NRIC VII

Network Reliability and Interoperability Council VII

December 2005

FOCUS GROUP 2A

Homeland Security Infrastructure

Final Report

This page intentionally left blank.

Table of Contents

1. Introduction

The Network Reliability and Interoperability Council (NRIC) VII is a partnership of the Federal Communications Commission, the communications industry and public safety to facilitate enhancement of emergency communications networks, homeland security, and best practices for the telecommunications industry.[1]

This report documents the efforts undertaken by the NRIC VII Focus Group 2A with respect to the review and updating of Homeland Security Infrastructure Best Practices.

1.1 Structure of the NRIC VII

The structure of the Network Reliability and Interoperability Council is as follows:

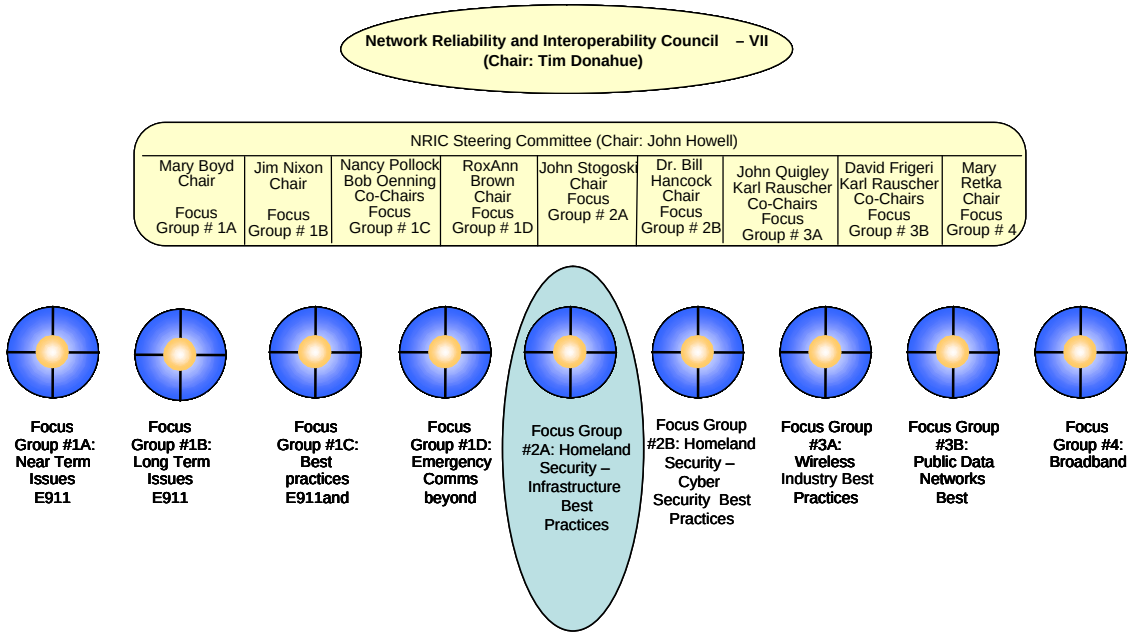

Figure 1

[1] NRIC web page, www.nric.org.

Focus Group 2A Team Members

Focus Group 2A consists of 34 active members.

NAME	COMPANY/AGENCY
Tim Bowe	Sprint
Bonnie Bushnell	NYISO
Rick Canaday	AT&T
Robert Clark	MCI
Michael Clements	SAVVIS
Dick Craft	Verizon
Steve Dworkin	Battery Corp.
Bob Fairbairn	Motorola
Perry Fergus	Booz Allen Hamilton/NCS
Chris Gutman-McCabe	CTIA
Bob Holley	Cisco
Keith Hopkins	Qwest
Frank Horsfall	Nortel
Robin Howard	Verizon
Dan Jenkins	Intelsat
Rick Kemper	CTIA
Hank Kluepfel	SAIC
Rick Krock	Lucent
Anil Macwan	Lucent
Chuck Madine	Federal Reserve
Spilios Makris	Telcordia
Steve Malphrus	Federal Reserve
Archie McCain	BellSouth
Chris Oberg	Verizon Wireless
David Phillips	Sprint
Karl Rauscher	Lucent
Art Reilly	Cisco
Jim Runyon	Lucent
Molly Schwarz	Schwarz Consult.
Larry Stark	NCS
John Stogoski - Chair	Sprint
Craig Swenson	MCI
Howard Washer	Battery Corp.
Albert Young	Cox
Power Subject Matter Experts Consulted	
Robert Burditt	SBC
Charlie Romano	Verizon
Art Kirk	Lucent
Morgan Barnes	BellSouth
Myron Balthozar	Sprint
Curtis Ashton	Qwest
Don Kennedy	BellSouth
Pam Gurule	BellSouth

Figure 2

2. Objective, Scope, and Methodology

2.1 Objective

The NRIC VII Council has been charged with reviewing and improving the Homeland Security Best Practices that were adopted by the NRIC VI Council. The NRIC VII Charter for Focus Group 2A states:

> "By December 16, 2005, the Council shall present a final report that describes, in detail, any additions, deletions, or modifications that should be made to the Homeland Security Best Practices that were adopted by the preceding Council."[2]

In an effort to provide appropriate focus on both Infrastructure and Cyber Security Best Practices, two Focus Groups were assigned to this objective. Focus Group 2A examined the Infrastructure Best Practices, and Focus Group 2B reviewed the Cyber Security Best Practices. A Non-Disclosure Agreement was prepared by the NRIC VII Steering Committee to provide additional protection for parties that chose to bring sensitive information to the Focus Group for discussion.

