FEDERAL COMMUNICATIONS COMMISSION
CONSUMER & GOVERNMENTAL AFFAIRS BUREAU

DRAFT TRIBAL COMMUNICATIONS SECURITY PLAN

A Plan to Assist Tribes in Protecting Communications Infrastructure

June 2004

DRAFT TRIBAL COMMUNICATIONS SECURITY PLAN

TABLE OF CONTENTS

EXECUTIVE SUMMARY
DRAFT TRIBAL COMMUNICATIONS SECURITY PLAN

The Importance of Planning to Protect Communications Infrastructure

The critical infrastructure of our Nation includes telecommunications and information systems. Telecommunications systems are vital to achieve homeland security and public safety objectives and to connect governments and communities. On July 10, 2003, the Commission announced its Homeland Security Action Plan. The Plan defines the Commission's homeland security goals as well as the approach it will take to achieve these goals. The Action Plan relies heavily on partnerships with other government entities, industry, and citizen groups. Among many goals, the Action Plan announced the goal to work together with Tribes, Tribal organizations and leaders to develop a plan Tribes can use to assist in protecting communications infrastructure. As the Federal Communications Commission (FCC or Commission) has certain trust responsibilities when dealing with federally-recognized Tribes, it is the responsibility of the FCC to consult with and assist Tribal governments on telecommunications matters.

Protecting Critical Communications Infrastructure and the *Communications Vulnerabilities Assessment Worksheet*

The step-by-step *Draft Communications Vulnerabilities Assessment Worksheet* (*Worksheet*) is designed to assist Tribal Governments in planning for the physical protection of critical communications infrastructure in their communities. The *Worksheet* provides a framework to identify a Tribe's critical communications infrastructure and analyze potential vulnerabilities. The selected Best Practices (drawn from selected materials and voluntary Best Practices of the Network Reliability and Interoperability Council) provides recommended solutions to address such vulnerabilities.

The *Worksheet* identifies eight categories of vulnerabilities internal to communications infrastructure that must be assessed: Environment; Power; Hardware; Software; Networks; Payload; Policy; and Human. Examples of the factors to be considered in assessing vulnerabilities in each of the eight categories are provided, based on the findings of NRIC VI. The plan also recommends assessing the vulnerabilities of other infrastructures which may affect communications.

Standardized and Interoperable Public Safety Communications

Public Safety communications are critical to Homeland Security. The Secretary of the Department of Homeland Security recently promulgated the National Incident Management System (NIMS). The NIMS is a template that enables Federal, State, Local and Tribal governments, and private-sector and nongovernmental public safety organizations, to prepare for, prevent, respond to and recover from domestic incidents. The NIMS requires interoperable communications systems for both incident and information management. Starting in FY2005, NIMS compliance and interoperability will be required to receive Federal funding and grants to enhance public safety infrastructure, including public safety communications equipment.

BACKGROUND

FCC Involvement in Homeland Security and the Tribes

American Indian Tribes and Alaska Native Village governments, along with their State, Local and Federal counterparts play an important role in our Nation's homeland security planning and in protecting critical infrastructure. Critical infrastructure includes communications and information management systems. Access to secure telecommunications networks and information technology empowers economic development. It is essential to the future growth and strengthening of Tribal life – bringing significant benefits to Tribal financial, social, political, healthcare and educational systems.

Telecommunications systems can be used to meet important homeland security and public safety objectives and to connect governments and communities. It is the responsibility of Tribal governments, their leaders and representatives, to plan and provide for the safety and security of Tribal Nations and their communities and the systems that are so integral to Tribal communities.

As the Federal Communications Commission (FCC or Commission) has certain trust responsibilities when dealing with federally-recognized Tribes that devolve from the unique government-to-government trust relationship it shares with Tribes and the inherent sovereign status of Tribes, it is the responsibility of the FCC to consult with and assist Tribal governments on telecommunications matters. The *Communications Vulnerabilities Assessment Worksheet* (*Worksheet*) is designed to assist Tribal Governments in their task of planning for the protection of critical communications infrastructure in their communities.

Recent changes in Federal law pertaining to public safety, particularly in the area of public safety communications will affect emergency response efforts in all jurisdictions, including those in Tribal lands. Accordingly, and in furtherance of the FCC's strategic goal for Homeland Security, this document provides a brief overview of the National Incident Management System (NIMS) and National Response Plan (NRP).[1]

FCC and Homeland Security

The Homeland Security mission of the FCC is to evaluate and strengthen measures for protecting the Nation's communications infrastructure; facilitate rapid restoration of that infrastructure in the event of disruption; and develop policies that promote access to effective

[1] The FCC's strategic goal for Homeland Security is to provide leadership in evaluating and strengthening the Nation's communications infrastructure, in ensuring rapid restoration of that infrastructure in the event of disruption, and in ensuring that essential public health and safety personnel have effective communications services available to them in emergency situations. To fully and effectively carry out its role in promoting homeland security, network protection, interoperability, redundancy, and reliability, the FCC established the following objectives: (1) Evaluate and strengthen measures for protecting the Nation's communications infrastructure; (2) Facilitate rapid restoration of the U.S. communications infrastructure and facilities after disruption by a threat or attack; and (3) Develop policies that promote access to effective communications services by public safety, public health, and other emergency and defense personnel in emergency situations. *See* http://www.fcc.gov/homeland.

communications services by public safety, public health, and other emergency personnel in emergency situations.[2]

In July 2003, the FCC created the Office of Homeland Security (OHS) within the Enforcement Bureau. OHS assists the Chief of the Enforcement Bureau in his support of the Defense Commissioner, oversees rulemaking proceedings relating to the Emergency Alert System and operates the Communication and Crisis Management Center (CCMC). OHS also supports the Homeland Security Policy Council (HSPC) and other FCC Bureaus in achieving the objectives established in the Homeland Security portion of the Commission's Strategic Plan. OHS provides intra- and inter-agency coordination on all matters concerning homeland security, National Security/Emergency Preparedness (NS/EP), public warning and continuity of government.

The HSPC is comprised of senior staff from each of the Commission's Bureaus and is directed by the Chief of Staff for the Commission. The mission of the HSPC is to assist the FCC in: evaluating and strengthening measures for protecting communications services; ensuring rapid restoration of communications services and facilities that have been disrupted as the result of threats to, or actions against the Nation's homeland security; ensuring that public safety, health and other emergency and defense personnel have effective communications available to them to assist the public as needed; and fostering the implementation of new technologies that promote homeland security.

On July 10, 2003, the Commission announced its Homeland Security Action Plan. The Plan defines the Commission's homeland security goals as well as the approach it will take to achieve these goals. The Plan relies heavily on partnerships with other government entities, industry, and citizen groups. The Action Plan announced the FCC's goal of working with tribal organizations and leaders and other relevant federal government agencies develop a plan that tribes can use to assist in protecting communications infrastructure. The *Worksheet*, based largely on selected materials and voluntary Best Practices of the Network Reliability and Interoperability Council (NRIC) VI was developed to satisfy this objective.

