

**THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE**



***NSTAC Report to the President on
Communications Resiliency***

April 19, 2011

TABLE OF CONTENTS

EXECUTIVE SUMMARY ES-1

1.0 INTRODUCTION..... 1

 1.1 Background and Charge 1

 1.2 Approach 1

 1.3 Assumptions 2

 1.4 The Modern Communications Network..... 3

2.0 FUTURE STATE OF THE NETWORK: 2015 3

 2.1 General Vision..... 4

 2.2 Key Communications Trends Impacting Network 2015..... 4

 2.3 The Network 2015 Challenges 8

 2.4 Internet Protocol-Based Services 10

 2.5 Public Safety Communications in Network 2015 12

 2.6 Service Provider Best Practices..... 14

3.0 STRESSING THE NETWORK 15

 3.1 Scenario 1: Multiple Terrorist Attacks in the National Capital Region 15

 3.2 Scenario 2: Catastrophic Earthquake in San Francisco..... 21

 3.3 Scenario 3: Cyber Attack 29

 3.4 Scenario 4: Massive Internet Disruptions 34

4.0 RECOMMENDATIONS..... 39

APPENDIX A: PARTICIPANT LIST A-1

APPENDIX B: ACRONYMS..... B-1

APPENDIX C: GLOSSARY C-1

APPENDIX D: CONGESTION..... D-1

**APPENDIX E: NATIONAL CYBERSECURITY AND COMMUNICATIONS
INTEGRATION CENTER AND NATIONAL CYBER INCIDENT RESPONSE PLAN.....
..... E-1**

**APPENDIX F: FEDERAL AND STATE RESPONSE STRUCTURES (RELEVANT TO
SCENARIO 2).....F-1**

**APPENDIX G: TECHNICAL DISCUSSION OF THE ROUTING AND ADDRESSING
CONCEPTS PRESENTED IN SCENARIO 4..... G-1**

APPENDIX H: BIBLIOGRAPHY H-1

EXECUTIVE SUMMARY

Natural disasters, terrorist attacks, or other large-scale incidents can have devastating impacts on the Nation's public and private communications networks and the critical functions they support. The potential for local and national security consequences resulting from a cyber attack or system corruption can be equally devastating to critical infrastructure and key resources (CIKR). The Federal Government manages or participates in a number of initiatives focused on improving the interoperability and resilience¹ of present-day communications. While it would be near impossible to develop and maintain networks that are invulnerable to disruption, ensuring long-term communications resilience requires that the Government understand future systems and the future technology landscape when investing in and planning for durable, survivable communications for Government officials, first responders, and CIKR owners and operators.

In January 2010, the Executive Office of the President's (EOP) National Security Staff requested that the President's National Security Telecommunications Advisory Committee (NSTAC) examine the Nation's resiliency in ensuring essential levels of operability for an array of communications services, ranging from simple voice communications to integrated voice, data, and video applications. Specifically, the EOP charged the NSTAC with providing recommendations on "options for investments or actions" the Government could take to enhance the survivability or availability of communications for emergency response personnel, CIKR owners and operators, and State and local authorities during a time of natural disaster, man-made attack, or crisis.

The NSS also requested that the NSTAC undertake its study on networks expected to be in place five or ten years in the future and examine how these future networks could survive under different crisis scenarios in an attempt to identify the significant trends and transformations that will drive future patterns in usage, service provisioning, technology development, network architecture, and security. To do so, the NSTAC discussed and projected changes to the communications network between 2010 and 2015 and arrived at a common understanding of the anticipated general state of the communications network in 2015.

The NSTAC reasoned that the evolution of the communications network will be driven by changes in technology, applications, content, devices, and increased requirements for capacity, bandwidth, and spectrum. By 2015, the core network will have largely completed the transition to Internet Protocol (IP) technology. Nevertheless, the NSTAC projected that users at the edge of the network may experience a longer transition period to IP-based services, particularly for voice services, as users will retain older voice technologies due to sunk costs. Manufacturers will also leverage existing equipment by simply augmenting this equipment and upgrading its security. Despite the continued existence of circuit-switched technologies in 2015, the network will evolve and interoperate at a rapid pace to support the next generation of services, increased volume of network traffic, and current and emerging technologies.

¹ Presidential Policy Directive-8: *National Preparedness* defines resilience as the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies.

To assist in identifying specific areas of resiliency in which to focus, the EOP provided the NSTAC with four scenarios: multiple terrorist events in the National Capital Region; a catastrophic earthquake in the San Francisco Bay Area; a cyber attack; and massive Internet disruptions. As the NSTAC and subject matter experts addressed each of the scenarios, participants highlighted areas of concern regarding communications resilience, as well as possible options for Government engagement to improve existing programs or invest in emerging technologies or initiatives. The NSTAC arrived at an understanding of the high-level impacts of each scenario, came to consensus upon the key findings with respect to resilience, and crafted scenario-specific recommendations to the President.

The NSTAC proposes the following recommendations, organized by scenario. The NSTAC deems those recommendations denoted by a symbol are of highest priority for the President. The NSTAC recommends the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*:

Scenario 1: Multiple Terrorist Attacks in the National Capital Region

- ❖ Request that Congress fund the Department of Homeland Security's (DHS) priority services efforts to continue industry and Government collaboration and to ensure that advanced national security and emergency preparedness (NS/EP) communication services are operational when needed.
- Encourage DHS to file comments with the Federal Communications Commission (FCC) in its appropriate public safety broadband dockets. In its filed comments, DHS should recommend that the FCC continue working closely with industry as it builds the nationwide interoperable public safety mobile broadband network, as recommended in the FCC's *National Broadband Plan*.
- Encourage DHS to petition the FCC to issue a declaratory ruling to confirm that network service providers may lawfully offer IP-based priority access services to NS/EP authorized users.
- Encourage Congress to continue funding DHS' Science and Technology Directorate to pursue interoperability solutions for emergency responders and ensure that DHS allocates the funds to interoperability programs.
- ❖ Direct DHS to build future alerting capabilities that consider all potential multi-platform technologies to ensure that the public can receive timely and accurate alerts, warnings, and critical information about emergencies regardless of the communications technologies used.
- ❖ To accelerate efforts to fulfill DHS' National Cybersecurity and Communications Integration Center (NCCIC) mission and, to ensure that this significant mission is fully operational by the 2015 timeframe, direct DHS to accomplish the following as soon as possible:

- Leverage the success of the existing NCCIC incident response mechanism by ensuring sufficient funding levels are dedicated to the mission; and
- Direct the rapid expansion of personnel resources, including training, to guarantee that the cyber and communications incident response mechanisms are absolutely viable and fully mission-capable by 2015.

Scenario 2: Catastrophic Earthquake in California

- Direct DHS and other appropriate departments and agencies to support collaboration between State and local government and industry to determine the most effective and appropriate mechanisms for restoring critical communications services.
- ❖ Direct the Department of Defense (DOD) and other appropriate departments and agencies to enhance the utility of and reliance on satellite systems to provide alternate communications when terrestrial-based communications infrastructure is impaired.
- Direct the Federal Emergency Management Agency (FEMA), in coordination with other DHS agencies and DOD, to identify, support, and integrate relevant tactical emergency communications support capabilities across the Federal Government.

Scenario 3: Cyber Attacks

- ❖ Direct DHS to explore the viability of developing a separate “out-of-band” data network to support communications between carriers, Internet service providers (ISP), vendors, and additional CIKR owners and operators during a severe cyber incident that renders the public Internet unusable.
- Charge DHS with continuing to develop and test the *National Cyber Incident Response Plan* and proceeding to implement the additional stages of the NCCIC, which will include greater private sector involvement.
- ❖ Direct that the appropriate Government certification and accreditation processes, such as the Defense Federal Acquisition Regulations System and the Defense Information Assurance Certification and Accreditation Process, verify the existence of sufficient vendor diversity both when acquiring equipment and when operating and installing a network.

Scenario 4: Massive Internet Disruptions

- ❖ As recommended under Scenario 3, direct DHS to explore the viability of developing a separate data network to support communications between carriers, ISPs, vendors, and

additional CIKR owners and operators during a severe cyber incident that renders the public Internet unusable.

- ❖ Direct the Office of Science and Technology Policy, in coordination with DOD, DHS, and other appropriate departments and agencies, to establish a single, high-level forum for ongoing technical and policy dialogue between Government and key industry service providers, focused on issues of potentially strategic consequence in the foreseeable future timeframe.
- Direct DHS to institute an expanded program of national-level exercises that include Government agencies and infrastructure providers.
- ❖ Encourage the Office of Management and Budget to continue funding for departments' and agencies' development of security enhancements within the core infrastructure, such as Internet number resource certification (e.g., Resource Public Key Infrastructure).

1.0 INTRODUCTION

Natural disasters, terrorist attacks, or other large-scale incidents can have devastating impacts on the Nation's public and private communications networks and the critical functions they support. The potential for local and national security consequences resulting from a cyber attack or system corruption can be equally devastating to critical infrastructure and key resources (CIKR). The Federal Government manages or participates in a number of initiatives focused on improving the interoperability and resilience² of present-day communications. While it would be near impossible to develop and maintain networks that are invulnerable to disruption, ensuring long-term communications resilience requires that the Government understand future systems and the future technology landscape when investing in and planning for durable, survivable communications for Government officials, first responders, and the general population.

1.1 Background and Charge

In January 2010, the Executive Office of the President's (EOP) National Security Staff (NSS) requested that the President's National Security Telecommunications Advisory Committee (NSTAC) examine the Nation's resiliency in ensuring essential levels of operability for an array of communications services, ranging from simple voice communications to integrated voice, data, and video applications. Specifically, the NSS charged the NSTAC with providing recommendations on "options for investments or actions" the Government could take to enhance the survivability or availability of communications for emergency response personnel, CIKR owners and operators, and State and local authorities during a time of natural disaster, man-made attack, or crisis.

To further refine the tasking, the EOP requested that the NSTAC's effort focus on networks expected to be in place five or ten years in the future and examine how these future networks could survive under different local, regional, national, or multi-location crisis scenarios occurring in that future network environment. The EOP also asked the NSTAC to study the resilience of the network beginning immediately after an incident and extending through a 45-90 day timeframe and to determine how to restore the availability and connectivity of the surviving communications infrastructure within 0-90 days following an incident.

1.2 Approach

The EOP proposed seven principles as critical success factors by which the task force could examine the resiliency of the network, including:

- Redundancy (multiplicity, spares);
- Diversity (multiple approaches and suppliers);
- Agility (ability to shift);
- Adaptability (ability to adjust);

² Presidential Policy Directive-8: *National Preparedness* defines resilience as the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies.

- Prioritization (dedicated or shared resource);
- Geography (diversity, proximity); and
- Hardening (ability to withstand direct force).

The EOP also provided the task force with four specific scenarios designed to stress the future network to further refine the scope of the study. The scenarios concerned instances of multiple terrorist attacks in the National Capital Region (NCR); a catastrophic earthquake in the San Francisco Bay Area; a cyber attack; and massive Internet disruptions.³ Following receipt of the scenarios, the NSTAC engaged their companies' subject matter experts (SME) in discussions to evaluate each scenario individually. When holding the discussions with SMEs, the NSTAC posed four generic questions for each scenario to provide a uniform platform for data collection and analysis. The questions addressed the anticipated impacts of the scenario, the potential impacts on communications between technicians, and the actions that both industry and Government should take now to mitigate the possible impacts.

The NSTAC also agreed to project evolution and changes to the network only five years into the future rather than ten years. It determined that, given the rapid pace of change within today's network, five years would yield sufficient transformation and convergence to force a reevaluation of today's mechanisms and approaches to ensuring resiliency. Additionally, the NSTAC assumed that, by 2015, the network will have evolved to an almost entirely Internet Protocol (IP) packet-based structure and away from circuit switching, but will retain a fundamental architectural resemblance to today's network; today's trends will continue, but at a quickened pace.

1.3 Assumptions

Several characteristics of the NSTAC's approach to this effort were unique in comparison to previous NSTAC efforts. First, the NSTAC was challenged to establish a vision of the future network in which to address resilience. The NSTAC was also asked to analyze network resiliency in 2015 in the context of four distinct scenarios. The NSTAC recognizes that these unique aspects of its approach carry certain assumptions:

The future of the network is fundamentally uncertain. Future projections will always be predicated on subjective analyses and predictions that may not hold true. The NSTAC's specific technical assumptions are described in Section 2.0: "Future State of the Network: 2015". The NSTAC focused on the technical drivers of change in the future network rather than the policy drivers. Legislative, regulatory, and political change will occur alongside network evolution and may amplify or restrict some of the technological trends that this report identifies.

The majority of the findings are scenario-specific. The EOP developed specific scenarios that highlighted challenges to the resiliency of our Nation's communications infrastructure. Given the detail provided for each scenario, the report reflects specific impacts or mitigation activities unique to that particular incident, geographic region, or response actions. Thus, some findings

³ The scenarios provided in Section 3.0 are verbatim as received from the EOP.

are valid mainly in the context of the scenario discussed. Wherever possible, however, the NSTAC extrapolated scenario-specific findings to general findings for the 2015 environment.

The specific issues emphasized in the scenarios largely exclude other co-dependencies and externalities. Each of the four scenarios implicates adjacent equities and capabilities outside its immediate scope, such as the presumed continuous availability of electric power. However, the NSTAC's intent was to focus narrowly on the given scenarios in order to more clearly illuminate issues related to the four topics. Scenario 2 presents the only exception, as it specifically addresses the co-dependency of the communications and power sectors.

1.4 The Modern Communications Network

The modern communications network is a network of networks and encompasses both circuit switched and IP-based networks. The network includes but is distinct from today's Internet, which is defined as "a collective electronic network of computers and computer networks which are inter-connected throughout the world."⁴ Modern networks depend on three fundamental functions occurring in the core network:

- *Addressing*: specifying the destination of the message;
- *Routing*: specifying the path the message uses to arrive at its destination; and
- *Transport*: the physical medium that carries the message.

All communications-based applications and services, including telephone calls, email, text messages, Internet, chat, file transfers, and video, fundamentally depend on the networks to provide addressing, routing, and transport. Just as the driver of an automobile requires the destination address, knowledge of the route, and an actual road, communications delivery requires similar addressing, routing, and transport mechanisms.

This report details some of the technologies used to implement addressing (Domain Name System [DNS]), routing (Border Gateway Protocol [BGP]), and transport (glass and metallic cables, cellular towers, switches and routers) that are currently in use and expected to remain in use through 2015. Regardless of the specific technology, the principles of addressing, routing, and transport will remain constant.

2.0 FUTURE STATE OF THE NETWORK: 2015

The NSTAC's first priority was to arrive at a common understanding of the general state of the communications network in 2015. The goal was not to map the precise evolution of the network, but rather identify the significant trends and transformations that will drive future patterns in usage, service provisioning, technology development, network architecture, and security.

⁴ Perkins, Steven C. Perkins. "Internet Terminology and Definitions." Available at: <http://www.rci.rutgers.edu/~au/workshop/int-def.htm>

2.1 General Vision

Changes in technology, applications, content, devices, and increased requirements for capacity, bandwidth, and spectrum drive the evolution of the communications network. By 2015, the core network is largely expected to complete the transition to IP technology; in fact, most major carriers and Commercial Mobile Radio Service (CMRS) providers have already transitioned their networks to an IP Multimedia Subsystem (IMS) core environment. Manufacturers will also continue to leverage large volumes of existing equipment by simply augmenting this equipment and upgrading its security. These factors suggest that the network will undergo rapid transformation by 2015. Nevertheless, users at the edge of the network may experience a longer transition period to IP-based services, particularly for voice services, as users will retain older voice technologies due to sunk costs.

Despite the continued existence of circuit-switched voice technologies in 2015, the network will continue to evolve and operate at a rapid pace to support the next generation of services, increased volume of network traffic, and current and emerging technologies. The communications network in 2015 will emphasize core interoperability technology, access, applications, and security to offer a seamless end-user experience.

2.2 Key Communications Trends Impacting Network 2015

The NSTAC identified the following trends as the most significant drivers of network evolution and change approaching 2015.

- **Video and multimedia services:** High-definition video and multimedia services delivered via broadband and mobile phones will become standard in the future network. 2015 will see a dramatic increase in services, such as video streaming and digital television both in fixed connections and on mobile devices, driven by consumer demand. Faster wireless network connections will enable and encourage heightened mobile data usage, leading to exponential growth in mobile traffic worldwide. Cisco Systems, Inc., predicts that global mobile data traffic will increase 26-fold between 2010 and 2015. Mobile video traffic in particular will drive this growth, as video usage will at least double every two and a half years and will account for two-thirds of global mobile data traffic in 2015.⁵ Equipment manufacturers predict that mobile broadband subscribers, which numbered 600 million at the end of 2010, will increase to as many as five billion by 2016.⁶ Figure 1, below, depicts predictions for increased mobile data usage approaching 2015. Although mobile data traffic will grow rapidly by 2015, it will remain a small percentage of overall data traffic given the spectrum limitations inherent in wireless infrastructure.

⁵ Cisco Systems, Inc. Cisco Visual Network Index. June 2010.

⁶ O'Brien, Kevin. *New York Times*. "Data Seen Overwhelming Cell Networks." February 16, 2011.

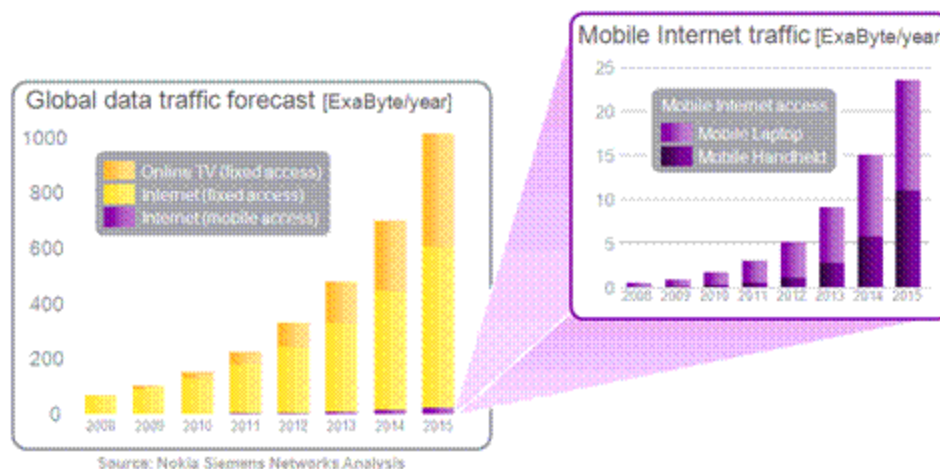


Figure 1 Data Usage Approaching 2015

- **Applications:** Application stores, including Android, Apple iTunes/iPhone App Store, BlackBerry App World, Amazon, Baidu, and others, will become a delivery mechanism for software to mobile communications devices. These applications stores and the information accessibility they enable are primarily cloud-based. As applications usage rises, technical developments at the application level—including customer self provisioning and social networking applications—will become more prevalent. The CMRS applications stores will provide additional protection by offering a guarantee for security, activation, provisioning, and billing. Social media and social networking applications and games will continue to dominate online activity.
- **Broadband and Fourth Generation (4G) Technology:** Higher-speed broadband mechanisms will be the predominant way users acquire applications and services. Fixed (wired) broadband will be the prevalent delivery mechanism, but mobile (wireless) broadband, such as Long-Term Evolution (LTE) and Worldwide Interoperability for Microwave Access (WiMax), will expand as the demand for broadband increases. Currently, LTE is globally adopted by 180 operators in 70 countries, and WiMax is deployed in 146 countries.^{7,8} The continued push to universalize broadband access nationwide may also shift the landscape in service provision, as broadband will reach previously un-served and underserved locations. Accompanying the globalization of broadband access, 4G wireless technologies will become prevalent by 2015.
- **Devices and equipment:** As 4G technology is deployed, new mobile devices will emerge to meet demand and device cost will decrease. The lowered cost may drive growth in consumers' purchases of wireless devices that they can customize to their desired specifications by installing selected applications and services. Enhancements and new developments in machine-to-machine technology and consumer electronics, such as

⁷ Global Mobile Suppliers Association. "GSA Confirms LTE as the Fastest Developing System in the History of Mobile Telecommunications, 180 Operators Now Investing," 12 January 2011. Available at: http://www.gsacom.com/news/gsa_315.php4.

⁸ WiMax Forum. Press Release. "WiMax Deployments Go Global with 519 in 146 Countries." Available at: www.wimaxforum.org/news/2030.

smartphones and Internet-enabled televisions, home appliances, medical devices, and automobiles, will continue to become more common. Currently available femtocell technology may also become more widely deployed. Femtocells are small wireless devices that can provide wireless coverage over a particular area, such as a building or city block, to relieve congestion and free up capacity on commercial networks.⁹

- **Dispersed but connected workforce:** Workforce mobility will expand with more of the workforce working remotely through telework arrangements. As a result, Internet traffic and related service delivery will continue to shift from traditional business delivery mechanisms to residential customers.
- **Service provider consolidation:** Service providers will consolidate network and transmission infrastructure equipment to facilitate more optimized management and operation of services, reduce costs, and keep pace with workforce dispersal. This consolidation will allow for greater geographic diversity of services, as a wider array of services will be available in different markets, while still employing a common infrastructure and network substrate.
- **Satellites and Global Positioning Systems (GPS):** Applications and devices in 2015 will become more reliant on satellites and GPS as more location-based services are deployed and an increasing number of devices integrate an embedded GPS capability. Evolution in satellite technology will continue expanding satellites' capacity to carry voice and data services, further enabling satellites to serve as an alternative communications system, albeit with more limited application than terrestrial systems.¹⁰ Satellite networks can be configured to provide nationwide point-to-point, line-of-sight connectivity without requiring an Internet connection, allowing satellites to provide an alternative closed IP-based network isolated from and independent of today's public Internet.
- **Identity management (IdM):** Emergent policies may have an impact in this area by 2015.¹¹ Current Government and private sector IdM systems, however, are numerous and stove-piped, causing duplicative, inefficient, and uncoordinated IdM efforts. Private sector owners and operators of the Nation's information and communications infrastructure, along with Government, have a vested interest in exploring potential solutions to issues and affects related to identity fraud; such solutions can reduce the frequency and impact of attacks on network infrastructure and services, especially during emergencies.¹²
- **Cloud computing:** Data storage usage in the cloud will increase significantly approaching 2015, as cost reduction measures will promote data center consolidations

⁹ Legislation introduced in late 2010 would require the installation of femtocells in all Federal buildings. See S.3995, "*The Federal Wi-Net Act*".

¹⁰ For previous NSTAC findings on GPS and satellites, see the *NSTAC Report to the President on Commercial Satellite Communications Mission Assurance*, November 2009.

¹¹ The EOP's draft *National Strategy for Trusted Identities in Cyberspace* (NSTIC), released in summer 2010, seeks to enhance the security, functionality, and interoperability of systems and processes used to assert identity online. The NSTAC submitted comments on the draft NSTIC, previously called the *National Strategy to Secure Online Transactions*, in May 2010 and June 2010.