2.2 Scope

The scope of this document is limited to Infrastructure Best Practices and does not address Cyber Security Best Practices.

This report contains the following:

- Background information and additional guidance for the intended audience in the use of the Best Practices reviewed by Focus Group 2A
- Analysis of existing NRIC Best Practices related to Infrastructure Security
- Recommended additions, deletions and modifications to those existing Best Practices
- Identification of new Infrastructure Security Best Practices
- Areas for future attention of NRIC Councils

2.3 Methodology

Early in the NRIC VII cycle, Focus Group 2A discussed the name and scope of the Homeland Security Focus Group to determine the subject to be addressed. The members agreed that the "infrastructure" topic should include those common services and network elements that support communication networks regardless of the specific technology (wireline, wireless, satellite, cable, etc.). Through focus group meetings, conference calls, sub-team sessions, and separate meetings of subject matter experts (See section 5.4 Power and section 5.5 Blended Attack of this report), the focus group examined over 500 Best Practices producing a revised set for the Council. Spurred by the 2004 and 2005 hurricane seasons, which created challenges never before experienced by industry or the Government on United States soil, incident command, power supply, security controls, government coordination of operations and access were main subjects for discussion. These discussions provided team members the opportunity to share experiences and the associated business practices.

[2] NRIC VII Charter, www.nric.org

Special coordination was required with a number of Focus Groups in order to ensure conflicting Best Practice recommendations were not submitted by each Focus Group. These Focus Groups were: Focus Group 1C “E911 - Public Safety Best Practices,” Focus Group 2B “Homeland Security-Cyber Security,” Focus Group 3A “Wireless Networks,” and Focus Group 3B “Public Data Networks.”

The focus group examined the Best Practices from previous NRIC Councils, with the exception of cyber security Best Practices, which were reviewed by Focus Group 2B. To select specific Best Practices, the team reviewed the existing work from previous focus groups which were chartered to address network reliability, physical security and disaster recovery. Relevant Best Practices were collected to form the homeland security infrastructure set (See Figure 3).

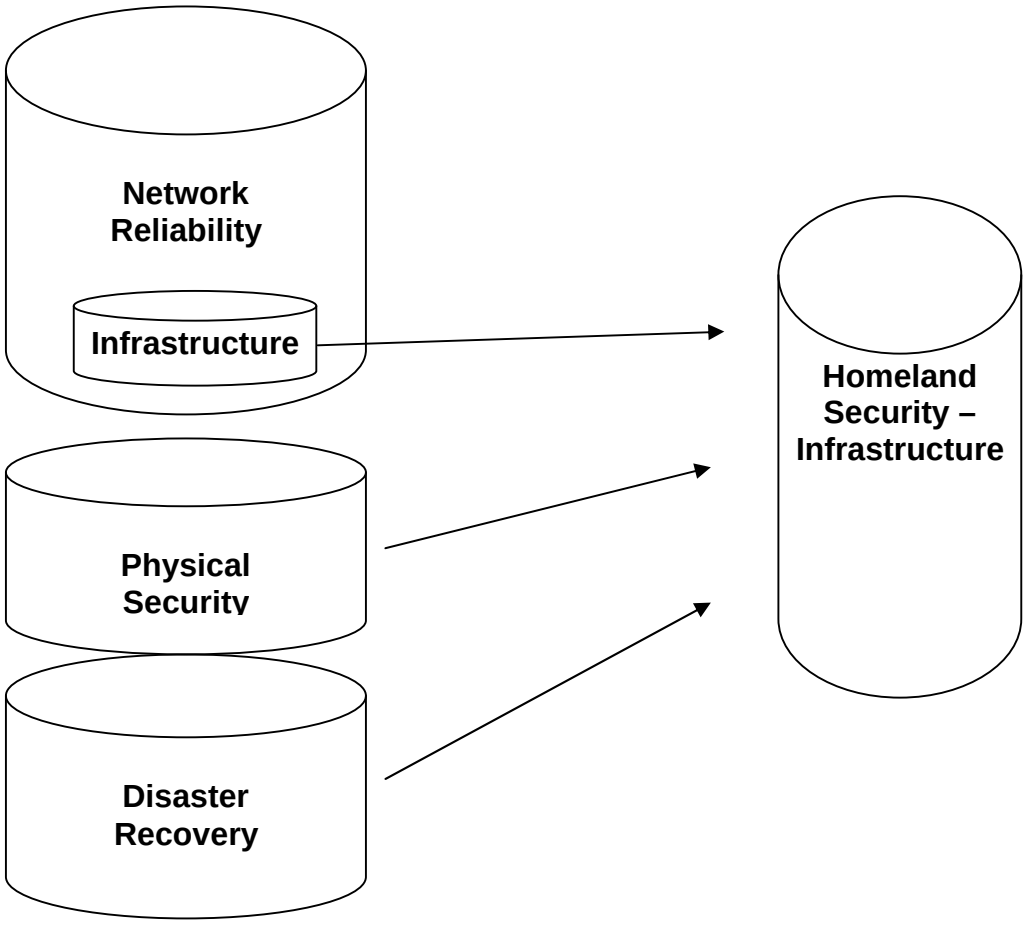

Figure 3

The team grouped the Best Practices into five main categories—core infrastructure, hardware/software, physical security, disaster recovery, and power. Focus group members volunteered to review Best Practices assigned to one or more of these categories based on their area of expertise, thereby creating five sub-teams (See Figure 4).