NRIC VI was responsible for assessing vulnerabilities in communications infrastructure and determining how best to address vulnerabilities due to terrorist activities, natural disasters, or similar types of occurrences. The *Worksheet* is based largely on the Final Report of the NRIC VI Homeland Security Physical Security Focus Group (Focus Group 1). Focus Group 1 developed Best Practices applicable to prevention and restoration.[3]

[2] See http://www.fcc.gov/homeland/#action_plan.

[3] *See* http://www.nric.org/fg/nricvifg.html. NRIC Best Practices are statements that describe the industry's guidance to itself for the best approach to addressing a concern and are the most authoritative list of such guidance for the communications industry. NRIC Best Practices are voluntary and intended to give guidance on how best to protect the U.S. communications infrastructure. A detailed description of the NRIC Best Practices' intended use is provided in the Focus Group final report entitled Homeland Security – Physical Security – Final Report available at http://www.nric.org/fg/nricvifg.html. In addition, several Best Practices were developed specifically to address Blended Cyber and Physical Attack concerns. *See* http://www.bell-labs.com/user/krauscher/nric/

The FCC Action Plan also proposed finalizing a Memorandum of Understanding (MOU) with the Department of Homeland Security (DHS)[4] to enhance the FCC's ongoing program to promote the Best Practices of the NRIC and work with DHS to promote Best Practices of the Media Security and Reliability Council (MSRC).[5]

In the spring of 2004, staff within the FCC's Office of Intergovernmental Affairs (IGA) began to review relevant statutes, rules and policies to formulate a framework to protect communications infrastructure to share with Tribes and begin the consultation process. The *Worksheet* was developed to serve as such a framework.

A FRAMEWORK FOR PLANNING

Homeland Security depends on the reliability of services that are provided over the communications infrastructure. Network facilities on which public communications services are provided must be protected, particularly critical infrastructure facilities. Businesses that support the communications infrastructure must be secured. Buildings, information and personnel must be protected. This is where the term "physical security" is most commonly understood in the context of communications.

The *Worksheet* recommends that Tribal planners begin by identifying and defining what constitutes critical communications infrastructures. Generally, such distinction applies to points of concentration, facilities supporting high traffic, network control and operations centers, and equipment supplier technical support centers. It is critical for planners then to identify and analyze vulnerabilities in the communications infrastructure and consider the potential consequences if the vulnerabilities are exploited. Planners are encouraged to review current physical security programs to determine what vulnerabilities are addressed through day-to-day responsibilities. "Vulnerability" is defined, for the purpose of the *Worksheet*, as a characteristic of any aspect of the interdependent communications infrastructure that renders it, or some portion of it, susceptible to damage or compromise.

For the purpose of the *Worksheet*, "threat" is defined as anything with the potential to damage or compromise the communications infrastructure or some portion of it. This includes threats from natural events, intentional malicious human acts, and unintentional human acts. There are a consistent set of threat factors that should be analyzed as part of the decision making process in developing an effective security plan:

- What are the known threats?
- What is the probability of the threat being exercised?
- Are there any threats with sudden increased likelihood of being used in attacks?
- What vulnerabilities do these threats exercise?
- What is the impact if vulnerability is successfully exercised by a threat?

[4] See Appendix A for DHS Organization for Critical Infrastructure Protection Planning. See Appendix B for relevant hyperlinks.

[5] *See* http://www.bell-labs.com/user/krauscher/nric/#Homeland_Security_Best_Practices and Appendix C for additional information on the NRIC.

- How are the critical facilities being protected?
- What is the cost vs. the benefit of the measure(s) to be implemented?
- What is the ease with which the measures can be accepted and utilized by the people impacted by the program?

COMMUNICATIONS VULNERABILITIES ASSESSMENT WORKSHEET

Among other things, NRIC VI was responsible for identifying areas for attention and describing Best Practices to: (1) prevent disruptions of public telecommunications services and the Internet from terrorist activities, natural disasters, or similar types of occurrences; (2) aid in disaster recovery and service restoration; (3) identify issues to ensure that commercial telecommunications services networks (including wireless, wireline, satellite, and cable public telecommunications networks) can meet the special needs of public safety emergency communications, including means to prioritize, as appropriate, public safety usage of commercial services during emergencies. NRIC VI also had responsibilities with respect to Network Reliability and Interoperability, Broadband Deployment and various other topics.

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). Organizations should carefully evaluate the vulnerabilities and risks inherent in their environments, internal power systems, hardware, software, networks, payload, policies and personnel, and should consider implementing appropriate Best Practices to address these risks. Each Best Practice can have associations with any combination of five industry roles:

- Service Providers - An organization that provides services for content providers and for users of a computer network. The services may include access to the computer network, content hosting, server of a private message handling system, news server, etc. A company, organization, administration, business, etc., that sells, administers, maintains, charges for, etc., the service. The service provider may or may not be the operator of the network.
- Network Operators - The operator responsible for the development, provision and maintenance of real-time networking services and for operating the corresponding networks.
- Equipment Suppliers - An organization whose business is to supply network operators and service providers with equipment or software required to render reliable network service.
- Property Managers - The responsible party for the day-to-day operation of any facility (including rooftops and towers), usually involved at the macro level of facility operations and providing service to a communications enterprise. This responsibility may include lease management, building infrastructure operation and maintenance, landlord/tenant relations, facility standards compliance.
- Government - Government includes Federal, State and Tribal and Local.

It is essential to assess the vulnerabilities of communications infrastructure and other infrastructure on which it relies and to implement sufficient "Best Practices" to protect the infrastructure and plan for disaster recovery.[6]

The NRIC Vulnerabilities Assessment is a four stage process: (1) Assess vulnerabilities; (2) Analyze changing circumstances and reassess vulnerabilities; (3) Plan for business continuity and disaster recovery; and (4) Adopt applicable NRIC Best Practices. After conducting a Vulnerabilities Assessment, NRIC encourages planners to reevaluate the condition of their vulnerabilities before adopting and implementing relevant Best Practices.

Following the vulnerabilities list is a summary of selected NRIC Best Practices.[7] These highlighted, voluntary Best Practices are provided to serve as suggested solutions planners should consider in protecting critical communications infrastructure. Not all Best Practices are applicable to each component of the industry. Service providers, network operators and equipment suppliers each provide a separate, and many times distinct, component to the totality of the industry. Some Best Practices may be applicable only to certain network configurations instead of the broad range of services that exist within the industry. When viewed as a whole, many of the Best Practices support the general principles regarding plans as follows: (1) it is important that a formal plan be in place, (2) that such a plan adequately cover the Vulnerabilities, and (3) that such a plan be uniformly applied at all locations within the company.

The *Worksheet* identifies eight categories of vulnerabilities internal to communications infrastructure that must be assessed: Environment; Power; Hardware; Software; Networks; Payload; Policy; and Human. Examples of the factors to be considered in assessing vulnerabilities in each of the eight categories are provided, based on the findings of NRIC VI. The plan also recommends assessing the vulnerabilities of other infrastructures which may affect communications.