¹² *NSTAC Identity Management Task Force Report*, May 2009. Page 11.

and drive increased enterprise usage. The Federal Government has also mandated that departments and agencies begin transitioning services to the cloud by the end of 2011.¹³ Figure 2 and Figure 3 illustrate the current evolution of cloud computing network architecture. Clouds will be:

- *Private*: Operated for a single organization and either managed by that organization or a third party;
- *Community*: Shared by several organizations and either managed by the organizations or by a third party;
- *Public*: Available to the general public or a large industry group and owned by an organization selling cloud services; or
- *Hybrid*: A composition of private, public, and/or community clouds, which operate separately but are linked by technology that allows for portability.¹⁴

“Thin” clients and custom application integration will drive cloud-based data services, with application stores reliant on cloud infrastructure and network services to store and deliver data to end users.

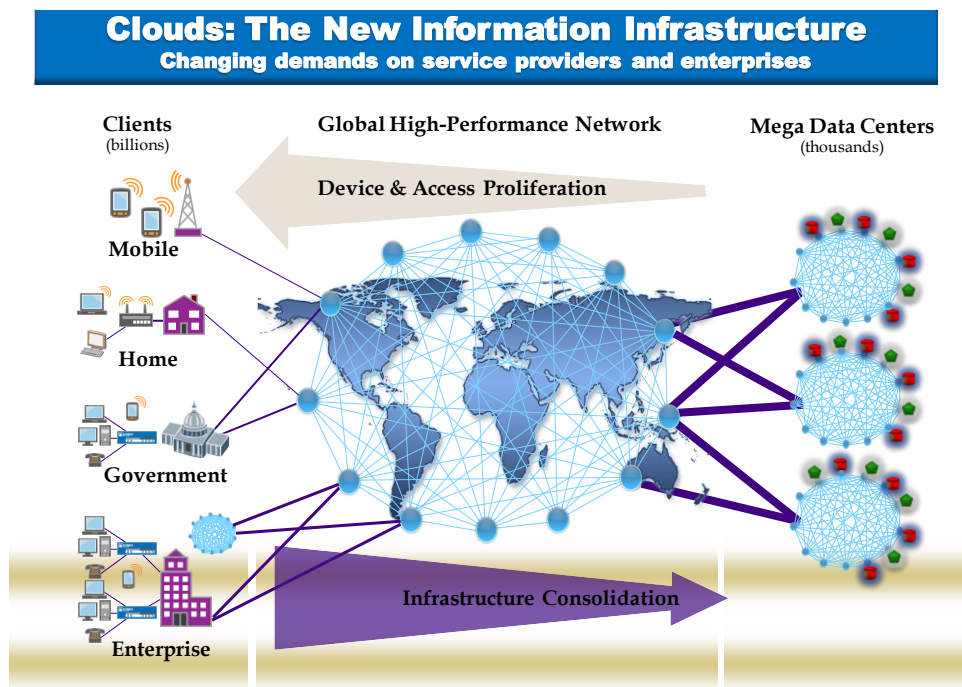


Figure 2 Cloud Architecture¹⁵

¹³ *InsideDefense*. “DSB to Study Cloud Computing, Mission Resilience,” February 9, 2011.

¹⁴ Mell, Peter and Grance, Tim. “The NIST Definition of Cloud Computing.” Version 15. October 7, 2009.

¹⁵ Source: *Juniper Networks*, 2010.

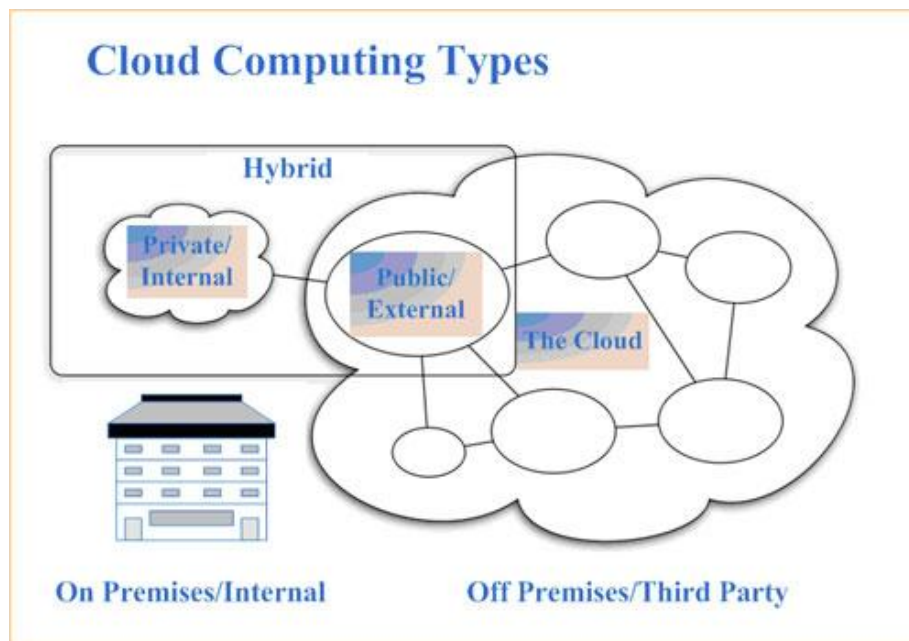


Figure 3 Private, Public, and Hybrid Clouds¹⁶

2.3 The Network 2015 Challenges

The NSTAC identified the following challenges as the most significant considerations in evaluating network resiliency in 2015.

- **Network complexity:** The growth in the network's features and capabilities by 2015 will lead to increased complexity. Greater automation will mitigate some of the complexity to the end user, but will not eliminate the difficulties of trouble-shooting or debugging network issues when they occur.
- **Bandwidth availability:** Ever-increasing bandwidth demands, particularly from the rapid growth in video services, will challenge service providers' delivery approach in 2015. Service providers will need to be particularly cognizant of the potential difficulty of sustaining bandwidth-intensive applications in a severely congested network situation.
- **Priority services:** Priority services such as Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) will remain a key means of ensuring that high-priority users can access the network during periods of congestion. In order for priority services to meet the needs of a wider user base in 2015, GETS and WPS will have to evolve to the future IP environment and retain sufficient funding and commitment from the appropriate Government agencies.
- **Spectrum availability:** The continued ability to use mobile broadband wireless devices and networks in 2015 can only be sustained if sufficient spectrum is made available to alleviate congestion and if bandwidth is provided for an ever-increasing set of wireless

¹⁶ Source: *IT Knowledge Portal*, available at: <http://www.itinfo.am/eng/cloud-computing>.

user applications. In its *National Broadband Plan*, the Federal Communications Commission (FCC) has a stated goal of making 500 megahertz (MHz) of spectrum available for broadband within 10 years, of which 300 MHz is to be made available for mobile use within five years.¹⁷ The Government will be challenged to meet these goals and establish aggressive timelines to satisfy rising broadband demands and ensure that allocated spectrum is sufficient. Some analysts predict that the FCC's spectrum objective is insufficient and the timeframe for freeing spectrum too long. Others observe increasing tensions between the FCC and television broadcasters over FCC-mandated spectrum re-allocation.¹⁸

- **Security for CMRS networks:** Wireless services and service providers will face a unique set of challenges and threats approaching 2015. Security for mobile devices will gain heightened importance; fast device release cycles, vulnerable technical architectures, increased connectivity options, inexperienced users, and the need for more personalization options will leave mobile devices and IP-based mobile communications vulnerable to a wide and growing range of threats. At the network level, operators will seek to control the impact of potential malware outbreaks at the gateway, which can spread quickly and infect large numbers of devices. The trend towards cross-platform viruses and criminally-motivated, for-profit malware, coupled with the success of feature-rich handsets, will pose critical challenges. CMRS networks will need to address security by placing proven content-screening technology at the gateway.
- **Cloud computing security:** The expansion of cloud computing is accompanied by continued security concerns and uncertainty around cloud regulation and standards. These factors will make enterprises reluctant to take full advantage of the cloud, hindering large-scale cloud adoption if concerns remain unresolved.¹⁹ In particular, the lack of interoperability standards for moving from one cloud to another and transferring workloads between cloud networks makes the adoption of a public or hybrid cloud challenging for many enterprises. Finally, the availability of the network and transaction-enabling services, such as DNS for remote access of cloud-based content, will become more critical to cloud deployment. Security threats to DNS infrastructure can equally impact cloud services.
- **Internet Protocol version 6 (IPv6) implementation:** In the near-term, IPv6 implementation may be hampered by the reluctance or inability of end users to adopt the new addressing protocol due to capital expenditures in non-IPv6 legacy equipment. Businesses will have to ensure that all network equipment and software is IPv6-enabled at the time of implementation. Although the technology is available, as of 2010, few equipment users at the network edge have begun to update their equipment. As discussed in section 2.4, the Internet in 2015 will continue to operate in an Internet Protocol version 4 (IPv4) and IPv6 "dual stack" mode. As handling of dual-stack traffic will occur

¹⁷ FCC's *National Broadband Plan*., p. xii.

¹⁸ *The Washington Post*. "TV Broadcasters Resist FCC Proposal to Surrender More Airwaves." January 19, 2011.

¹⁹ A recent study by Forrester Research found that 54 percent of companies surveyed reported data breaches in cloud-based services in 2010. Violino, Bob. *Network World*. "Study: Cloud Breaches Show Need For Stronger Authentication." January 18, 2011. Available at: <http://www.networkworld.com/news/2011/011811-study-cloud-breaches-show-need.html>.

mostly through software pending updates to hardware and firmware, any potential security vulnerabilities arising from the dual-stack mode have yet to be fully understood.

- **Evolving malware attacks:** As in the past, malware attacks and attack complexity will continue to grow and evolve in parallel with the network's evolution. The attacks will be conducted at different network levels and users will be subject to an increasing number of threats, including voice and text spam attacks, viruses, trojans, spyware, adware, third party infected applications, crimeware, and denial-of-service attacks.
- **Cybersecurity:** The IMS core network and its access points (local, long distance, international, wireless, cable, broadcast, and satellite) will face new risks due to the growing number of mobile device attack vectors and the increasing number of these devices on the future network. Highly sophisticated cyber attacks targeting these devices may cause network denial-of-service, resulting in system availability degradation at points least advantageous to recovery operations. Network security elements, such as end-to-end malware detection, are implemented in most IP-based networks today. But the range of security threats will broaden, infrastructure will evolve, and responsibility for security will become increasingly dispersed between service providers, third parties, and end users. As more third parties independently develop and sell services to end users, service providers will find it difficult to exert the same level of control over infrastructure and services traditionally in their domain.
- **Legacy equipment:** Current network architecture and equipment will remain in place in 2015, even as the network evolves and delivery mechanisms change. Many service providers will continue to support existing and legacy equipment, including many communications devices with embedded wireless capabilities used today, in order to take advantage of sunk capital costs. But some older equipment will be incompatible with newer equipment, services, and applications.
- **Workforce mobility:** As mobile devices allow the workforce to work remotely, changes in the geographic dispersal of the workforce will challenge service providers to reevaluate their overall service delivery approach. In general, service delivery will have to evolve to support a more mobile workforce, as access needs shift from businesses to residences and mobile consumers.
- **Physical security:** In a physical attack against the communications infrastructure, CIKR interdependencies and vulnerabilities would become readily apparent. Current vulnerabilities in areas such as power generation, transportation, and oil/gas distribution will continue to impact the resilience and redundancy of the network in 2015. In particular, the availability of power and/or restoration of power will dictate the rapidness and effectiveness of communications restoration efforts during a crisis. The increasing concentration of services and applications in different data centers may also increase vulnerability to physical attacks. Data security and access control will also be key challenges in the shift to cloud computing.

2.4 Internet Protocol-Based Services

In the 2015 network, most service and content delivery to the end user will be IP-based. Providers will increasingly deliver voice services through Voice over IP (VoIP) and data

communications will employ a common underlying IP network fabric. See Figure 4 for a depiction of the new network, separated into three layers: services and applications, the core, and access.

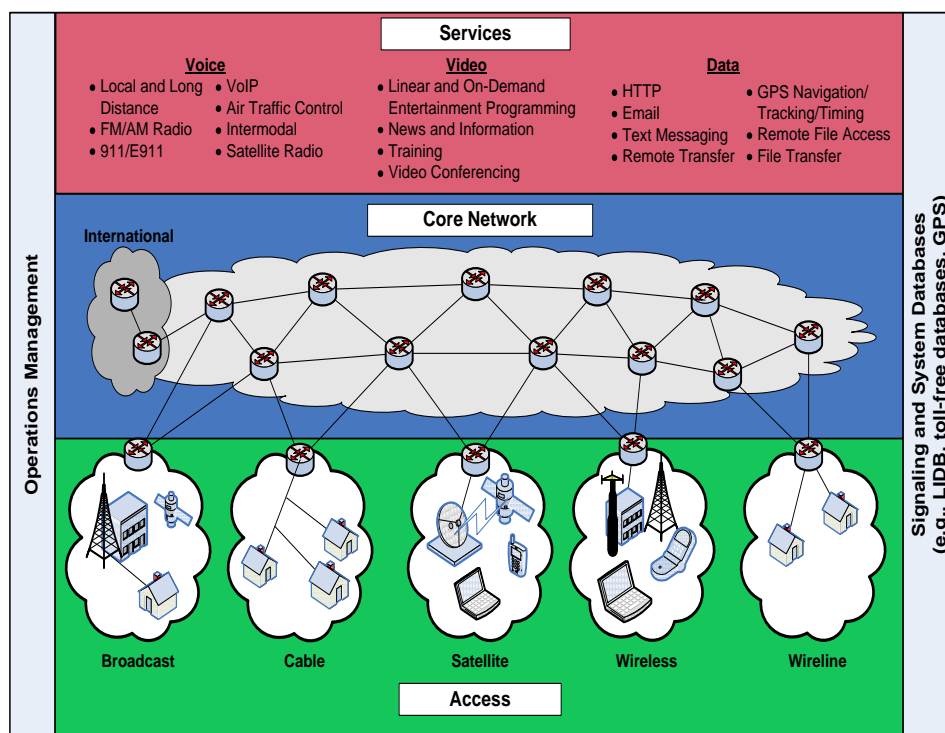


Figure 4 Communications Network Layers²⁰

The IP core will expand its transport capabilities and become more intelligent, with more network devices analyzing and applying security and routing policy based on information above the network layer. The rapid spread of multimedia applications and user-generated content in a mobile environment will compel efforts to make the network more autonomous and better equipped to support increased traffic flow. To keep pace with the increased volume and more complex network traffic, Internet access speeds will exceed 1 Gigabit per second (Gbps). Additional bandwidth will likely be allocated first to wireless transport for radio towers, followed by large enterprise organizations for their business applications and finally to large bandwidth consumer services to support technologies such as 3D television and telecommuting. In order to enable delivery of 1 Gbps service capacity, transport networks will require additional capacity. Efforts to enhance the efficiencies of network protocols to reduce overhead are also underway.²¹

IP will continue to operate on a multitude of lower-layer protocols in 2015. Physical and Link Layer protocols (e.g. Ethernet, Multi-Protocol Label Switching [MPLS], Asynchronous Transfer Mode [ATM], and Synchronous Optical Networking [SONET]) will continue to exist; however,

²⁰ Source: *NSTAC Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic*, November 2008.

²¹ As one example of such initiatives, Google is working on designs for a new protocol that it hopes will make Internet communications twice as fast as under current protocols. See Erica Naone, "The Slow-Motion Internet," *Technology Review*, Massachusetts Institute of Technology, March/April 2011.

changes at the application layer will occur at a significantly higher rate. The future IP environment will be divided between connection-oriented infrastructure, such as IMS and Session Initiation Protocol (SIP), and connectionless services, including traditional Internet data services. Network interoperability and new applications will continue to drive the demand for gateways, as well as multi-service and cross-services access systems and platforms, in order to meet the need for multi-protocol interoperability. Gateways will enable service providers to extend the reach of applications across multi-protocol networks, including signaling system 7 (SS7), IP, cable, and wireless, as well as IMS and SIP.

From 2009 to 2010, the networks began to deploy IPv6 in a dual stack manner that allows transitional co-existence with IPv4 for the foreseeable future. In February 2011, the Internet Assigned Numbers Authority (IANA) allocated the last of the IPv4 address blocks to the Regional Internet Registries (RIR), signaling the full depletion of the free pool of available IPv4 addresses.²² However, the full transition from IPv4 to IPv6 will be expensive and complicated, affect all Internet users, and require significant attention and effort in order to avoid service disruptions. The transition is expected to require several years to complete due to the existence of millions of legacy devices that are not upgradable to IPv6 and the need for all devices to continue communicating during the transition. For any given application, neither the server required for delivery nor its clients may be upgradable to IPv6. Therefore, network operators must make this application transparently available to IPv6 clients while simultaneously continuing to support IPv4 devices until they can be upgraded or replaced. This process will extend well past 2015.

As network servers and other elements are installed alongside or transitioned to IPv6, network operators use two principal methods to ensure continued access to services by client devices. Operators are installing Network Address Translation (NAT) Protocol capabilities that intermediate between IPv4-only client devices and IPv6 servers and are making non-upgradable IPv4 servers available to IPv6 clients. Newer network servers and client devices are increasingly being installed or upgraded to dual stack software that allows them to communicate directly with either IPv4 or IPv6 devices.

2.5 Public Safety Communications in Network 2015

Public safety operations require effective command, control, coordination, communication, and information sharing tools to support law enforcement, firefighting operations, emergency medicine, search and rescue, and other critical response services. Emergency response personnel at all levels of government and across multiple disciplines must be able to communicate as needed, on demand, and as authorized. While many State and local agencies have modernized and expanded their mission-critical voice systems through initiatives such as Federal grant programs, or are in the process of doing so, the communications challenges for those working on the front lines in public safety have not been eliminated. Emerging solutions such as Next Generation 911 (NG911), integrated command centers, broadband wireless, mobile computing, video, and location services promise enhanced access to information that permits safer, smarter

²² Number Resource Organization. "Free Pool of IPv4 Address Space Depleted," 3 February 2011. Available at: <http://www.nro.net/news/ipv4-free-pool-depleted>.

decision-making and faster outcomes. As technology continues to evolve, public safety will need to assimilate, assess, and integrate applications using available voice, data, and video streams for incident response. Approaching 2015, key public safety communications trends will include:

- **Public safety system consolidation:** Many jurisdictions and public safety agencies are consolidating their systems by developing radio networks to cover counties, regions, and States and merging their communications dispatch centers across agencies and political boundaries. Shared statewide radio systems are typically designed to consolidate the communications of multiple State agencies into a single system, thereby providing strong interoperability. The public safety community will continue to deploy large-scale Statewide and regional mission-critical voice networks in the coming years.
- **Interoperability, convergence, and roaming:** Public safety users will increasingly need to interoperate with a larger community of emergency responders, including Federal law enforcement, border security, emergency response personnel, and private critical infrastructure owners and operators. Incident response coordination will remain complex as public safety's private networks interface with commercial networks and users' devices are allowed access to both private and public networks. As public safety demands for high-bandwidth applications increase, public safety officials and other critical infrastructure users will look to roam onto public networks and commercial infrastructure through priority service agreements.
- **Future broadband wireless networks:** Future broadband wireless networks promise to enable powerful and innovative solutions that will add real-time awareness to emergency responder communications. As these new broadband networks will need to meet demanding public safety requirements, developers will face long-term technological challenges to assure that public safety requirements drive development of future, integrated solutions. The public safety community will also seek broadband resiliency by setting quality of service requirements similar to current mission-critical voice. These may include capabilities like push-to-talk, one-to-many communications, group calls, prioritization, hybrid simplex/duplex capabilities known as "talk-around," and two-way video.
- **Emerging capabilities:** Evolving public safety command and control will leverage new sources and inputs, telematics, video, text, and social networking to provide enhanced situational awareness. As new multi-network devices will support these new applications, it will become necessary for providers to manage voice, data, and video information to optimize real-time decision making. New data sources based on the location, type of incident, and assigned personnel will stress resources and highlight the need to prioritize and distribute only the most relevant data to responders in the field.
- **Specialized public and private devices:** Public safety officials will choose from a portfolio of tiered devices offering the necessary ruggedness and ergonomics for public safety environments. These devices will also support various modes of operation from 3G to 4G and access to private and public networks. Adverse conditions require devices that are designed and tested to be simple and intuitive, based on human factor research on how individuals react in stressful situations. Portable data devices with advanced display

and interface technologies offering survivability and performance in the most demanding environments will also be available to support operations in the field by 2015.

- **Emergency alerting capabilities:** The Nation's 911 emergency call system and emergency alert systems are critical to ensuring that people can reach emergency responders and receive important information during incidents. NG911 and Next Generation Emergency Alerting (NG Alerting) technologies are expected to be deployed by 2015.

2.6 Service Provider Best Practices

As telecommunications service providers, Internet Service Providers (ISP), and cloud providers look to 2015, market incentives will remain the fundamental driver of industry practices and standards; companies will continue to offer services that are as resilient and secure as customers' preferences dictate. In 2015, service providers will likely reinforce many of today's best practices with respect to resiliency, while also further developing and deploying new initiatives.

- **Network traffic management:** Telecommunications carriers employ various methods for managing network traffic during periods of heightened use and congestion. For example, wireline carriers can implement call blocking, which gives priority to outgoing calls from a particular area by blocking incoming calls. Blocking can occur at the national or local level, usually at the origination site, to minimize congestion in the impacted area. Wireless carriers also manage network capacity at cellular sites as traffic and congestion move throughout a geographic area. Carriers may reduce the quantity or speed of delivery for video or other high-bandwidth services to prioritize voice traffic; this technique would likely be applied at the ingress of the network at the IP layer.²³
- **Investments in infrastructure:** ISPs and telecommunications carriers will continue to update their infrastructure to support heightened network demand so that they may remain competitive in the market and retain customers. As smartphone usage increases and equipment makers develop new devices to match demand, CMRS carriers will also increase bandwidth to support regular daily communications. In accordance with engineering best practices, CMRS carriers will also continue to expand network transport infrastructure as demand requires.
- **DNS security:** By 2015, DNS Security Extensions (DNSSEC) and similar initiatives are expected to be widely deployed throughout the network. DNSSEC should address most problems concerning DNS object-level integrity, but will be of little use if the availability of DNS infrastructure is impacted. The Resource Public Key Infrastructure (RPKI), a database currently under development, will also provide a security framework for verifying the association between organizations and their Internet resources.
- **BGP security:** Approaching 2015, industry will continue to explore Secure BGP (SBGP) and Secure Origin BGP (SoBGP), which seek to validate the accuracy and authorization of routes. RPKI will also help protect BGP information from route hijacks

²³ For more information on network management practices, see the *NSTAC Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic*, November 2008.

and similar object-level attacks, although it will not protect the BGP protocol itself. RPKI could allow for new secure routing policies or other BGP security protocols that will help mitigate some network vulnerabilities. Additionally, a repository of the Internet number resources that could be used to develop inter-domain data path anti-spoofing controls would further minimize the network infrastructure's vulnerability to attacks and assist with network-level protection of DNS.

- **Incident response planning:** Carriers, ISPs, and other entities responsible for maintaining and restoring the network will continue to update and exercise incident response plans to protect key infrastructure during an incident. Response planning will help service providers understand the nature and extent of their dependencies on various components of the network, and allow them to establish predetermined methods to work around network failures. During an incident, service providers may have to work together to decide which infrastructure is most critical to maintain.
- **Security incident category research:** Industry will continue to research firewall enhancements and methods to dynamically quarantine malware to shorten the timeframe for identifying the source of a botnet incident. Industry will likely also conduct research into botnet disruption, more secure network devices, negative testing against devices, and network credentialing.