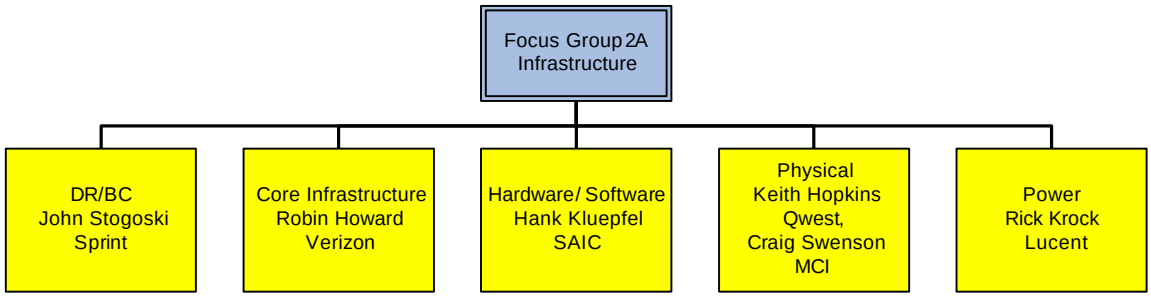

Figure 4

The goals of Focus Group 2A in reviewing the Best Practices were to:

- Remove duplication
- Add clarity
- Ensure proper context
- Verify links and references
- Remove contradictions

In addition, each team reviewed its respective set of Best Practices looking to refine the Best Practices to address evolving technologies and changing threats. The teams then validated the changes, turning to an extended circle of subject matter experts when necessary. By reviewing each Best Practice with these goals in mind, the usability and consistency of the Best Practices was improved.

For instance, the Focus Group determined that there was significant duplication of Best Practices and made an effort to remove the redundancy. The duplication was caused by simultaneous efforts to create Best Practices for disaster recovery, physical security, and public safety in NRIC VI. Consequently, the Focus Group spent significant time and effort ensuring that key concepts were not lost when a Best Practice was recommended for deletion because of duplication.

An example of a Best Practice modified based on target audience, usability, accuracy, and relevance to current issues/environments would be Best Practice number 7-7-5001, where “positive identification” was replaced with “two factor identification” to clarify the capabilities of the technology today. Best Practice 7-7-5001 states:

- 7-7-5001 Service Providers, Network Operators and Equipment Suppliers should establish additional access control measures that provide two factor identification (e.g., cameras, PIN, biometrics) in conjunction with basic physical access control procedures at areas of critical infrastructure, as appropriate, to adequately protect the assets.

Decisions to delete a Best Practice included timeliness, technical feasibility and cost effectiveness. For example, Best Practice number 6-6-5147 states:

- 6-6-5147 To ensure the success and integrity of existing industry-government information sharing and coordination processes (e.g., NSTAC, NSIE, NCC, ISAC), Service Providers, Network Operators and Equipment

Suppliers should actively participate in and endorse the NCS transition to the Department of Homeland Security.

This Best Practice was recommended for deletion based on timeliness. While industry continues to work actively with DHS, industry supported the NCS transition process to DHS, therefore the BP is obsolete and was deleted. Other DHS related Best Practices that remain relevant are being reissued.

Going forward Best Practices should continue to be reviewed to remove duplication, add clarity, ensure proper context, verify that links are active/updated, verify that references are correct, and address evolving technologies, applicability, and changing threats. In addition, they need to be reviewed in a manner in which the entire set of Best Practices is considered.

3. Intended Use of NRIC Best Practices

As stated on the NRIC website, "The Homeland Best Practices are intended to give guidance on how best to protect the U.S. communications infrastructure. Decisions of whether or not to implement a specific Best Practice are intended to be left with the responsible organization (e.g., Service Provider, Network Operator, or Equipment Supplier).

Mandated implementation of these Best Practices is not consistent with their intent. The appropriate application of these Best Practices can only be done by individuals with sufficient competence to understand them. Although the Best Practices are written to be easily understood, their meaning is often not apparent to those lacking experience and/or expertise in the specific job functions related to the practice. Appropriate application requires understanding of the Best Practice impact on systems, processes, organizations, networks, subscribers, business operations, complex cost issues and other considerations. With these important considerations' regarding intended use, the industry is concerned that government authorities may inappropriately impose these as regulations or court orders."[3]

4. Environment

The nation's focus on homeland security over the last four years produced a number of initiatives aimed at improving the security, reliability and recoverability of the communications networks. These initiatives include public and private sector partnerships as well as corporate initiatives aimed at improving internal capabilities. Business leaders understand the importance of security, reliability and business continuity in today's environment. These are considered CEO level issues which have thus produced a corresponding level of attention within organizations.