1. Environmental Vulnerabilities

A. Assess Vulnerabilities - The Environment includes buildings, trenches where cables are buried, space where satellites orbit, the ocean where submarine cables reside. Each environment is affected by environmental factors such as fire, floods, ice and snow. Some factors related to the environment may be controlled or mitigated while others may not. Assess vulnerabilities such as:

- Potential for release of contaminants due to chemical, biological, radiological incidents resulting in the inability to access critical infrastructure contamination.
- Insufficient surveillance/monitoring – e.g., intrusion alarms, environmental detection and suppression systems.
- Public availability of information revealing, among other things, the location of critical communications infrastructure - e.g., signage designating critical infrastructure buildings, compliance with laws/regulations to make sensitive data

[6] For a glossary of terms used see http://www.nric.org/fg/nricvifg.html.
[7] *See* http://www.bell-labs.com/user/krauscher/nric/.

public, sensitive information posted on the internet, internal information unnecessarily provided, unauthorized monitoring of signals.
- Lack of staffing at sites containing critical communications infrastructure – e.g., unmanned facilities remote locations.
- Non-compliance with established protocols and procedures.

B. Adopt Best Practices - Communications infrastructure companies typically are already providing elements of physical security in an overall plan or strategy. Very few, if any, do this exactly the same way. Tribal planners are encouraged to work with communications infrastructure companies with facilities on tribal lands to ensure that environmental vulnerabilities are assesses as part of its critical infrastructure plan.

2. Power Vulnerabilities

A. Assess Vulnerabilities - Power includes the internal power systems, batteries, grounding, high voltage and other cabling, fuses, back-up emergency generators and fuel. Power is often overlooked as a critical basic element of the communications infrastructure.[8] Without power, networks will not function. Any power problem has the potential to become a catastrophe, potentially damaging other equipment and personnel. The power infrastructure also has the potential for being turned into a weapon to be used to harm the network and network personnel. Assess vulnerabilities such as:

- Uncontrolled access - Vulnerabilities must be considered in light of Commission regulations. Rules that require service providers and network operators to allow others to access their premises (i.e. co-location by other service providers) might make controlling access to power infrastructure difficult.
- Critical fuel characteristics - combustion, contamination, availability.
- Critical battery characteristics - combustion, limitations.
- Ineffective alarm management - monitoring, response.
- Improper physical location - batteries, fuel tanks, generators, feed lines, switch gear.
- Voltage / frequency limitations.
- Unsafe laws and local requirements.
- Lack of training.
- Improper parts availability - lack of parts, unusable parts.
- Single points of failure in power systems.
- Power system competencies that are not adequately maintained - service providers and network operators need adequate levels of competent staff to maintain the power infrastructure.

B. Adopt Applicable NRIC Best Practices – Some Best Practices intended to improve security may be at odds with environmental rules and policies, i.e. buried fuel storage tanks and distribution lines may be more secure but also may pose a risk of environmental contamination.

[8] The communications infrastructure is also dependent on the commercial energy. This commercial power is external to the communications infrastructure.

Planners should consider carefully applicable regulations and competing considerations in their planning.

3. Hardware Vulnerabilities

A. Assess Vulnerabilities - Hardware includes the broad category of physical electronics-related components that are part of communications systems. Hardware systems include: frames, cabinets, circuit packs and cables. Electronic hardware equipment includes switches, routers, transport equipment, transmission equipment, access equipment, satellites, dishes, undersea cables, microwave repeaters, cell sites, etc. Assess vulnerabilities such as:

- Chemical vulnerabilities due to corrosive gas, humidity or impact of temperature changes.
- Physical vulnerabilities due to shock, vibration, strains, torque.
- Electromagnetic energy vulnerabilities.
- Environmental vulnerabilities due to temperature, humidity, dust.
- Hardware life cycle vulnerabilities caused by lack of equipment replacement or adequate repairs.

B. Adopt Applicable NRIC Best Practices – Some priorities are beyond the scope of this *Worksheet* such as control of hardware development and issues pertaining to nuclear attack, hardness to radiation, solar flares, etc. Tribal planners are nevertheless encouraged to consider such vulnerabilities and to adopt relevant Best Practices.

4. Software Vulnerabilities

A. Assess Vulnerabilities - Software issues include the physical storage of software releases, development and test loads, version control and management and chain of control delivery. Critical operational software is an essential element in the continued operation of communications infrastructure. Assess vulnerabilities such as:

- Intentional or unintentional destruction of critical operational software.
- Unauthorized modification of critical operational software – intentionally or unintentionally introducing a weakness in installed systems.
- Compromise of critical operational software - with the intent of discovering operational features or methods of interception.
- Unrestricted access control – source media, binary media, system documentation, lab facilities, computing hardware, visitor control, network access points, network interconnect points.
- Poor network design and implementation – unsecured distribution channels, unsecured research and development network channels, non-segregated access from office systems.
- Lack of design and operational oversight – design error, susceptibility to rogue code insertion, simultaneous use of multiple versions, interception of media during delivery.

- Use of Off-Site developers – Unsecured off-site facilities, inadequate non-disclosure agreements (NDA), inadequate service level agreements (SLA), unsecured teleworker sites, offshore developers or contractors agreements.
- Equipment implementation issues – default access points, susceptibility to cascade failure, unsecured wireless access points, poorly positioned free-space optics, wireless access for updates, etc.

B. Adopt Best Practices – Existing NRIC Best Practices effectively address software vulnerabilities. Perform a thorough risk assessment to support the decision making process.

5. Network Vulnerabilities

A. Assess Vulnerabilities - Networks can interconnect with other networks and contain sub-networks. The networks that support the United States' communications infrastructure are immense both in terms of communications services provided and geographic coverage. Networks should be designed with capabilities that minimize or mitigate the impact of failures on the services provided. Assess vulnerabilities such as:

- Lack of redundancy/diversity.
- Unanticipated results of automation.
- Unwarranted geographic concentration.
- Inter-network conflicts.
- Problems caused by interconnecting networks.
- Problems caused by capacity limits.
- Uniqueness of mated pairs.
- Synchronization.
- Complexity.
- New Technology.
- Improperly managed changes/upgrades.

B. Adopt Best Practices – Existing NRIC Best Practices effectively address network vulnerabilities. Perform a thorough risk assessment to support the decision making process.

6. Payload Vulnerabilities

A. Assess Vulnerabilities - Protecting network payload is an essential element in the continued operation of the nation's communications infrastructure. Payload includes information transported across the infrastructure, traffic patterns and statistics, information interception and information corruption. Whether analog or digital, wireline or wireless, voice or data, payload is the major source of communication as well as a major component of commerce, public safety, transportation, national security, and emergency response. Attacks against payload fall into one of the following three categories: (1) Interception of critical network payload; (2) Modification of critical network payload; or (3) Interruption of critical network payload. Assess vulnerabilities such as:

- General – Insufficient inventory of critical components

- Internal Network – Data corruption, data interception, control signal interception
- External Network – Data corruption, data interception, control signal interception

Traditional physical security methods (perimeter security, document classification, change management), when applied to payload transmission environments, are vital to security. Recognizing the physical aspects to payload (transmission channels, routing equipment, etc.) is essential to properly secure critical communications infrastructure.