3.0 STRESSING THE NETWORK

The following sections provide the EOP's four scenarios, followed by the findings and recommendations for each scenario. NSTAC members consulted with their companies' SMEs to identify each scenario's anticipated impacts to the communications network, possible mitigation activities, and specific steps that industry or the Government could take to enhance resiliency.

3.1 Scenario 1: Multiple Terrorist Attacks in the National Capital Region

3.1.1 Issue

The following scenario, which describes a succession of terrorist attacks launched throughout the NCR, is intended to emphasize the impacts of severe congestion on the region's wireless networks. Heightened network usage would strain local telecommunications carriers' capacity and potentially threaten communications between priority users such as first responders, law enforcement personnel, Federal officials, and technical restoration personnel. Given the importance of first responders' immediate response efforts, the scenario's analysis prioritizes communications availability for the public safety community. The scenario assumes that the terrorist incidents have no impact on physical infrastructure, as the intent is to stress the communications network's capacity.

3.1.2 Scenario

Multiple terrorist events have been successively launched throughout the NCR over consecutive weeks, with further attacks predicted with little or no warning. Communications assets have not been destroyed, but cellular infrastructure is inundated with people trying to call loved ones, receive calls, and send pictures or videos from their phones. Communications infrastructures

are seeing rapid surges in usage as people seek information on the attacks, including through the use of mobile devices and through WiFi networks. The complexity, scope, and potential consequences of these terrorist threats require that there be a rapid and decisive level of coordination among law enforcement, criminal investigation, protective activities, emergency management functions, and technical expertise across all levels of government, which have been struggling to maintain consistent communications.

3.1.3 Impacts

Because the scenario assumes the events cause no physical destruction to the communications infrastructure, the Internet, Public Switched Telephone Network (PSTN), and private and public networks may experience congestion but would remain operational. Local and nationwide broadband communications infrastructure, broadcast radio, and television would also be fully functional.

Immediately following the incident, news media reports would likely create alarm among the general population and spur a sharp increase in mobile phone usage. Cellular communications could spike within minutes of the news broadcasts, initially in the areas of high-density employment and proximity to the incident and then along major commuting routes that support the populations' movement throughout the region. Heightened usage would stress local telecommunications carriers' network capacity and could result in periods of network congestion on public cellular infrastructure throughout the NCR. As users would experience prolonged delays in completing voice calls, critical public and private national security and emergency preparedness (NS/EP) communications users would rely heavily on priority services such as GETS and WPS to access the public network during this period of wireless congestion. Congestion could also increase switched-circuit use within the region, leading to "all circuits are busy" messages. Depending on the events, the NCR's inbound enhanced 911 (E-911) lines could be saturated with calls from citizens requiring emergency assistance. Wireless congestion could also hamper citizens' ability to reach first responders, as wireless E-911 call originations account for between 25 to 60 percent of all calls received by Public Safety Answering Points (PSAP). Any network congestion experienced on wireless networks would likely inhibit call completions to PSAPs as well.²⁴

Although the scenario is unlikely to create widespread service outages in the NCR, the surge in demand could impede commercial network customers from accessing and using the network as they would under normal conditions. The precise levels of congestion resulting from this scenario would be difficult to predict and would depend on the nature, duration, and exact locations of the events; nonetheless, the network user experience would be substantially reduced.

The incidents would also put into motion the full range of public safety and emergency response activities across all levels of government, jurisdictions, and multiple incident response support

²⁴ According to the National Emergency Number Association, 240 million 911 calls are received annually by PSAPs across the Nation, and this volume of calls continues to increase. The number of 911 calls placed by people using wireless phones has radically increased. Public safety personnel estimate that about 50 percent of the millions of 911 calls they receive daily are placed from wireless phones, and the FCC estimates that this percentage is growing. See FCC Consumer & Government Affairs Bureau, "Wireless 911 Services," available at: www.fcc.gov/cgb/consumerfacts/wireless911srvc.html.

functions. Critical public safety tasks would include maintaining command and control of all metropolitan police and fire departments participating in the response, including from the District of Columbia, Maryland, and Virginia; activating Emergency Operations Centers; activating emergency alert and notification systems; distributing alerts and guidance to emergency responders, county and city employees, and private partners such as hospitals, clinics, and private citizens; coordinating with law enforcement, homeland security officials, and the Federal Emergency Management Agency (FEMA); coordinating with the Department of Defense (DOD) and military disaster response elements; and assisting with evacuations or the movement of people, if necessary. The potential scale of public safety coordination could incorporate as many as 50 separate public safety agencies.²⁵

3.1.4 Findings

Critical response personnel would continue to rely heavily on priority services, such as GETS and WPS, to improve their access to the wireline and wireless public networks during a period of congestion. Ensuring priority services in a converged 2015 environment will require continued funding, along with a well-defined, end-to-end priority access protocol, hardware/software authorization, and the ability to authenticate the user, application, and device. Priority access to the public network is a vital communications channel for authorized users during an emergency. In 2007, the Department of Homeland Security's (DHS) Office of the Manager, National Communications System (OMNCS) completed the first of several phases of work to develop priority services standards. The first phase laid the foundation for industry to plan for future NS/EP voice services and the next two phases will develop video and data standards within the industry's IMS architecture, including an analysis of potential call connection combinations and various evolving network architectures.²⁶ As of early 2011, priority service capabilities are available to authorized users in the wired and wireless networks. But as telecommunications technologies migrate from circuit-switched networks to IP-based networks, priority services will need to keep pace with new, enhanced capabilities within the carrier networks. In particular, priority services must ensure that the user and/or the mission-critical application have priority across current and newer domains, such as WiFi, 4G platforms, and the Internet. These same capabilities will also be essential to promote public safety usage of wired and wireless commercial networks in the face of congestion.

The public safety community may require additional spectrum to support video and other high-bandwidth demands during times of emergency; spectrum management policies must ensure that capacity is properly allocated among users, available networks, and technologies. The public safety community relies on a finite portion of regulated spectrum, allocated for

²⁵ On September 11, 2001, Federal, State, and local emergency responders in the Washington, D.C., area were able to communicate because they had a mutual-aid interoperability plan, which was developed in response to the 1982 Air Florida plane crash in Washington, D.C. At that time, agencies could not communicate with each other, hampering rescue efforts. Regional planning produced successful procedures for mutual-aid interoperability on September 11, 2001. See Public Safety Wireless Network. *Answering the Call: Communications Lessons Learned from the Pentagon Attack*, February 1, 2003, available at:

<http://www.safecomprogram.gov/NR/rdonlyres/8839D9BA-9104-4EE1-BC43-E8431C500F95/0/AnsweringCallLessonsPentagonAttack.pdf>.

²⁶ Currently ongoing as of early 2011.

exclusive public safety use, in order to limit interference and manage access to the spectrum.²⁷ Although this dedicated spectrum will support the core of the public safety broadband network, public safety users often require access to additional capacity during the most severe crises. This need for additional capacity will increase in 2015, as high-bandwidth applications, in particular mobile video, will place additional demands on the public safety community's own private network. To secure additional capacity, emergency responders—as a user-class—may benefit from obtaining priority access to commercial network spectrum under terms similar to those used by the commercial carriers in allocating spectrum between NS/EP WPS users and the public at large. The current allocation of commercial wireless spectrum for WPS reflects a balance between individual NS/EP user needs and the needs of commercial customers who require spectrum for their own purposes, including 911 calls.

With the establishment of the FCC's proposed nationwide public safety broadband network, which will use LTE as the standard, the commercial wireless networks may be able to allocate, on demand, a portion of their commercial spectrum for public safety use.^{28,29} Since the public safety community will still be in the early stages of deploying and using LTE networks in 2015, the technical mechanisms to provide additional spectrum, as well as the need, benefits, and risks of dynamically re-allocating that spectrum, may not yet be sufficiently understood to be supported at that time.

A coordinated, multi-jurisdictional response to terrorist events in the NCR that draws emergency responders and law enforcement officials from outside jurisdictions would require equipment interoperability and roaming and frequency reuse agreements. In the immediate aftermath of an event, the NCR public safety community would have to share vital voice and data information across disciplines and jurisdictions quickly and seamlessly, including inbound requests for assistance coming from the PSAP dispatch centers or PSAPs that answer citizens' calls for police, firefighting, and ambulance services. Past incidents have proven the continued challenge and need for all emergency responders, regardless of jurisdiction, to possess the right multi-hazard communications equipment. By 2015, technologies such as software-defined radios will be prevalent in the responder community, but continued investment in this technology will be imperative. Some of the historical issues associated with interoperability will also be mitigated in 2015 by the adoption of LTE as the data standard for the FCC's proposed public safety 700 MHz mobile broadband network. Even with this network, however, the need to support ever-increasing volumes of high-bandwidth applications, such as computer-aided dispatch, law enforcement databases, and video surveillance, may lead to congestion in the public safety network, as well.

²⁷ In the NCR, the public safety community has built and operated two pilot broadband wireless networks operating in the 700 MHz band of spectrum. These initiatives have involved 20 local and Federal agencies, encompassing hundreds of data card users, and have been used to support critical communications during major regional events such as the 2008 Presidential inauguration.

²⁸ A critical issue the *National Broadband Plan* addresses is how to ensure the availability of broadband communications for public safety and emergency response on a cost-effective and technically feasible basis.

²⁹ Gross, Grant. *Tech World*. "FCC Sets LTE as Standard for Public Safety Network," January 26, 2011. Available at:

http://www.techworld.com.au/article/374496/fcc_sets_lte_standard_public_safety_network/?fp=2&fpid=1&rid=1.

While emergency alerting systems are vital to notifying the public of a threat, the development and deployment of numerous different alerting capabilities approaching 2015 could compound network congestion without proper design, testing, and prioritization. Future emergency alerting systems will likely draw upon all available means of communication to ensure that the public can receive timely and accurate alerts, warnings, and critical information about all types of incidents. Alerts could be broadcast on local media outlets, sent to wireless and wireline phones within the affected area, posted on Internet feeds and Web sites, and issued through any communications outlet serving the affected area. The development of multiple systems by multiple alert providers, however, raises the risk that these competing systems may inadvertently stress the commercial networks to the detriment of overall network performance and may interfere with message delivery to the end user.

To facilitate communications incident response coordination, the NCC, within DHS' National Cybersecurity and Communications Integration Center (NCCIC), would continue to serve as a vital hub for industry and Government collaboration. Both the NCC and the NCCIC have formalized structures designed to facilitate 24x7 Government-industry collaboration to determine how best to protect communications assets, prepare for a possible next attack, and share information to aid in response efforts.³⁰ As congestion clogs public networks, the NCC could help coordinate the response activities and maintain situational awareness among Government and industry partners.

3.1.5 Scenario 1 Recommendations

The NSTAC recommends the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*³¹

- ❖ **Request that Congress fund DHS' priority services efforts to continue industry and Government collaboration and to ensure that advanced NS/EP communication services are operational when needed.** Historically, the Government has funded commercial telecommunications efforts to develop, maintain, and upgrade GETS and WPS, as the costs to provide these services to their small user base would be prohibitive to individual companies. But these programs face an uncertain future due to insufficient funding. In particular, funding constraints may undermine the development of new capabilities or the ability of priority services to meet the needs of additional public safety users. In fiscal year 2008, the Administration sought \$52 million to perform research and development of next generation priority services programs and received only \$21 million from Congress.³² The President should make clear to Congress that, in the absence of additional funding between 2010 and 2015, the only incremental additions to priority

³⁰ See Appendix E for additional information.

³¹ Recommendations denoted by a symbol are those the NSTAC has deemed to be of highest priority to the President.

³² Government Accountability Office. *Emergency Communications: National Communications System Provides Programs for Priority Calling, but Planning for New Initiatives and Performance Measurement Could be Strengthened*. Report GAO-09-822. August 2009.

services will include VoIP applications. Congressional funding should ensure that DHS develops and deploys future IP video and data priority services.³³

- **Encourage DHS to file comments with the FCC in its appropriate public safety broadband dockets.³⁴ In its filed comments, DHS should recommend that the FCC continue working closely with industry as it builds the nationwide interoperable public safety mobile broadband network, as recommended in the FCC's *National Broadband Plan*.** This will aid in the development of spectrum management policies that ensure spectrum capacity is properly allocated among users, available networks, and technologies.
- **Encourage DHS to petition the FCC to issue a declaratory ruling to confirm that network service providers may lawfully offer IP-based priority access services to NS/EP authorized users.³⁵** Service providers must maintain the authority to ensure that networks remain capable of providing priority communications for NS/EP authorized users in the future.³⁶
- **Encourage Congress to continue funding DHS' Science and Technology Directorate to pursue interoperability solutions for emergency responders and ensure that DHS allocates the funds to particular interoperability programs.** For example, a DHS contract in 2008 led a private contractor to develop the first-ever multiband radio that allows police officers, firefighters, and emergency medical service personnel to communicate with partner agencies using a single radio capable of operating on multiple radio bands.³⁷ DHS should continue funding this and similar initiatives.
- ❖ **Direct DHS to build future alerting capabilities that consider all potential multi-platform technologies, to ensure that the public can receive timely and accurate alerts, warnings, and critical information about emergencies regardless of**

³³ In addition, the November 2008 *NSTAC Report to the President on National Security and Emergency Preparedness Internet Protocol-Based Traffic* recommended that the President establish a policy requiring Federal departments and agencies to: 1) ensure their enterprise networks are properly designed and engineered to handle high traffic volume; 2) manage traffic through quality of service programming in its routers to prioritize traffic, including NS/EP traffic; and 3) expand the use of managed service agreements to provision NS/EP services within the new IP-based environment. The report also recommended that the President require Federal departments and agencies to remain actively involved in standards development of priority services on IP-based networks by supporting efforts to provide adequate funding to develop timely solutions across all technology platforms and committing appropriate resources to actively participate in and lead the global standards bodies' efforts to address NS/EP IP-based priority services.

³⁴ These dockets include WT Docket No. 06-150: *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229: *Amendment of Part 90 of the Commission's Rules*, and WP Docket No. 07-100: *Third Report and Order and Report and Fourth Further Notice of Proposed Rulemaking*.

³⁵ Without FCC permission, priority services would violate Section 202(a) of the *Communications Act of 1934*, as priority services constitute preferential treatment by carriers. In 2000, the FCC issued an order establishing that the priority services offered to NS/EP authorized users were *prima facie* lawful under the *Communications Act*. Consistent with this ruling, the FCC should further confirm that the same is true with regard to IP-based priority access services offered by IP-based providers to NS/EP users.

³⁶ The NSTAC made a similar recommendation in its 2008 *Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic*. Such a petition could be filed in the FCC's open docket, WCB Docket No. 04-36: *IP-Enabled Services*.

³⁷ DHS Science and Technology Directorate Press Release. "DHS Launches Multiband Radio Project," February 27, 2008.

the communications technologies used. When constructing or evolving new alerting systems, system designers should consider all potential multi-platform technologies, but must also deconflict alerting systems and potentially consider prioritizing which of the alerting systems take precedence over others in times of congestion. Alerting systems in the converged 2015 environment should be engineered and tested regularly, both individually and in parallel with other systems, to ensure system functionality and receipt of messages.

- ❖ **To accelerate efforts to fulfill DHS' NCCIC mission and, to ensure that it is fully operational by the 2015 timeframe, direct DHS to accomplish the following as soon as possible:**
 - Leverage the success of the existing NCCIC incident response mechanisms by ensuring sufficient funding levels are dedicated to the mission;
 - Direct the rapid expansion of personnel resources, including training, to guarantee that the cyber and communications incident response mechanisms are absolutely viable and fully mission capable by 2015.

3.2 Scenario 2: Catastrophic Earthquake in San Francisco

3.2.1 Issue

The following earthquake scenario is intended to stress the resilience of the communications network in a situation of incapacitated physical infrastructure. The immediate call congestion impacts outlined in Scenario 1 will also be present in this scenario, and the findings and recommendations associated with congestion and prioritization outlined in Scenario 1 are thus also assumed for Scenario 2. The primary distinction between the two scenarios, however, would be the significant loss of life, damage to telecommunications and other supporting critical infrastructures, and severe damage to transportation ingress and egress. The findings and recommendations outlined below highlight these considerations. This assessment is also predicated on the assumption that the highest priority actions would be those that enable response, support survivor needs within the first 72 hours after the incident, and address some of the first-week issues to ensure transition to longer-term recovery.³⁸

3.2.2 Scenario

The San Francisco Bay area has been hit with a catastrophic earthquake affecting more than seven million people. There is severe damage in most communities, with unstable soil in San Francisco and Oakland. Other effects include fires, flooding, landslides and ground ruptures. These cumulative effects have destroyed major cellular and Internet infrastructures, as well as land mobile radio repeaters and gateways. 3G/4G towers that remain operational are almost fully saturated with traffic and their batteries last an average of only eight hours. The

³⁸ This approach is consistent with FEMA's "Whole of Community Framework for Catastrophic Planning and Response" initiative. See FEMA Office of Response and Recovery, "International Recovery Forum," 12 January 2011, available at http://www.recoveryplatform.org/assets/meetings_trainings/irf2011/Presentations/Forum/Keynote%20Speech%20-FEMA-Ms.Zimmerman.pdf.

devastation of communications infrastructure has left responders without a reliable network to use for coordinating emergency response operations. Neither 911 service nor public safety radio communications are functioning sufficiently. In addition, mutual aid communications are scarcely available and repairs are urgently needed. The major power plant for the region was hit severely, and it will take weeks to restore electric power to the San Francisco Bay Area. There is an urgent need to provide power to charge portable electronic devices.

3.2.3 Impacts

In the initial hours following the earthquake, the most devastating human impacts near the earthquake's epicenter would be significant fatalities and a large number of injured requiring emergency medical attention. For an earthquake between the magnitudes of 7.7 to 7.9, with an epicenter near the mouth of the San Francisco Bay, FEMA and the California Office of Emergency Services (OES) project up to 3,300 fatalities, 12,300 people with serious injuries, 1,700 people requiring search and rescue, and hundreds of thousands of displaced citizens requiring shelter.³⁹ Immediate hazards could include fires, collapsing structures, flooding from broken water mains, exposed electrical hazards, or leaking fuel. The likely occurrence of aftershocks would exacerbate these hazards and increase the risks to rescue and response personnel.

Significant damage to critical infrastructure in the immediate area of impact could include a loss of above-ground communications infrastructure (cellular sites, broadcast towers, and transmission facilities), in-building wireless access, and significant disruption to underground transport modes impacting wireline, power, water and fuel lines. FEMA and the California OES estimate that 789,000 households would lose electric power on the day of the earthquake's impact and by the end of the first week, 229,000 households would remain without power.⁴⁰ Physical structures surrounding critical infrastructure, such as offices and homes, could also suffer significant structural damage even despite retrofitting. Transportation infrastructure such as roads, bridges, and rail lines, would also be disabled. By some estimates, transbay bridges, ports, and airports could continue to show damage up to 90 days following a major earthquake.⁴¹ Since transportation infrastructure tends to be physically coincident with other underground transport modes such as fiber, pipeline, water, electricity, and fuel, damage to transportation infrastructure would imply existence of damage to the underlying infrastructure.

In the regions surrounding the most impacted area, communications would likely continue to operate or be quickly restored, with the exception of communications facilities that rely on the damaged underlying infrastructure located in the impacted area (in particular, transport infrastructure). Lack of transport integrity would be the primary cause of communications outages in the surrounding areas, followed by lack of power for those facilities that rely on commercial power and do not have alternate power sources. Depending on damage in the area of primary impact, commercial power would be available in small, confined areas. The further removed from the immediate impacted area, the higher the probability that CIKR would remain

³⁹ DHS, FEMA, and California OES. *Interim San Francisco Bay Area Earthquake Readiness Response: Concept of Operations Plan (CONPLAN)*. 23 September 2008, p. 2-2.

⁴⁰ CONPLAN, p. 2-2.

⁴¹ Association of Bay Area Governments. *Taming Natural Disasters: Multi-Jurisdictional Local Hazard Mitigation Plan for the San Francisco Bay Area*, 2010 Update.

intact and operational. This outer perimeter of service would provide the most secure area for managing command and control of response operations as well as the starting point for restoration efforts, allowing service operators to work in a bulls-eye pattern to bring service back closer to the epicenter. Regions, States, and municipalities have integrated this approach into their disaster response plans.

Earthquake Planning

The San Francisco Bay Area Earthquake Readiness Response: Concept of Operations Plan (CONPLAN) describes the joint State and Federal response to a catastrophic earthquake in the Bay Area. The CONPLAN contains projected impacts, objectives, courses of action and decision points, response capabilities, and response actions. More than 70 local, regional, State, Federal, and private sector entities assisted in preparing the CONPLAN. The plan is consistent with the principles of FEMA's National Incident Management System and will be implemented in accordance with the National Response Framework, the State of California Emergency Plan, and the Standardized Emergency Management System. (For additional information on Federal response roles and responsibilities, see Appendix F.)

3.2.4 Findings

A key challenge would be to ensure basic communications among local, State, and Federal officials and emergency responders in the impacted zone. As earthquake damage is usually concentrated near the earthquake's epicenter and may have a more limited geographic reach than other disasters, notably hurricanes, technical analysis of restoration efforts during past earthquakes can help planners project future communications needs and understand standard best practices in earthquake zones. Most regions, States and localities in known earthquake zones have exemplary disaster planning for these events and have pre-identified likely command and control locations with a high level of survivability. The challenge, however, would be to establish communications channels between the functioning infrastructure or assets in these pre-identified command and control locations and the responders or officials working within the impacted zone, where communications may not be available.

Numerous Government agencies sponsor individual programs and systems that could contribute immediate tactical communications support during emergencies to fill this identified gap. However, there is a continued need to identify and list all relevant capabilities across the Federal Government; inform State or regional authorities regarding these programs and their limitations; establish request and response procedures that consider policy, authority, and funding arrangements; and, as feasible, embrace selected programs within planning and exercises. FEMA, for example, may deploy one or more of its nationwide Mobile Emergency Response Support (MERS) detachments equipped with tactical communications capabilities to enable incident command and control between Federal, State, and local officials. MERS units are scalable and flexible in their composition.⁴² The U.S. Strategic Command (USSTRATCOM) has

⁴² A MERS unit could include Land Mobile Radio, portable radios and repeaters, satellite communications, line of sight microwave units, VoIP and Radio over IP, secure communications equipment, and communications technicians. FEMA briefing to the NSTAC, February 1, 2011.

developed mobile communications packages that provide connectivity to an impacted zone and U.S. Northern Command (NORTHCOM) provides similar communications packages.⁴³ State and regional planners may not have identified all such relevant capabilities, however, much less integrated them into response plans and exercises.

Communications providers would likely be able to provide initial, but limited, damage estimates for Government and CIKR owners/operators, as well as for their network's current operational capabilities. Communications service providers, through their network operations centers (NOC), may not have full visibility into their network status in the immediate aftermath of the incident, but should be able to provide confirmation of what communications infrastructure and assets are still operational. Service providers would likely experience areas of geographically isolated service, where connectivity would be available within a confined area, but transport disruptions would inhibit connectivity to the larger networks for both wireline and wireless network elements. Detailed assessments or confirmation of network impacts would not be forthcoming in the immediate aftermath of the earthquake, as providers would have limited access to their infrastructure.

