diameter, CHAP authentication.

He argued that the drawback is that service providers haven't yet adopted these 3G standards, so most continue using 2G-security capability, without the enhanced security features available in

3G. Of note, he projected that in the future, one will see multiple layers of encryption and security occurring simultaneously.

Mr. Carroll concluded by explaining the group's participation in the NSTAC's wireless task force. Two primary tasks on wireless priority service and wireless priority access are underway in order to provide recommendations back to the full NSTAC committee and on to the President. The same process was followed for wireless network security, and those recommendations are just now reaching completion.

6.3 Perspectives on IEEE 802.11

Brian Miller, Defense Segment Wireless Security Lead at Booz Allen Hamilton, replaced Les Owens in presenting perspectives on 802.11 Security.

Mr. Miller described WiFi as a very hot technology due to its many benefits. However, numerous studies have proven that WiFi's current WEP security is inadequate. One step up the ladder of quality security is WPA (WiFi Protected Access), with features such as 128-bit cryptographic key size, 48-bit key life, and Replay Action Uses 1V. The final solution that the IEEE is moving toward is the RSN (Robust Security Network), which provides AES based encryption, CCM algorithms for data integrity, and a much longer cryptographic key life.

He noted that the industry should be looking to WPA and RSN for security solutions in the long term, but noted that WPA should be used only in the interim, eventually being phased out by RSN.

As a concluding point, Mr. Miller announced that NIST has released a special publication on wireless network security, Bluetooth, and handheld devices, providing guidance for securing existing wireless networks and additional policy for WEP.

6.4 Applications of 802.11

David Ward, Senior Attorney at the FCC, shared an in-situ example of the applications of 802.11.

Mr. Ward gave a short description of the communications situation at the Mount Sinai-NYU hospital to which the first 9/11 medical evacuees were taken. Due to a communications breakdown, re-location of evacuees had to be made with some consequent medical neglect of injuries and loss of life. Mr. Ward, who teaches at a nearby engineering school in addition to his duties at the FCC, took his engineering class to NYU for a class project to see how they could come up with an 802.11 self-healing network for the hospital.

6.5 Questions and Discussion from the Audience

While ANSI-accredited standards bodies are inherently open, the standards that ensue are public. However, government ITAR (International Trafficking and Arms Regulation) limits certain technologies from global export. Hence security standards can be shielded from public scrutiny.

Additionally, wireless 802.11 standards need to be upgraded with software rather than hardware upgrades.

7 CORE NETWORK SECURITY STANDARDS

This session addressed the standards, currently available and on the horizon, that will address key security issues. Mr. Fred Lucas and Mr. Herb Bertine presented the work of ITU-T Study Groups 16 and 17. Ms. Allison Mankin and Mr. Steve Bellovin presented Transport and Security divisions within IETF.

Complementary to the morning sessions, this session focused on the core network. Specific issues addressed were how to evolve from the SS7 environment to the network control space, where there are new protocol, and new management structures being put in place to enable voice over packet services. The session explored standards efforts in ITU and IETF areas, focusing on network control plane (or signaling plane) supporting the work presented in previous sessions.

Moderator John Kimmins introduced the keynote speaker Mr. Dave McCurdy, President of the Electronics Industries Alliance and Executive Director of the Internet Security Alliance.

7.1 Keynote address: "Prudent Steps Industry Should Take to Help Secure Cyber Space"

Presented by Dave McCurdy, in his capacity as Executive Director of the Internet Security Alliance.

ISA was launched in April of 2001 as a collaborative effort between the Electronic Industries Alliance (EIA), a federation of high tech trade associations, and the CERT coordinating center at Carnegie Mellon.

The Internet Security Alliance is an industry leading, cross-sector, international organization that brings in Internet operators and users and engages them in security standards discussions, resulting in development of best practices and standards.

Mr. McCurdy highlighted the importance of information assurance, critical information infrastructure protection, and Internet security.

His data showed that the incident rate of attacks has skyrocketed in the past five years, with 70,000 reported this year alone. He highlighted the financial impacts of various attacks, including "SirCam," "Code Red," "Love Bug," and "Nimda." He emphasized that the most riveting issue to CEOs is the financial implications of security. His bottom line was to argue for a business case to drive the implementation of improved security practices and standards.

7.2 ITU-T Study Group 17

Herb Bertine, Co-Chair of ITU-T Study Group 17 and Director of Standards and Intellectual Property at Lucent Technologies, presented the security standardization activities of the ITU-T.

The International Telecommunication Union (ITU) is a specialized agency of the United Nations. Specifically, ITU-T deals with telecommunications standards, including security issues, at the policy and technical levels. It is an industry and government partnership, with over 650 companies and 189 governments around the world who contribute to setting telecom standards. ITU-T has more than 2,800 recommendations in effect and approves about 300 recommendations each year.

Mr. Bertine noted that the main objectives of ITU-T SG 17's effort -- as the lead study group in ITU-T for communication systems security -- are to prioritize work in this field and to develop core security recommendations. A substantial number of recommendations on security are already in place. Ongoing and upcoming security efforts in SG 17 include:

- *Authentication (X.509)*, with enhancements as a result of more complex uses and ongoing IETF work.
- *Security Architecture* for end-to-end communications.
- *Telebiometrics* methods, devices and solutions for security purposes.
- *Security Management*, in risk assessment, identification of assets, and implementation characteristics.
- *Mobile Security* for low power, small memory size, and small display devices.

Mr. Bertine also summarized the security efforts of the other ITU-T study groups, whose work can be found at ITU's website. He finished by drawing attention to several resources on security, including a catalog of ITU-T security recommendations, a compendium of security definitions, and results from two ITU workshops on security held May 2002 in Seoul, Korea. These are available at < http://www.itu.int/ITU-T/studygroups/com17/cssecurity.html >.

7.3 ITU-T Study Group 16

Fred Lucas, Rapporteur for SG-16, presented the work of Study Group 16.

Mr. Lucas introduced the Emergency Telecommunications Services (ETS) work in ITU-T SG-16.

The initial work was completed on International Emergency Preference Scheme (IEPS), and continued through International Emergency Multimedia Scheme (IEMS), which together are referred to as ETS or Telecommunications Disaster Relief (TDR).

The work currently being done relating to TDR includes the following deliverables:

- *An emergency telecommunications systems concept* – first draft due Fall 2003.
- *An emergency telecom requirements Recommendation* – first draft due Fall 2003.
- *A systems framework showing how various components support emergency telecom requirements interwork* – due Spring 2004.

Mr. Lucas concluded by listing considerations of technical, operational, policy, legal, and regulatory issues to be taken into account with this work.

7.4 Internet Engineering Task Force (IETF) – Transport

Allison Mankin, IETF Area Director (Transport) and Senior Research Scientist at Lucent Technologies, reviewed IETF work.

Ms. Mankin is one of 13 area directors of the IETF, and is responsible for Transport (or end-to-end communications, as this summit has referred to it). IETF does a great deal of intense security review, and develops protocols by consensus.

The Transport area covers a broad range of topics, and divides into major working groups for VoIP:

- *SIPPING/SIP* - Working groups review requirements and develop new methods in SIP (Session Initiation Protocol).
- *SIMPLE* - Produces SIP-based presence and instance messaging based on IETF's overall architecture.
- *AVT* - Produces RTP (Real Transport Protocol) and its payloads and profiles of RTP.
- *MMUSIC* - Produces SDP (Session Description Protocol).
- *SIGTRAN.*
- *GEOPRIV* - Produces a protocol object that combines privacy policy directives with geographic information.

She concluded by saying that SIP has strong "mandatory-to-implement" security. What is missing are the operational security needs, because users aren't present. In addition, the use of security protocols is not mandatory, but people need to articulate the real risks for these security requirements. If this works, these paper protocols can become practical protocols.

7.5 Internet Engineering Task Force (IETF) – Security

Steve Bellovin, IETF Area Director (Security) presented IETF work.

Mr. Bellovin discussed some particular and technical requirements for Internet security. His security area of IETF has two main missions: 1) to devise security protocols; and 2) to advise other areas about security, ensuring that other protocols have necessary security features.