B. Adopt Applicable NRIC Best Practices - The adoption of Best Practices and physical security solutions significantly dependent on economic considerations. Implementation levels will vary from organization to organization. Tribal planners are encouraged to weigh competing considerations in identifying and implementing appropriate solutions.

7. Policy Vulnerabilities

A. Assess Vulnerabilities - Policy includes industry standards, industry cooperation, and industry interfaces with governments (including Local, State, Federal, Tribal), and various legal issues. NRIC identified eight general categories of policy vulnerabilities:

- Lack of awareness of Emergency Preparedness Priority Services (NS/EP Priority Services).[9]
- Evolving technologies on emergency restoration.
- Lack of or insufficient definition of corporate policy directing adequate physical security measures.
- Poor organization/operations to implement or enforce existing security policy.
- Lack of physical security standards, or existing security standards not adopted or implemented.
- Foreign ownership/interests in critical communications infrastructure.
- Inadvertent negative impact of government regulations –e.g., regulations or laws that inhibit or limit meeting of security needs and adoption of Best Practices.
- Physical security vulnerabilities introduced due to collocation/multi-tenant arrangement or requirement.
- Physical security vulnerabilities introduced due to outsourcing.
- Inadequate protection of physical security information (e.g., floor plans, camera locations, physical security plans).
- Cross-subsidiary barriers to resource sharing - There may be barriers to cross-subsidiary resource sharing that limit optimal emergency restoration. These barriers may include legal, technical and policy issues.
- Failure to protect critical infrastructure information (CII).[10]
- Lack of focal point needed for disaster coordination.[11]

[9] *See* Appendix B, description of the National Communications System.
[10] *See* Appendix B, description of the Protected Critical Infrastructure Information (PCII) Program.
[11] *See* Appendix B, description of the National Coordinating Center Telecommunications Infrastructure Information Sharing and Analysis Center (NCC Telecom ISAC).

B. Adopt Appropriate Best Practices - Some Best Practices intended to improve security may be at odds with policies or existing regulations. Tribal planners are encouraged to balance competing considerations in identifying and implementing appropriate solutions that fit within policy constraints.

8. Human Vulnerabilities

A. Assess Vulnerabilities – Human vulnerabilities include intentional and unintentional behaviors, limitations, and education and training, human-machine interfaces, and ethics. Analyze human vulnerabilities with consideration to external threat to the communications networks (in the form of attacking one or more network elements) as well as threats to the personnel (such as hijacking, kidnapping or blackmailing). Additionally, both intentional threats from the communications personnel to the network (e.g., from disgruntled employees) as well as unintentional threats from communications personnel to the network (e.g., human errors caused due to confusion, anxiety, etc.) should be analyzed.

- Human – Physical, cognitive, ethical.
- User Environment – User interface, job function, corporate culture.
- Human-User Interaction.

B. Adopt Relevant Best Practices – Organizations should conduct restoration training exercises. Inherent to training for security and other restoration personnel is a need to include simulated events. Thus, access control procedures can be appropriately tested. During actual restoration, the human physical and cognitive vulnerabilities may play a significant part, and training is an effective countermeasure to address these. Senior management must demonstrate commitment to corporate security. The corporate culture should require employees to abide by security requirements and play an active role in maintaining the security of the enterprise. Too often, employees being "helpful" or "friendly" open the doors (literally) to intruders, without recognizing the security risk this creates. The use of voluntary background checks for employees with access to critical sites should be considered.

9. Assess Vulnerabilities of Other Infrastructures

- Assessing Vulnerabilities of Other Infrastructures - The communications network is vulnerable to blended physical and cyber attacks. Physical security is dependent, in part, on cyber security. Cyber security depends on physical security, and the communications infrastructure is dependent on other infrastructures, e.g., the energy infrastructure. There are numerous vulnerabilities associated with interdependencies. Assessing the vulnerabilities of other infrastructures is beyond the scope of this *Worksheet*.

Selected NRIC Best Practices

There are 776 NRIC Best Practices. NRIC Best Practices are recommended procedures and methods that provide the telecommunications industry guidelines to follow when providing service, equipment, and support. With such a large number, it is difficult for many companies to

decide which Best Practices to implement. NRIC recommends that entities should implement sufficient Best Practices to protect communications infrastructure. That said, some are set forth here for the convenience of the reader. These selected voluntary Best Practices fall into six categories:

Ensure Backbone Critical Network Reliability

- Provide physical diversity on critical routes.
- Ensure diversity of power and timing sources - Ensure intra-office diversity of all critical resources including spare equipment, power systems, timing sources and signaling leads (e.g., SS7).
- Ensure availability of emergency/backup power generators 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) - Emergency/backup power generators should be located onsite, when appropriate. Consider contingency contracts in advance with clear terms and conditions for mobile generators.

Provide Redundancy in E911 Architectures and Emergency Services

- Back-up primary public safety access point (PSAP) with an alternate destination - Alternate PSAP may be either administrative telephones or another jurisdiction's PSAP positions.
- Provide dual 911 tandems in E911 architectures - Dual active 911 tandem switch architectures enable circuits from the caller's serving end office to be split between two tandem switches. Diverse interoffice transport facilities further enhance the reliability of the dual tandem arrangement. Diversity is also deployed on interoffice transport facilities connecting each 911 tandem to the PSAP serving end office.
- Provide diverse Automatic Location Identification (ALI) and Mobile Positioning Center (MPC) systems.
- Redundancy of connections to emergency services personnel - Redundancy and diversity should be applied to designated vital network links that enable a community to respond to emergencies including those directly connected to emergency services personnel. Security practices and concepts should also be applied to the critical systems supporting link redundancy and diversity. Critical links include point-to-point private circuits used by public safety networks for radio site communications, but obtained from commercial landline communication providers. Types of links that are critical to the provision of emergency aid include communication links from the PSAP location to law enforcement dispatchers and/or response personnel; Emergency medical service (EMS) dispatchers and ambulance response units; Fire fighter dispatchers and response personnel; etc.

Disaster Preparedness

- Test network operational readiness through planned drills or simulated exercises - Exercises should be unannounced and as authentic as practical with scripted parts for team members. Callout rosters to notify appropriate personnel and emergency phone lists should be verified. Coordinate disaster exercises with other service providers, public

safety providers and vendors. Conduct after-action review immediately to identify lessons learned.

- Documented plans to respond to disasters - service providers and network operators should have documented plans or processes to assess damage to network elements, outside plant, facility infrastructure, etc. for implementation immediately following a disaster.
- Preparing for natural disasters. Place standby generators on line and verify proper operation of all subsystems.
- Maintain 24/7 emergency call center - service providers, network operators and equipment suppliers should establish and maintain (or contract for) a 24/7 emergency call center for internal communications. Ensure staff has access to all documentation pertinent to emergency response and up-to-date call lists. Number of call center should be published so personnel know where to report information.
- Review responses to all emergency events - service providers, network operators, equipment suppliers and property managers should perform after-action reviews of all emergency response and restoration events to capture lessons learned (e.g., early warning signs) and to enhance emergency response and restoration plans accordingly. Reviews should include analysis to identify countermeasures to prevent or mitigate the impact of future incidents and to quickly and effectively restore from such events in the future.
- Periodically test 911 Contingency Plan - Once a contingency plan is developed, it should be tested at least annually. Tests can be: (1) desktop check tests (using a checklist to verify familiarity of "what to do in case of"); (2) procedures verification test (verify that established procedures are followed in a simulation); (3) simulation test (similar to a fire drill, e.g., simulating a disaster and monitoring the response); (4) actual operations test (cause an event to happen, e.g., power or computer failure and monitor the response, etc.)