Physical damage would impede access to sites for the purposes of assessing the damage, restoring service, or deploying alternative communications such as cells-on-wheels (COW), back-up generators, and other equipment. A key challenge in providing emergency communications would be the loss of transport capabilities connecting local services to the broader infrastructure and a lack of accessibility to the immediate impacted area. Alternate means of transport would need to be leveraged to deliver the necessary equipment to restore communications. Helicopters might provide one possible means of transport and ships stationed off the coast may also provide platforms for deployed communications equipment. Use of these transportation mechanisms for restoration activities are not routinely exercised, however, and would not be immediately available for use in an emergency event. Additionally, responders may be able to use unmanned aerial vehicles (UAV) equipped with an airborne communications package. Such a vehicle can stay airborne for a much longer period than a manned aircraft and can provide coverage over a wide geographical area. Still, significant issues concerning communications compatibility and interoperability, frequency spectrum, and airspace would have to be resolved. Since these capabilities are DOD assets, FEMA and DOD would need to coordinate with State and local authorities to ensure that memoranda of agreement (MOA) allow for temporary spectrum use for such assets. Involved parties should arrange such MOAs well before an emergency.

Satellites would be an effective means of supporting communications requirements for search and rescue efforts and other critical response activities. Given the potential damage to underlying terrestrial infrastructure, satellite communications would be a prominent means of bridging communications between local, tactical operations and command and control capabilities. Satellite communications could be especially useful for search and rescue communications plans, which presume communications self-sufficiency for localized, tactical work. While satellite services can play an important role in providing access or coverage, it is nearly impossible to predict if there will be sufficient satellite capacity serving the specific geographic area in question to fulfill the range of potential services that might be required. In

⁴³ USSTRATCOM briefing to the NSTAC, February 8, 2011.

previous incidents, satellite operators have sought to accommodate public safety requirements with available capacity. Pre-positioning of bandwidth, capacity-sharing among entities, and prioritization of bandwidth are also useful tools to offset concerns of satellite bandwidth supply shortfalls.

Ensuring the functionality of surviving communications infrastructure would require maintaining adequate power and fuel supplies after the first 72 hours. Shutdown of and damage to petroleum refining, pipeline, storage, and distribution systems would create an immediate shortage of fuel, including fuel for ground transportation, air transportation, and generators. In general, local governments do not have extensive supplies of fuel for sustained operations.⁴⁴ Communications providers maintain a stockpile of portable generating equipment and design their networks to operate with alternate forms of power. However, the Association of Bay Area Governments estimates that customers of the region's largest electric power company, Pacific Gas & Electric, could expect to remain without power for 72 to 96 hours.⁴⁵ Furthermore, a catastrophic earthquake could significantly disrupt fuel supplies for up to a month, thereby increasing competition for available fuel among all critical sectors and leaving insufficient fuel for some CIKR. If the earthquake disabled substantive portions of the electric grid, fuel shortages could become a protracted issue frustrating infrastructure recovery. While the San Francisco CONPLAN acknowledges the need to establish fuel distribution networks for response operations, it is not clear if the Communications Sector qualifies as a critical facility and would have access to some of that fuel. In contrast, other private sector facilities, such as hospitals, are specifically identified as fuel recipients.⁴⁶

The degree of redundancy in the transport architecture will determine how much disruption the earthquake causes to the various networks. In addition to fiber transport, many carriers achieve redundancy by using microwave transmission to connect facilities, such as cell towers, back to an aggregation point, with fiber then connecting to the NOC. The microwave connection may need to be re-established prior to restoring service. Many carriers also achieve greater resiliency in their transport by accessing fiber laid out in a ring configuration. While major portions of the ring may survive an earthquake, immediate service restoration to that site may be hindered if access from the communications facility to the ring is impeded or disrupted.

The San Francisco Bay Area is a major interconnection and routing hub for numerous networks both domestically and internationally; communications outages in the Bay Area could therefore have an impact on traffic outside the immediate region. While the vast majority of traffic would be re-routed or diverted in the immediate aftermath of the event, certain areas would experience communications isolation or the inability to connect with the larger networks. Cloud services may also be impacted if large data centers are located in the immediate area of the earthquake, as they could suffer damage or lose power, and support staff may be unable to gain access. These impacts would be amplified if the region's key communications providers and enterprise managers do not have a mutual understanding of each others' business operations or are not able to collaborate on resiliency measures. A lack of mitigation strategies,

⁴⁴ CONPLAN, p. 2-8.

⁴⁵ Association of Bay Area Governments. *Taming Natural Disasters: Multi-Jurisdictional Local Hazard Mitigation Plan for the San Francisco Bay Area*. 2010 Update.

⁴⁶ CONPLAN, p. 4-13.

such as diversified interconnection transport technologies or designated alternate sites to handle mission-critical functions, could also magnify the impact.⁴⁷ Finally, local businesses with outdated or no communications continuity plans with their respective service providers may find that they would be bypassed by communications restoration efforts.

A number of alternative communications technologies would likely be leveraged to augment or replace the capacity or availability of damaged facilities. Many of the following technologies are already integrated into deployable FEMA and DOD units, including:

- **WiFi:** WiFi hotspots can be deployed quickly and wireless devices are increasingly able to connect to WiFi. The propagation characteristics of WiFi spectrum, however, are very limited, and can only be deployed to locations with access to transport and power.
- **WiMax:** WiMax hotspots can also be deployed quickly and have the advantage of greater geographic propagation. Like WiFi, WiMax can only be deployed to locations with access to transport and power.
- **Satellite:** Satellite-based networks can provide an alternative to terrestrial communications and are often used to restore communications in the event of disabled or disrupted fiber-based and terrestrial wireless communications networks. Many operators of terrestrial wireless and fiber-based networks contract in advance to pre-position satellite capacity in order to ensure operational continuity in the event of network disruptions. For unanticipated network disruptions, satellite-based restoration services may be made available for restoration or surge requirements, necessitating the contracting of satellite capacity and rapid deployment of satellite ground equipment; this equipment could include transportable earth stations or mobile COWs that can restore terrestrial wireless capabilities. Satellite capacity is subject to availability, but capacity is generally obtainable over the continental United States on short notice with considerable options to expand. Additionally, mobile satellite phones are often relied upon in the first hours following an emergency, whether to provide mobility or to offer initial voice and lower speed data communications until higher-speed, more established communications networks can become operational.
- **Broadcast Radio:** Radio and broadcast towers can provide a means of efficiently communicating with large numbers of individuals. While the broadcast area of these facilities cannot be modified spontaneously, they can be adjusted over time to provide greater coverage in the short- to mid-term. These modifications would need the regulatory support of the FCC.
- **Microwave:** Microwave can be implemented to provide additional transport capacity and replace damaged fiber connectivity. Additional microwave solutions, such as antennas installed on COWs, can achieve relatively large bandwidth capabilities at fairly long distances. Microwave and WiFi played important roles in the restoration efforts following the 2010 earthquake in Haiti. Leveraging this capability for rapid deployment would require spectrum analysis and regulatory support from the FCC.
- **Peer-to-Peer Capabilities:** Peer-to-peer handset capabilities are a requirement for next generation public safety networks and are also available in some commercial wireless

⁴⁷ NSTAC Financial Services Task Force Report. April 2004, p. 22.

networks. It is likely that this handset-to-handset communications would be the baseline communications utilized in the immediate impact area for tactical operations by emergency responders. However, handset users would require a means of communicating with command and control operations headquarters outside of the impacted zone.

- **Shared Resources (SHARES) High Frequency (HF) Radio Program:** SHARES provides Federal, State, and industry organizations a means to communicate NS/EP information via the existing HF radio resources of when normal communications are destroyed or unavailable.

3.2.5 Scenario 2 Recommendations

The NSTAC recommends the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions* (recommendations denoted by a symbol are those the NSTAC has deemed to be of highest priority to the President):

- **Direct DHS and other appropriate departments and agencies to support collaboration between State and local government and industry to determine the most effective and appropriate mechanisms for restoring critical communications services.** In particular:
 - Encourage the development and funding of large-scale, tactical response support capabilities that incorporate the resources and expertise of multiple carriers. Given the rapidly evolving nature of networks and the services they provide, any support strategy should be consistently updated while also remaining available should the need arise. Given the potential cost of large-scale support, it may be appropriate to conduct this planning at the State or regional level. If planning is implemented at the regional level, transport support associated with these strategies may need to be provided at the Federal level.
 - Once the appropriate mechanisms have been selected, support the development of protocols and contracts at the State or regional level to ensure the resources are available when needed.
 - Since continuation of essential, critical services delivered by both Government and the private sector CIKR can be better assured with ready access to fuel, direct that States assess the projected fuel needs to sustain critical services for 30 days, and incorporate contractual arrangements with fuel providers to ensure the availability of those fuels within 48 hours to an impacted zone.
 - Bolster existing but under-funded programs that aim to pre-position emergency power generation equipment at critical facilities and sites and replace above-ground electric and telecommunications infrastructure with underground structures.⁴⁸

⁴⁸ Association of Bay Area Governments. *Taming Natural Disasters: Multi-Jurisdiction Local Hazard Mitigation Plan for the San Francisco Bay Area*. 2010 Update.

- ❖ **Direct DOD and other appropriate departments and agencies to enhance the utility of and reliance upon satellite systems to provide alternate communications when terrestrial-based communications infrastructure is impaired.** To ensure ubiquitous, redundant, and resilient disaster communications, satellite-based communications should become a required component of critical communications networks. In particular, the President should direct the appropriate department or agency to:
 - Investigate the possibility of investing in additional pre-positioned, leased satellite capacity to restore commercial communications transport in the event of an emergency and ensure that appropriate satellite ground equipment is in place to augment satellite capacity and equipment.
 - Expand Federal interoperability grant funding and guidance to encourage NS/EP entities to acquire mobile satellite communications equipment and ensure that critical staff are educated and trained in satellite use. Emergency response drills and exercises that include the use of mobile satellite communications should also be mandated.
 - Modify public safety communications grant funding programs to require that State interoperable communications plans place greater emphasis on satellite communications generally to provide resiliency during a disaster.⁴⁹
- **Direct FEMA, in coordination with other DHS agencies and DOD, to identify, support, and integrate relevant tactical emergency communications support capabilities across the Federal Government.** When such capabilities are identified, inform State, regional, or local authorities regarding these programs and their limitations; establish request and response procedures for their use, considering policy, authority, and funding arrangements; and, as feasible, embrace selected programs within State, regional, or local planning and exercises. Such an approach will allow planners across all levels of government to leverage existing communications infrastructure, as well as consolidate efforts to concentrate on the most cost-effective solutions and benefit from any economies of scale. The President should further:
 - Direct the Office of Management and Budget (OMB) to continue to support FEMA's planning for the provisioning of deployable communications packages through pre-positioned, nationwide MERS, as well as overall FEMA efforts to investigate and integrate new emergency communications technologies in response activities.
 - Direct FEMA to investigate the use of DOD aerial unmanned vehicles to provide tactical communications capabilities over a broad geographic region.
 - Coordinate and utilize DOD expertise to provide technical advice in the area of airlift transport in the joint Government-private sector planning outlined above, and assess

⁴⁹ Widespread telecom disruption following the March 11, 2011, earthquake and tsunami in Japan made satellite links typically used for entertainment an important source of emergency communications in some areas. In the days immediately following the disaster, the International Telecommunications Union shipped 78 satellite telephones equipped with GPS terminals for search-and-rescue personnel to use, and an initial 37 Broadband Global Area Network terminals. See "Rural Satellite Services Helping Urban Japan," *Aerospace Daily & Defense Report*, March 21 2011.

whether NORTHCOM capabilities might be incorporated into FEMA support missions.

3.3 Scenario 3: Cyber Attack

3.3.1 Issue

In the following cyber attack scenario, a previously unidentified flaw, or “bug,” in a major router or router family is exploited in such a way that the edge of the Internet is affected rather than the Internet’s core. The scenario assumes that the impacted router is the last one owned by an ISP just before the circuit enters the customer’s premise, rather than the customer’s own equipment. The scenario also assumes that the vulnerability is only present in one router family by a specific major vendor, but is not necessarily present in other router families by the same vendor, or in routers built by other vendors. Finally, while a botnet is used as the distribution mechanism for this hypothetical attack, botnets themselves are not the issue that this scenario addresses.⁵⁰

3.3.2 Scenario

A bug in a major router manufacturer's software was discovered by a research team with close ties to a Foreign Intelligence Service (FIS). This bug causes all versions of the vendor's router operating system to mark all interfaces “down” when a special set of packets transit any interface. Fortunately, the packets are not forwarded once received and parsed; since all interfaces are “down” the out-going interfaces are unable to send packets. Before the vendor was notified, a member of the research team provided the vulnerability to an agent of the FIS. The FIS was able to duplicate the vulnerability and quickly developed workable exploit code. The FIS then “rented” several botnets and loaded the exploit code onto millions of infected machines worldwide. At a coordinated time, all of the infected machines simultaneously created the special packets needed to exploit the vulnerability and sent them to random locations across the Internet.

3.3.3 Impacts

A severe botnet attack, as in this scenario, could disrupt certain inter-network-based communications within minutes. Botnets targeting the edge of the Internet would exploit vulnerabilities in routers that connect organizations to it, but would have minimal effect on the “core” routers. The attack would stop network interfaces and prevent routers from forwarding packets on all interfaces, thus interfering with all services that transit through routers at the Internet’s edge. These services include voice, data, and video capabilities.⁵¹ An incremental

⁵⁰ A similar technical situation existed in July and August 2003 with respect to vulnerabilities in Cisco’s Internetwork Operating System and Microsoft’s Windows Operating System. The Blaster Worm, released on August 11, 2003, could have used this attack vector to cause the same type of impact to users of Cisco’s routers. Technical details on the vulnerabilities are available at <http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml> and <http://www.microsoft.com/technet/security/bulletin/ms03-026.mspx>.

⁵¹ Internet routers could be carrying “non-Internet” traffic if that traffic is being tunneled through the Internet via a virtual private network (VPN) or similar cryptographic separation. However, even a VPN is technically “Internet traffic” while using the Internet so is not immune from Internet availability problems. It is possible, but not highly likely, that control of “non-Internet” switching systems might use the Internet as transport. For example, an engineer might use the Internet to connect into a router via an Internet-connected interface on that router, even

attack could have a more widespread impact than a single, simultaneous attack. As technicians work to respond to these outages, route flapping would occur, causing general instability in the highly converged network environment of 2015. Even flapping on 20-30 percent of routes could have a detrimental ripple effect across the entire Internet; this churn in the network would occur even if the attack only impacted one vendor's software.

3.3.4 Findings

Software vendors lack a reliable means of obtaining access to and distributing the necessary software fixes in the face of severe public Internet network isolation, but most service providers have multiple communications channels between their NOCs to isolate and resolve problems when in-band communications fail. The botnet's impact on edge routers and the services that transit through them is likely to cause major network isolation, making it difficult for vendors to distribute a software patch via the Internet to repair the downed routers. Although service providers may establish ad-hoc communications channels between NOCs to distribute information about outages and patches, widespread network isolation would make NOC-to-NOC and NOC-to-vendor cooperation difficult.

Network technicians and NOCs would require alternative communications channels that are independent of the infrastructure that the NOCs support. Although network technicians have many communications channels available for their use, the network isolation resulting from this scenario would likely impede coordination between technicians on mitigation activities. A converged 2015 network environment is likely to increase technicians' dependence on services that transit through the impacted edge routers as well as on technologies that may be connected to the routers, thereby having a significant impact on all available communications channels. Technicians may have other ad hoc, non-technology-based means of communicating with each other, such as in-person visits in regions where companies are geographically close, but the condensed attack timeframe would reduce the viability of these methods.

Network technicians would be challenged in quickly and accurately uncovering the cause of a widespread router outage. Identifying the technical cause of the attack and the impacted network traffic would be difficult, particularly if the incident happens quickly and without warning. A zero-day attack staged with several major botnets that simultaneously send specially crafted packets through edge routers, causing all interfaces to be marked as down, would frustrate the process of identifying and understanding the problem. Widespread network isolation would make information sharing very challenging. Fortunately, most service providers have the expertise and tools needed to identify the malicious traffic that is triggering the issue, but network isolation might prevent them from being able to exchange information between and within providers. Once a communications channel is available, technical information could be communicated to the vendors, which in turn could develop a patch or identify potential solutions to restore the affected routers. While attribution of the attack is important for national security or law enforcement purposes, determining the technical cause of the outage and developing a technical solution to restore the impacted routers would be service providers' priority effort.

though the router's other interfaces are used for a private IP network that does not connect to the Internet. From a technical perspective, MPLS or ATM switches could also be disrupted, which in turn disrupt the higher-level protocols passing through them. Furthermore, VoIP packets transit through an Internet router, even though they may terminate on both ends in an analog telephone.

Substantial variation in the expected timeframe for mitigating the effects of the attack and restoring services introduces a degree of uncertainty into any mitigation and response planning. The length of time required to mitigate the attack's impacts would vary depending on how long it takes vendors to identify the vulnerability being exploited and develop a software patch. Identifying and fixing the software problem could take vendors a day or more, depending on the exploit's design and sophistication. After the problem has been resolved, vendors could distribute a permanent patch within days, but this would again depend on the complexity of the problem and any additional dependencies identified in the software. The vendors' need to coordinate in the face of a wide-scale network outage would add to the complexity and uncertainty.

The Government's back-up communications systems predominantly support voice communications and are not as clearly defined with respect to data and video capabilities. To back-up essential services communications, the Federal Government has many alternative communications avenues that are either not connected to the public Internet or have minimal dependence on Internet services. However, most of these alternative communications channels are designed for voice communications. As video and data requirements increase, the Government may be unprepared to support these capabilities using current back-up systems immediately following an Internet incident. In addition, as the Government transitions to an all IP approach for voice, video, and data communications, these future networks will become more susceptible to issues that affect commercial routers on the public Internet. Existing back-up communications such as HF radio or dedicated copper/cable/fiber circuits will likely not support the high data rates needed to accommodate future NS/EP applications.

The Government has made efforts to develop out-of-band capabilities that would provide critical voice and data communications to Government and private sector stakeholders. One such capability, the Critical Infrastructure Warning Information Network (CWIN), is a network composed of 161 Government and private sector members.⁵² However, independent analysis suggests that no single DHS authority has responsibility for fostering relationships with CWIN members, impeding it from achieving its full operational value.⁵³ Previously, the Government funded and operated a separate capability for coordinating the restoration of the PSTN, known as the Alerting and Coordination Network (ACN), but this system has since been dismantled. The CWIN and ACN provide lessons learned that could serve as useful starting points for designing a robust capability optimized to coordinate responses to future attacks against future networks.

⁵² According to DHS, CWIN is "DHS' only survivable network, a critical communications platform not dependent on the Public Switch Network (PSN) or the public Internet that can communicate both data and voice information in a collaborative environment in support of infrastructure restoration. CWIN provides a survivable, dependable method of communication allowing DHS to communicate with other federal agencies, state and local government, the private sector, and international organizations in the event that primary methods of communication are unavailable." *DHS, Privacy Impact Assessment for the Critical Infrastructure Warning Information Network*, January 7, 2006.

⁵³ McManis and Monsalve Associates. *Critical Infrastructure Warning Information Network Need and Mission Risk Assessment Study: Interim CWIN Need and Mission Risk Assessment Report*. Prepared for DHS Office of Infrastructure Protection and Office of Cybersecurity and Communications, November 1, 2010.

The inter-carrier incident response process in 2015 would require a centralized coordination structure rather than ad hoc methods used today, which are based largely on personal and business relationships. To date, nearly all carriers and ISPs have relied on command and control structures within their companies' incident response procedures for determining how an incident is handled and how the company coordinates with other entities on mitigation activities. Recognizing the desire for a more formal, centralized coordination structure for cyber incident response that spans the public and private sectors, DHS is currently evolving processes and structures to improve public-private coordination on cyber incident handling via the publication of the *National Cyber Incident Response Plan (NCIRP)* and the creation of the NCCIC.⁵⁴

However, both structures are in their early stages of development and have unresolved questions as to the precise extent and nature of private sector involvement. Neither structure has been used to respond to a cyber incident of the scale proposed in this scenario, nor is it known whether a formal, coordinated approach to a large cyber incident would be more effective than the decentralized, ad hoc approach currently in use. Both of these initiatives were exercised during the Federal Government's 2010 Cyberstorm III National Level Exercise and showed that greater private sector involvement in the national incident handling process is imperative. In an effort parallel to the NCCIC's establishment, private sector Information Sharing and Analysis Centers (ISAC) conducted an entirely private sector information sharing, analysis, and collaboration pilot program in 2010, with a Phase 2 follow-on effort slated to begin in 2011. The pilot program sought to improve cyber detection, prevention, mitigation and response capabilities through creating enhanced situational awareness and a common operating view of the cyber domain. The Phase 2 follow-on activity, which furthers the integration of the private sector and public sector operational capabilities, should help inform the national downstream incident response capability.^{55,56}

Diversity in communications systems components, including software, hardware, networking paths, design approaches, and operational procedures, will increase resiliency to attacks that target specific technologies or operational procedures. A cyber incident that targets a specific vendor's equipment could be devastating if the Government is reliant on that specific vendor's equipment for key or critical functions. In this scenario, the attacker targeted and exploited a specific vulnerability in a specific router family. If the attack occurs in only one type of hardware or a specific version of software, then routers from other vendors or routers from the same impacted vendor that are running a different version of software would likely continue to operate. This phenomenon has occurred repeatedly with enterprise software, notably in office productivity software such as email, word processing, graphics, and Web browsers that are in widespread use across Government and industry. In most cases, loss of productivity due to faults in one software product could be mitigated by using other similar software, an effect that is characteristic of a "monoculture" situation in which only a single or very small number of choices exist. However, true diversity should encompass many product and service choices. Since diversity in products introduces new problems and costs, such as training and

⁵⁴ See Appendix E.

⁵⁵ NSTAC Cybersecurity Collaboration Task Force. *Report on the Outcomes and Lessons Learned from the Sector Operational Organization Cross-Sector Information Sharing, Analysis, and Collaboration Pilot Program*, January 19, 2011.