He discussed major working groups for:

- *IPSec*, which provides security at the IP layer protects all protocols but with poor granularity.
- *S/MIME* was intended as a secure email protocol, but has become an object protocol.
- *PKIX* was designed to produce the X.509 protocol, and underpins many other security-related standards.
- *TLS* (or Transport Layer Security) protects secure web traffic and is used in SIP as a secure transport mechanism.
- *Kerberos* was adopted by Microsoft in Win2K, so it's necessary to extend the protocol as necessary.

He summarized the Security Area Advisory Group (SAAG) as a forum to discuss the progress of various security protocols plus major security issues in other areas. The Security Directorate acts as security advisor to help with implementation and use.

Other major efforts coming out of the security area are:

- *Guidance Documents*:
    - Guide to security considerations.

- Security building blocks.
- Applicability statements for various security protocols.

– *Designing in security from the start*.

Overall goals for IETF Security include:

– *All protocols should have strong security features designed in*: features must be realistic, given likely deployment patterns.

– *Protocols should not have inherent weaknesses*.

– *Security choices are documented*.

– *Use of security protocols is not mandatory*.

7.6 Questions and Discussion from the Audience

There was some discussion of a complement in the ITU, and what is being done about mobile ad-hoc routing and security. The IETF works directly with the ITU via a wide range of collaborative efforts. It was noted that in regard to Recommendation 706, the sole US-centric input has come from NCS. There is a desire and need for further input from a greater variety of sources.

It was asked whether there are promising efforts in the industry to collect data to justify security from a financial perspective. The response was that it has become a priority concern, but it has not yet been backed by investment. Survival of telecom businesses has superceded the survival of systems of security.

8 EVOLUTION OF CORE NETWORKS

The session included experts discussing security issues surrounding optical networking and IPv6. Moderator Art Reilly, Senior Director of Technology Systems at Cisco, introduced panelist from the Optical Internetworking Forum (OIF), the IPv6 Forum, and IETF. Ipv6 working group panelists discussed the evolution of networks from circuit-switched to packet-switched technologies and optical networking leading to next generation networks.

8.1 Optical Internetworking Forum (OIF)

Joe Berthold is Vice President of Network Architecture at Ciena, an ATIS Board Member, and President of OIF.

The mission of OIF is to foster the development and deployment of interoperable products and services for data switching and routing using optical network technologies. Mr. Berthold highlighted the unique aspects of the OIF, namely its function as an industry forum to bring optical and data technologies together to enable the Internet to scale more effectively. It serves a unique function in bringing data and transport professionals together.

Unlike standards bodies, industry forums such as OIF are driven by vendor needs and initiatives. The goal of OIF therefore is not to generate paper, but to generate operable solutions, such as:

- *Implementation agreements, based upon*:
    - Carrier group's requirements.
    - Existing standards and specifications when available.
    - New solutions when necessary.
- *Interoperability testing procedures*: ensuring compliance to implementation agreements and, ultimately, interoperable products and networks.
- *Input into other standards bodies*: via formal liaisons in place with numerous other organizations (e.g., ITU, IETF).

Mr. Berthold summed up the relevance of OIF by saying it answers the business need of lower operations costs through automation.

8.2 OIF Forum from A Member Company Perspective

Renée Esposito, Associate with Booz Allen Hamilton, reviewed security initiatives within the OIF.

OIF's approach to security is to provide security per application, listing security requirements for signaling, including security requirements for the management plane, auditing, and logging. This list of security requirements evolved into a document in the security sections in both UNI and NNI.

OIF provides a profile of IPSec by providing limiting options, allowing for flexibility while providing configuration guidance on such things as modes, algorithms, and addressing that should be used. Guidance on pre-placed keys and re-keying was also provided.

A Management Plane Security document that provided profiles for protocol security was then developed covering all different Network Management Access methods, including:

- *Command Line Access* - Kerberos, SSH, Lower Layer Protection with SSL, TLS, or IPSec.
- *MIB-based Management* - SNMPv3, SSL, or TLS (if running over TCP), IPSec.
- *Web-based Management* - SSL or TLS, IPSec.

This is done to provide protocols and descriptions on how to implement them, in order to cover secure requirements. Each document starts by listing the security requirements needed, and all security protocols are mapped to the security requirements to show they have been filled.

Ms. Esposito noted OIF's new work in conjunction with T1M1, specifically how OIF furthered their document by providing guidance on how to implement protocols. In turn, the OIF adopted some of T1M1's terminology, and refers to their document within their own. She concluded by outlining ongoing efforts at OIF:

- Resolve comments on straw ballot voting round of *Security Extension for UNI 2.0 and NNI.*
- Continue work on *Security for Management Interfaces to Optical Network Elements*.
- Identify other evolving Implementation Agreement documents that should have security defined.
- Auditing and Logging Implementation Agreement, a possible new effort.

8.3 IPv6 Forum

Jim Bound, Chair of IPv6 Forum Technical Directorate and North American IPv6 Taskforce, spoke on the IPv6 Forum.

Mr. Bound described the work of IPv6 Forum, an international forum founded by implementers: not to build standards, but instead promote, influence, provide technical/business expertise, and guidance for the deployment of IPv6.

He clarified some theoretical versus practical understandings in regards to IPv4 and IPv6, namely:

- *The Internet has 36% of the IPv4 address space left* – But China or Mobile IP Cell Phones could use it up in one year.
- *IPv4 and IPv6 use the same IPSec Protocol* - IPv4-NAT precludes peer-to-peer security, and IPv6 supports peer-to-peer security.
- *IPv4 has stateful auto configuration* - The 101st Airborne Division requires IPv6 stateless auto-configuration at point of entry for an engaged operation.

In the face of IPv4-NAT's insufficiencies, IPv6 has several advantages:

- Larger Address Space (NAT not required leaving IP address identification and security intact).
- Stateless auto-configuration of addresses.
- Mobile IPv6 security and routing optimizations.
- IPSec is *mandatory* for compliance.

Mr. Bound built a strong business case for adopting IPv6 for providers:

- Large scale Mobile IP device deployment cannot happen with an IPv4-NAT Internet service.
- Large scale peer-to-peer gaming for consumers with peer-to-peer security cannot happen with an IPv4-NAT Internet service.
- Large scale, US-wide homeland defense within cyberspace cannot happen with an IPv4-NAT Internet service.
- Global business-to-business communications from the US with Asia and Europe will require IPv6.
- The cost of not deploying IPv6 in the US *now* is great.

Mr. Bound's key message was that the United States is in a prime position to step into this new technology, with a basis of IPv6 commercial products, wireless and wireline integration beginning, and heavy US investment in Europe and Asia. He warns that the US may lag behind in this technology, if it does not act quickly and decisively.

Mr. Bound listed the extended standards work for IPv6, with core IPv6 standards, mobile IPv6, and IPSec ready for deployment.

- *IETF Near Term Requirements*:

  - Multi-homing for IPv6.
  - Authentication, Authorization, and Accounting (AAA).
  - Multicast Routing Protocols with Multicast Security.
  - Additional IPv6 Transition Work.
- *3GPP Near Term Requirements*:
  - Add IPv6 as requirement to core in 3GPP+ Release Strategy.
  - Add Mobile IPv6 to core in 3GPP+ Release Strategy.
  - Add 802.11b integration to 3GPP+ Release Strategy.
- *IEEE POSIX 1003* should be doing new APIs for IPv6 and security, not the IETF; but instead work with the IETF and 3GPP as a liaison.

He concluded by again encouraging standards bodies to move in a time-to-market manner, noting that it cannot take ten years to build a standard, and -- if need be -- the IPv6 Forum will step in and build standards as needed on a more timely basis.

8.4 IETF IPv6 Working Group

Margaret Wasserman presented as Co-Chair of IETF IPv6 and IPv6 Operations Working Group.

Ms. Wasserman explained that IPv6 is a new version of the Internet Protocol (IP), and a successor to the widely deployed IPv4. Its purpose is to support the continued growth and technological advancement of the Internet.