Physical Security

- Alarm access to facilities in areas of critical infrastructure - Alarm and continuously monitor all means of facility access (e.g., perimeter doors, windows) to detect intrusion or unsecured access (e.g., doors being propped open).
- Limit access to facilities in areas of critical infrastructure to essential personnel.
- Secure portable generators - Provide security from theft of portable generators. Trailer mount generators and equip with wheel locks.

Educating the Public

- Educate the public on the proper use of abbreviated dialing access codes (211, 311 and 511 services). Service providers should work with public safety service and support providers to educate the public on the proper use of abbreviated dialing access codes to enable 911 network and personnel to be exclusively focused on emergencies.

Cyber Security[12]

- Secure communications for Operations, Administration, Management and Provisioning (OAM&P) communication traffic - To prevent unauthorized users from accessing OAM&P systems, service providers and network operators should use strong authentication for all users. To protect against tampering, spoofing, eavesdropping and session hijacking, use a trusted path for all important OAM&P communications between network elements, management systems and staff. Examples of trusted paths include separate private-line networks (VPNs), or encrypted tunnels. Sensitive OAM&P traffic mixed with customer traffic should be encrypted. OAM&P traffic to customer premises equipment should also be via a trusted path.
- Protect Domain Name Server (DNS) servers against compromise. Service providers should protect against DNS server compromise by implementing physical security, removing all unnecessary platform services, monitoring industry alert channels for vulnerability exposures, scanning DNS platforms for known vulnerabilities and security breaches, implementing intrusion detection on DNS home segments, not running the name server as root user, minimizing privileges where possible, and blocking the file system from being compromised by protecting the named directory.
- Prepare a disaster recovery plan to implement upon DNS server compromise.
- Ensure secure access to SS7 - Ensure SS7 signaling interface points (SIPs) that connect to Internet Protocol (IP), private and corporate network interfaces are hardened, protected with packet filtering firewalls; and enforce strong authentication. Similar safeguards should be implemented for e-commerce applications to the SS7 network. Implement rigorous screening on internal and interconnecting signaling links. Operators should be particularly vigilant with respect to signaling traffic delivered or carried over IP networks. Network operators that use the public Internet for signaling, transport or maintenance communications, and any maintenance access to network elements should employ authentication, authorization, accountability, integrity and confidentiality mechanisms (e.g., digital signature and encrypted VPN tunneling).
- SS7 authentication - Mitigate limited SS7 authentication by enabling logging for SS7 element security-related alarms on SCPs and STPs, such as: unauthorized dial up access, unauthorized logins, logging of changes and administrative access logging. Establish login and access controls that establish accountability for changes to node translations and configuration. Operators should be particularly vigilant with respect to signaling traffic delivered or carried over IP networks. Operators making use of dial-up connections for maintenance access to network elements should employ dial-back modems with screening lists. One-time tokens and encrypted payload VPNs should be the minimum.
- Respond to compromised DNS or name record corruption by implementing pre-defined disaster recovery plan - Elements may include but are not limited to: (1) bring-on

[12] Cyber security issues are beyond the scope of this document but are noted to alert the reader to plan appropriately for cyber security. See e.g., NRIC Report on Cyber security http://www.nric.org/fg/nricvifg.html. The National Strategy to Secure Cyberspace is an implementing component of the National Strategy for Homeland Security and is complemented by a National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. The National Strategy to Secure Cyberspace http://www.whitehouse.gov/pcipb/ identifies steps that State and Local governments, private companies and organizations, and individual Americans can take to improve cyber security.

additional hot or cold spare capacity; (2) bring up a known good DNS server from scratch on different hardware; (3) reload and reboot machine to a known good DNS server software from bootable CD or spare hard driv); and (4) reload name resolution records from a trusted back-up. Conduct after-action review immediately to identify lessons learned.

- Recover from DHCP-based Denial of Service (DOS) Attack - If a Dynamic Host Configuration Protocol (DHCP) attack is underway, isolate source to contain attack. Then, plan to force all DHCP clients to renew leases in a controlled fashion at planned increments. Re-evaluate architecture to mitigate similar future incidents.
- Apply SS7 network security base guidelines including checklists and adhere to industry security standards – Review specific Best Practices for the appropriate guidance all service providers should have for any network element (call agent, feature server, soft switch, cross connect, gateway, database).

Standardized Public Safety Communications - The NIMS and NRP

Public Safety communications is critical to Homeland Security. In assessing a tribe's critical communications infrastructure, particular attention should be given to infrastructure dedicated to public safety communications. Recent changes in Federal law pertaining to public safety, particularly in the area of public safety communications will affect emergency response efforts in all jurisdictions, including those in Tribal lands. In furtherance of the FCC's strategic goal for Homeland Security,[13] this document provides a brief overview of the National Incident Management System (NIMS) and National Response Plan (NRP).

On March 1, 2004, the Secretary of the Department of Homeland Security (DHS) promulgated the NIMS.[14] The NIMS is a template that enables Federal, State, Local and Tribal governments, and private-sector and nongovernmental public safety organizations to prepare for, prevent, respond to and recover from domestic incidents, regardless of cause, size, or complexity, including acts of catastrophic terrorism. NIMS requires interoperable communications systems for both incident and information management. NIMS incorporates incident management Best Practices and national standardization to promote homeland security, network protection, interoperability, redundancy, and reliability.[15]

There are six components of NIMS: (1) Command and Management - NIMS standardizes incident management for all hazards and all levels of government. Incident command structures are based on three constructs: Incident Command System (ICS); Multi-

[13] Among other things, the FCC's strategic goal for Homeland Security is to provide leadership in ensuring that essential public health and safety personnel have effective communications services available to them in emergency situations. *See* http://www.fcc.gov/homeland.

[14] *See* March 1, 2004 Memorandum from Tom Ridge, Secretary, DHS addressed to, among others, Tribal Leaders and Tribal First Responders seeking cooperation and assistance as the NIMS and the associated NRP are further developed and implemented.

[15] On February 28, 2003, the President issued Homeland Security Presidential Directive (HSPD)-5 "Management of Domestic Incidents" http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html which directed the Secretary of DHS to develop and administer the NIMS. The NIMS is set out at http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf.

agency Coordination Systems; and Public Information Systems; (2) Preparedness - NIMS establishes specific measures and capabilities that jurisdictions and agencies should develop and incorporate into an "all hazards" context within the system; (3) Resource management - Mechanisms to describe, inventory, track, and dispatch resources before, during, and after an incident; (4) Communications and Information Management - Promotes Effective Communications. Information and intelligence sharing are critical aspects of domestic incident management. It enables essential functions to provide a common operating picture and interoperability for incident management at all levels. Integrated Communications requires a common communications plan, common terminology and interoperable two-way communications. (5) Supporting Technologies – NIMS promotes national standards and interoperability for supporting technologies. It provides an architecture for science and technology support to incident management; and (6) Ongoing Management and Maintenance - A multi-jurisdictional, multi-disciplinary NIMS Integration Center will provide strategic direction and oversight of NIMS in both maintenance and improvements. The purpose of the NIMS Integration Center is to publish standards, guidelines, and compliance protocols for determining whether a Federal, State, Tribal, or local entities are compliant.