⁵⁶ See Appendix E.

interoperability complexities and increased cases of obsolescence, a balance is needed between using only one approach or product and maintaining a dozen or more different components and systems. This balance may differ for each organization depending on its unique needs. One organization may achieve sufficient diversity by ensuring two or more separate network paths into a building or campus, whereas a different organization may find that its diversity needs require different types of clients, operating systems, and application software within an office.⁵⁷

3.3.5 Scenario 3 Recommendations

The NSTAC recommends the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*:⁵⁸

- ❖ **Direct DHS to explore the viability of developing a separate “out-of-band” data network to support communications between carriers, ISPs, vendors, and additional CIKR owners and operators during a severe cyber incident that renders the public Internet unusable.** This capability should exist on a network connecting entities’ NOCs that is independent of the Internet. Its design, development, installation, operation, maintenance, and periodic exercises should be a Government project executed in coordination with commercial infrastructure stakeholders. Such a capability should also contemplate if and how to incorporate international partners.
- **Charge DHS with continuing to develop and test the NCIRP and with proceeding to implement the additional stages of the NCCIC, which will include greater private sector inclusion.** DHS should recognize that the rapidly changing technologies and threats in the cyber domain dictate that the NCIRP be constantly tested and updated in order to remain relevant. Additionally, DHS should work to more fully integrate the private sector into the NCCIC’s operations, including at higher levels of classification. The private sector may face legal, regulatory, and business competition hurdles before full integration can be achieved, but executive Government leadership can help industry overcome these issues. Strong private sector involvement in the Government’s cyber incident response planning and operations is essential for improving the resiliency of the Nation’s cyberspace backbone.
- ❖ **Direct that the appropriate Government certification and accreditation processes, such as the Defense Federal Acquisition Regulations System and the Defense Information Assurance Certification and Accreditation Process, verify the existence of sufficient vendor diversity both when acquiring equipment and when operating and installing a network.**

⁵⁷ For past NSTAC recommendations concerning diversity assurance capabilities, requirements, and best practices, see the *NSTAC Financial Services Task Force Report*, April 2004.

⁵⁸ Recommendations denoted by a symbol are those the NSTAC has deemed to be of highest priority to the President.

3.4 Scenario 4: Massive Internet Disruptions

3.4.1 Issue

The following scenario describes the impacts of a major disruption to the Internet DNS addressing and BGP routing systems. The core of the Internet, which constitutes traffic control mechanisms that enable the connection of edge systems, relies on both systems. The scenario assumes that the transport layer of the 2015 network remains dependent on the reliable operation of these systems, while the deployment of hybrid equipment in the public network creates potential dependencies across traditional Internet services and non-Internet communications functions. Appendix G contains detailed technical documentation of the systems referenced in the scenario.

The more widespread deployment of DNSSEC expected by 2015 will help resolve problems concerning compromised DNS data. The continued development of RPKI will also help protect BGP information, although not BGP itself, and could allow for new secure routing policies or other BGP security protocols that would help mitigate network vulnerabilities.

3.4.2 Scenario

Internet administrators notice that their BGP and DNS infrastructure show signs of anomalous activity beyond what is normally experienced on a daily basis. Over a period of a few weeks, several major Autonomous System (AS) operators report to the United States Computer Emergency Readiness Team (U.S. CERT) that the BGP routers connecting their AS' completely stopped routing for periods of a few seconds to several minutes, then worked fine for several hours before again seeing short-duration problems. Likewise, multiple DNS Top Level Domain (TLD) operators also report an increase in anomalous behavior in their authoritative and secondary name servers, and five of the thirteen DNS root server operators also reported similar issues. These types of attacks continue for several weeks and are noted as nuisances but have little effect on Internet operations. Eventually the problems disappear, and there is no attribution to the source(s) of the attacks. No changes are made in the operational procedures of the BGP router and DNS server owners. Several months later, wide-spread BGP outages covering about two-thirds of all peering and exchange points occur simultaneously and a significant portion of the commercial TLDs and the DNS roots are "unstable" as reported by the DNS community. While .gov and .mil do not appear to be targets, the Government's dependency on Internet services has caused network disruptions between Government organizations, inside the DOD's Non-classified Internet Protocol Router Network and of course between the DOD and the Defense Industrial Base.

3.4.3 Impacts

The scenario's disruptions to BGP and DNS would target the fundamental architecture of today's Internet and any devices that link to or utilize this architecture. Attacks to BGP and DNS would thus impact many communications that rely on the Internet. The scenario would cause immediate outages for some edge systems, with the scope of outages increasing over a period of hours. Widespread BGP outages may also interrupt traffic routing as end users attempt to connect to various services. The routes used for these connections may be disrupted between network nodes and the communications transport layer; a BGP disruption could thus inhibit

call/data completion. DNS and MPLS also both typically rely on BGP as an underlying connection establishment mechanism.

As VoIP services rely more and more on the IP and DNS protocols and infrastructure, a BGP or DNS failure would impact any VoIP connectivity provided via IP-based networks. A BGP failure would also disrupt video transmissions that are migrating to an IP-based infrastructure.

DNS Failure

Operators of DNS resolvers cache DNS responses, which initially minimize the outage's impact on edge systems. As cached responses expire, the ability of DNS resolvers to obtain updated responses may be degraded when a significant number of authoritative root servers and TLD servers are unreachable due to BGP outages impacting server accessibility. Resolvers will attempt to connect to any available server, which may increase DNS failures due to query failure or may have cascading effects that result in query volume overloading the capacity of operational servers.

The combination of DNS and BGP failures could have an immediate, widespread impact to end users. It could prevent end users from receiving critical security patches or vendors' updates, or result in misconnections by routing users to sites other than their intended destination.

3.4.4 Findings

Given the complexity of systemic interdependencies within the Internet, the effects and duration of the service outages would differ depending on an array of factors. Network technicians lack a clear understanding of the precise impacts and timeframe of a severe BGP and/or DNS failure. If BGP updates stopped, then updated route announcements would not be distributed and forwarding information loops could occur; if the route tables were poisoned through polluted or hijacked prefixes, then propagation of incorrect routing data could cause network instability or misconnections and potentially enable man-in-the-middle (MITM) attacks. Effects would also vary depending on the method or purpose of attack (distributed denial-of-service, MITM, etc). Service outages could range from hours to weeks or months, depending on the extent of the DNS and BGP instability.

Compromised routes could also limit the ability of root server operators and TLD registry operators to monitor or access their systems, complicating their efforts to detect, identify and isolate the attack, or apply any remediation controls. Additionally, they may be unable to push updates to their servers or patch vulnerabilities that are being exploited. An attack that affects the implementation of infrastructure protocols, including BGP and DNS, would require that vendors patch implementations, causing a longer disruption than if the routing experienced failure to service-specific routes or operators. Redundant and diverse application, operating system, network equipment, and service operations that are utilized today help mitigate the impact from this type of attack.

Network operators may be able to develop manual work-around processes to avoid or respond to the BGP disruptions, but small service providers might have less capability to tolerate and respond to these types of DNS and BGP disruptions due to economic and staffing limitations. In some specialized cases, service providers could also use other static or dynamic routing protocols, as an alternative to BGP, in scoped deployment models.

In the highly converged future network environment, many users would be unlikely to realize that some devices perform multiple functions that could be wholly impacted by a failure in just one function. Multi-service network elements that perform multiple functions, such as operating BGP while also switching phone calls, could be affected by the routing instability that would occur as a result of a BGP or DNS failure. Examples of such technologies are those performing both IP routing and MPLS virtual private networks (VPN). Telecommunications carriers in particular are unlikely to understand the full extent of their equipment's linkages to and dependence upon the public Internet's infrastructure. These critical interdependencies highlight the need for alternative communications capabilities that do not depend on switching systems reliant on BGP.

Increased virtualization, multi-central processing unit (CPU) hardware and new system architectures will be more common by 2015, providing the ability to partition platform components and minimize dependencies so as to potentially lessen the impact of a DNS or BGP failure or other system instability. Failures in BGP and DNS will impact the three sections of modern routing and switching systems, which includes the control plane, forwarding plane, and management plane. Where these planes are not sufficiently separated, a BGP disruption could affect the entire platform. Today, many carrier-grade routers isolate these planes and ensure a separate path to the routing subsystem from the user data forwarding plane. Some current equipment is also designed to separate the general purpose CPU function from the forwarding and switching capability so that the CPU could be saturated while leaving the packet switching capability intact. This multi-CPU hardware has the ability to assign and prioritize individual tasks to individual CPUs, which would lessen the impact of BGP and DNS disruptions. If one individual virtual machine is suffering BGP issues that are consuming memory or process cycles, a properly engineered multi-CPU or virtualized router will not allow that machine to cause disruptions in other virtual machines.

Routing and Switching System Planes

- 1. The control plane consists of signaling and routing protocols used to generate IP forwarding table information.***
- 2. The forwarding plane dictates how a device forwards data from source to destination (ingress and egress interfaces).***

Industry would require the ability to know to what degree the Internet is dependent on private networks or to what degree private networks and converged network services are protected and

*isolated from the collateral effects of BGP and DNS attacks on the Internet.*⁵⁹ Private networks and converged network services commonly share the same network substrate as the global Internet infrastructure. The Internet itself is a loosely interconnected network of networks with no single administrative control and many global participants. The security and stability of network services, such as the routing system and DNS, rely on sufficient capacity and stability of the networks' interconnections. The dependencies introduced by this substrate may not be intuitively obvious to the operators. Private networks and converged network services may be vulnerable to attacks or instability in the routing system or DNS even where those services may be contained within a single participant's network. The shift to cloud computing may allow for more virtual networking that is constructed to the customer's specifications, but the extent of this customer-specific design is uncertain. The potential public network vulnerability from cloud based private networks is dependent on the degree that a particular cloud is isolated from the Internet.

Additionally, the Internet routing systems and DNS are vulnerable to instability and threats originating from private networks. Many operators of root and TLD DNS servers protect their services from zero-day attack vulnerabilities by applying the principle of diversity, which entails architecting services that avoid common system dependencies or fate-sharing. Operators consider upstream vulnerabilities not only within their own environment, but also from the network layer interconnections to the DNS servers. This approach has been effective for protecting infrastructure within the immediate control of the service operators and with adjacent networks.

During core network incidents, the ability to coordinate recovery operations requires the availability of autonomous networks independent of the public Internet. The impact of BGP and DNS disruptions would hinder normal communications that rely on the public Internet. Effective collaboration and coordination across Government agencies and core infrastructure providers to restore a system is contingent on access to a communications network that is independent of the public Internet. In order to avoid shared dependencies, the technical design of such a network must be based on the same protocols and autonomy objectives while still using discrete systems. Even should such a system meet these design specifications, autonomous networks may face difficulty verifying to their customers their degree of network isolation, especially given that physical diversity does not implicitly yield logical diversity. Moreover, even in an entirely closed private network, interactions with the customer could introduce misbehavior that could influence the router at the edge and still disrupt traffic.

The principle of agility can only be achieved by regularly exercising the network's processes and procedures under a full range of scenarios with a wide range of cross-sector participants. Government agencies and infrastructure providers must be prepared to coordinate the recovery of core network services when the disruption limits accessibility to primary communications systems. Prior to the recovery operation, these organizations must have defined their roles and responsibilities, rights and obligations for data collection and use, and the processes and procedures for operating on an alternate network.

⁵⁹ In this context, the term "private network" describes a network that uses private IP address space, following the standards set by RFC 1918 and RFC 4193. These networks are characterized as private because they are not globally delegated and the IP packets they address cannot be transmitted onto the public Internet.

Today, there exists no functional tie-in between what Internet number registries, such as the Regional Internet Registries, allocate and what is actually routed on the Internet. While protocols such as SBGP and SoBGP have been proposed, today's routing system lacks inherent object-level security. Cryptographic verification mechanisms do not currently exist in BGP to validate the integrity of a route advertisement, and no secure framework to attest that a particular AS has been authorized to either originate or provide transitive connectivity to a particular Internet number resource, such as an AS or a set of IP addresses. The concern therefore is that any user operating an AS could assert reachability for any set of address space via BGP in the global routing system. Operators are then individually responsible for determining whether the advertised destinations are legitimate, as well as precisely who "holds" which number resources and what ingress routing policy should be applied to a BGP peer on a per-prefix and per-path basis. Several initiatives are underway to provide resource certification for Internet numbers, including RPKI.⁶⁰

Current high-level policymaking fora that address the Internet and technology policy issues pertaining to this scenario are insufficiently inclusive, improperly structured, and lack technical rigor. Existing fora and meetings are infrequent, brief, highly structured, and generally only encourage the most senior executives in Government and industry to engage in discussion. These limitations inhibit rich discussion of emergent, complex, or highly technical issues, including balanced evaluation of alternatives involving significant time, resources and impact. While there are some fora that support detailed examination of narrow aspects of critical technology—such as the annual, three-day Biometrics Consortium Conference—none engages with sufficient breadth across the entire potential space of interest to NS/EP communications. A more effective model would be a body that is created, populated, guided and maintained in recognition of the scope, depth, complexity and importance of world-changing technology developments in the information technology and communications policy arenas.

3.4.5 Scenario 4 Recommendations

The NSTAC recommends the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*:⁶¹

- ❖ **As recommended under Section 3.3.5, direct DHS to explore the viability of developing a separate out-of-band data network to support communications between carriers, ISPs, vendors, and additional CIKR owners and operators during a severe cyber incident that renders the public Internet unusable.** (See Section 3.3.5 for complete recommendation.)
- ❖ **Direct the Office of Science and Technology Policy (OSTP), in coordination with DOD, DHS, and other appropriate departments and agencies, to establish a single, high-level forum for ongoing technical and policy dialogue between Government and key industry service providers, focused on issues of potentially strategic**

⁶⁰ See Appendix G for additional information on resource certification.

⁶¹ Recommendations denoted by a symbol are those the NSTAC has deemed to be of highest priority to the President.

consequence in the foreseeable-future timeframe. This dialogue must be comprehensive, technically rigorous, and open-ended, with sufficiently broad scope to address current and emergent aspects of interdependency, system/process convergence, new hardware capabilities, and the evolution of private networks, inter alia. Such a dialogue is intended to complement, not replace, existing fora addressing tactical aspects of network operations.

- **Direct DHS to institute an expanded program of national-level exercises that include Government agencies and infrastructure providers.** These exercises should be designed to:
 - Broaden the base of organizational engagement in Government and industry;
 - Progressively increase the scope, complexity and potential-consequence scenarios of such exercises, to permit further refinement, testing and exercising of plans and procedures by both Government and industry;
 - Identify and detail systemic effects and interdependencies of all kinds; and
 - Support development of and continued exercising of out-of-band and autonomous coordination capabilities and procedures to restore Internet infrastructure services.

- ❖ **Encourage OMB to continue funding for departments' and agencies' development of security enhancements within the core infrastructure, such as Internet number resource certification (e.g., RPKI).** This should be achieved via focused investment in applied research and development projects directly relevant to this scenario and the technology processes it addresses.

4.0 RECOMMENDATIONS

The following is a consolidation of recommendations under the four scenarios, presented in sections 3.1-3.4. The NSTAC deems those recommendations denoted by a symbol are of highest priority for the President. The NSTAC recommends the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*:

Scenario 1: Multiple Terrorist Attacks in the National Capital Region

- ❖ **Request that Congress fund DHS' priority services efforts to continue industry and Government collaboration and to ensure that advanced NS/EP communication services are operational when needed.** Historically, the Government has funded commercial telecommunications efforts to develop, maintain, and upgrade GETS and WPS, as the costs to provide these services to their small user base would be prohibitive to individual companies. But these programs face an uncertain future due to insufficient funding. In particular, funding constraints may undermine the development of new capabilities or the ability of priority services to meet the needs of additional public safety users. In fiscal year 2008, the Administration sought \$52 million to perform research and

development of next generation priority services programs and received only \$21 million from Congress.⁶² The President should make clear to Congress that, in the absence of additional funding between 2010 and 2015, the only incremental additions to priority services will include VoIP applications. Congressional funding should ensure that DHS develops and deploys future IP video and data priority services.⁶³

- **Encourage DHS to file comments with the FCC in its appropriate public safety broadband dockets.**⁶⁴ In its filed comments, DHS should recommend that the FCC continue working closely with industry as it builds the nationwide interoperable public safety mobile broadband network, as recommended in the FCC's *National Broadband Plan*. This will aid in the development of spectrum management policies that ensure spectrum capacity is properly allocated among users, available networks, and technologies.
- **Encourage DHS to petition the FCC to issue a declaratory ruling to confirm that network service providers may lawfully offer IP-based priority access services to NS/EP authorized users.**⁶⁵ Service providers must maintain the authority to ensure that networks remain capable of providing priority communications for NS/EP authorized users in the future.⁶⁶
- **Encourage Congress to continue funding DHS' Science and Technology Directorate to pursue interoperability solutions for emergency responders and ensure that DHS allocates the funds to particular interoperability programs.** For example, a DHS contract in 2008 led a private contractor to develop the first-ever multiband radio that allows police officers, firefighters, and emergency medical service personnel to

⁶² Government Accountability Office. *Emergency Communications: National Communications System Provides Programs for Priority Calling, but Planning for New Initiatives and Performance Measurement Could be Strengthened*. Report GAO-09-822. August 2009.

⁶³ In addition, the November 2008 NSTAC Report to the President on National Security and Emergency Preparedness Internet Protocol-Based Traffic recommended that the President establish a policy requiring Federal departments and agencies to: 1) ensure their enterprise networks are properly designed and engineered to handle high traffic volume; 2) manage traffic through quality of service programming in its routers to prioritize traffic, including NS/EP traffic; and 3) expand the use of managed service agreements to provision NS/EP services within the new IP-based environment. The report also recommended that the President require Federal departments and agencies to remain actively involved in standards development of priority services on IP-based networks by supporting efforts to provide adequate funding to develop timely solutions across all technology platforms and committing appropriate resources to actively participate in and lead the global standards bodies' efforts to address NS/EP IP-based priority services.

⁶⁴ These dockets include WT Docket No. 06-150: *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229: *Amendment of Part 90 of the Commission's Rules*, and WP Docket No. 07-100: *Third Report and Order and Report and Fourth Further Notice of Proposed Rulemaking*.

⁶⁵ Without FCC permission, priority services would violate Section 202(a) of the *Communications Act of 1934*, as priority services constitute preferential treatment by carriers. In 2000, the FCC issued an order establishing that the priority services offered to NS/EP authorized users were *prima facie* lawful under the *Communications Act*. Consistent with this ruling, the FCC should further confirm that the same is true with regard to IP-based priority access services offered by IP-based providers to NS/EP users.

⁶⁶ The NSTAC made a similar recommendation in its 2008 *Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic*. Such a petition could be filed in the FCC's open docket, WCB Docket No. 04-36: *IP-Enabled Services*.

communicate with partner agencies using a single radio capable of operating on multiple radio bands.⁶⁷ DHS should continue funding this and similar initiatives.

- ❖ **Direct DHS to build future alerting capabilities that consider all potential multi-platform technologies, to ensure that the public can receive timely and accurate alerts, warnings, and critical information about emergencies regardless of the communications technologies used.** When constructing or evolving new alerting systems, system designers should consider all potential multi-platform technologies, but must also deconflict alerting systems and potentially consider prioritizing which of the alerting systems take precedence over others in times of congestion. Alerting systems in the converged 2015 environment should be engineered and tested regularly, both individually and in parallel with other systems, to ensure system functionality and receipt of messages.
- ❖ **To accelerate efforts to fulfill DHS' NCCIC mission and, to ensure that it is fully operational by the 2015 timeframe, direct DHS to accomplish the following as soon as possible:**
 - Leverage the success of the existing NCCIC incident response mechanisms by ensuring sufficient funding levels are dedicated to the mission;
 - Direct the rapid expansion of personnel resources, including training, to guarantee that the cyber and communications incident response mechanisms are absolutely viable and fully mission capable by 2015.

Scenario 2: Catastrophic Earthquake in the San Francisco Bay Area

- **Direct DHS and other appropriate departments and agencies to support collaboration between State and local government and industry to determine the most effective and appropriate mechanisms for restoring critical communications services.** In particular:
 - Encourage the development and funding of large-scale, tactical response support capabilities that incorporate the resources and expertise of multiple carriers. Given the rapidly evolving nature of networks and the services they provide, any support strategy should be consistently updated while also remaining available should the need arise. Given the potential cost of large-scale support, it may be appropriate to conduct this planning at the State or regional level. If planning is implemented at the regional level, transport support associated with these strategies may need to be provided at the Federal level.
 - Once the appropriate mechanisms have been selected, support the development of protocols and contracts at the State or regional level to ensure the resources are available when needed.
 - Since continuation of essential, critical services delivered by both Government and the private sector CIKR can be better assured with ready access to fuel, direct that States assess the projected fuel needs to sustain critical services for 30 days, and

⁶⁷ DHS Science and Technology Directorate Press Release. "DHS Launches Multiband Radio Project," February 27, 2008.

incorporate contractual arrangements with fuel providers to ensure the availability of those fuels within 48 hours to an impacted zone.

- Bolster existing but under-funded programs that aim to pre-position emergency power generation equipment at critical facilities and sites and replace above-ground electric and telecommunications infrastructure with underground structures.⁶⁸

❖ **Direct DOD and other appropriate departments and agencies to enhance the utility of and reliance upon satellite systems to provide alternate communications when terrestrial-based communications infrastructure is impaired.** To ensure ubiquitous, redundant, and resilient disaster communications, satellite-based communications should become a required component of critical communications networks. In particular, the President should direct the appropriate department or agency to:

- Investigate the possibility of investing in additional pre-positioned, leased satellite capacity to restore commercial communications transport in the event of an emergency and ensure that appropriate satellite ground equipment is in place to augment satellite capacity and equipment.
- Expand Federal interoperability grant funding and guidance to encourage NS/EP entities to acquire mobile satellite communications equipment and ensure that critical staff are educated and trained in satellite use. Emergency response drills and exercises that include the use of mobile satellite communications should also be mandated.
- Modify public safety communications grant funding programs to require that State interoperable communications plans place greater emphasis on satellite communications generally to provide resiliency during a disaster.⁶⁹

• **Direct FEMA, in coordination with other DHS agencies and DOD, to identify, support, and integrate relevant tactical emergency communications support capabilities across the Federal Government.** When such capabilities are identified, inform State, regional, or local authorities regarding these programs and their limitations; establish request and response procedures for their use, considering policy, authority, and funding arrangements; and, as feasible, embrace selected programs within State, regional, or local planning and exercises. Such an approach will allow planners across all levels of government to leverage existing communications infrastructure, as well as consolidate efforts to concentrate on the most cost-effective solutions and benefit from any economies of scale. The President should further:

- Direct the Office of Management and Budget (OMB) to continue to support FEMA's planning for the provisioning of deployable communications packages through pre-

⁶⁸ Association of Bay Area Governments. *Taming Natural Disasters: Multi-Jurisdiction Local Hazard Mitigation Plan for the San Francisco Bay Area*. 2010 Update.

⁶⁹ Widespread telecom disruption following the March 11, 2011, earthquake and tsunami in Japan made satellite links typically used for entertainment an important source of emergency communications in some areas. In the days immediately following the disaster, the International Telecommunications Union shipped 78 satellite telephones equipped with GPS terminals for search-and-rescue personnel to use, and an initial 37 Broadband Global Area Network terminals. See "Rural Satellite Services Helping Urban Japan," *Aerospace Daily & Defense Report*, March 21 2011.

positioned, nationwide MERS, as well as overall FEMA efforts to investigate and integrate new emergency communications technologies in response activities.

- Direct FEMA to investigate the use of DOD aerial unmanned vehicles to provide tactical communications capabilities over a broad geographic region.
- Coordinate and utilize DOD expertise to provide technical advice in the area of airlift transport in the joint Government-private sector planning outlined above, and assess whether NORTHCOM capabilities might be incorporated into FEMA support missions.