She emphasized the advantages of IPv6, and specified that a larger address space is absolutely necessary for growth of imbedded nodes that will be coming onto the Internet in the coming years through Internet-enabled cell phones, home equipment, and car infotainment systems.

She presented the work of IETF in addressing IPv6 related technologies and security issues, and emphasized that IPv6 is *not* a security protocol, but it does enable more secure networks. By eliminating NAT in the architecture, IPv6 avoids the possibility of a single point of failure or attack in a network.

In terms of security, IPv6 provides a superior base over IPv4 in three ways:

- End-to-end security (IP Security).
- Robust, resilient, reliable networks.
- Ad hoc networks for emergency response and military applications.

8.5 Questions and Discussion from the Audience

During the question and answer period it was emphasized that it should be assumed that -v4 and -v6 would coexist for some time. Providers should soon provide home users with a mechanism to use site-local -v6 addresses, which would allow them to tunnel IPv6 pockets to each other over -v4 addresses.

Participants were interested in a baseline timeline for IPv6 as a common protocol. While there are timelines in Japan for rollout of IPv6 by 2005, the US has no planned date yet for full backbone capability.

The possibility of number address portability was also raised in relation to IPv6, with a response opinion offered that this will be essential for NAT elimination, but the issue has not reached consensus within working groups.

What emerged from this session was the importance of designing-in security to data and optical networking. IPv6 was positioned not as a security protocol, but as an enabler to provide end-to-end secure addresses, which helps to thwart security attacks. Lastly, it was consistently noted that there are opportunities in the US to accelerate the evolution of US implementation of IPv6.

9 USER, ENTERPRISE, and APPLICATION SECURITY STANDARDS

This session focused on improving the efficiency and effectiveness of network protection infrastructure and architecture, and how interoperable and scalable solutions can be provided within and among multi-service provider networks. It addressed technical issues and standards needs relative to firewall, media security, secure access, physical security, and meeting requirements of ETS, VoIP, and network management.

Moderator Larry Holmberg, SVP of Sales, Marketing, and Customer Support at Agilent Technologies, began by emphasizing the importance of shared leadership in theory and practice, and how the ATIS Summits to date have helped pull these to the forefront. He then introduced the panelists from leadership groups who are working in this area: Mr. Richard Graveman of the ATM Forum, Mr. Jim McEachern from the MSF, Mr. Eric Burger from the ISC, and one end-user, Mr. Ron Ross of the NIAP.

9.1 ATM Forum

Richard Graveman, Chair for the Security Working Group, presented on the ATM Forum.

ATM is a connection-oriented layer two virtual circuit cell relay technology with some higher layer protocols for signaling, routing, and interworking.

ATM's main security concerns include:

- *Attacks on users' data and applications* - Authentication, integrity, confidentiality, privilege, availability, quality of service, traffic flow confidentiality.
- *Attacks on the network infrastructure* - Availability, performance, theft of service, control (through addressing, signaling, routing, network management, etc.).
- *Attacks on network elements (switches, routers)* - Access: Physical, software, network connectivity management and administrative interfaces.
- *Attacks on interface with higher layer protocols*, e.g., IP and voice-over packet.

The ATM Forum's Security Specifications mostly address protocol security. They are specifications, not standards or products, and their main tool is cryptography.

ATM has already produced a number of security specifications, namely:

- ATM Security Specification v1.1, ATM Security v1.1 PICS.
- UNI 4.0 Security Addendum, PNNI 1.1 Security Signaling Addendum.
- Control Plane Security.
- Addendum to PNNI v1.0–Secure Routing.
- Securely Managing an ATM-NE.
- Security Re-negotiation, Addendum to Security 1.1.

Mr. Graveman articulated several lessons learned in the ATM realm:

1. When security is being done at the lower levels there are greater constraints;
2. Security should be nested, so that in the case of different policies or different administrative domains, security agents should be properly paired to implement different policies in the wide-area versus local part of the network; and
3. Authentication should be tightly coupled with key management, to prevent intervention between the two.

He repeated previous comments that protocol providers should offer a full set of security services, and users should choose what they need and where. Lastly, even though many protocol uses don't require negotiation, it will be needed for a future scaling of security.

9.2 Multiservice Switching Forum

Jim McEachern, Board Member of MSF, presented the work underway at the Multiservice Switching Forum.

The Forum focuses on development from the architectural framework through interoperability testing. Mr. McEachern noted that MSF does not develop protocols, but merely profiles protocols and provides feedback to standards organizations.

MSF is looking at next-generation networks, and is somewhat focused on IP as well as ATM and MPLS.

Interoperability is a key focus. They recently held a conference with multi-vendors and multi-carriers testing simultaneously in three labs in Europe, North America, and Asia.

Security dovetails with the direction of MSF. Following the interoperability conference, the MSF began to update and extend functional architecture, including an update of existing implementation agreements, and extending this functional architecture though a series of solutions that add new physical architecture scenarios and -- where appropriate -- additional implementation agreements.

He concluded by saying the MSF is just beginning to look at security and legal intercept in a network deployment context; because MSF draws on standards developed elsewhere, input from people working on these protocols is welcome.

9.3 International Softswitch Consortium (ISC)

Eric Burger, Member of the Board, ISC, and CTO of SnowShore Networks, Inc., spoke on the ISC.

Mr. Burger focused on the work ISC is doing in network security, namely the advancement of packet based networks through the support of services; helping to find products, applications, and total solutions for carriers; and focusing on any packet transport medium.

Their strength is educating service providers on what is available, educating vendors on service provider needs, and educating end-users on how to take advantage of the packet technologies, with the government and issues of lawful security being a focus.

ISC has undertaken network border control. It considers the interface between carriers and large enterprise and small home offices, each of which has different security needs and concerns. The concept is to maintain network security while supporting lawful intercept. Mr. Burger noted that IPv6 will largely take care of some of these security issues, but there is a need in the interim between now and its implementation in 5-10 years.

ISC recently met with the FCC and FBI regarding lawful intercept, and discussed security, privacy issues, and an increase in end-to-end encryption, while the FBI wants reduced encryption to make their eavesdropping easier. Lastly, the ISC is working on a safe-harbor document negotiated between carriers, vendors, and the government, stipulating that a carrier who follows these provisions and makes them available to government agencies will have complied with the CALEA law.

9.4 National Information Assurance Partnership (NIAP)

Ron Ross is with the National Institute of Standards and Technology, and is Director of the NIAP.

NIST partners with the NSA to help federal partners navigate the maze of commercial products offered and available to build more secure systems. Mr. Ross immediately points out, however, that the notion of a truly secure system is a near impossibility.

However, while it is possible to put greater security capabilities into systems, building more secure systems requires:

- Well defined system-level security requirements and security specifications.
- Well designed component products.
- Sound systems security engineering practices.
- Competent systems security engineers.
- Appropriate metrics for product/system security testing and evaluation.
- Comprehensive security planning and life-cycle management.

Mr. Ross described security as an overarching system with technology-based and non-technology-based components. NIAP is looking for a total solution that combines these security issues, with the ultimate objective of greater customer confidence that systems are secure enough to do the job.

NIST and NSA have together developed support tools and programs to enhance secure systems:

- *Standardized Security Requirements and Specifications*:
    - NIAP protection profile development project.
    - Private sector protection profile contributions.
- *Product Testing and Evaluation Programs*:
    - NIAP Common Criteria Evaluation and Validation Scheme.
    - NIST Cryptographic Module Validation Program.
- *Security Implementation Guidance*:
    - DISA Security Technical Implementation Guides.
    - NIST Special Publications and NSA Security Reference Guides.
- *System Certification and Accreditation*.

In summary, building a more secure system is a difficult task: it relies on good requirements, good component products, and good testing evaluation techniques that customers can understand and use to make a credible risk-based decision of whether to put a system into operation.

9.5 Questions and Discussion from the Audience

One point raised was that though this session covered 99% of security issues, the missing gap in security is *continual* compliance and governance. It's important to move from periodic or installation-only compliance towards a continual model.

Some clarification on the ISC Safe Harbor document was requested, in terms of what it contains and whether there is a release date set. In response, Mr. Burger replied that the Safe Harbor allows carriers to comply without going out of business. The Safe Harbor documents have been drafted, are currently being reviewed by CALEA, and are expected to be available within a couple of months.