A primary directive of the NIMS is to implement a unified and integrated National Response Plan. The NRP integrates current Federal domestic prevention, preparedness, response, and recovery plans into a single all-discipline, all-hazards plan for responders. The NRP, using the NIMS framework, provides structure for national level policy and operational direction for federal support to State, Local and Tribal incident managers and for exercising direct federal authorities and responsibilities.[16] The NRP establishes a process and structure to integrate current Federal domestic prevention, preparedness, response, and recovery plans into a single all-discipline, all-hazards plan for responders.[17] With responders using the same standardized procedures, they will all share a common focus, and will be able to place full emphasis on incident management when a homeland security incident occurs, whether terrorism or natural disaster. In addition, national preparedness and readiness is enhanced since all of the Nation's emergency teams and authorities are using a common language and set of procedures.

Jurisdictional compliance with certain aspects of the NIMS and the INRP for public safety communications is possible in the short-term, such as adopting the basic tenets of the Incident Command System (ICS). Other aspects of the NIMS, however, such as sections pertaining to public safety data and communications systems interoperability, require further development and refinement.

---

[16] http://www.dhs.gov/dhspublic/display?theme=43&content=1936&print=true. On October 10, 2003, DHS released an Interim National Response Plan (INRP) which will remain in effect until the final NRP is promulgated. Among other things, the INRP establishes: a National Homeland Security Operations Center (HSOC), located at DHS headquarters as the primary national-level hub for operational communications and information pertaining to domestic incident management that operates on a 24/7 basis; an Interagency Incident Management Group (IIMG) made up of senior representatives from Federal departments and agencies, non-governmental organizations, as well as DHS components to facilitate national-level situation awareness, policy coordination, and incident coordination; A Joint Field Office (JFO) responsible for integrating Federal activities at a local incident site to better facilitate coordination between Federal, State, Local and Tribal authorities. The JFO is expected to incorporate existing entities such as the Joint Operations Center, the Disaster Field Office, and other Federal offices and teams that provide support on scene.

[17] Additional web links are found in Appendix B.

Starting in FY2005, NIMS compliance and interoperability will be required to receive Federal funding and grants to enhance public safety infrastructure, including public safety communications equipment. Planners must consider NIMS in all planning to protect critical public safety infrastructure. The NIMS Integration Center (NIC) will publish compliance protocols for determining whether entities have adopted the aspects of the NIMS that are in place by October 1, 2004. It will develop and facilitate national standards for NIMS education and training, first responder communications and equipment, typing of resources, qualification and credentialing of incident management and responder personnel, and standardization of equipment maintenance and resources.

Appendix A
The FCC and Homeland Security

The Homeland Security mission of the FCC is to evaluate and strengthen measures for protecting the Nation's communications infrastructure; facilitate rapid restoration of that infrastructure in the event of disruption; and develop policies that promote access to effective communications services by public safety, public health, and other emergency personnel in emergency situations.[18]

Chairman Michael K. Powell serves as Defense Commissioner for the FCC. The Defense Commissioner directs the homeland security, national security and emergency preparedness, and defense activities of the Commission and is responsible for keeping the Commission informed of significant developments in the field of homeland security, emergency preparedness, defense, and any related activities that involve formulation or revision of Commission policy in any area of responsibility of the Commission. He represents the Commission in homeland security, national security and emergency preparedness, and defense matters; acts as the Homeland Security and Defense Coordinator in representations with other agencies with respect to planning for the continuity of the essential functions of the Commission under emergency conditions; serves as the principal point of contact on all matters pertaining to the Department of Homeland Security; is authorized to take such measures as will assure continuity of the FCC's functions with a minimum of interruption. The Chief of the Enforcement Bureau, (David H. Solomon) acts as Alternate Homeland Security and Defense Coordinator.

In July 2003, the FCC created the Office of Homeland Security (OHS) within the Enforcement Bureau. OHS assists the Chief of the Enforcement Bureau in his support of the Defense Commissioner, oversees rulemaking proceedings relating to the Emergency Alert System and operates the Communication and Crisis Management Center (CCMC). OHS also supports the Homeland Security Policy Council (HSPC) and other FCC Bureaus in achieving the objectives established in the Homeland Security portion of the Commission's Strategic Plan. OHS provides intra- and inter-agency coordination on all matters concerning homeland security, National Security/Emergency Preparedness (NS/EP), public warning and continuity of government. The Director of OHS is James Dailey; the Deputy Director is Gregory M. Cooke; the Assistant Director is Dan Emrick. Within OHS, the CCMC provides a 24-hour-a-day, seven-day-a-week central communications point of contact and crisis management and emergency response center for the agency, including handling a wide variety of incoming and outgoing

[18] See http://www.fcc.gov/homeland/#action_plan. The FCC's strategic goal for Homeland Security is to provide leadership in evaluating and strengthening the Nation's communications infrastructure, in ensuring rapid restoration of that infrastructure in the event of disruption, and in ensuring that essential public health and safety personnel have effective communications services available to them in emergency situations. To fully and effectively carry out its role in promoting homeland security, network protection, interoperability, redundancy, and reliability, the FCC established the following objectives: (1) Evaluate and strengthen measures for protecting the Nation's communications infrastructure; (2) Facilitate rapid restoration of the U.S. communications infrastructure and facilities after disruption by a threat or attack; and (3) Develop policies that promote access to effective communications services by public safety, public health, and other emergency and defense personnel in emergency situations. *See* http://www.fcc.gov/homeland.

secure and non-secure national and international communications by telephone, facsimile, and radio circuits, and U.S. Coast Guard search and rescue communications circuits. The CCMC Director is David Prescott.

The HSPC is comprised of senior staff from each of the Commission's Bureaus and is directed by the Chief of Staff for the Commission. The mission of the HSPC is to assist the FCC in: evaluating and strengthening measures for protecting communications services; ensuring rapid restoration of communications services and facilities that have been disrupted as the result of threats to, or actions against the Nation's homeland security; ensuring that public safety, health and other emergency and defense personnel have effective communications available to them to assist the public as needed; and fostering the implementation of new technologies that promote homeland security.

The HSPC is organized as follows: Director, Bryan Tramont; Deputy Dirctor Linda Blair; Special Counsel Peter Tenhula; Senior Advisor, Jim Dailey. Members include: Jeff Carlisle(Wireline Competition Bureau); Kris Monteith (Consumer and Governmental Affairs) Bureau; Linda Haller (International Bureau); Jeff Goldthorp (Office of Engineering and Technology); Jane Mago (Office of Strategic Planning & Policy Analysis); Linda Blair (Enforcement Bureau); Barbara Kreisman (Media Bureau); Catherine Seidel (Wireless Telecommunications Bureau); Sue Steiman (Office of General Counsel); Paul Jackson (Office of Legislative Affairs); Bill Spencer (Office of Managing Director); and Meribeth McCarrick (Office of Media Relations).