Scenario 3: Cyber Attacks

- ❖ **Direct DHS to explore the viability of developing a separate “out-of-band” data network to support communications between carriers, ISPs, vendors, and additional CIKR owners and operators during a severe cyber incident that renders the public Internet unusable.** This capability should exist on a network connecting entities’ NOCs that is independent of the Internet. Its design, development, installation, operation, maintenance, and periodic exercises should be a Government project executed in coordination with commercial infrastructure stakeholders. Such a capability should also contemplate if and how to incorporate international partners.
- **Charge DHS with continuing to develop and test the NCIRP and with proceeding to implement the additional stages of the NCCIC, which will include greater private sector inclusion.** DHS should recognize that the rapidly changing technologies and threats in the cyber domain dictate that the NCIRP be constantly tested and updated in order to remain relevant. Additionally, DHS should work to more fully integrate the private sector into the NCCIC’s operations, including at higher levels of classification. The private sector may face legal, regulatory, and business competition hurdles before full integration can be achieved, but executive Government leadership can help industry overcome these issues. Strong private sector involvement in the Government’s cyber incident response planning and operations is essential for improving the resiliency of the Nation’s cyberspace backbone.
- ❖ **Direct that the appropriate Government certification and accreditation processes, such as the Defense Federal Acquisition Regulations System and the Defense Information Assurance Certification and Accreditation Process, verify the existence of sufficient vendor diversity both when acquiring equipment and when operating and installing a network.**

Scenario 4: Massive Internet Disruptions

- ❖ **As recommended under Section 3.3.5, direct DHS to explore the viability of developing a separate out-of-band data network to support communications between carriers, ISPs, vendors, and additional CIKR owners and operators during a severe cyber incident that renders the public Internet unusable.** (See Section 3.3.5 for complete recommendation.)

- ❖ **Direct the Office of Science and Technology Policy (OSTP), in coordination with DOD, DHS, and other appropriate departments and agencies, to establish a single, high-level forum for ongoing technical and policy dialogue between Government and key industry service providers, focused on issues of potentially strategic consequence in the foreseeable-future timeframe.** This dialogue must be comprehensive, technically rigorous, and open-ended, with sufficiently broad scope to address current and emergent aspects of interdependency, system/process convergence, new hardware capabilities, and the evolution of private networks, inter alia. Such a dialogue is intended to complement, not replace, existing fora addressing tactical aspects of network operations.
- **Direct DHS to institute an expanded program of national-level exercises that include Government agencies and infrastructure providers.** These exercises should be designed to:
 - Broaden the base of organizational engagement in Government and industry;
 - Progressively increase the scope, complexity and potential-consequence scenarios of such exercises, to permit further refinement, testing and exercising of plans and procedures by both Government and industry;
 - Identify and detail systemic effects and interdependencies of all kinds; and
 - Support development of and continued exercising of out-of-band and autonomous coordination capabilities and procedures to restore Internet infrastructure services.
- ❖ **Encourage OMB to continue funding for departments' and agencies' development of security enhancements within the core infrastructure, such as Internet number resource certification (e.g., RPKI).** This should be achieved via focused investment in applied research and development projects directly relevant to this scenario and the technology processes it addresses.

APPENDIX A:

**PARTICIPANT LIST
TASK FORCE MEMBERS, GOVERNMENT PERSONNEL,
AND OTHER PARTICIPANTS**

APPENDIX A: PARTICIPANT LIST

TASK FORCE MEMBERS, GOVERNMENT PERSONNEL, AND OTHER PARTICIPANTS

TASK FORCE MEMBERS

Rockwell Collins, Incorporated
Teledesic, LLC
AT&T, Incorporated

CSC
Juniper Networks, Incorporated
Qwest Communications International, Incorporated
Raytheon Company
Sprint Nextel
Telcordia Technologies, Incorporated
VeriSign, Incorporated
Verizon Communications, Incorporated

Mr. Ken Kato, Chair
Mr. Doug Carter, Vice Chair
Ms. Julie Thomas
Ms. Liz Gunn
Mr. Guy Copeland
Mr. Jim Bean
Ms. Kathryn Condello
MG Bill Russ
Ms. Allison Growney
Ms. Louise Tucker
Mr. Bill Gravell
Mr. Michael Hickey

OTHER PARTICIPANTS

AT&T, Incorporated

Bank of America Corporation

Blue Ridge Networks
The Boeing Corporation
Clearview Wireless, LLC

CSC

Hughes Network System, LLC
Intelsat General
Microsoft Corporation

Motorola Corporation
National Cable and Telecommunications Association
Qwest Communications International, Incorporated

Ms. Rosemary Leffler
Mr. John Nagengast
Mr. Jacobus van der Merwe
Mr. Nilesh Jadav
Mr. Larry Schaeffer
Mr. Michael Tracy
Ms. Joan Grewe
Mr. Bob Steele
Mr. Scott Hilliard
Mr. Jason Murphy
Mr. Kevin Considine
Mr. Jay Estep
Mr. Rajeev Gopal
Ms. Karen Yasumura
Mr. Pat Arnold
Mr. Bryan Casper
Ms. Monika Machado
Ms. Cheri McGuire
Mr. Mike Alagna
Mr. Andy Scott
Mr. Chris Garner
Mr. Anil Simlot
Mr. Douglas Tiarks

Raytheon Company

Mr. Andrew White
Mr. James Jester
Mr. Brian Markus
Mr. Frank Newell
Mr. Joel Stanley
Mr. Sam Black
Ms. Patricia Cooper
Mr. Jim Holgerson
Mr. Arun Handa
Mr. Dennis Mok
Mr. Bob Mayer
Mr. Tom Soroka
Mr. Matt Larson
Mr. Danny McPherson
Mr. Joe Waldron
Mr. Heath Henderson
Mr. Mark Krause
Mr. Marcus Sachs

Satellite Industry Association

Sprint Nextel
Telcordia Technologies, Incorporated

US Telecom Association

VeriSign, Incorporated

Verizon Communications, Incorporated

GOVERNMENT PERSONNEL

Department of Defense

Maj. Eric Dixon
Ms. Hilary Morgan
Mr. Joe Wassel
Mr. Rick Bourdon
Ms. Sue Daage
Mr. Mike Echols
Ms. Helen Jackson
Mr. Thomas Murphy
Mr. Frank Suraci
Mr. Andy Ozment
Mr. Eric Panketh
Mr. Larry Zelvin
Mr. David Bray
Mr. John Healy
Ms. Jennifer Manner
Mr. Eric Edwards
Mr. Charles Hoffman

Department of Homeland Security

Executive Office of the President

Federal Communications Commission

Federal Emergency Management Agency

APPENDIX B:

ACRONYMS

APPENDIX B: ACRONYMS

4G	Fourth Generation
ACN	Alerting and Coordination Network
AS	Autonomous System
ASN	Autonomous System Numbers
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BOTNET	Robot Network
C&A	Certification and Accreditation
CA	Certification Authority
CDMA	Code Division Multiple Access
CIKR	Critical Infrastructure and Key Resources
CMRS	Commercial Mobile Radio Services
CONPLAN	Concept of Operations Plan
COW	Cells-on-Wheels
CPU	Central Processing Unit
CRL	Certificate Revocation Lists
CRTF	Communications Resiliency Task Force
CWIN	Critical Infrastructure Information Warning Network
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DNS	Domain Name System
DNSSEC	DNS Security Extensions
DSLAM	Digital Subscriber Loop Access Multiplexer
DOD	Department of Defense
E911	Emergency 911
EE	End Entity
EOP	Executive Office of the President
ESF	Emergency Services Function
EWP	Emergency Wireless Protocol
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIS	Foreign Intelligence Service
GBPS	Gigabit per second
GETS	Government Emergency Telecommunications Service
GPS	Global Positioning System
HF	High Frequency

IANA	Internet Assigned Numbers Authority
IdM	Identity Management
IETF	Internet Engineering Task Force
IGP	Internet Gateway Protocol
IMS	Internet Protocol Multimedia Subsystem
IP	Internet Protocol
IPv4	IP version 4
IPv6	IP version 6
IRR	Internet Routing Registry
ISAC	Information Sharing Analysis Center
ISP	Internet Service Provider
JCC	Joint Coordinating Center
KIDNS	Key in Domain Name Server
LAN	Local Area Network
LIR	Local Internet Registry
LTE	Long-Term Evolution
MERS	Mobile Emergency Response Support
MHZ	Megahertz
MITM	Man-in-the middle
MOA	Memorandum of Agreement
MPLS	Multi-Protocol Label Switching
NANOG	North American Network Operations Group
NAT	Network Address Translation
NCC	National Coordinating Center
NCCIC	National Communications and Cybersecurity Integration
NCIRP	<i>National Cyber Incident Response Plan</i>
NCR	National Capital Region
NCS	National Communications System
NG911	Next Generation 911
NIPRNET	Non-classified Internet Protocol Router Network
NIR	National Internet Registries
NOC	Network operations center
NORTHCOM	U.S. Northern Command
NRF	National Response Framework
NS/EP	National security and emergency preparedness
NSS	National Security Staff
NSTIC	<i>National Strategy for Secure Online Transactions</i>
OES	Office of Emergency Services

PSAP	Public Safety Answering Points
PSTN	Public Switched Telephone Network
RIR	Regional Internet Registry
RIPE NCC	RIPE Network Coordination Centre
RPKI	Resource Public Key Infrastructure
RPSS	Routing Policy System Security
SBGP	Secure BGP
SFI	Settlement free interconnection
SHARES	Shared Resources High Frequency Radio Program
SIDR	Secure Inter-domain Routing
SIP	Session Initiation Protocol
SME	Subject Matter Expert
SOBGP	Secure Origin BGP
SONET	Synchronous Optical Networking
SS7	Signaling System 7
TLD	Top Level Domain
UAV	Unmanned Aerial Vehicle
US-CERT	United States Computer Emergency Readiness Team
USSTRATCOM	United States Strategic Command
VoIP	Voice over Internet Protocol
WiMax	Wireless Interoperability for Microwave Access
WPS	Wireless Priority System

APPENDIX C

GLOSSARY⁷⁰

⁷⁰ The definitions for the terms contained in this glossary came primarily from the following sources: *McGraw-Hill Dictionary of Computing & Communications*; *Microsoft Computer Dictionary*, Fifth Edition; *Oxford Dictionary of Computing*, Sixth Edition; and *Newton's Telecom Dictionary*. Definitions were also drawn from the following Web sites: www.dhs.gov; www.fcc.gov; www.ietf.com; www.ncs.gov; www.nist.gov; and www.pcmag.com.

APPENDIX C: GLOSSARY

4G: The fourth generation (4G) of cellular wireless standards, succeeding third and second generation standards. 4G is designed to increase data transfer speeds for mobile wireless communications, facilitating increased mobility and new data services.

Alerting and Coordination Network: An emergency voice communications network connecting telecommunications service providers' Emergency Operations Centers and Network Operations Centers (NOC) to support national security and emergency preparedness telecommunications network restoration coordination, transmission of telecommunications requirements and priorities, and incident reporting when the Public Switched Network is inoperable, stressed, or congested.

Application: A software program that carries out some useful task. Database managers, spreadsheets, communications packages, graphics programs and word processors are all applications.

Asynchronous System: A system that operates under distributed control, with concurrent hardware components communicating and synchronizing on channels.

Asynchronous Transfer Mode: A high speed packet-switching technology based on cell-oriented switching and multiplexing that uses 53-byte packets to transfer different types of information, such as voice, video, and data over the same communications network at different speeds.

Bandwidth: A measure of the amount of data that can travel a communications path in a given time, usually expressed as thousands of bits per second or millions of bits per second.

Border Gateway Protocol: A Gateway Protocol that routers and other non-router devices employ in order to exchange appropriate levels of routing information.

Botnet: A collection of computers compromised by malicious bots controlled by the same intruder. Bots are automated software programs that can execute commands.

Broadband: A communications band with a wide range of frequencies that can carry multiple messages at a time.

Cache: A small, fast storage buffer integrated in the central processing unit of some large computers, which stores recently-used information for easy accessibility.

Cells-on-Wheels: Mobile cellular towers that are used temporarily until a permanent tower is operational.

Cellsite On Wheels: A trailer with antenna and transmitting/receiving hardware used to provide temporary cell phone service in emergencies, special events, remote testing and repair, until a permanent tower can be erected.

Central Processing Unit: The principal operating component of a computer, containing the circuits to interpret and execute instructions.

Circuit Switching: The method of providing communication services through a switching facility, either from local users or other switching facilities.

Cloud Computing: An Internet-based or intranet-based computing environment wherein computing resources are distributed across the network (i.e., the cloud) and are dynamically allocated on an individual or pooled basis and are increased or reduced as circumstances warrant to handle the computing task at hand.

Code Division Multiple Access (CDMA): A broad spectrum technology for cellular networks based on the Interim Standard-95 from the Telecommunications Industry Association.

Commercial Mobile Radio Service: A Federal Communications Commission (FCC) designation for any carrier or licensee whose wireless network is connected to the public switched telephone network and/or is operated for profit.

Control Plane: Signaling and routing protocols used to generate Internet Protocol (IP) forwarding table information.

Convergence (fixed-mobile): The point at which all the Internet-working devices share a common understanding of the routing topology.

Critical Infrastructure Information Warning Network: A network that provides a survivable, dependable method of communication allowing the Department of Homeland Security to communicate with other Federal agencies, State and local governments, the private sector, and international organizations in the event that primary communication methods are unavailable.

Cybersecurity: The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and users' assets.

Denial of Service: A computerized assault, usually planned, that seeks to disrupt access to the Internet.

Domain Name System (DNS): A distributed database system used in the Internet and on private Intranets for translating names of host computers into addresses. The DNS also allows host computers not directly on the Internet to have registered names in the same style.

Domain Name System Security Extensions (DNSSEC): A set of extensions to the DNS protocol that add security features that protect against certain kinds of attacks, such as DNS cache poisoning.

Domain Name System Top Level Domain (TLD): The right-most label in a domain name, and the highest tier of the tree-like DNS structure. Particular organizations are responsible for operating TLDs.

Forwarding Plane: The routing and switching plane that dictates how a device forwards data from source to destination (ingress and egress interfaces).

Gateway: An entrance or exit into a communications network. Technically, a gateway is an electronic repeater device that intercepts and steers electrical signals from one network to another. Generally, the gateway includes a signal conditioner which filters out unwanted noise and controls characters. In data networks, gateways are typically a node on both two networks that connects two otherwise incompatible networks.

Global Positioning System: A constellation of 24 orbiting satellites that allow for determining precise position anywhere on earth to within one meter's accuracy, both height and longitude/latitude.

Global System for Mobile Communications: A set of standards for second generation cellular networks currently maintained by the 3rd Generation Partnership Project (3GPP).

High-Frequency Radio: A radio that operates on radio spectrum bands of 3 to 30.

Identity Management: The structured creation, capture, syntactical expression, storage, tagging, maintenance, retrieval, use and destruction of identities by means of diverse arrays of different technical, operational, and legal systems and practices.

Information Sharing and Analysis Center (ISAC): Facilitates voluntary collaboration and information sharing among Government and industry in support of Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions* and the national critical infrastructure protection goals of Presidential Decision Directive 63, *Protecting America's Critical Infrastructures*. Gathers information on vulnerabilities, threats, intrusions, and anomalies from multiple sources, and performs analysis with the goal of averting or mitigating impacts upon the telecommunications infrastructure.

Internet: A collective electronic network of computers and computer networks which are inter-connected throughout the world.

Internet Assigned Numbers Authority: The organization responsible for all "unique parameters" on the Internet, including IP addresses. Each domain name is associated with a unique IP address and a numerical name consisting of four blocks of up to three digits each, e.g. 204.146.46.8, which systems use to direct information through the network.

Internet Core (core gateway): Consists of the primary routers in the Internet.

Internet Edge: The network infrastructure that provides connectivity to the Internet and that acts as the gateway for the enterprise to the rest of cyberspace. The Internet edge serves other building blocks that are present in a typical enterprise network.

Internet Protocol: The set of standards responsible for ensuring that data packets transmitted over the Internet are routed to their intended destinations.

Internet Protocol Multimedia Subsystem (IMS): An open, standardized, “operator friendly,” Next Generation Networking multi-media architecture for mobile and fixed IP services. IMS is a VoIP implementation based on a 3GPP variant of SIP, and runs over standard IP. It is used by telecom operators in integrated networks to offer network controlled multimedia services,

Internet Protocol Version 4: The current version of IP, which is the fundamental protocol on which the Internet is based; the address field is limited to 32 bits.

Internet Protocol Version 6 (IPv6): The new protocol designed to replace and enhance the present protocol, IPv4. IPv6 has 128-bit addressing, auto configuration, new security features and supports real-time communications and multicasting.

Land Mobile Radio: Consists of various services utilizing regularly-interacting groups of base, mobile, portable, and associated control and relay stations for private radio communications by eligible users.

Local Area Network: A communications network connecting various hardware devices together within a building by means of a continuous cable, an in-house telephone voice-data system, or a radio-based system.

Long-Term Evolution (LTE): The next-generation 4G technology for both Global System for Mobile Communications and CDMA cellular carriers. Approved in 2008 with download speeds up to 173 Mbps, LTE was defined by the 3GPP in the 3GPP Release 8 specification.

Malware: Software created and distributed for malicious purposes, such as invading computer systems in the form of viruses, worms, or other plug-ins and extensions that mask other destructive capabilities.

Man-in-the-Middle Attack: A form of attack in which the intruder intercepts messages between parties in a public key exchange.

Management Plane: The routing and switching plane that implements the interaction with management applications.

Microwave: Electromagnetic waves in the radio frequency spectrum above 890 Megahertz and below 20 Gigahertz that are a common form of transmitting telephone, facsimile, video and data conversations used by common carriers as well as by private networks. Microwave is the frequency for communicating to and from satellites.

Multiprotocol Label Switching: A family of Internet Engineering Task Force standards in which IP networks can make forwarding decisions based on a pre-allocated label to setup a Label Switched Path (LSP).

National Coordinating Center: The national center that facilitates the exchange among government and industry participants regarding vulnerability, threat, intrusion, and anomaly information affecting the telecommunications infrastructure.

National Cybersecurity and Communications Integration Center: The Department of Homeland Security's 24-hour, coordinated watch and warning center that aims to improve national efforts to address threats and incidents affecting the Nation's critical information technology and cyber infrastructure.

National Strategy for Trusted Identities in Cyberspace: A national strategy that seeks to identify ways to raise the level of trust associated with the identities of individuals, organizations, services, and devices involved in certain types of online transactions.

Network Address Translation: The process used when an organization's network uses private IP addresses and external communications must be converted to use public addresses as they cross the boundary between public and private networks.

Network Operations Center: A location that monitors the operation of a network and usually provides efforts to solve connectivity and network problems. The NOC provides management of the terrestrial infrastructure by looking at configuration management and lock-down status/network systems monitoring.

Out-of-Band: The quantified ability of a system, subsystem, equipment, process, or procedure to provide communications among stakeholders in the event the Public Switched Network (PSN) and/or Internet services became unavailable.

Peering: A relationship established between two or more Internet Service Providers (ISP) for the purpose of exchanging traffic directly, rather than doing so through a backbone Internet provider.

Public Safety Answering Point: A call center that responds to 911 emergency calls from the public and dispatches emergency services such as police, firefighting, and ambulance services.

Public Safety Broadband Network: The FCC's proposed nationwide, interoperable mobile broadband network reserved for public safety's use.

Public Switched Telephone Network: The worldwide voice telephone network accessible to all those with telephones and access privileges.

Resilience: Presidential Policy Directive-8: *National Preparedness* defines resilience as the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies.

Resource Public Key Infrastructure: A system that enables users of public networks, such as the Internet, to verify the authenticity of data that has been digitally signed by the originator of the data.

Roaming: The ability to use a single communications device, such as a mobile phone, across different cells or access points without losing the network connection.

Router Flapping: Occurs when a malfunctioning router keeps going in and out of service, forcing neighboring routers to keep updating their routing tables, until all of the processing power is being siphoned off and no traffic is being forwarded, resulting in an Internet brownout.

Route Hijacking: An illegal change to a DNS server that directs a URL to a different Web site.

Router (core router): A part of the backbone that serves as the single pipe through which all traffic from peripheral networks must pass on its way to other peripheral networks.

Routing: The process of forwarding data to its destination.

Session Initiation Protocol (SIP): An IP telephony signaling protocol that is widely used to start and terminate voice calls over the Internet. Supporting two-way and multi-party calls, SIP can be used for any real-time media transmission over an IP network, including video calling and conferencing.

Signaling System 7 (SS7): A protocol used in the public switched telephone system that typically employs a dedicated 64-kilobit data circuit to carry packetized machine language messages about each call connected between and among machines of a network to achieve connection control.

Spectrum: A continuous range of frequencies, usually wide in extent within which waves have some specific common characteristics.

Synchronous Optical Network: A high-speed network that provides a standard interface for communications carriers to connect networks based on fiber optic cable.

Thin Client: A low-cost computing device that works in a server-centric computing model, accessing applications from a central server or network.

Unmanned Aerial Vehicle: An aircraft that is not flown by a pilot; can be remote-controlled from a ground control station or fly autonomously based on pre-programmed flight plans or automation systems.

Voice over Internet Protocol: The technology used to transmit voice conversations over a data network using IP. Such a data network may be the Internet or a corporate Intranet.

WiFi: Wireless local area networks that utilize unlicensed radio frequencies but are compatible with and may be connected to a wired Ethernet local area network. Typical application is the wireless, high-speed connection of a portable computer to the Internet.

Wireless Interoperability for Microwave Access (WiMAX): A wireless wide area network technology that allows ISPs and carriers to offer last-mile connectivity to homes and businesses without having to route wires. WiMAX also provides high-speed data in a mobile setting.

Zero-Day Attack: A work, virus, or other malicious, network-mediated exploit that is launched and hits users on the same day as or even before the public announcement of the system vulnerability that the attack exploits.

APPENDIX D
CONGESTION⁷¹

⁷¹ This appendix was originally contained in the NSTAC's November 2008 *Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic*.

APPENDIX D: CONGESTION

Before it can transit an Internet protocol (IP) network, a stream of data is separated into packets. Each IP packet includes both a header, which specifies source, destination, and other information about the traffic, and the message data itself. When the amount of traffic carried by a link or node exceeds its capacity, congestion in the IP network environment occurs and results in a deteriorated quality of service level, such as packet delay or loss.⁷² With delay insensitive applications, such as e-mail or instant messaging, the effects of packet delay or loss in the IP network will likely go unnoticed by the end user.⁷³ For delay-sensitive applications, such as Voice over Internet Protocol, real-time gaming, or IP television, packet delay or loss can affect the application's ability to operate or its quality of service. Service providers design and manage their networks to avoid or minimize network congestion and to be able to prevent and respond to network events.

Congestion can occur in many places along a user's communications path. One cause of congestion can be a mismatch in speed between networks. For example, national security and emergency preparedness-authorized users who rely on a low-speed local area network connection, such as a 10 megabit-per-second (Mbps) Ethernet, that connect to servers on high speed networks, such as a 155 Mbps asynchronous transfer mode over Optical Carrier-3, may experience congestion at the interface between the networks. Additionally, if a 10 Mbps connection is supporting hundreds of users within an office, congestion could occur as the users send/receive data due to the size of the connection. The user will only experience performance as good as the slowest link.