10 VENDOR ROUNDTABLE: Business Perspectives on Security

The objective of the "Vendor Roundtable" is to elicit comments and discussion from participating companies, relative to their perceptions of the needs for security as defined by the service providers and government customers versus the "business" perspectives necessary to develop affordable and deployable methods to achieve adequate security protection.

The Moderator for the Session was Susan Schramm, Senior Vice President – Carrier Markets, Siemens Information and Communication Networks, and Second Vice Chairman of the ATIS Board of Directors.

Panelist for the Session were Paul Mankiewich, Mobility Solutions CTO, Lucent; Chris McLelland, Director, Security Solutions, Cap Gemini Ernst & Young; Rod Wallace, Director, Office of CTO, Nortel Networks; Aristotle Balogh, Senior Vice President – Operations &Infrastructure, VeriSign; and Paul Tshirlig, Solutions Architect, Agilent Technologies.

Ms. Schramm, the Session Moderator, initiated panel discussion by summarizing several common themes from service providers and government officials; namely, that all stakeholders

must work together to address security, that security must be "built-in" to the standards and not retrofitted, and that industry faces a tremendous challenge in creating business cases that ensure return-on-investment (ROI).

Question 1: Ms Schramm asked each panelist to comment on how their organization approach security, both in developing products that include security and how they face the challenge of justifying the investment for security measures.

Mr. Tshirlig responded that Agilent utilizes a two-fold approach to security. First, Agilent employs an SS7 monitoring system called Access 7, and an NGN Analysis System principally concerned with 3rd generation networks which covers protocols H323, SIP, MGCP, SGCP, and RPT. By marrying these two systems together, Agilent is able to enhance its troubleshooting capability to obtain an end-to-end view of network management or trunk signaling issues. Secondly, Agilent has developed a Security Consultant arm that builds personalized customer profiles to determine protocols being used, assess personal vulnerabilities, and examine personnel policies in order to give a set of customer-specific recommendations.

Mr. Balogh from VeriSign commented that justifying a business case from VeriSign perspective was easy, given their business in running all DNS services for .com, .net, .org, and others. Since any attack that takes down the DNS or compromises route certificates would have a devastating impact on the Internet and e-commerce, VeriSign cannot afford not to dedicate necessary resources on security measures. As such, VeriSign focuses its security development dollars on two elements: 1) managing the human risk element through monitoring, training, and designing out the possibility of error; and 2) finding tools that reduce mean time to detection.

Mr. Wallace noted that Nortel draws a distinction between business cases for security products and product-security. In cases where service providers want security products to secure their service offerings, such as firewalls and VPN's, the business case follows normal lines. The more complicated cases are when service providers – wanting to assure the integrity of their revenue-generating networks – want product-security. The business case in this circumstance is more complicated, for service providers and vendors alike, because there is no positive revenue base in this case – it's similar to asking for insurance. To get dollars allocated to product-security, Nortel considers several factors. First, by working closely with customers, commonalities in required security features across a broad client-base are defined to drive economies of scale down. Secondly, once security features are defined, they are then broken into manageable portions and phased-in to the product, whereby circumventing the need for an "all-or-nothing" budget discussion. And lastly, customers have to ask for the features. If customers ask for largely the same features, such as those specified in standards like T1M1, business cases are much easier to make.

Mr. Mankiewich from Lucent commented that, as a system integrator, working with customers and colleagues to determine security needs is of utmost importance, to identify commonalities and drive down development cost. Incorporating security measures (without an immediate return on investment) also become more palatable from a long-term perspective, if there is an effective argument that it will limit a company's liability or that the long-term financial loss would be too great not to do it now. As an example, Lucent has already dedicated resources to become "Environmentally Green" for long-term pay-off. Mr. Mankiewich also noted the need for a collaborative approach to create a national business case that would address industry-wide losses if security measures were not uniformly incorporated.

Mr. McLelland noted that CGE&Y approaches security from a business perspective versus a technical one. Based on survey results from North America and Europe, CGE&Y was able to develop a holistic approach to security solutions that builds security capabilities from the ground up. With survey in hand, an "Adaptive Security Index" with 47 questions was developed around

how IT security integrates with business. CGE&Y's fundamental approach pertains to mitigating the human factor rather than improving security via a technical approach. The human element is the toughest threat to overcome.

Question 2: Ms. Schramm asked Agilent if they have noticed an expressed increase in security interest.

Mr. Tshirlig responded that, in fact, there has been a marked increase in security requirements. Approximately 20-30% of the content in Requests for Proposals (RFPs) and Responses for Information (RFIs) received today pertain to security requirement. In comparison, just one year ago, these RFPs outlined very little security requirements. This increase in demand has led Agilent to its current security approach.

Question 3: After 9/11, the communications industry expected to see more demand for or at least more awareness of security within the US,. With the global presence of large vendors today, Ms. Schramm asked Nortel how they managed product development plans to span the two interests – nationally and internationally.

Mr. Wallace responded that, generally, requests from US network operations do not differ greatly from global demands for security. The US exception is in areas of specific legislative acts (i.e., CALEA). It is the global network transformation which is driving the need to make security technologies more network-ready (e.g., Ethernet to Wide Area, Packet to Voice, and WLAN to core network). The concern is more with how to make network interfaces faster, scalable, and available. Bringing security technologies into a networking context is really the strategy on the product side.

Question 4: Ms. Schramm noted that, as heard during the Security Summit, a tremendous amount of concern surrounds wireless security. As such, Lucent was asked to comment on what the next steps were, from a holistic approach, to solve wireless security concerns.

Mr. Mankiewich responded that third generation wireless (3G) has done a lot to address security issues and close up security-gaps that were prevalent in first -- and even to some extent second -- generation wireless systems. Today's problem pertains to 802.11. Given that 802.11 is viewed as synergistic with 3G wireless, efforts have been made to integrate it into wireless network offerings. Because of the level 802.11 insecurity, however, it has since been turned off, and will not be totally integrated into wireless systems until its level of security is on par with wireless. This is especially true given the hand-off capability between the two systems. To address the concern, a united industry must push to get standards sorted out and security applied to the technology. The problem with this approach, however, is that there is no obvious economic driver to push forward the necessary security changes. Moreover, if or when security is finally addressed, there is no economic driver to push the revisions into the marketplace. There is no incentive for 802.11 users to upgrade. This is unlike the wireless industry, where service providers have a vested interest in moving its customers to 3G and, hence, subsidize equipment upgrades.

Mr. McLelland countered saying that 802.11 is insecure not because of a flawed protocol, but rather because is was never designed to be secure. He emphasized that security is about knowing the risks of using a given protocol, and is all about operating with a known and acceptable level of risk. In addition, depending on how it is used, 802.11 could be made secure.

Question 5: Given the responsibility industry has placed on service providers for secure networks, Ms. Schramm asked CGE&Y to comment on the responsibilities by the enterprise.

Mr. McLelland responded that there are thousands upon thousands of security products available today to secure critical data. The approach to security has to be from a holistic point of view where focus is on the entire enterprise -- not just the technology or policies and procedures. Also, security must be addressed in the very beginning of a project: where it is more cost effective. Companies should not avoid implementing security measures due to the fear of spending a large amount of money; they simply need to spend their dollars wisely.

Question 6: A representative from the FCC asked the panelist if they could clarify their statements relevant to security around 802.11. Namely, the statement made by CGE&Y that 802.11 could be secure depending on how it's used.

Mr. McLelland answered that including dynamically changing web keys to provide encryption is one method. And once you establish the encrypted tunnel, it is similar to being on a wireline network.

Mr. Mankiewich commented that one concern is the peer-to-peer capability of 802.11, and placing the responsibility on the user to correctly set-up the equipment. This is vastly different from 3G wireless, where equipment is automatically configured. If 802.11 is not properly configured, a peer user could compromise the network even through an established secure tunnel, referred to as "split tunneling." Split tunneling is a vulnerability inherit in any VPN network and not exclusive to 802.11, however.