On July 10, 2003, the Commission announced its Homeland Security Action Plan. The Plan defines the Commission's homeland security goals as well as the approach it will take to achieve these goals. The Plan relies heavily on partnerships with other government entities, industry, and citizen groups. The Action Plan announced the goal to work together with tribal organizations and leaders and other relevant federal government agencies develop a plan that tribes can use to assist in protecting communications infrastructure.

Appendix B

Department of Homeland Security

The National Strategy for Homeland Security and the Homeland Security Act of 2002 served to mobilize and organize our nation to secure the homeland from terrorist attacks. A primary reason for the establishment of the CHS was to provide the unifying core for the vast national network of organizations and institutions involved in efforts to secure our nation.

In the event of a terrorist attack, natural disaster, or other large scale emergency, DHS assumes primary responsibility for ensuring that emergency response professionals are prepared for any situation. This entails providing a coordinated, comprehensive Federal response to any large scale crisis and mounting recovery efforts.

DHS is organized into several directorates: Information Analysis and Infrastructure Protection; Border and Transportation Security; Emergency Preparedness and Response; Science and Technology; and Management. The Information Analysis and Infrastructure Protection Directorate (IAIP) is responsible for critical infrastructure protection. State, Local, and private entities have one primary contact to coordinate protection activities within the Federal government, including vulnerabilities assessments, strategic planning efforts, and exercises. In addition, the IAIP team is responsible for coordination of planning and provision of National Security and Emergency Preparedness (NS/EP) communications for the Federal government. IAIP is the focal point for intelligence analysis, infrastructure protection operations, and information sharing. IAIP merges the capability to identify and assess a broad range of intelligence and information concerning threats, map that information against the nation's critical infrastructures, issue warning, and take appropriate preventative and protective action. IAIP has integrated the functions of five Federal government entities into the new IAIP organizational structure (the Critical Infrastructure Assurance Office, the National Communications System (NCS), the Federal Computer Incident Response Center, the National Infrastructure Protection Center, and the Office of Energy Assurance), and has hired an impressive array of talent from the Federal government, State government, and the private sector.

IAIP is comprised of two primary components: the Office of Information Analysis and the Office of Infrastructure Protection. The Office of Infrastructure Protection, in partnership with the Office of Information Analysis, Federal, State, Local, private and international entities protects America's critical infrastructures from both a physical and cyber perspective. The Office is responsible for identifying critical infrastructure and national assets; identifying and assessing vulnerabilities; normalizing analyzing and prioritizing assets and critical infrastructures; implementing protective programs in coordination with State, Local, Federal and Tribal entities; and measuring the effectiveness of its actions. The Office of Infrastructure Protection is organized into several entities: Strategic Partnerships Office; Plans and Program Office; National Cyber Security Division; Protective Security Division; National Communications System; and the Infrastructure Coordination Division.

The National Communications System (NCS),[19] now part of DHS, consists of 23 Federal member departments and agencies and is responsible for ensuring the availability of a viable national security and emergency preparedness communications system during times of national emergency and natural disasters. The NCS provides priority telecommunications services to the NS/EP community, which includes Federal government agencies, State, Local and Tribal governments, and certain private industries. These services are provided through NCS-administered programs and provide priority treatment in the public telecommunications network for those with NS/EP missions, ensuring their telecommunications capabilities in support of critical NS/EP functions. Key programs include the Government Emergency Telecommunications Service (GETS), which provides for priority access and transport in the local and long distance segments of the public network; the Telecommunications Service Priority (TSP) program, which enables the priority provisioning and restoration of critical telecommunications services for NS/EP users; the Telecommunications Electric Service Priority (TESP) program, which promotes (on a voluntary basis) the inclusion of critical telecommunications facilities in electric service providers priority restoration plans; the Wireless Priority Service (WPS), which provides priority cellular network access; and the Shared Resources (SHARES) program, which provides a single, interagency emergency message handling system by bringing together existing HF radio resources of Federal, State, Tribal and industry organizations.

The Protected Critical Infrastructure Information (PCII) Program[20] went into operation February 20, 2004. The PCII Program exempts from disclosure to the general public critical infrastructure information provided to DHS. The PCII Program Office is part of the DHS's Information Analysis and Infrastructure Protection (IAIP) Directorate. It is responsible for receiving submissions, determining if the information qualifies for protection and, if validated, sharing it with authorized entities for use as specified in the CII Act. Non-Disclosure Agreements (NDA) may need to be executed between Tribal entities and industry and/or other government bodies in order to provide a framework for controlling the distribution of proprietary information.

The National Coordinating Center Telecommunications Infrastructure Information Sharing and Analysis Center (NCC Telecom ISAC)[21] is the joint telecommunications industry/Federal Government operation established by the NCS to assist in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services or facilities. The NCC Telecom ISAC operates much like the interconnected and interdependent network systems that make up the telecommunications industry. The telecommunications infrastructure is the framework of interdependent telecommunication networks and systems, including both physical and software components, by which the telecommunications industry conducts, transmits, or receives information of any nature, by wire, radio, optical, or other electromagnetic systems. Representatives from all segments of the telecommunications sector work together with government to help protect the telecommunications infrastructure from hazards, ranging from cable cuts to natural disasters to information network attacks and terrorist attacks. The

[19] *See* http://www.ncs.gov.
[20] *See* www.DHS.gov/pcii.
[21] *See* http://www.ncs.gov/ncc_text/main-p.html.

members feed information and requests into the 24x7 Watch and Analysis Operation, which manages the Telecom ISAC information sharing process and provides the central analysis function for the ISAC. For the NCC ISAC, most critical infrastructure protection is now considered to be National Security and Emergency Preparedness (NS/EP) communications and issues range from assessing the aftermath of a hurricane to determining the source of a cyber attack. For example, August 14, 2003 a massive power outage affected large parts of the northeastern United States and eastern Canada creating the largest blackout in North American history, affecting an estimated 50 million people and covering an area of approximately 9,300 square miles. It also affected 100 power plants, of which 22 were nuclear power plants, and several critical infrastructures, including telecommunications, banking and finance, energy, and transportation. The NCC Telecom ISAC, the Federal Emergency Management Agency (FEMA), and Department of Transportation (DOT) coordinated the supply of fuel and generators to the affected areas to ensure that communications systems remained online. The NCC Telecom ISAC also coordinated with Canada's Office of Critical Infrastructure Protection and Emergency Preparedness, and with the Electricity Sector ISAC.