The communications industry is in the midst of fundamental changes that are having a dramatic impact on the operating environment. New services are being developed and network convergence is blurring traditional segmentation of the communication sector. The interconnected nature of the networks produces dependencies across the various

[3] NRIC web page, "Best Practice Tutorial, Intended Use of NRIC Best Practices", www.nric.org

network operators and service providers. These networks are using an assortment of technologies to deliver communication services to their customer base. These changes have been observed through the expanding NRIC Membership which now includes wireless, satellite, cable, and Internet service providers.

The continued transition to Internet Protocol and the development of new applications (i.e., Voice over IP, Instant Messaging), have created new communication services. This infrastructure has distinct transport, service, and application levels served by an expanding group of companies. All of these levels have physical components that could be impacted by natural or man-made incidents.

5. Key Discussion Areas

The following sections discuss some of the key areas that were examined by FG2A. This should not be considered an all inclusive list for this large subject. Given the format of the NRIC Best Practices, it is sometimes difficult to convey the complete message in a single Best Practice or set of Best Practices. This section is intended to provide background information and guidance.

5.1 Security Strategy

The objective of security is to reduce the level of risk to a company while balancing the associated costs and value of the assets being protected. How a company approaches security can have a major influence on the overall success of the program. Security programs include all phases of the security lifecycle from general governance to the operational responsibilities. An overall corporate strategy is used to integrate these functions into the business.

A policy framework is needed to enumerate the company's security directives. This policy provides the foundation for the employees who make decisions and run the business on a day to day basis. Policies should focus on what needs to be accomplished and leave the details of the implementation to the groups responsible. To be successful, a mechanism for updating the policy should be established.

The organizational structure of the security functions needs to be well conceived and positioned to deliver effective results. Given the diverse group of communication companies, centralized and decentralized models are successfully being used in today's environment. Both models, however, require senior executive involvement to provide sufficient authority and direction for the functions.

A well-managed security program is based on good information and thoughtful decision making. Ongoing security planning addresses the evolving environment and adapts to changes in business strategy. Decisions regarding security are based on risk, which includes factors such as threats, vulnerabilities, probability and cost. Many of the infrastructure Best Practices discuss specific methods for increasing a company's protection and lessening the probability of impact from an incident. The challenge is that a simple checklist is not realistic given the diverse community and the broad spectrum of environments in which the industry operates. The size and function of a company factor into the level of security that is appropriate. One size [of security] will not fit all. It is the

security officer's responsibility to make decisions on the best manner in which to protect an asset given the specific risks to that asset.

A key factor in making security decisions is the level of importance or value of the asset to the business. Hurricane Katrina further illustrated that communication providers must take into consideration their role in the nation's overall communication capability when evaluating a specific asset's value. The level of security for that asset needs to be proportional to its value. Best Practice 7-7-5010 states:

- 7-7-5010 Service Providers, Network Operators and Equipment Suppliers should deploy security measures in proportion to the criticality of the facility or area being served.

The communications infrastructure is spread throughout the country and, therefore, is exposed to a variety of threats. Different regions around the country are more prone to certain types of natural events. For instance, the south east region endures hurricane level storms on a seasonal basis. Northern parts of the country are prone to ice damage. Facilities within a high profile city need different protection than those located in rural locations. The threat of terrorism has introduced another vector that needs to be applied to the equation. Security managers need to implement measures that address the threats that correspond to the given location.

Today's global environment and economic conditions are driving the creation of complex business relationships. While there is always debate on business strategy, it is clear that security must be addressed early in the process. Understanding the risks of a given business decision allows the organization to accept the consequences and take proper precautions. Companies need to be able to make business decisions with the full set of information available. Best Practices 7-6-5024 and 7-6-5025 state:

- 7-6-5024 Service Providers, Network Operators and Equipment Suppliers should include security as an integral part of the strategic business planning and decision making process to ensure that security risks are properly identified and appropriately mitigated.

- 7-6-5025 Service Providers, Network Operators and Equipment Suppliers should include security as an integral part of the merger, acquisition and divestiture process to ensure that security risks are proactively identified and appropriate plans are developed to facilitate the integration and migration of organizational functions (e.g., Due Diligence investigations, integration of policy and procedures).

In addition to planning, a security strategy needs to address the operational components that address day-to-day security events. No amount of planning will prevent all possible incidents. Incidents include such items as direct attacks, inadvertent actions and direct policy violations. Monitoring, compliance and incident response functions provide the capability to respond to these incidents and minimize the potential impact to the business. There are numerous Best Practices which provide guidance on the operational aspects.

In summary, managing security is an ongoing process that must include well-informed decision making. Environments, threats and technologies change over time. Business leaders must balance security, functionality and cost to be effective. Having security addressed in the standard operations of the business is one of the keys to good security.

5.2 Access Control

Access control has always been a significant concern in the communications industry, but the events of September 11, 2001 forever changed the way the industry views this subject. Access is one of the key elements used by attackers to compromise their target. As the ease of access increases, the level of effort required by an individual to execute a successful attack decreases. The goal is to manage access to company assets by supporting the business needs while minimizing risk. Assets can be physical objects, such as offices, equipment and devices, or information such as employee data, network designs and travel schedules for key executives. Focus Group 2A examined the traditional physical security aspects of access control, and Focus Group 2B addressed the cyber security aspects.