Mr. Wallace cautioned that while 802.11 may be fine for simple data transfer, as used today, it is likely to mature to the point of delivering real Ethernet-like services (i.e., voice, hi-fidelity, etc.). It is under this circumstance where 802.11 insecure networking is of concern and consequently needs to be addressed.

Question 7: Given where the industry is today with regards to limited resources and the need to focus on priorities, Ms. Schramm asked the panelist to comment on what are their priorities in security.

Panelists responded that as technical solutions are developed, and security tools created, efforts must be made to mitigate the human-risk factor in security by assuring a consistent approach and proactive implementation of appropriate security measures. Panelists also believe industry needs to unite and tackle security from a holistic approach. As an industry, security standards must be developed, interoperability testing must be performed, and product-security developed. Given all that is required, no single industry segment can do it alone.

Ms. Schramm summarized the session and outlined the next logical steps: 1) get organized; 2) get an economic model; 3) drive-home the consequences of not implementing security; 4) raise awareness nationally; 5) place the human element in the solutions set; and 6) design-in the ability to protect. Ms. Schramm stated that clearly the greatest call to action is continuing the dialogue and continuing working together. Collaboration needs to stay at the forefront and not be an afterthought.

Question 8: A Summit attendee commented that there is obviously an absence of business cases, and was concerned insofar as how standards people were going to be supported as they continue to develop standards.

Panelists responded that, unquestionably, the manufacturing segment of the industry find it extremely difficult to support standards solutions that are unrealistic from a business or operational perspective. For this reason, organizations must be internally aligned to ensure the intersection of standards activities and business needs. Augmenting standards with NRIC "Best Practices" is also a viable approach, especially in addressing the human-factors issues.

11 OVERVIEW OF NRIC VI HOMELAND SECURITY BEST PRACTICES

Moderator P.J. Aduskevicz, Network Vice President of Network, Disaster Recovery, Reliability and Security for AT&T, and member of the ATIS Board of Directors, stated the purpose of this session was to provide an overview of the Network Reliability and Interoperability Council (NRIC) and its Best Practices. NRIC Best Practices are the most authoritative list of guidance for the communications industry, assembled through industry expertise and experience. Leaders of the NRIC and its Focus Groups described the role and importance of this effort, its accomplishments to date, and its ongoing work.

11.1 NRIC VI Homeland Security Focus Groups

Jeff Goldthorp is an NRIC VI Designated Federal Officer for the FCC.

NRIC is a Federal Advisory Committee (FAC) of the Federal Communications Commission (FCC) that convenes executives from the communications industry to develop Best Practices to promote network reliability and interoperability. NRIC VI was re-chartered after 9/11 to specifically consider how industry could best prepare itself for such attacks in the future.

Focus Group 1 of NRIC VI deals exclusively with Homeland Security, and divides into areas of physical security, cyber-security, public safety, and disaster recovery. Physical and cyber-security Focus Groups have developed a Best Practices policy, and are spending the rest of the year doing outreach. Disaster recovery developed a procedure with the National Communications Center (NCC) for maintaining an emergency contact list and published a mutual aid report.

11.2 Homeland Security and Physical Security – Focus Group 1A

Karl Rauscher, Director in Network Reliability Office, Lucent, leads NRIC VI's Focus Group 1A, which addresses issues of physical security.

FG-1A has completed the following work to date:

- Issued a report on Homeland Security Physical Security Prevention Report, Issue 1.
- Issued 4 recommendations:
  1. NRIC VI-1A-01: NRIC VI Physical Security Prevention Best Practices
  2. NRIC VI-1A-02: Chemical and Biological Agents in Air Handling Systems
  3. NRIC VI-1A-03: Voluntary National Background Checks

4. NRIC VI-1A-04: Review Infrastructure-related Mergers and Acquisitions

– Identified 21 areas for attention.

– Recommended 200 Best Practices.

In addition, the Focus Group is working to:

– Conduct a survey of current practices from the entire industry that addresses homeland defense.

– Report on current disaster recovery mechanisms, techniques, and best practices, and develop any additional best practices

– Coordinate with the Homeland Security Cyber Security Focus Group (1B) to assure that vulnerabilities in the public telecommunications networks and the Internet are assessed.

Mr. Rauscher made the distinction that FG-1A focuses on vulnerability assessment versus threat assessment, because while threats may change, vulnerabilities remain constant.

11.3 Homeland Security and Cyber Security – Focus Group 1B

Bill Hancock, Cable and Wireless, leads NRIC VI's Focus Group 1B, which addresses issues of cyber-security.

Focus Group 1B is concerned with generating Best Practices for cyber-security, in both the telecommunications sector and Internet services. They delivered a "Prevention" set of Best Practices in December 2002, and are slated to release a "Restoration" set of Best Practices in March of 2003.

The group is divided into eight working teams to generate Best Practices in the areas of Fundamentals & Architecture, OAM&P (operations, administration, maintenance and provisioning), AAA (authentication, accounting, audit), services, signaling, personnel, users, and incidents.

Mr. Hancock followed by listing Group 1B's driving principles in Cyber Security Best Practices:

– *Capability Minimization*: Allow only what is needed re: services, ports, addresses, users, etc. Disallow everything else, and turn it off if you're not using it.

– *Partitioning and Isolation*.

– *Defense in Depth*: a.k.a. "belt & suspenders"; Application, host, and network defenses.

– *KISS*: Complexity makes security harder.

– *General IT Hygiene*: Backups, change control, privacy, architectures, processes, etc.

– *Avoid Security by Obscurity*: A proven BAD IDEA™.

Mr. Hancock emphasized that Best Practices in all these cases are implementable. They tighten up infrastructure against preventable bugs like the "cyber worm" to more serious threats such as nation-states engaging in cyber wars.

He concluded by issuing next steps for Group 1B:

- Publish preventative cyber-security Best Practices for Industry comment and improvement, following NRIC's acceptance of December 2002, cyber-security deliverables.
- Refinement of recovery Best Practices for March 2003, deliverables.
- Creation of a March 2003, cover document with:
    - General cyber-security recommendations.
    - Strategic cyber-security issues.
    - Technology issues that require resolution for future Best Practices.
- Additional refinement and addition of Best Practices for prevention and recovery as reviews are completed by NRIC membership.

11.4 Service Provider Perspective on NRIC VI

Pam Stegora-Axberg, Senior Vice President at Quest and NRIC VI Steering Committee Chair, offered Qwest as a case study in the implementation of NRIC VI Best Practices.

Ms. Stegora Axberg advocated that implementation of Best Practices requires a conscious evaluation of their potential benefits when applied to the uniqueness of each company. After evaluation by Qwest, this means Best Practices are either incorporated into a daily process, initiated via a project, initiated via a new process, or are determined to have non-relevance to Qwest and are set aside.

Qwest communicated and implemented Best Practices via:

- An internal newsletter article.
- SME based evaluations via teleconference, conference calls, and/or Best Practice work.
- Specific topics selected for Network Reliability Week.
- Standard process bulletins and Methods of Procedures.

She clearly stated that by implementing these NRIC VI Best Practices, Qwest has experienced overall network performance improvement.

In closing, Ms. Stegora Axberg invited greater participation in NRIC VI by all in attendance. She believes that focus group participation is a critical part of the process, not just the outcome. In addition, the work of Best Practices is measured in how one gets adoption and penetration in their own business, and this is best facilitated by having company representatives actively involved in the participation themselves.

In summarizing this session, Moderator P.J. Aduskevicz reviewed NRIC's history and gave a nod to the expertise and long hours put in by NRIC's volunteer advisory councils and focus groups. She encouraged all participants to make use of this work and access NRIC VI's Best Practices available on their website < http://www.nric.org >.

11.5 Questions and Discussion from the Audience

Moderator Aduskevicz summarized the salient points made by the NRCI VI panelists (i.e., security must be included from the beginning and government and industry should implement the

Best Practices expected from NRIC VI as quickly as possible). She then opened the floor to questions and thanked the participants for their time and effort.

A question was raised in regard to whether any thought has been given to tax incentives for the incorporation of security practices. NRIC has taken an education approach instead, and hopes that incentives are built through demonstrating a strong business case.