Congestion can also occur in a network node, such as a router or switch, from traffic aggregation in which traffic from multiple input ports is destined for a single output port. Traffic exceeding the line speed of the output port will be buffered and placed in a queue. Waiting in the queue will add delay to the traffic and overfilling the queue will lead to packet loss and degraded application performance. A congested edge, enterprise, or customer premise router can reduce bandwidth and lead to packet loss. A router placed at the edge of the network to connect various types of users, such as residential, cellular, satellite, or enterprise clients, to the core network may experience congestion at peak traffic times or during network events. At such times, it may not be able to attain the optimum data transfer speeds if a router is congested as packet buffers reach capacity. Congestion in edge routers has the potential to adversely affect the performance of applications that depend on the routers to function effectively. This is also true for the edge router at the receiving end. If a router is receiving more inquires than it is designed to handle, the users may experience a delayed response. Service providers generally strive to manage capacity on edge router resources so that users do not experience congestion where their traffic enters the network.

Congestion for digital subscriber line or dial-up customers is generally not at the digital subscriber loop access multiplexer (DSLAM); rather, it is the transport from the Internet service

⁷² Use of the term congestion should not be construed to mean a stoppage of data flow; rather it is a delay in the delivery of packets until sufficient network capacity is available to carry them to a device or application.

⁷³ With these types of services, data can be sent on a store and forward basis, meaning that the data is sent when the transmission path is available. Since the action is not in real-time, the receiver is unaware of the delay.

provider (ISP) point of presence to the DSLAM. An inadequate number of ports on the network access server at the ISP can lead to congestion. Further, an overloaded Web server could experience congestion during a period of high use. In addition, a user may overload their personal computer with multiple tasks, thus leading to slower service and ineffective applications use.

APPENDIX E

**NATIONAL CYBERSECURITY AND COMMUNICATIONS
INTEGRATION CENTER AND
NATIONAL CYBER INCIDENT RESPONSE PLAN**

APPENDIX E: NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER AND NATIONAL CYBER INCIDENT RESPONSE PLAN

National Cybersecurity and Communications Integration Center

In October 2009, the Department of Homeland Security (DHS) launched the National Cybersecurity and Communications Integration Center (NCCIC), a 24-hours-a-day, 7-days-a-week watch and warning center for cyber incidents affecting critical national cyber infrastructure. The NCCIC integrates the National Coordinating Center and the United States Computer Emergency Readiness Team, unifying both entities' operations in a joint watch floor. The NCCIC has plans to expand to integrate the National Cybersecurity Center, additional private sector partners, and international entities. It was originally formed in response to recommendations by the President's National Security Telecommunications Advisory Committee (NSTAC), the Government Accountability Office, and an industry-Government working group.⁷⁴

National Cyber Incident Response Plan

The National Cyber Incident Response Plan (NCIRP) outlines a national response strategy for significant cyber incidents. Using the response principles and structures laid out under the *National Response Framework* and its corresponding *Cyber Incident Annex*, the NCIRP establishes a strategic framework and assigns organizational roles and responsibilities for coordinating a cyber response to Federal, State, local, tribal, and territorial governments, as well as the private sector and international partners. During Fall 2010, DHS exercised the interim NCIRP in Cyberstorm III, which involved participants from various Federal organizations.

Joint Coordinating Center (JCC) Pilot Program

The Sector Operational Organization Cross-Sector Information Sharing, Analysis, & Collaboration Pilot Program [Joint Coordinating Center (JCC) Pilot Program] was a six-month pilot effort intended to develop the private sector's information sharing capabilities for cyber incidents. Specifically, it identified and tested a program model design for cross-sector collaboration, with possible use for future integration with the Government, to facilitate a joint, integrated, public-private operational capability as recommended in the May 2009 *NSTAC Report to the President on Cybersecurity Collaboration*.⁷⁵ Though developed under the auspices of the NSTAC, the program was formally launched by the operational organizations of four participating sectors, which included the Communications Information Sharing and Analysis Center (ISAC) and four individual NSTAC companies representing the Communications Sector, the defense industrial base's Defense Security Information Exchange, the financial services ISAC, and the information technology ISAC.

⁷⁴ For DHS' press release on the NCCIC, see: http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm.

⁷⁵ NSTAC Cybersecurity Collaboration Task Force. *Cybersecurity Collaboration Report: Strengthening Government and Private Sector Collaboration through a Cyber Incident Detection, Prevention, Mitigation, and Response Capability*, May 2009.

APPENDIX F
FEDERAL AND STATE RESPONSE STRUCTURES
(RELEVANT TO SCENARIO 2)

APPENDIX F: FEDERAL AND STATE RESPONSE STRUCTURES (RELEVANT TO SCENARIO 2)

Current Federal, State, and regional disaster response plans proscribe immediate response activities and assign roles and responsibilities. Under the *National Response Framework's* (NRF) Emergency Support Function (ESF) #2 – *Communications*, the National Communications System (NCS) serves as the primary coordinating agency for ESF #2 and shares responsibility with the Federal Emergency Management Agency (FEMA) as co-primary agencies on all response activities involving communications.⁷⁶ Specifically, the NCS coordinates national security and emergency preparedness communications support and FEMA is responsible for efforts to restore public safety networks and first responder communications. A Joint Field Office serves as the focal point for coordination among Federal entities and with industry service providers to restore services.

Department of Defense (DOD) assets, and particularly U.S. Northern Command, can participate in civil support missions as directed by the Secretary of Defense or the President. Such missions are generally in support of a leading Federal agency, as stipulated in the NRF. Under DOD's Pre-scripted Mission Assignments, organized by ESF #2, DOD has pre-prepared and pre-coordinated first responder communications packages ready for deployment upon approval by the Secretary of Defense. DOD can also use Defense Support of Civil Authorities communications assets.

⁷⁶ For some information on the ESF #2 functions, see FEMA's *National Response Framework, Emergency Support Function #2 Communications Annex*.

APPENDIX G

TECHNICAL DISCUSSION OF THE ROUTING AND ADDRESSING CONCEPTS PRESENTED IN SCENARIO 4

APPENDIX G: TECHNICAL DISCUSSION OF THE ROUTING AND ADDRESSING CONCEPTS PRESENTED IN SCENARIO

4

Routing, AS Numbers, BGP

The Internet is a loosely interconnected network of networks. The Border Gateway Protocol (BGP) is the de facto protocol for inter-domain routing on the Internet. In order to operate a network on the Internet, an operator must first obtain a routing domain identifier, known as an autonomous system (AS) number, and Internet Protocol (IP) version 4 (IPv4) or IPv6 address space from a regional internet registry (RIR), local internet registry (LIR), or Internet service provider (ISP). The operator then provisions physical circuits between routers on their network and connects them with routers on peer networks using underlying physical and link layer technologies.⁷⁷ Once connectivity is established, a BGP session is provisioned between the AS routers. The BGP process in the router is configured to exchange network layer destination reachability information, in the form of route advertisements, with each BGP peer.⁷⁸ A route represents one or more contiguous IPv4 or IPv6 addresses, is encoded in the form of prefix/len (e.g., 10.0.0.0/8), and includes an array of attributes associated with the route, such as its origin code. It also contains the routing metric information (e.g., MED or LOCAL_PREF), and a list of the AS' the routing information has traversed.⁷⁹

While protocols such as Secure BGP (SBGP) and Secure Origin BGP (soBGP) have been proposed, there is no inherent object-level security in the routing system today. No cryptographic verification mechanisms exist within BGP to validate the integrity of a route advertisement, nor is there a secure framework to verify that a particular AS has been authorized to either originate or provide transitive connectivity to a particular Internet number resource.⁸⁰ Furthermore, while developers are working to create a Resource Public Key Infrastructure (RPKI) to provide resource certification for Internet numbers, there currently exists no functional tie-in between what Internet number registries allocate and what is actually routed on the Internet.⁸¹

As a result, anyone operating an AS could assert reachability for any set of address space via BGP in the global routing system. There are very few actions operators can take to verify if the advertised destinations are legitimate or determine precisely who holds what number resources and what ingress routing policy should be applied to a BGP peer on a per-prefix and per-path basis. The effect is that inter-domain routing on the Internet generally has very weak prefix-level security policies.

⁷⁷ Examples of physical and link layer technologies include packet over SONET or Gigabit Ethernet.

⁷⁸ This is typically based on business terms of the interconnection agreement.

⁷⁹ The list of the AS' routing information is also known as the AS_PATH.

⁸⁰ Resources include an AS or set of IP addresses.

⁸¹ RPKI is a security framework for verifying the association between resource holders and their Internet resources. See the next section for additional information on RPKI.

Network interconnections, referred to as peering relationships, are generally broken into two categories: bi-lateral settlement free interconnection (SFI) relationships or transit customer/service provider relationships. Under typical bi-lateral SFI relationships, networks of equal size or objective agree to provide reachability and connectivity to only customers and internal address space on their network. Under transit customer relationships, one party agrees to propagate received routes to other peers, asserting reachability as an intermediary network for the IP addresses in question and provide the paying party with connectivity to local networks and all or a subset of Internet destinations. This is a unidirectional function; not only does it propagate routes from the customer to upstream networks, but also dictates if the networks share BGP routes learned from other SFI peers. It may also provide routes and connectivity to local and customer networks.

Because there is no single authority to arbitrate who is authorized to assert reachability for what address space, each AS autonomously determines which routes it wishes to install and use locally, which it propagates to other customers or peers, and which it chooses to discard. While this affords a great deal of flexibility and autonomy to network operators, it is highly insecure and prone to malice and error. This model of routing on the Internet has been referred to as routing by rumor.

There are several other factors that must be considered when discussing routing. For example, IP routing employs a hop-by-hop, destination-based forwarding paradigm. Each router individually determines where to forward a packet based on the destination address and each AS normally employs a common routing policy set for routers within that AS. From a functional level, BGP attempts to route traffic over the Internet based on:

- The most specific route, e.g., preference of a /24 over a /20 route;
- The route with the highest preference;⁸² and
- The route with the shortest AS path length.

The routes with the highest preference are the result of ISPs normally preferring routes learned from customers over equal routes learned from peers. For example, if an ISP learns a route for 1.0.0.0/24 from a peer in New York City with one AS hop, but learns the same route from a transit customer in Singapore that is five AS hops away, the ISP would likely forward packets to that destination via the Singapore path. There is no notion of transaction latency, IP hops, or AS path length; it is based simply on the most specific route and business relationships.⁸³

This method of determining routing preferences has a very negative effect on the routing system. With only a small number of global Internet transit providers, if an organization purchases transit services from a larger global network, then it is highly probable that any equal-length prefix the organization advertises into the routing system will be preferred by that network provider and all of that provider's customers over any other path of equal or shorter length from other Internet providers. Therefore, if there is no mechanism for operators to validate the authenticity of route

⁸² This is dictated most strictly by business relationships.

⁸³ This holds true where IPv4 addresses are nominally scoped at not longer than /24 on the Internet today; however, this will likely change with the IPv4 free pool depletion.

announcements from peers or customers, then route hijacks can have far-reaching effects. If there are two routes of equal length in the routing system and all other attributes are the same, then topological proximity will dictate the direction in which traffic bound for the destination is directed.⁸⁴

Some attempts are being made to filter routes learned from customers at the ISP level, but very little explicit filtering of prefixes occurs between larger networks today. Some routing policy generation occurs based on Internet Routing Registry (IRR) data and RIPE Network Coordination Centre (RIPE NCC) also developed several useful Routing Policy System Security (RPSS) hooks from their RIR allocation structure to help authorize IRR object population. Even then, the IRRs are largely insecure in their current incarnation; unless the IRRs can be marked with cryptographically-verifiable, validated RIR allocation data, then it will be largely impossible to secure the routing system.⁸⁵

Furthermore, if a PKI or similar system were established for Internet number resource certification, rooted to align with the inherent delegation graph model, and employed a resource certification system, operators would cede autonomy and flexibility to external stakeholders.^{86,87} This would introduce a new dependency into the Internet routing infrastructure. The politics of such new architecture frameworks at the routing system and network layer would be complex, as are any technologies and circular dependencies that may exist or be introduced as a result.

Many nations and international organizations have taken note that Internet number resource certification and an RPKI are being directly employed by the routing system. The RPKI that operators employ to effect routing policy generation on the Internet places the Internet Assigned Numbers Authority (IANA), the RIRs, and RPKI elements in the critical path for routing and network connectivity, which concerns many operators and wider community constituents. As such, it will be necessary to have some intermediation functions that permits operators to verify who holds which number resources and enables network operators, nation-states, and organizations to apply policies that best align with their security and connectivity objectives and allows fallback capabilities in the event that the RPKI becomes unavailable or otherwise unusable.

One additional item to note is that routing domains do not inherently follow national boundaries. If RPKI exists, it is possible that it could become a mechanism for engendering state-level censorship. AS' that operate in multiple nations will likely have to be redesigned, with routing system prefixes deaggregated, in order to align with national boundaries. Routing stability, scalability, and security issues may result.

Resource Public Key Infrastructure⁸⁸

⁸⁴ Topological proximity may be measured through AS path length or Interior Gateway Protocol metrics.

⁸⁵ For example, via a system such as RPKI that is being defined by the IETF's Secure Inter-Domain Routing Working Group, or via a similar mechanism such as in-addr.arpa delegation graph and KIDNS certificates.

⁸⁶ The inherent delegation graph model is from the Internet Assigned Numbers Authority to RIR, then from RIR to ISP.

⁸⁷ A resource certification system would generate static routing policy or enable a dynamic secure Internet routing policy function.

⁸⁸ Information on RPKI was obtained at: <http://isoc.org/wp/ietfjournal/?p=597>.

Resource certification, also referred to as RPKI, is a robust security framework for verifying the association between resource holders and their Internet resources.^{89,90} It describes the structure of the certification framework used by resource certificates. The intent of the RPKI is to construct a robust hierarchy of X.509 certificates that allows relying parties to validate assertions about IP addresses and AS numbers and their use.

The structure of the RPKI as it relates to public use of IP number resources is designed to mirror the structure of the distribution of addresses and AS' in the Internet. IANA manages the central pool of number resources and publishes a registry of all current allocations. IANA does not make direct allocations of number resources to end users or LIRs, but allocates blocks of number resources to the RIRs. The RIRs perform the next level of distribution, allocating number resources to LIRs, National Internet Registries (NIRs), and end users. NIRs perform allocations to LIRs and end users and LIRs allocate resources to end users. (See Figure 1.)

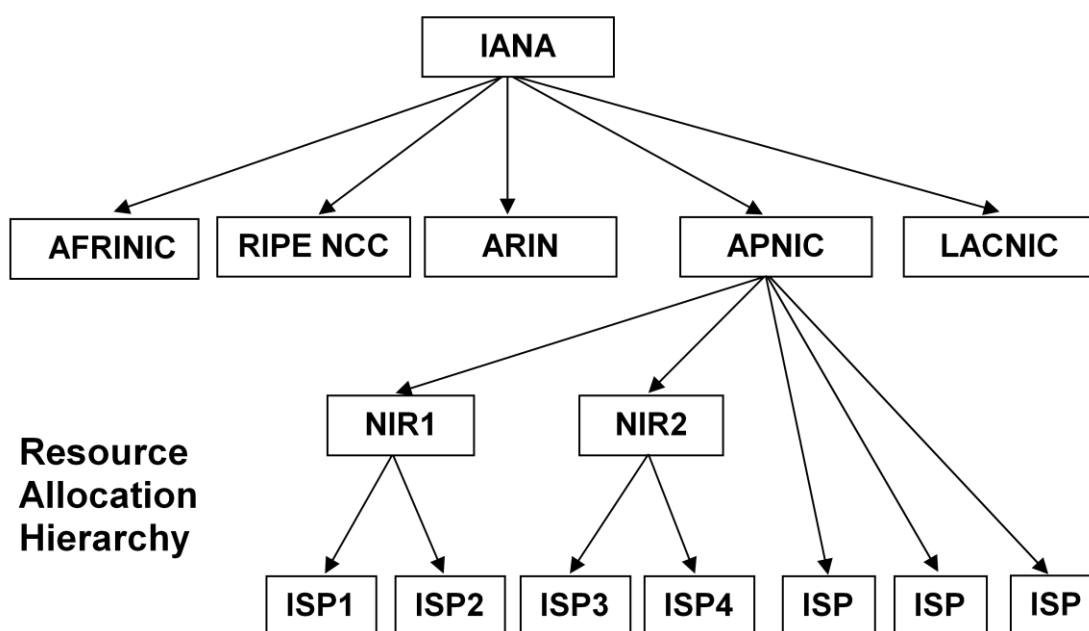


Figure 1 RPKI Resource Certificate Hierarchy

The RPKI mirrors this allocation hierarchy. One interpretation of this model would have IANA manage a root RPKI key. Using this key, IANA would issue a self-signed root certificate and subordinate certificates to each of the RIRs, describing the complete set of number resources that have been allocated to that RIR at the time of issuance in the certificate's resource extension. The certificate would also hold the public key of the RIR and would be signed by the private key of IANA. Each RIR would issue certificates that correspond to allocations made by that RIR, where those certificates' resource extension lists all the allocated resources. The certificate would also include the public key of the recipient of the resource allocation, signed with the

⁸⁹ In this context, resource holders are organizations such as RIRs, LIRs, ISPs, or end-user organizations, while Internet resources are IPv4 and IPv6 address blocks and AS numbers.

⁹⁰ This has been an initiative that has been developed within the Internet Engineering Task Force's Secure Inter-Domain Routing Working Group and among the various RIRs.

private key of the RIR. If the recipient of the resource allocation is an LIR or an NIR, then it, too, would issue resource certificates in a similar manner. (See Figure 2.)

The common constraint with this certificate structure is that an issued certificate must contain a resource extension with a subset of the resources that are described in the resource extension of the issuing authority's certificate. This corresponds to the allocation constraint that a registry cannot allocate resources that are not registered to it. One implication of such constraint is that if any party holds resources allocated from two or more registries, then it will hold two or more resource certificates to describe the complete set of its resource holdings.

Validation of a certificate within RPKI is similar to conventional certificate validation within any PKI: establishing a chain of valid certificates that are linked by issuer and subject from a nominated trust anchor Certification Authority (CA) to the certificate in question. There are two additional constraints in RPKI: (1) that every certificate in this validation path must be valid; and (2) that the IP number resources described in each certificate are a subset of the resources described in the issuing authority's certificate.

Within this RPKI, all resource certificates must have the IP addresses and AS resources present and marked as a critical extension. The contents of these extensions correspond exactly to the current state of IP address and AS number allocations from the issuer to the subject.

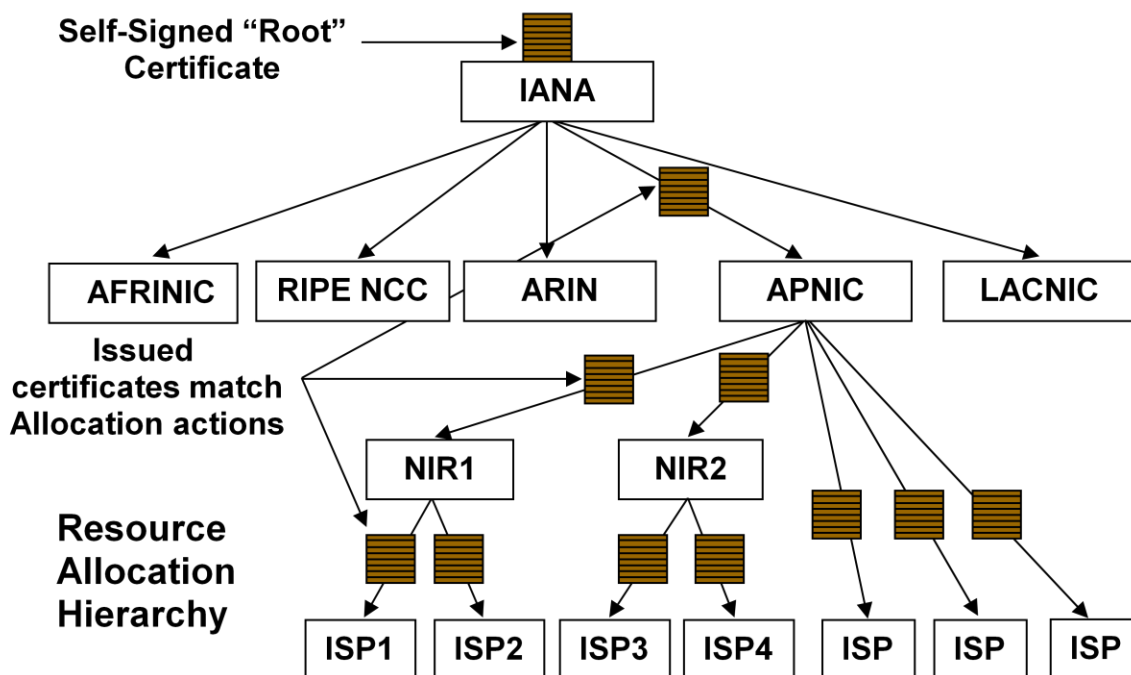


Figure 2 RPKI Resource Certificate Hierarchy With Self-Signed "Root" Certificate

Any resource holder in a position to further allocate resources to other parties must be in a position to issue resource certificates that correspond to these allocations. Similarly, any holder who wishes to use RPKI to digitally sign an attestation needs to be able to issue an End Entity (EE) certificate to perform the digital signing operation. For that reason, all issued

certificates that correspond to allocations are certificates whose CA capability has been enabled. Each CA certificate is also capable of issuing subordinate CA certificates that correspond to further sub-allocations as well as issuing subordinate EE certificates that correspond to generation of digital signatures on attestations.

The RPKI makes conventional use of Certificate Revocation Lists (CRL) to control the validity of issued certificates. Every CA certificate in the RPKI must issue a CRL according to the CA's nominated CRL update cycle. A CA certificate may be revoked by an issuing authority for a number of reasons, including key rollover, a reduction in the resource set associated with the certificate's subject, or termination of the resource allocation. To invalidate the authority or attestation that was signed by a given EE certificate, the CA issuing authority that issued the EE certificate simply revokes the EE certificate.

Resource certificates are intended to be public documents and all certificates and objects in the RPKI are published in openly accessible repositories. Together, these repositories form a complete information space; ensuring that the entire RPKI information space be available is fundamental to securing the public Internet's inter-domain routing system. Other uses of the RPKI might permit use of subsets, such as the single chain from a given EE certificate to a Trust Anchor, but routing security is considered against all known publicly routable addresses and AS numbers; therefore, all known resource certification outcomes must be available. Essentially, the RPKI's intended use in routing contexts is not a case in which each relying party may make specific requests for RPKI objects to validate a single object, but one in which each relying party will perform a regular sweep across the entire set of RPKI objects to ensure that the relying party has a complete understanding of the RPKI information space.

This aspect of the RPKI represents some interesting challenges in that rather than have a single CA publish all the certificates produced in a security application at a single point, the RPKI permits the use of many publication points in a widely distributed fashion. Each CA is able to issue RPKI objects and publish them using a locally managed publication point. It is incumbent upon relying parties to synchronize a locally managed cache of the entire RPKI information space at regular and relatively frequent intervals.