FEMA is part of the DHS's Emergency Preparedness and Response Directorate. On March 1, 2003, FEMA became part of the U.S. Department of Homeland Security. FEMA's mission is to lead the effort to prepare the nation for all hazards and effectively manage federal response and recovery efforts following any national incident. FEMA also initiates proactive mitigation activities, trains first responders, and manages Citizen Corps, the National Flood Insurance Program, and the U.S. Fire Administration. FEMA has more than 2,600 full time employees. They work at FEMA headquarters in Washington D.C., at regional and area offices across the country, the Mount Weather Emergency Operations Center, and the National Emergency Training Center in Emmitsburg, Maryland. FEMA also has nearly 4,000 standby disaster assistance employees who are available for deployment after disasters. Often FEMA works in partnership with other organizations that are part of the nation's emergency management system.

Homeland Security Information Network Initiative- On February 24, 2004, DHS, as a part of its Homeland Security Information Network Initiative, expanded its computer-based counterterrorism network to all 50 states, five territories, Washington, D.C., and 50 other major urban areas.[22] This communications system, designed to strengthen the two way flow of threat information and with a mission to prevent terrorist attacks, will deliver real-time interactive connectivity among state and local partners and with the DHS Homeland Security Operations Center (HSOC) through the Joint Regional Information Exchange System (JRIES). Each new area's Homeland Security Advisor will receive software licenses, technology, and training to participate in the information sharing and situational awareness. The broadened JRIES community will include state Homeland Security Advisors, Adjutant Generals (National Guard), Emergency Operations Centers, and local emergency services. Priorities of this network are detecting threats to infrastructure, locating attack targets, and mapping suspicious activity by suspected terrorists. One of the principal JRIES counterterrorism functions will be to exchange information and facilitate the analysis of an activity believed related to terrorism.

[22] *See* http://www.dhs.gov/dhspublic/display?theme=35&content=3348.

DHS Working Level Offices with respect to Communications Issues, including Public Safety Communications

DHS Office of State and Local Government Coordination – This office is responsible for coordination with State and Local First Responders, Emergency services and Governments. It is the primary point-of-contact (POC) within DHS for exchanging information with State, Local, Territorial, and Tribal homeland security personnel. It is responsible for identifying homeland security-related activities, Best Practices, and processes.

Homeland Security Funding Task Force - On March 15, 2004, DHS announced a Homeland Security Funding Task Force composed of State, County, City, and Tribal representatives to examine the funding process and ensure that DHS funds move quickly to local first responders. The Task Force will identify State and Local funding solutions that work effectively and can be extended to situations where there are impediments to the efficient and effective distribution of State and Local homeland security funds. Governor Mitt Romney of Massachusetts is Chair and Mayor Donald L. Plusquellic of Akron, Ohio is vice chair. The Tribal representative to the Task Force is Arlen P. Quetawki, Sr., Governor, Zuni Tribe, Office of the Governor, Zuni, New Mexico.

DHS SAFECOM Program Office – SAFECOM was established in the spring of 2002 to address the wireless communication needs of public safety organizations. The SAFECOM Program Office is part of the IAIP Directorate. SAFECOM serves as the umbrella program within the Federal government to help Local, Tribal, State and Federal public safety agencies to improve public safety response through more effective and efficient interoperable wireless communications. SAFECOM is working with existing Federal communications initiatives and key public safety stakeholders to address the need to develop better technologies and processes for the cross-jurisdictional and cross-disciplinary coordination of existing and future communications systems. SAFECOM@dhs.gov.

Appendix C

Selected Web Sites: National Strategy, DHS, NRIC Best Practices & Sample Emergency Response Plans

Executive Office of the President

National Strategy for Homeland Security
http://www.whitehouse.gov/homeland/book/

National Strategy for the Protection of Critical Infrastructures and Key Assets
http://www.whitehouse.gov/news/releases/2003/02/20030214-12.html.

The National Strategy to Secure Cyberspace
http://www.whitehouse.gov/pcipb/

Management of Domestic Incidents, HSPD - 5
http://www.fas.org/irp/offdocs/nspd/hspd-5.html

Critical Infrastructure identification, Prioritization and Protection, HSPD - 7
http://www.fas.org/irp/offdocs/nspd/hspd-7.html

National Preparedness, HSPD - 8
http://www.fas.org/irp/offdocs/nspd/hspd-8.html

Department of Homeland Security

DHS Home Page
http://www.dhs.gov

DHS Organization
http://www.dhs.gov/dhspublic/theme_home1.jsp

National Communications System (NCS)
http://www.ncs.gov

National Coordinating Center Telecommunications Infrastructure Information Sharing and Analysis Center (NCC Telecom ISAC)
http://www.ncs.gov/ncc_text/main-p.html

Applying for and Receiving Grants and Funds from DHS
http://www.dhs.gov/dhspublic/display?theme=38
http://www.dhs.gov/dhspublic/display?theme=18

National Information Management System (NIMS)
http://www.dhs.gov/dhspublic/display?theme=15&content=3254

Interim National Response Plan (INRP)
http://www.dhs.gov/interweb/assetlibrary/Initial_NRP_100903.pdf
http://www.dhs.gov/dhspublic/display?theme=43&content=1935&print=true
http://www.dhs.gov/dhspublic/display?theme=43&content=1936&print=true

Homeland Security Information Network
http://www.dhs.gov/dhspublic/display?theme=35&content=3348.

Emergency and Disaster Planning and Preparation
http://www.dhs.gov/dhspublic/display?theme=14

National Security Emergencies - Terrorism
http://www.dhs.gov/dhspublic/display?theme=14&content=446

SAFECOM - http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0339.xml;
http://www.fcw.com/geb/articles/2004/0412/web-safecom-04-16-04.asp

The Office of State and Local Government Coordination is the point of contact to facilitate and coordinate DHS programs that impact state, local, territorial and tribal governments.
http://www.dhs.gov/dhspublic/display?theme=9&content=3400

Response & Recovery to Emergencies and Disasters
http://www.dhs.gov/dhspublic/display?theme=15&content=23

Preparedness
http://www.fema.gov/preparedness

FCC

http://www.fcc.gov/homeland

http://www.fcc.gov/homeland/#action_plan

NRIC

NRIC http://www.nric.org.html

NRIC Focus Group 1: Homeland Security Subcommittee Reports and Recommendations: 1.A – Physical Security; 1.B: Cyber Security; 1.C: Public Safety; and 1.D: Disaster Recovery and Mutual Aid - http://www.nric.org/fg/nricvifg.html

NRIC VI Physical Security Final Report and Best Practices
http://www.nric.org/fg/nricvifg.html

NRIC Best Practices - http://www.bell-labs.com/cgi-user/krauscher/bestp.pl

Sample Emergency Response Plans

The Tribal Capability Assessment for Readiness (CAR) is a self-assessment instrument that states, local jurisdictions and tribal governments use to identify the strengths and weaknesses in their emergency management programs.
http://www.fema.gov/preparedness/slt_readiness.shtm

Sample Plan, Colville Reservation Comprehensive Emergency Management Plan
http://www.colvilletribes.com/CEMP.pdf

Sample Plan, Arizona Emergency Response & Recovery Plan
http://www.dem.state.az.us/serrp/serrp.htm

Sample Plan, Washington State Military Department
http://www.emd.wa.gov/5-prep/prgms/serc/serc-plans/01-lepc-guide-toc.htm