12 SUMMIT SUMMARY AND IDENTIFICATION OF FOCUS AREAS

The Summit concluded with a summary of significant security themes and issues that were presented and discussed during the two days. The summary was developed by Art Reilly, Senior Director of Technology Standards, Cisco; Hank Kluepfel, Corporate Vice President for Corporate Development, SAIC; and Ed Hall, Vice President for Technology, ATIS. Mr. Hall presented the Summary with the assistance of Mr. Reilly and Mr. Kluepfel.

The Summary began with the identification of ten "common security themes." Mr. Hall noted that certain points were reiterated throughout the summit by various presenters and an effort was made to capture them so they could be used as a guide to help pilot any work effort that may follow as a result of the Summit. The ten common security themes are:

1. *A Holistic Approach to Security*: A need exists to address security from an end-to-end, interoperable, and comprehensive approach, rather from a simpler, issue-by issue approach.
2. *Security should be Network-based*.
3. *Quick identification and response to new security realities as they occur*.
4. *Security should be built into a standard and not be retrofitted.*
5. *Security features should be part of the architecture of network elements*: Each network element should be designed with interoperable security features in mind.
6. *Return on Investment (ROI) for security functionality*: As security standards are developed for implementation, carrier's ROI must be considered. Backward compatibility is an essential element.
7. *SDOs (standards development organizations) understanding and documenting operational security needs and facilitate implementation*: Proper resources and appropriate expertise must be involved with the development and implementation of security standards.
8. *Coordination of standards activities*: There are no resources for additional standards organizations and duplication of effort. An effort must be made to coordinate work among existing SDOs.
9. *Industry and governmental cooperation*: Concerted efforts need to continue to build and maintain strong industry and government cooperation on security matters.
10. *Need for a balanced approach between end-to-end security and lawful intercept*: Specifically, there may be a limit to the amount of "back-doors" available for law enforcement before network security is encumbered with complexity (and cost incurred by the provider.)

Mr. Hall continued the Summit Summary by introducing three Focus Areas. These focus areas were developed in an attempt to "bundle" all identified issues discovered during the Summit into specific potential work-development efforts. The three Focus Areas are:

1. *Operational Partnership with Stakeholders to Facilitate Distributed Implementation of Security*. The industry could benefit from an organization focused on addressing particular issues such as: a risk and benefit analysis for the transition from IPv4 to IPv6, S/MIME, SIDTRAN and more; and looking closely at standard implementation issues to develop a set of "good practices". The organization could also study the need for interoperability testing to include the need for live stress testing. Other issues may include defining testing protocols and building formats and strategies that advocate business cases in the support of standards development.
2. *Government and Industry Partnership*. The industry and government should partner more closely to hasten the adoption of NRIC VI Best Practices, and to review the NSTAC document from the Wireless Task Force, which contains recommendations on wireless security for possible standards development and coordination for wireless priority access service (PAS) and network security. A recommendation was made to review the NSTAC Network Security and Vulnerability Task Force report as it relates to SDOs and provide recommendations for implementation.
3. *Standards Processes*. There remains an enormous need for the coordination of developing standards and the implementation of existing standards such as the ATIS committee T1, T1M1.5./2002-125R2, a document that pertains to Network Management. The promotion of cooperation and collaboration between SDOs working on similar topics (such as lawful intercept, which is being worked by numerous SDOs) needs to be accomplished. Above all, economic models and business cases must be considered in the standards development process. Standards management and business strategy will drive implementation. It was further identified that the industry is suffering form the lack of change/patch management, a tool used by network managers to track which security upgrades have or have not been implemented.

Mr. Hall concluded the Summary Session by commenting that the common themes and Focus Areas identified should be used to initiate the development of technical/operational standards and steer the industry in the speedy implementation of those standards.

13 ATIS NEXT STEPS AND SUMMIT ACKNOWLEDGEMENTS

ATIS President and CEO Susan Miller officially closed the Summit by summarizing the purpose of bringing together the leading standards organizations as well as the key technical officers of the industry and US Government. Her three key points are:

1. Telecommunications networks are security targets, posing significant security threats.
2. Security concerns are impacting and delaying of next-generation services.
3. There is a need for standards to be prioritized and coordinated across the industry.

She explained the strategic steps ATIS has taken in identifying and prioritizing the top industry issues; namely the formation of the ATIS Technical and Operations (TOPS) Council. She further explained that of the 16 priority issues identified by TOPS Council, Security was one of the "Critical" top five. The TOPS Council is now in the process of formulating focus groups. A focus group, chaired by an ATIS Board member, is populated with mid-to-senior-level management

experts from ATIS member companies, whose sole objective is to examine each critical issue and develop a work-plan to produce implementable, end-to-end solutions, driven by real business needs.

Susan Miller announced that Ms. P.J. Aduskevicz, Vice President for AT&T's Network and Disaster Recovery Reliability and Security and ATIS Board member, will be chairing the TOPS Council focus group on Security Issues including Network, IP Network, and Wireless 802.11 Security. This focus group will use the findings of this Summit, previously reported by Ed Hall, to define a coordinated standards development program for network security, as well as a timeline for completion of standards and other work that fulfill the requirements outlined during the Summit.

The Summit concluded following Susan Miller's comments thanking the Summit's Steering Committee for developing the program; the Summit's presenters, moderators, sponsors and participants, with a special note of thanks to Howard Schmidt, the newly-named chair of the President's Critical Infrastructure Protection Board; and the ATIS Board of Directors, for helping make this ATIS event a success.

APPENDIX 1 Standard Developer's Matrix of Activities for Communication Security

A.1 Introduction

The ATIS Security Summit, "Security of Service Provider Infrastructure in the Era of Convergence" on February 4-5, 2003 in Washington, D.C., will identify how interoperable and scalable security solutions can be provided and maintained within and among multi-Service Provider networks.

Technical sessions are intended to stimulate and enable Forums and standards development organizations (SDO) to determine how technical standards developers have responded and continue to respond to these security needs by developing technical solutions for end-users, enterprises, service providers, equipment providers, manufacturers, and network operators to use to address, mitigate, and contain specific security threats while also protecting privacy, reliability, and interoperability functionality.

To assist SDOs in collecting, identifying, and promoting past, current, and future development efforts relevant to security, the enclosed matrices have been provided. Information collected will be distributed during the summit.

A.2 Instructions

Standard developers submitting the enclosed matrices should provide a brief, but yet revealing, snapshot of relevant work-efforts, standards, and/or ongoing projects. As such, references, standard numbers, and/or project numbers are encouraged. Inclusion of hyperlinks to specific URL's for more detail or precise information would also be helpful. The objective of this exercise is to give readers a catalog of SDOs and work-efforts to determine what security issues have been, or are currently being, developed and where.

Please provide the answers to the following in your presentation:

1. *Organization* – This is the name of the Service Provider, Government Department/Agency, Industry Forum, Consortium, or Standards Development Organization.
2. *Description of Activity (Target Completion)* – This is a short description of the activity being performed and an indication of the projected completion date (year and quarter is sufficient). This description should be clear enough to give an understanding of the work. In some cases, a title of the work is sufficent.
3. *Dependencies* – You should provide a description of the dependencies between organizations. If the listed activity needs another activity in the same or a different group to be completed first, then it would be listed as a dependancy. If this work is based on another activity or references another activity, then it is dependant on that activity being completed.
4. *Area of Work* – That is, CMRS, Satellite, WLAN, etc.
5. *Open System Infrastructure Security* – Using the OSI model, please describe the characteristics needed for Physical, Data-Link, Network, and Transport needs.
6. *Inter-connection, Personnel, and Management* – That is, characteristics needed.

If you have questions, the conference planning committee is eager to help. Do not hesitate to contact Jim Crandall, ATIS Director of Industry Forums, at < jcrandall@atis.org > or via phone at +1 (202) 434-8855.