Access control can be described as having two objectives for meeting its goal. One, only those with the appropriate need and the proper authorization should be allowed into whatever is being protected. Two, only items which are intended and authorized to leave should be taken from the place protecting the asset. This is commonly approached by the following:

1.) Creating a plan that is commensurate with the criticality and vulnerability of the asset being protected
2.) Effectively implementing the plan (to include record retention, access verification, system testing and repairs and maintenance) and
3.) Ensuring a means to revoke access when no longer needed

Identification of individuals is an integral part of access control and one of the risks businesses need to manage. It is one thing to limit access by key or by card, but quite another to be reasonably sure the person using the key or the card is in fact the person originally authorized for access. In the end, there should be a process that is established and enforced that deals with the identification and admittance of individuals into facilities. Best Practice 7-7-5021 states:

- 7-7-5021 Service Providers, Network Operators, Equipment Suppliers and should establish and enforce access control and identification procedures for all individuals (including visitors, contractors, and vendors) that provide for the issuing of ID badges, and the sign-in and escorting procedures where appropriate.

The plan for access control is tightly coupled to the overall design of the facility. When constructing a new facility, security personnel can integrate ingress and egress control points into the design and minimize vulnerabilities. It is more common, however, that security personnel are faced with mitigating the design vulnerabilities of a pre-existing facility. This situation poses challenges due to limitations of the existing facility and increased costs. Regardless of which situation is faced, the security design process needs to be integrated into the building selection/construction process.

Best Practice 7-7-5026 states:

- 7-7-5026 Service Providers, Network Operators, Equipment Suppliers and Property Managers should include security as an integral part of the facility construction process to ensure that security risks are proactively identified and appropriate solutions are included in the design of the facility. Where appropriate, this review may include consideration elements such as facility location selection, security system design, configuration of lobby, limitation of outside access points (both doors and windows), location of mailroom, compartmentalization of loading docks, design of parking setbacks, placement and protection of air handling systems and air intakes, structural enhancements, and ramming protection. Consider sign off authority for security and safety on all construction projects.

The characteristics of communications facilities are very diverse ranging from large office buildings to cellular towers. Physical security managers need to select the security solutions appropriate for the given location. Obviously, a different solution would be implemented for a cellular tower or a regeneration site as opposed to a switch site. The NRIC Best Practices include guidance on the use of identification badges, electronic access cards, traditional key locks and proprietary master- key solutions. Each “system” considered for deployment has unique characteristics and is not without risk to compromise. Any conceptual plan at a critical site should consist of multiple layers wherever possible. Guard services, CCTV, alarm systems, and access log monitoring are some of the methods for enhancing protection. Best Practice 7-7-5005 states:

- 7-7-5005 Service Providers, Network Operators and Equipment Suppliers should conduct electronic surveillance (e.g., CCTV, access control logs, and monitoring) at critical access points.

Communication infrastructure is commonly located at shared facilities with other communication operators or other infrastructure providers such as power companies. This methodology is used to minimize costs and the impacts on neighboring communities. The situation, however, raises the level of complexity in managing access to those locations. Landlords and Property Managers have taken an increased role in the protection of both their tenants and buildings while continuing their day-to-day operation of the facility. These security roles and responsibilities include both procedural and structural requirements along with coordination with their tenants. The Focus Group reviewed Best Practices applicable to Property Managers in an effort to provide guidance in the implementation of security policies, procedures and design techniques in facilities that house critical communication infrastructure.

Best Practice 7-7-5151 states:

- 7-7-5151 Property Managers, Service Providers and Network Operators located in the same facility should coordinate security matters and include all tenants in the overall security and safety notification procedures, as appropriate.

Coordination between the tenant and the Property Manager is essential when developing access control plans. The process begins with the tenant disclosing the

presence of critical communication infrastructure in the facility and working with the Property Manager on the requirements necessary to protect that equipment. A working partnership between all tenants must exist to achieve workable agreements on policy and procedures.

As technology continues to develop and the industry further evolves, systems and processes will be modified accordingly. Done correctly, access control can deter, or it can detect and assist in the identification of someone attempting to make unauthorized access.

5.3 Asset Diversity

Diversity is an important element in the design of networking infrastructure and information systems. Diversity is the establishment of separation of assets in order to decrease the likelihood that a single event will disrupt the operation of an overall business process. Unfortunately, the amount of damage caused by a future event is not a known quantity.

Business decisions need to be made on the amount of asset separation that is deemed acceptable for a given cost and the associated level of risk an organization is willing to accept. As the distance increases, the risk will generally decrease. When designing diversity for a network, engineers take into consideration the threats to its reliability. Threats can be localized to a given device such as configuration errors and hardware failures. Threats can also be against an entire building or geographic area such as natural disasters and terrorist bombings. In networking, there is logical diversity and physical diversity. Many times logical diversity is designed at the functional level, however the actual provisioning of services produces a problem with physical diversity. Both aspects should be considered.

Network Operators and Service Providers strive to maintain a high level of availability for the services they offer. Technology and configuration contribute to a reliable infrastructure. NRIC focus groups have focused on inter-office and intra-office diversity and those management systems required for the operation of the services. SONET technology has enabled carriers to implement ring configurations which provide two physical paths between switch sites. The deployment of SONET rings within the network increases overall reliability by mitigating affects from cable cuts. Best Practice 7-7-0731 states that:

- 7-7-0731: Network Operators should provide physical diversity on critical inter-office routes when justified by a risk or value analysis.