For that reason, the RPKI has introduced an additional mechanism in its publication framework: the use of a manifest enabling relying parties to determine if they have been able to retrieve the entire set of RPKI published objects from each RPKI repository publication point or if there has been some attempt to disrupt the relying party's access to the entire RPKI information set. It also implies that the RPKI publication point access protocols should support the efficient function of a synchronization comparison so that a locally managed cache of the RPKI needs call for uploading only those objects that have been altered since the previous synchronization operation.

The Domain Name System (DNS)

DNS Primer

This section provides a brief overview of some important DNS concepts. Figure 3, below, shows the process of the recursive name server sending several DNS queries to look up or resolve the

domain name *www.cnn.com*. First, the user types *www.cnn.com* into a Web browser. To display the page, the Web browser needs the IP address of CNN's Web server to connect and retrieve the page. DNS resolution translates the name of the Web site into the Web server's IP address.

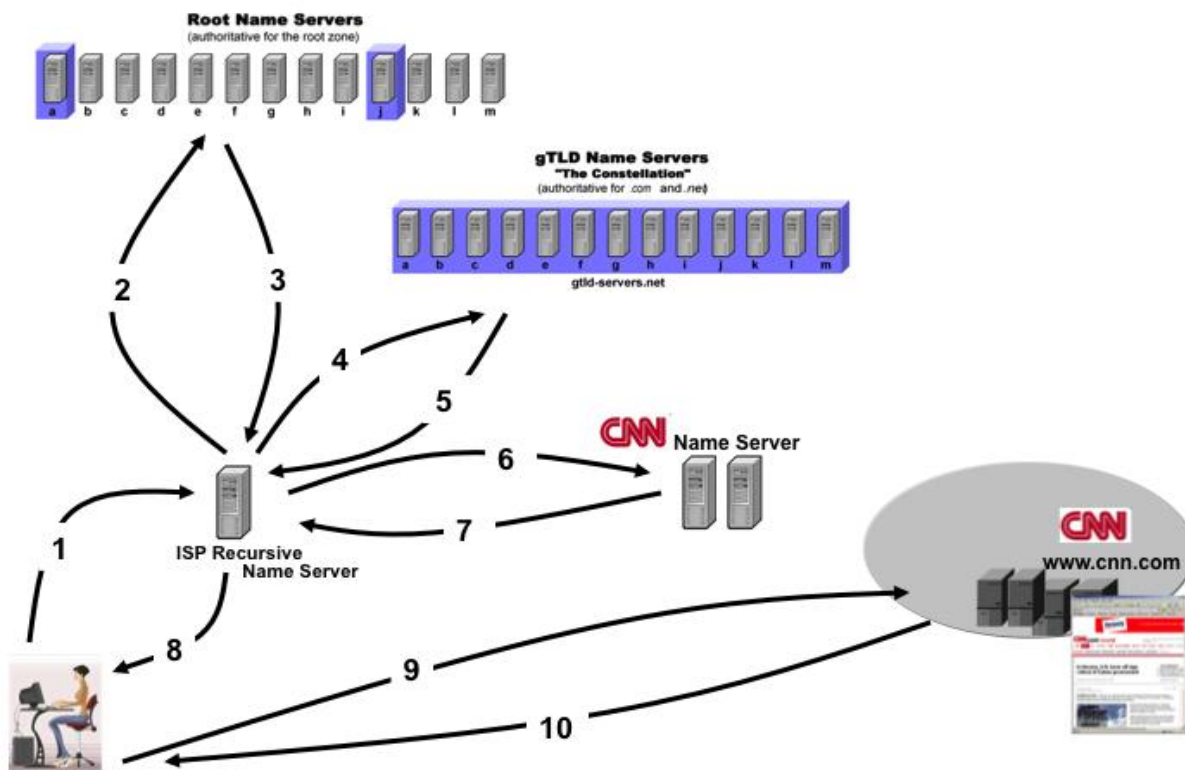


Figure 3 DNS Resolution Process

The DNS client on the user's computer, called a resolver, sends a DNS query to a nearby recursive name server asking "What is the IP address of *www.cnn.com*?" As the figure illustrates, the recursive name server is responsible for obtaining responses from the authoritative name servers that are necessary to answer this question. Every device that uses DNS—PCs, smart phones, iPads, etc.—needs a recursive name server to answer its DNS queries.⁹¹ The recursive name server sends queries to multiple authoritative name servers, each of which stores different DNS information. When asked a question, an authoritative name server can provide either the answer or a referral, which directs the recursive name server to query a different authoritative name server.

DNS follows a hierarchy in which each level delegates to the level below. At the top of this hierarchy is the root zone, which contains information about the level below. The root then delegates to the top-level domains (TLD), such as .com, .net, .uk, etc.⁹² The root name servers store the information in the root zone and answer questions from recursive name servers.

⁹¹ Recursive name servers are found mainly at ISPs (to handle queries from their customers' devices) and on enterprise networks.

⁹² Currently, there are 294 TLDs in the root zone.

Continuing down the hierarchy, there are authoritative name servers for every domain at each level.

Figure 3 also illustrates the DNS resolution process. When the recursive name server receives the DNS query asking, “What is the IP address of *www.cnn.com*?” (See Figure 3, Arrow 1), it first searches for answers to previous DNS queries; if the recursive name server has recently been asked about the IP address in question, it would be able to answer immediately. However, in this example, the recursive name server does not have the IP address for *www.cnn.com* in its cache, so it has to start querying various authoritative name servers to find the answer. The process is described below:

- The recursive name server starts the resolution process by querying one of the root name servers, asking the server to provide the IP address of *www.cnn.com*. (Arrow 2)
- If the root name servers do not know that IP address, as they only have information about the level directly below in the hierarchy, the root server replies to the recursive name server with a referral to the *.com* servers. (Arrow 3)
- The recursive name server follows this referral and asks one of the *.com* name servers to provide the IP address of *www.cnn.com*. (Arrow 4)
- If the *.com* servers does not know that IP address, they can provide a referral to the *cnn.com* name servers. (Arrow 5)
- The recursive name server again follows the referral and this time asks one of the *cnn.com* name servers for the IP address of *www.cnn.com*?” (Arrow 6)
- If this name server knows the answer, it provides the *www.cnn.com* IP address. (Arrow 7)
- The recursive name server caches this reply and can answer the resolver on the user’s computer that submitted the original query, providing the desired IP address. (Arrow 8)

Now that the user’s computer has the IP address of *www.cnn.com*, the Web browser can connect to CNN’s Web server (Arrow 9) and retrieve the CNN Web page (Arrow 10) to display it.

DNS Security Vulnerability

DNS was designed over 25 years ago without considering the potential future security environment. This lack of security makes DNS vulnerable to a wide range of attacks based on forgery, or spoofing.

DNS queries and replies are typically sent over the Internet in one packet. The fundamental security vulnerability with DNS lies in the fact that the sender of a DNS query believes the response he or she receives, regardless of whether or not the site has been compromised. An attacker only needs to spoof a single packet to insert a bogus reply before the legitimate reply arrives.

If an attacker can spoof a response to a recursive name server, the recursive name server will cache the bad data and redistribute it to anyone who subsequently visits the site. This condition is called cache poisoning. If an ISP’s recursive name server were to have a poisoned cache of a

popular Web site, many people could be directed to the wrong Web site, potentially leading to identity theft and the installation of malware on users' computers.

DNS Security Extensions

Techniques have been developed to make it easier to detect spoofed replies; however, these techniques only make spoofing harder, not impossible. A solution would require the querier to know *with certainty* that the reply it receives is the appropriate one. Fortunately, the DNS security extensions (DNSSEC) closes this vulnerability in DNS using public key cryptography. DNS data is now digitally signed and DNS responses include not only the data requested, but also a digital signature for that data. If the querier knows and trusts the public key corresponding to the private key that signed the DNS data, then it can validate that data as legitimate.

With DNSSEC, every DNS domain needs a public/private key pair and all data in the domain is digitally signed. Each level in the DNS hierarchy is signed separately; for example, the data in the root zone is signed, the DNS data held by VeriSign in *.com* is signed, and the DNS data held by CNN in *cnn.com* is signed, etc. Note that the DNS data is signed before it is sent to the authoritative name servers to be handed out as answers to queries. DNSSEC separates *signing the data* from *servicing the data*. This design means that DNS replies do not have to be signed as they are sent by authoritative servers; the data stored on authoritative servers is already signed.

The digital signatures on DNS data are verified at the recursive name server using a process called DNSSEC validation. In the earlier resolution example, recall that each domain's DNS data is signed by a private key and needs to be verified using a public key. In order for the recursive name server to find the appropriate public key, each domain publishes its public key in DNS. When a recursive name server sees DNS data signed with a particular private key, it can find the corresponding public key using DNS itself and then perform the cryptographic verification of the digital signature. A problem arises if the recursive name server is unsure whether or not to trust the public key that it found in DNS.

Any time public key cryptography is used, knowing whether or not a public key can be trusted is an issue. In a secure Web browsing context, this problem is solved with certificates, which serves as a statement from a CA showing who owns a particular public key. The CA signs certificates with its private key. Users will need to validate a certificate before trusting its contents, meaning they need access to the CA's public key. This public key is widely distributed: all popular Web browsers ship with the public keys of all the popular CAs. Since multiple CAs' keys are trusted by all browsers, a user can choose for which CA he wants to issue a certificate.

In DNSSEC, there are no certificates and no certificate authorities; instead, a domain's parent in the hierarchy is the only one that can verify the authenticity of its public key. For example, only *.com* can vouch for *cnn.com*'s public key, because *.com* is the DNS parent of *cnn.com*. *Cnn.com* publishes its public key and sends it to the *.com* registry. The *.com* registry signs *cnn.com*'s public key and publishes the resulting signature in *.com*. If a recursive name server performing DNSSEC validation already knows and trusts the *.com* public key, it will trust the signature on the *cnn.com* public key and therefore trust the *cnn.com* public key itself, which it can then use to verify signed data in the *cnn.com* domain. The concept of one key signing another key to verify

its validity is called a chain of trust. In DNSSEC, the chain of trust starts at the root zone, which is the equivalent of a certificate authority's public key. The root zone's public key will be widely configured in recursive name servers all over the Internet. Once a recursive name server trusts the root zone's public key, it can use it to build a chain of trust from the root to a TLD (such as *.com*) to a second-level domain (such as *cnn.com*), as far as necessary to ultimately verify signed data.

What DNSSEC Provides

DNSSEC provides two new features to DNS: (1) authentication of DNS data so users can ensure that, for example, a DNS response claiming to contain the IP address of *www.cnn.com* really came from CNN; and (2) integrity of DNS data to allow users to detect when DNS data has been tampered with as it traveled over the network. Once widely deployed, DNSSEC will prevent cache poisoning as long as recursive name servers are performing DNSSEC validation and domains are signed with DNSSEC. DNSSEC does not, however, provide confidentiality for DNS data, address attacks against the name server; or secure the data on the destination Web site. In essence, DNSSEC offers protection against spoofing of DNS data. It provides a level of assurance that an individual has been routed to the correct destination.

APPENDIX H
BIBLIOGRAPHY

APPENDIX H: BIBLIOGRAPHY

Aiken, Peter et al. *Microsoft Computer Dictionary*. Fifth Edition. Microsoft Press. 2002.

“Are TVs and Smartphones the Future of the Internet?” *Connected World*. September 8, 2010. Available at: <http://connectedworldmag.com/latestNews.aspx?id=NEWS100907142809100>.

Armstrong, Nicholas J., et al. “Building Resilient Communities: A Preliminary Framework for Assessment.” *Homeland Security Affairs*. Volume VI No. 3. September 2010.

Association of Bay Area Governments. *Taming Natural Disasters: Multi-Jurisdictional Local Hazard Mitigation Plan for the San Francisco Bay Area*. 2010 Update.

Cisco Systems, Inc. *Cisco Visual Network Index*. June 2010.

Cisco Systems, Inc. and Global Business Network. *The Evolving Internet: Driving Forces, Uncertainties, and Four Scenarios to 2025*. August 25, 2010.

Cranton, Tim. “Cracking Down on Botnets.” Microsoft on the Issues Blog. February 24, 2010. Available at: http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/02/24/cracking-down-on-botnets.aspx

Department of Homeland Security, Federal Emergency Management Agency, and California Office of Emergency Services. *Interim San Francisco Bay Area Earthquake Readiness Response: Concept of Operations Plan*. September 23, 2008.

Department of Homeland Security Science and Technology Directorate. “DHS Launches Multiband Radio Project.” Press Release. February 27, 2008.

Executive Office of the President. Draft *National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy*. June 25, 2010.

“FCC Grants Public Safety Agencies Waivers to Build LTE Networks.” *Fierce Wireless*. May 16, 2010. Available at: http://www.fiercebroadbandwireless.com/story/fcc-grants-public-safety-agencies-waivers-build-lte-networks/2010-05-16?utm_medium=nl&utm_source=internal

Federal Communications Commission. *Connecting America: The National Broadband Plan*. March 2010. Available at: <http://download.broadband.gov/plan/national-broadband-plan.pdf>

Federal Communications Commission. “Wireless 911 Services.” Available at: www.fcc.gov/cgb/consumerfacts/wireless911srv.html.

Federal Communications Commission. WT Docket No. 06-150: *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229: *Amendment of Part 90 of the Commission's Rules*, WP Docket No. 07-100: *Third Report and*

Order and Report and Fourth Further Notice of Proposed Rulemaking; and WCB Docket No. 04-36, *IP-Enabled Services*. Available at: www.fcc.gov.

Federal Emergency Management Agency. *National Response Framework, Emergency Support Function #2 Communications Annex*.

Federal Emergency Management Agency Office of Response and Recovery. "International Recovery Forum." January 12, 2011. Available at: http://www.recoveryplatform.org/assets/meetings_trainings/irf2011/Presentations/Forum/Keynote%20Speech%20-FEMA-Ms.Zimmerman.pdf.

German, Kent. "AT&T, Verizon Execs Talk LTE Expansion." *CNET News*. September 16, 2010. Available at: http://www.cnet.com/8301-17918_1-20016765-85.html

Global Mobile Suppliers Association. "GSA Confirms LTE as the Fastest Developing System in the History of Mobile Telecommunications, 180 Operators Now Investing." January 12, 2011. Available at: http://www.gsacom.com/news/gsa_315.php4.

Graham, Amy. "Video Will Be Two-Thirds of All Mobile Data." *CNN*. February 3, 2011. Available at: http://articles.cnn.com/2011-02-02/tech/cisco.mobile.data_1_wireless-carriers-mobile-video-feature-phones?_s=PM:TECH.

Gross, Grant. "FCC Sets LTE as Standard for Public Safety Network." *Tech World*. January 26, 2011. Available at: http://www.techworld.com.au/article/374496/fcc_sets_lte_standard_public_safety_network/?fp=2&fpid=1&rid=1.

Gross, Grant. "Google, Verizon Make Net Neutrality Proposal." *Computer World*. August 9, 2010. Available at: http://www.computerworld.com/s/article/9180464/Update_Google_Verizon_make_Net_neutralit_y_proposal?taxonomyId=13

Gross, Grant. "Satellite, Public Safety Projects Win Broadband Awards." *Network World*. August 18, 2010. Available at: <http://www.networkworld.com/news/2010/081810-satellite-public-safety-projects-win.html?page=1>

Government Accountability Office. *Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving But Program Management Could be Strengthened*. GAO 10-772. September 23, 2010.

Government Accountability Office. *Emergency Communications: National Communications System Provides Programs for Priority Calling, but Planning for New Initiatives and Performance Measurement Could be Strengthened*. Report GAO-09-822. August 2009.

Hamblen, Matt. "Harris Corp Unveils Push-to-Talk Over IP Technology." *Computer World*. August 2, 2010. Available at:

http://www.computerworld.com/s/article/9179908/Harris_Corp_unveils_push_to_talk_over_IP_technology

InsideDefense. "DSB to Study Cloud Computing, Mission Resilience." February 9, 2011.

Jerome, Sara. "First Responder Devices Still Can't Talk to Each Other, Congress told." *The Hill*. May 27, 2010. Available at: <http://thehill.com/blogs/hillicon-valley/technology/100231-first-responder-devices-still-cant-talk-to-each-other-congress-told>

Kang, Cecilia. "FCC, Public Safety Groups at Odds Over Control of Nationwide Wireless Network." *The Washington Post*. June 9, 2010. Available at:

<http://www.washingtonpost.com/wp-dyn/content/article/2010/06/08/AR2010060805253.html>

Kang, Cecilia. "TV Broadcasters Resist FCC Proposal to Surrender More Airwaves." *The Washington Post*. January 19, 2011.

Krigman, Eliza. "Social Media and Games Dominate Online Activity." *Tech Daily Dose*.

August 12, 2010. Available at: <http://techdailydose.nationaljournal.com/2010/08/social-media-and-games-dominat.php>

Lipowicz, Alice. "First Responders Embrace Social Media." *Washington Technology*.

August 30, 2010. Available at: http://washingtontechnology.com/articles/2010/08/30/tech-trends-contractor-social-media-sidebar.aspx?admgarea=TC_HLS

Matthews, William. "Security Firm: 2009 Cyber Attack Stretched Over Months." *Defense News*. June 2, 2010. Available at: <http://www.defensenews.com/story.php?i=4653942>.

Marek, Sue. "Study: Mobile VoIP Users Will Top 100M in 2012." *Fierce Wireless*. May 27, 2010.

Available at: <http://www.fiercewireless.com/story/study-mobile-voip-users-will-top-100m-2012/2010-05-27>

Marsan, Carolyn Duffy. "Fed's IPv6 Plan Called a 'Game Changer.'" *Network World*.

September 28, 2010. Available at: <http://www.networkworld.com/news/2010/092810-ipv6-obama-plan.html>

Mearian, Lucas. "Wall Street Not Bullish on Cloud." *Network World*. September 27, 2010.

Available at: <http://www.networkworld.com/news/2010/092710-wall-street-not-bullish-on.html>

McGraw-Hill Dictionary of Computing & Communications. The McGraw-Hill Companies. 2003.

Mell, Peter and Grance, Tim. "The NIST Definition of Cloud Computing." Version 15. October 7, 2009.

Microsoft Malware Protection Center Blog. “What We Know and Learned from the Waledac Takedown.” March 25, 2010. Available at:

<http://blogs.technet.com/b/mmmpc/archive/2010/03/15/what-we-know-and-learned-from-the-waledac-takedown.aspx>.

Middleton, James. “AT&T to Launch LTE by Mid-2011.” *Telecoms*. September 16, 2010. Available at: <http://www.telecoms.com/22488/att-to-launch-lte-in-mid-2011>

Associated Press. “Motorola Unveils Public Safety Communications Plan.” May 18, 2010. <http://www.businessweek.com/ap/financialnews/D9FPCVOG0.htm>

Erica Naone. “The Slow-Motion Internet.” *Technology Review*. Massachusetts Institute of Technology. March/April 2011.

Newton, Harry. *Newton’s Telecom Dictionary*. 25th Anniversary Edition. New York: Flatiron Publishing, 2009.

NSTAC Cybersecurity Collaboration Task Force. *Report on the Outcomes and Lessons Learned from the Sector Operational Organization Cross-Sector Information Sharing, Analysis, and Collaboration Pilot Program*. January 19, 2011.

NSTAC Financial Services Task Force Report. April 2004.

NSTAC Report to the President on Identity Management Strategy. May 2009.

NSTAC Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic. November 2008.

NSTAC Report to the President on Commercial Satellite Communications Mission Assurance. November 2009.

Number Resource Organization. “Free Pool of IPv4 Address Space Depleted.” February 3, 2011. Available at: <http://www.nro.net/news/ipv4-free-pool-depleted>.

O’Brien, Kevin. “Data Seen Overwhelming Cell Networks.” *New York Times*. February 16, 2011.

Office of Senator Mark R. Warner. “Senators Snowe, Warner Introduce Legislation to Increase Wireless Coverage.” Press Release. December 3, 2010. Available at: http://warner.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=28093ff6-183c-441a-b2e0-7e2f727dc4a7&ContentType_id=0956c5f0-ef7c-478d-95e7-f339e775babf.

Oxford Dictionary of Computing. Sixth Edition. Oxford University Press. 2008.

Perkins, Steven C. “Internet Terminology and Definitions.” Available at: <http://www.rci.rutgers.edu/~au/workshop/int-def.htm>.

Presidential Policy Directive 8: *National Preparedness*, March 30, 2011.

Public Safety Wireless Network Program. *Answering the Call: Communications Lessons Learned from the Pentagon Attack*. January 2002. Available at:

<http://www.safecomprogram.gov/NR/rdonlyres/8839D9BA-9104-4EE1-BC43-E8431C500F95/0/AnsweringCallLessonsPentagonAttack.pdf>

Reed, Brad. "WiMax 2 Set to be Finalized in November." *Network World*. August 11, 2010. Available at: <http://www.networkworld.com/news/2010/081110-wimax2.html>

"R.I.P. Waledac: Undoing the Damage of a Botnet." The Official Microsoft Blog – News and Perspectives. September 8, 2010. Available at:

http://blogs.technet.com/b/microsoft_blog/archive/2010/09/08/r-i-p-waledac-undoing-the-damage-of-a-botnet.aspx

"Rural Satellite Services Helping Urban Japan." *Aerospace Daily & Defense Report*. March 21, 2011.

Sternstein, Aliya. "Debate Heats Up Over Police Access to Data in the Cloud." *NextGov*. September 24, 2010. Available at:

http://www.nextgov.com/nextgov/ng_20100924_5567.php?src=lingospot_top

Violino, Bob. "Study: Cloud Breaches Show Need for Stronger Authentication." *Network World*. January 18, 2011. Available at: <http://www.networkworld.com/news/2011/011811-study-cloud-breaches-show-need.html>

Wilson, Carol. "Disaster Recovery Turns Wireless & Cloudy." *Light Reading*. May 27, 2010. Available at: http://www.lightreading.com/document.asp?doc_id=192536&

WiMax Forum. "WiMax Deployments Go Global with 519 in 146 Countries." Press Release. December 17, 2009. Available at: www.wimaxforum.org/news/2030

Briefings

Alagna, Mike, Motorola. "Public Safety Communications: Progress, Challenges, and Future." April 8, 2010.

Bourdon, Rick, Branch Chief, National Communications System Technology and Programs Office. Update on Current Activities. March 11, 2010.

Dixon, Eric (Major), U.S. Northern Command (NORTHCOM). "USNORTHCOM Deployable Capabilities." July 8, 2010.

Edwards, Eric, Director, Disaster Emergency Communications Division, Response Directorate, Office of Response and Recovery, Federal Emergency Management Agency. “Disaster Emergency Communications.” February 1, 2011.

Manner, Jennifer, Deputy Bureau Chief, Public Safety and Homeland Security Bureau, Federal Communications Commission. “National Broadband Plan Recommendations.” March 9, 2010.

Pavlak, Robert, District of Columbia Office of the Chief Technology Officer. “Public Safety Wireless Broadband 700 MHz LTE Networks for Public Safety: DC Projects and Recommendations to the NSTAC Communications Resiliency Task Force.” February 8, 2011.

Rooney, Kevin, U.S. Strategic Command. “Phoenix Air-to-Ground Communications Network.” February 8, 2011.

Suraci, Frank, Government Emergency Telecommunications Service/Wireless Priority Services Program Manager, Office of the Manager, National Communications System. “NGN Priority Services Efforts brief to Communications Resiliency Task Force.” April 8, 2010.