Input for Wireline and Wireless Communications (CMRS, DSL, Cable, etc.):

Table 1 - Matrix of Activities

Standard Developer	Sub-group	Description of Activity (Targeted Completion)	Area of Work(s) (Ex.: DSL, CMRS, IP, etc.)	Dependencies (Ext. Coordination)	Open System Infrastructure (OSI) Security					Inter-connect[1]	Personnel & Physical[2]	Network Management
					Phys.	Data-Link	Network	Transport	Sess/Present/App			
ATM Forum		Protocol SEC	ATM			x			x			x
FCC NRIC (Network Reliability and Interoperability Council) www.nric.org		Network Reliability and Homeland Security Best Practices (4Q02, 1Q03)	US public networks: wireline, wireless, cable, satellite, and the Internet	ATIS NRSC, Facilities					Cyber Security	Interoperability	Environment, Power, Hardware, Software, Networks, Payload, Policy, Human	
IEEE Communications Society Technical Committee on Communications Quality & Reliability (CQR) www.comsoc.org/~cqr		International professional society aimed at building up Quality, Reliability and Security professionals in the communications industry. Deliverables are ongoing.	Academia, industry, and government; international public networks: wireline, wireless, cable, satellite, and the Internet	Ongoing work in ICC and GLOBECOMM conferences and annual workshop	Ongoing work in ICC and GLOBECOMM conferences and annual workshop	Ongoing work in ICC and GLOBECOMM conferences and annual workshop	Ongoing work in ICC and GLOBECOMM conferences and annual workshop	Ongoing work in ICC and GLOBECOMM conferences and annual workshop	Ongoing work in ICC and GLOBECOMM conferences and annual workshop	Ongoing work in ICC and GLOBECOMM conferences and annual workshop	Ongoing work in ICC and GLOBECOMM conferences and annual workshop	Ongoing work in ICC and GLOBECOMM conferences and annual workshop
MSF		Security and Legal Intercept Requirements Analysis	Multi-service packet networks	IETF, ITU-T			White paper on network level security requirements			Requirements		Requirements
MSF		Updated Reference Architecture	Multi-service packet networks	IETF, ITU-T			Ref Architecture					
T1	T1A1	End to end security performance metrics to quantify security impacts, e.g, additional delay in authentication, extra required capacity in privacy (3Q2004)	All networks	TBD			TBD					

[1] Interconnection includes, but not limited to, areas relevant to the connection of two networks, systems, or environment, *e.g.,* Access, Call Control, and Signaling. Specify focus.

[2] Physical in this context pertains to areas and elements outside the OSI's definition of "Physical Layer." Specify areas and/or elements.

Standard Developer	Sub-group	Description of Activity (Targeted Completion)	Area of Work(s) (Ex.: DSL, CMRS, IP, etc.)	Dependencies (Ext. Coordination)	Open System Infrastructure (OSI) Security					Inter-connect[1]	Personnel & Physical[2]	Network Management
					Phys.	Data-Link	Network	Transport	Sess/Present/App			
T1	T1A1	Performance related aspects of security. Quantify the performance of security services based on end-to-end security policies & services. Exclude security performance objectives (1Q2004)	All networks	TBD			TBD					
T1	T1A1	Performance Related Aspects of Security (3Q2004)	End to End Security Performance Metrics	Stable end to end security policies, to be determined			TBD					
T1	T1A1	Performance Related Aspects of Security (1Q2004)	Security Performance Impacts (“Costs”)	Security Services clarification, to be determined			TBD					
T1	T1E1	T1.320-1994 (R1999), Above-Baseline Electrical Protection for Designated Telecommunications Central Offices, and Similar-Type Facilities Against High-Altitude Electromagnetic Pulse (HEMP), protection from electromagnetic pulses coming from nuclear explosions.	Facilities	NRPA, IEC 801-02, ITU-T K.27, UL, ANSI electrical safety code	T1.320-1994 (R1999)							
T1	T1E1	Assorted projects on Electrical Protection of Telecommunication Structures and Equipment	Facilities	NRPA, IEC 801-02, ITU-T K.27, UL, ANSI electrical safety code	T1.308-2002, T1.313-2002, T1.316-2002, T1.318-2000, T1.328-2001, T1.333-2001, T1.334-2002							

Standard Developer	Sub-group	Description of Activity (Targeted Completion)	Area of Work(s) (Ex.: DSL, CMRS, IP, etc.)	Dependencies (Ext. Coordination)	Open System Infrastructure (OSI) Security					Inter-connect[1]	Personnel & Physical[2]	Network Management
					Phys.	Data-Link	Network	Transport	Sess/Present/App			
T1	T1E1	Project on physical design for CO environments - Common Physical System Requirements	Facilities		New (in 2002)							
T1	T1E1	Network Equipment Earthquake Resistance	Facilities	IEC, ANSI/IEEE-344	T1.329-2002							
T1	T1E1	Standards on ignitability, fire propagation, fire risk assessment	Facilities	NRPA, UL	T1.307-2002, T1.319-2002							
T1	T1M1	T1.233-1993 (R1999), Security Framework for TMN Interfaces; framework document providing basic security management capabilities, description of OSI security services	TMN									
T1	T1M1	T1.243-1995 (R1999), Baseline Security Requirements for TMN; describes minimum security requirements (e.g., identification, authentication, access control, privacy, audit	TMN									
T1	T1M1	T1.252-1996 (R2002), Security for the TMN Directory; describes secure communications via public key and security of the directory itself.	TMN									

Standard Developer	Sub-group	Description of Activity (Targeted Completion)	Area of Work(s) (Ex.: DSL, CMRS, IP, etc.)	Dependencies (Ext. Coordination)	Open System Infrastructure (OSI) Security					Inter-connect[1]	Personnel & Physical[2]	Network Management
					Phys.	Data-Link	Network	Transport	Sess/Present/App			
T1	T1M1	T1.259-1997, Security Transformation ASE for ROSE; provides PDU-level security at Application Layer; secure transfer of ROSE PDUs and information about the security; related to ITU-T Rec. Q.813	TMN									
T1	T1M1	T1.261-1998, Security for Q3 Messages; security of the OS-NE interface; five security levels for authentication, access control, etc.	TMN									
T1	T1M1	T1.268-2000, TMN PKI; various protocols supported for Q Interface (OS-NE) and X Interface (OS-OS); includes profile of IETF PKI (certificate extensions)	TMN									
T1	T1M1	Management Plane Security – American National Standard (ANS); Target Completion 2Q2003	Common Network Management Security standard for Network Elements (NEs) and Operations Support Systems (OSSs)	Liaison with: NSTAC NSIE, Gov NSIE, 3GPP, ATM Forum, DSL Forum, TR45, IEEE 802.3ah, OBF, OIF, TCIF, TM Forum, T1-TSCs			Included in proposed standard regarding NE and OSS interface security for network management.	Included in proposed standard regarding NE and OSS interface security for network management.	Included in proposed standard regarding NE and OSS interface security for network management.	Included in proposed standard regarding OSS/OSS interconnect interfaces.	Included in proposed standard regarding network management users or operators.	The general topic is Management Plane Security providing for Common Network Management Security
T1	T1M1	Management Plane Security. Detailed requirements for Management Plane Security. All aspects of Management Plane Security. (4Q2002)	All networks	TBD								x