In addition to the network backbone, network operators and service providers need to ensure reliability for the management of critical network functions. This includes the operations centers as well as the signaling and control functions. Companies need to consider the use of redundant facilities that are geographically separate. Designs supporting core signaling functions need to incorporate redundant, diverse capabilities so that a single event does not disrupt the overall function of the network. Given the interconnected nature of networks, a problem with one network can adversely impact other networks and increase the overall impact to the end users.

It needs to be noted that NRIC does not address the diversity issues associated with a customer's local access (i.e., last mile) solution for connecting to the backbone networks. This needs to be part of the solutioning process between the customer and Network Operator. This is a complex issue that includes the physical plant available for a given location as well as the need to assure continued diversity as the network evolves. The ATIS National Diversity Assurance Initiative (NDAI) is currently examining this topic.

5.4 Power

Power is a critical element of the communications infrastructure. Without power, networks will not function. In addition, even a seemingly small power problem has the potential to become a catastrophe, potentially damaging equipment, injuring personnel, and disabling communications. Power, as used here, includes commercial power and the internal power systems including batteries, grounding, cabling, fuses, back-up emergency generators and fuel.

A Focus Group 2A sub-team reviewed and made recommendations on the power Best Practices. Because power is such a complex topic, the focus group felt that it needed to convene a panel of power experts for further review. This panel of experts provided an additional level of review for the power Best Practices to ensure that they contained enough technical concepts and details to convey the needed message and provide guidance to the industry.

Each Best Practice stands on its own, however many of the Power Best Practices can be grouped into several broad categories which identify key aspects of communications power. Those categories are Security, Design, and Back-up Power. The fact that six power Best Practices talk specifically to maintaining security for various components of the power infrastructure indicates the potential problems that can be caused through unauthorized access to those components. Power might be considered the Achilles' heel of communications equipment, for without it, the equipment simply doesn't work. An example of a security Best Practice related to power is 7-7-5212 which states:

- 7-7-5212 Service Providers, Network Operators and Property Managers should consider placing generator sets and fuel supplies for critical sites within a secured area to prevent unauthorized access, reduce the likelihood of damage and/or theft, and to provide protection from explosions and weather.

Security of power equipment is intended to provide protection from both overt attack and unintentional disruption. In that respect the security-related power Best Practices are closely coupled with the design-related power Best Practices. By incorporating security into the power plant design, both inadvertent and intentional disruption can often be prevented. Twenty-four of the power Best Practices speak directly to, or touch upon, the design of the power plant and the components that comprise it. Some provide specific technical guidance such as 7-7-0651 which states:

- 7-7-0651 Network Operators, Service Providers, and Property Managers should consider providing diversity within power supply and distribution systems so that single point failures are not catastrophic. For large battery plants in critical offices, consider providing dual AC feeds (odd/even power service cabinets for rectifiers). Transfer switches should be listed to a UL

standard for Transfer Switch Equipment. When transfer breaker systems are used, they must be mechanically and electrically interlocked.

Best Practices go a long way to heading off power problems, however commercial power outages must be planned for, which leads to the third broad category for power Best Practices: back-up power. The disaster events of the past several years; hurricanes (natural), terrorist attack (man-made, intentional), or the East coast blackout (man-made, unintentional) have highlighted the fact that the loss of commercial power to communication installations is an ever-present possibility, and that back-up power systems should be installed to ensure that communications systems will continue to operate when commercial power fails. Twenty power Best Practices speak directly to back-up power, and they emphasize the need to not only provide back-up power sources but to periodically exercise those power sources to ensure that they can be counted upon when needed. Best Practice 7-7-5204 clearly identifies the need for back-up power:

- 7-7-5204 Service Providers, Network Operators and Property Managers should ensure availability of emergency/back-up power (e.g., batteries, generators, fuel cells) to maintain critical communications services during times of commercial power failures, including natural and manmade occurrences (e.g., earthquakes, floods, fires, power brown/black outs, terrorism). The emergency/back-up power generators should be located onsite, when appropriate.

Because of the critical nature of power, additional back-up plans and the exercising of those plans are also very important as highlighted in Best Practice 7-7-0695, which states:

- 7-7-0695 Network Operators, Service Providers, and Property Managers should develop and test plans to address situations where normal power back-up does not work (e.g., commercial AC power fails, the standby generator fails to start, automatic transfer switch fails).

Power is an essential element of providing communications services. The effort spent in designing a secure power plant, and providing and testing back-up systems is an investment in the reliability of the communications systems they support.

5.5 Blended Attacks

One of the fears of security professionals is the potential use of “blended attacks” by adversaries. In discussions it became apparent that there was confusion on what is considered a blended attack and there was a general feeling that there needed to be discussions with cyber experts to get their opinions on the subject. Consequently Focus Group 2A, Homeland Security-Infrastructure arranged for a face-to-face meeting with Focus Group 2B, Homeland Security-Cyber Security to examine the blended attack subject. Among the concerns was the need to protect specific vulnerabilities, involvement of specific infrastructures (telecommunications, power, transportation, etc.), and the infinite number of attack permutations that lend themselves to blended attacks.

Depending on one’s perspective, a blended attack can mean different things. Historically when discussing “blended attacks” the focus has been on cyber security

threats that use multiple methods to attack or propagate with the intention to harm.[4] For someone from a physical security background it could mean a physical attack at one location to divert attention from the real target that is attacked simultaneously or a short time later. These different perspectives led FG 2A and FG 2B to create a common definition of a blended attack that the groups would use in their discussions and in the analysis of blended attacks for the NRIC VII. The definition is as follows:

> A "blended attack" includes two or more cyber, physical, social engineering, or cross industry attack vectors, coordinated so as to either divert attention, or to multiply the collateral damage, of a criminal or terrorist attack.

In addition to the broader definition of a blended attack, the results of the discussion between the focus groups identified a need to address coordination issues. Historically, companies have designed their organizational structure with cyber security and physical security in separate "silos." This situation could be exploited if good coordination does not occur at the time of an incident. The Focus Groups agreed to create a new Best Practice addressing this issue. Best Practice 7-7-1109 states:

- 7-7-1109 Service Providers, Network Operators and Equipment Suppliers should establish a means to allow for coordination between cyber and physical security teams supporting preparedness, response, investigation and analysis.

This issue was further addressed by consolidating similar Best Practices for cyber and physical security stressing the strong relationship evolving between the functions. Establishing communication mechanisms, correlation analysis capabilities, and mutual aid agreements prior to an attack would be invaluable in recognizing and mitigating a blended attack.

Blended attacks is a complex issue that requires coordination within a company and industry, as well as with the government. More sophisticated processes and systems will be needed to support preparation, detection, response and recovery functions. In addition, care needs to be taken so as not to create a Best Practice that identifies a vulnerability, which in-turn is used in a blended attack. Mechanisms are needed to ensure the confidentiality of information pertaining to possible scenarios and processes for sharing sensitive information. The initial discussions held by Focus Group 2A and Focus Group 2B clearly identified the need for further analysis and discussion. Focus Group 2A recommends that further focus on blended attacks be considered as a future topic of the NRIC as well as other government forums.

5.6 Coordination between Industry and Government

In assuring the optimal reliability and interoperability of the nation's communications infrastructure, effective coordination between industry and government entities at all levels (e.g., local, state, federal government) is essential. Several NRIC Best Practices specifically address coordination issues in a number of important areas, ranging from industry support of government-specific requirements (e.g., law enforcement and public safety needs) to coordinated information sharing with government to support emergency

[4] Cyber Security Operations Handbook, Rittinghouse Hancock, Elsevier Digital Press, Chapter 18, p. 623

response and restoration. An overview of those industry and government coordination-related Best Practices is discussed in Section 5.6.1.

5.6.1 Industry and Government Coordination Best Practices

Per direction of successive NRC/NRIC charters, several iterations of Best Practices pertaining to industry and government coordination have been developed over the years. As a part of its review of Homeland Security Best Practices adopted by the preceding Council, Focus Group 2A paid particular attention to coordination-related Best Practices, and recommended improvements needed to better address the topic to ensure language consistency across the Best Practices, and to delete obsolete items.

It should be noted that NRIC Best Practices generally describe industry's guidance to itself and are geared toward an industry audience (e.g., service provider, network operator, equipment supplier). Best Practices addressing coordination between industry and government are no different, and generally provide guidance to industry in interfacing/interacting/participating with its government partners.

NRIC Best Practices address a variety of important industry and government coordination issue categories. For example, Best Practices have been developed to ensure processes are in place to meet government requests stemming from legal/regulatory drivers (e.g., support for court-ordered wiretaps, uniform outage reporting methods). For example Best Practice 7-7-0505 states:

- 7-7-0505 Network Operators and Service Providers should have procedures in place to process court orders and subpoenas for wire taps or other information.

Other Best Practices advocate joint industry and government cooperation to maintain a resilient network reliability and security posture (e.g., coordination of pre-plans and preventative measures) as well as to support development of standards and capabilities to meet evolving government and customer needs. Examples include:

- 7-7-0726 Network Operators should consider partnering with excavators, locators, and municipalities in a cable damage prevention program.

- 7-7-0584 Service Providers, Network Operators and Equipment Suppliers and Government representatives [of the National Security Emergency Preparedness (NS/EP) community] should work together to support appropriate industry and international organizations to develop and implement NS/EP standards in packet networks.

A category of Best Practices also addresses the need for effective information sharing mechanisms between industry and government entities, and the need to ensure that such shared information is adequately protected:

- 7-6-8066 Sharing Information with Industry and Government: Service Providers, Network Operators, and Equipment Suppliers should participate in regional and national information sharing groups such as the National Coordinating Center for Telecommunications (NCC), Telecom-ISAC, and the

ISP-ISAC (when chartered). Formal membership and participation will enhance the receipt of timely threat information and will provide a forum for response and coordination. Membership will also afford access to proprietary threat and vulnerability information (under NDA) that may precede public release of similar data.

- 7-7-5100 Service Providers, Network Operators and Equipment Suppliers should interact as needed with federal, state, and local agencies to identify and address potential adverse security impacts of new laws and regulations (e.g., exposing vulnerability information, required security measures, fire codes).