Standard Developer	Sub-group	Description of Activity (Targeted Completion)	Area of Work(s) (Ex.: DSL, CMRS, IP, etc.)	Dependencies (Ext. Coordination)	Open System Infrastructure (OSI) Security					Inter-connect[1]	Personnel & Physical[2]	Network Management
					Phys.	Data-Link	Network	Transport	Sess/Present/App			
T1	T1M1	Management Plane Security – American National Standard (ANS); Target Completion 2Q2003	Common Network Management Security standard for Network Elements (NEs) and Operations Support Systems (OSSs)	Liaison with: NSTAC NSIE, Gov NSIE, 3GPP, ATM Forum, DSL Forum, TR45, IEEE 802.3ah, OBF, OIF, TCIF, TM Forum, T1-TSCs			Included in proposed standard regarding NE and OSS interface security for network management	Included in proposed standard regarding NE and OSS interface security for network management	Included in proposed standard regarding NE and OSS interface security for network management	Included in proposed standard regarding OSS/OSS interconnect interfaces	Included in proposed standard regarding network management users or operators	The general topic is Management Plane Security providing for Common Network Management Security
T1	T1P1	Network Interworking & interoperability standards between GSM/PCS1900/GPRS/UMTS MAP-based and ANSI-41 MAP-based systems	GSM/3G mobile services and systems network-based	ETSI, 3GPP, ITU-R, TIA	TRQx-xxx1 (ANSI to MAP interface complete)	TRQx-xxx2 (complete)	TRx-xxx3 (under revision)			TRQx-xxx1-3 (complete)		
T1	T1P1	GSM/3G Radio, System and Network standards related to radio technology aspects of GSM/GPRS/EDGE/UMTS	GSM/3G mobile services and systems mobile-based	ETSI, 3GPP, ITU-R, TIA	TRQx-xxx1 (air-interface authent. complete)	PNx-xxx2 (128-bit encrypt in develop)					PN-xxx2 (UUI finger-print access in develop)	
T1	T1P1	Lawful Intercept standards. On-going support for Release 99, Release 4, and Release 5. New capabilities and modifications as necessary for Release 6 IMS. (4Q2003)	GSM, GPRS, UMTS	3GPP								
T1	T1P1	Wireless Wideband Internet Access (WWINA) Authentication (3Q2003)	I-CDMA, MCSB									
T1	T1P1	Wireless Priority Services (WPS) (4Q2003)	GSM, GPRS, UMTS	3GPP								
T1	T1P1	Enhanced Home Environment (HE) control of security (including positive authentication reporting) (4Q2003)	GSM, GPRS, UMTS	3GPP								

Standard Developer	Sub-group	Description of Activity (Targeted Completion)	Area of Work(s) (Ex.: DSL, CMRS, IP, etc.)	Dependencies (Ext. Coordination)	Open System Infrastructure (OSI) Security					Inter-connect[1]	Personnel & Physical[2]	Network Management
					Phys.	Data-Link	Network	Transport	Sess/Present/App			
T1	T1P1	Network Domain Security (4Q2003)	GSM, GPRS, UMTS	3GPP								
T1	T1P1	Support for subscriber certificates (4Q2003)	GSM, GPRS, UMTS	3GPP								
T1	T1P1	MExE Security analysis activity (4Q2003)	GSM, GPRS, UMTS	3GPP								
T1	T1P1	Security Aspects of Requirement for Network Configuration Independence (4Q2002)	GSM, GPRS, UMTS	3GPP								
T1	T1P1	Access security for IP-based services (4Q2002)	GSM, GPRS, UMTS	3GPP								
T1	T1P1	OSA security (4Q2002)	GSM, GPRS, UMTS	3GPP								
T1	T1P1	New security aspects of LCS (4Q2002)	GSM, GPRS, UMTS	3GPP								
T1	T1P1	IP network layer security (NDS/IP) (4Q2003)	GSM, GPRS, UMTS	3GPP								
T1	T1P1	Support of the Presence Service security architecture (4Q2003)	GSM, GPRS, UMTS	3GPP								
T1	T1P1	3GPP Generic User Profile security (4Q2003)	GSM, GPRS, UMTS	3GPP								
T1	T1P1	Release 6 User Equipment Management: Security aspects (4Q2003)	GSM, GPRS, UMTS	3GPP								

Standard Developer	Sub-group	Description of Activity (Targeted Completion)	Area of Work(s) (Ex.: DSL, CMRS, IP, etc.)	Dependencies (Ext. Coordination)	Open System Infrastructure (OSI) Security					Inter-connect[1]	Personnel & Physical[2]	Network Management
					Phys.	Data-Link	Network	Transport	Sess/Present/App			
T1	T1P1	Security Aspects of Multimedia Broadcast/Multicast Service (MBMS) (4Q2003)	GSM, GPRS, UMTS	3GPP								
T1	T1P1	WLAN Interworking Security WID (4Q2003)	GSM, GPRS, UMTS,WLAN	3GPP								
T1	T1P1	Security Management WID (4Q2003)	GSM, GPRS, UMTS,WLAN	3GPP								
T1	T1S1	T1.655-2001, SS7 - Upper Layer Security Capability; standard based on generic upper layer security described by ISO model	SS7				x			x		x
T1	T1S1	Lawfully authorized surveillance of packet based services under the CALEA law (1Q2003)	Packet-based wireline networks	TIA TR45	x	x	x	x	x	x	x	
T1	T1S1	Review of requirements for ETS and development of needed new standards and changes to existing standards. (4Q2003)	All wireline networks	TBD		x	x		x	x		
T1	T1S1	Interworking Security Issues between ITU-T SG 11 protocols and IETF internet protocols supporting voice over packet services. (TBD)	SS7, BICC, SIP-T	IETF, ITU-T SG 11			x		x	x		
T1	T1S1	Review of all SS7 standards for security issues with new architectures and linkage to new networks (e.g., Internet). (TBD)	SS7	ITU-T SG 11		x	x	x		x		

Standard Developer	Sub-group	Description of Activity (Targeted Completion)	Area of Work(s) (Ex.: DSL, CMRS, IP, etc.)	Dependencies (Ext. Coordination)	Open System Infrastructure (OSI) Security					Inter-connect[1]	Personnel & Physical[2]	Network Management
					Phys.	Data-Link	Network	Transport	Sess/Present/App			
TIA	TR-45	E9-1-1 for analog cellular, Position determination service for analog cellular, Wireless Network Communication for Emergency Message Broadcast, Wireless Enhanced Emergency Services, Emergency Services Data Communications, TMDA 3G - Digital Control Channel Layer support of emergency calls (including identification), TDMA 3G Wireless - System Assisted Mobile Positioning through Satellite (SAMPS) Teleservices (incl. analog system aspects, Layer 3 cdma2000 position location support, Position determination service for Dual Mode Spread Spectrum Systems, Position location capable CDMA Mobile Stations, and Lawfully Authorized Electronic Surveillance (LAES) for Packet Data.	CRMS TSB-119 IS-817 TSB-114 J-STD-34 J-STD-036 ANS 136 IS-2001 IS-2000 IS-801 TIA-916 PN--30047			X	X	X	X	X	X	

Standard Developer	Sub-group	Description of Activity (Targeted Completion)	Area of Work(s) (Ex.: DSL, CMRS, IP, etc.)	Dependencies (Ext. Coordination)	Open System Infrastructure (OSI) Security					Inter-connect[1]	Personnel & Physical[2]	Network Management
					Phys.	Data-Link	Network	Transport	Sess/Present/App			
TIA	TR-41	Security issues related to VoIP Telephony (incl. network security, IP network architectural security considerations, authentication, authorization, privacy, governmental requirements and the threat environment within the CPE/Enterprise space), Network architecture elements and functionality needed for providing E9-1-1 support for IP terminals in an Enterprise Network, Problems of locating VoIP terminals as it relates to E9-1-1 services, Technical criteria for terminal equipment to prevent harm to the telephone network, PBX and KTS Support for E9-1-1 Emergency Service Calling.										
TIA	TR-42	Security cabling systems in residences.										
TIA	TR-8	Security related aspects of Private Radio Systems (LMR), relating to PS users; including P25, wideband and broadband (via Project MESA).										

Standard Developer	Sub-group	Description of Activity (Targeted Completion)	Area of Work(s) (Ex.: DSL, CMRS, IP, etc.)	Dependencies (Ext. Coordination)	Open System Infrastructure (OSI) Security					Inter-connect[1]	Personnel & Physical[2]	Network Management
					Phys.	Data-Link	Network	Transport	Sess/Present/App			
TIA/ETSI Project MESA		The specifications and future broadband standards developed in the Project MESA process will be capable of extremely high levels of security, yet will contain standardized interfaces to public and private networks. It is anticipated that these interfaces will include, but not be limited to, the PSTN, private networks, public and private microwave systems, DS1 and DS3 Common Carrier services, and ISDN circuits, as they are applicable. MESA is only intended to carry high-speed, digital wireless services, which will supplement other public and private fixed stations, fiber, and hardwire services in place today.										
3GPP2		New work item involving WLAN interworking; may also involve security (authentication and authorization) considerations.										