5.6.2 Emergency Response and Restoration

Several of the existing coordination Best Practices address emergency response and restoration, and were generally proved effective in the recent response to Hurricanes Katrina and Rita. Hurricane Katrina was one of the worst natural disasters in the nation's history and had an extraordinary impact on the communications infrastructure in the Gulf States. More than three million people in the affected area lost phone service due to Hurricane Katrina's considerable damage to wireline and wireless switching centers and outside plant facilities.

Extraordinary response and restoration activities began almost immediately in the affected areas; much of the effort was performed by local industry and government employees, who had experienced personal losses themselves, yet continued to assist in restoring communications services to customers. NRIC Best Practices relevant to such emergency response and restoration efforts include both those stating general goals regarding industry cooperation with government at all levels, as well as targeted Best Practices that describe support of special government communications capabilities (e.g., TSP, GETS, and WPS) utilized during emergency response. Examples include:

- 7-7-1058 Service Providers, Network Operators and Equipment Suppliers should work collectively with local, state, and federal governments to develop relationships fostering efficient communications, coordination and support for emergency response and restoration.

- 7-7-5226 Service Providers, Network Operators and Property Managers should maintain liaison with local law enforcement, fire department, other utilities and other security and emergency agencies to ensure effective coordination for emergency response and restoration.

- 7-7-5127 Service Providers, Network Operators, Equipment Suppliers and Public Safety Authorities should provide a GETS (Government Emergency Telecommunications Service) card to essential staff critical to disaster recovery efforts and should consider utilizing Wireless Priority Service (WPS) for essential staff. Appropriate training and testing in the use of GETS & WPS should occur on a regular basis (i.e., in conjunction with testing of the corporate disaster recovery plan).

- 7-7-5112 Service Providers, Network Operators and Equipment Suppliers should, at the time of the event, coordinate with the appropriate local, state,

or federal agencies to facilitate timely access by their personnel to establish, restore or maintain communications, through any government security perimeters (e.g., civil disorder, crime scene, disaster area).

6. Areas for Future Discussion

At the time of report publication, both industry and government were still actively engaged in ongoing hurricane restoration efforts and are examining actions undertaken during the response to identify issues, lessons learned, and recommendations for incorporation into future plans, procedures and capabilities. In light of the ongoing analysis of response effectiveness as well as the amount of time remaining in the current NRIC VII cycle, Focus Group 2A deemed it premature to adopt specific recommendations pertaining to the recent hurricane response effort. The following items have been identified as some of the areas for future discussion.

- Provisioning security for assessment repair teams, staging areas, and facility sites during a crisis situation
- Facilitating access for vital communications and key infrastructure providers into impacted regions supporting response and restoration efforts
- Increasing the level of training and exercises (e.g., tabletop exercises) within and between industry, federal, state and local government
- Continuing efforts on addressing blended attacks, and possible engagement within other government forums

7. Appendix 1 – Abbreviations and Acronyms

ANSI - American National Standards Institute

ASP – Application Service Provider

ATIS – Alliance for Telecommunications Solutions

BITS - Financial Services Roundtable

CBRN - Chemical, Biological, Radiological, Nuclear

CCTV – Closed Circuit Television

CDMA – Code Division Multiple Access

CEV - Controlled Environment Vault

CLEC – Competitive Local Exchange Carrier

COW - Cell on Wheel

CTIA - Cellular Telecommunications and Internet Association

C-TPAT – US Customs Trade Partnership Against Terrorism

ERT – Emergency Response Team

FACA – Federal Advisory Committee Act

FEMA – Federal Emergency Management Agency

FCC – Federal Communications Commission

GETS – Government Emergency Telecommunications Service

HVAC –Heating, Ventilation and Air Conditioning

IEEE – Institute of Electrical and Electronics Engineers

IESNA – Illuminating Engineering Society of North America

IETF – Internet Engineering Task Force

INET – Internet

IP – Internet Protocol

ISAC – Information Sharing and Analysis Center

ISP – Internet Service Provider

ITU – International Telecommunication Union

IXC – Inter-Exchange Carrier

NANOG - North American Network Operators' Group

NCC – National Coordinating Center for Telecommunications

NCS – National Communications System

NEBS – Network Equipment Building System

NERC - North American Electric Reliability Council

NFPA - National Fire Prevention Association

NIPC – National Infrastructure Protection Center

NRC – Network Reliability Council

NRIC – Network Reliability and Interoperability Council

NRSC – Network Reliability Steering Committee

NSIE – Network Security Information Exchange

NSSE – National Special Security Event

NSTAC – National Security Telecommunications Advisory Committee

NS/EP – National Security and Emergency Preparedness

OSHA – Occupational Health and Safety Administration

RF – Radio Frequency

RFP – Request for Proposal

SLA – Service Level Agreement

SLB – Safety Light Beams

SME – Subject Matter Expert

SONET – Synchronous Optical Network

Telecom ISAC – Information Sharing and Analysis Center

TSP – Telecommunications Service Priority

WPS – Wireless Priority Service

8. Appendix 2 – Best Practices

For the complete list of additions, deletions and modifications to Best Practices recommended by Focus Group 2A, please refer to the document entitled “FG 2A_Best Practices_December 2005.”