Communications

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007

Homeland Security

Communications Sector Government Coordinating Council Letter of Agreement

The National Infrastructure Protection Plan (NIPP) provides the unifying structure for the integration of critical infrastructures and key resources (CI/KR) protection efforts into a single National program. The NIPP provides an overall framework for integrating programs and activities that are under way in the various sectors, as well as new and developing CI/KR protection efforts. The NIPP includes 17 Sector-Specific Plans (SSPs) that detail the application of the overall risk management framework to each specific sector.

The Communications SSP describes a collaborative effort among the private sector, Federal Government, and State governments to protect the Nation's Communications Infrastructure. This collaboration will result in the assessment of risk to the communications architecture and its functions that will help prioritize protection initiatives and investments within the sector and aid the identification of critical assets against specific threats. By signing this letter, the Communications Government Coordinating Council (GCC) members commit to the following:

- Support SSP concepts and processes and carry out their assigned functional responsibilities regarding the protection of CI/KR as described herein;
- Work with the National Communications System (NCS) and the Secretary of Homeland Security, as appropriate and consistent with their own agency-specific authorities, resources, and programs, to coordinate funding and implementation of programs that enhance CI/KR protection;
- Cooperate and coordinate with the NCS and the Secretary of Homeland Security, in accordance with guidance provided in Homeland Security Presidential Directive 7 (HSPA4-7), as appropriate and consistent with their own agency-specific authorities, resources, and programs, to facilitate CI/KR protection;
- Develop and maintain partnerships for CI/KR protection with appropriate State, regional, local, tribal, and international entities; the private sector; and non-governmental organizations; and
- Protect critical infrastructure information according to the Protected Critical Infrastructure Information Program or other appropriate guidelines, and share CI/KR protection-related infor-

mation, as appropriate and consistent with their own agency-specific authorities and the process described herein.

Signatories

Barry C. West
Chief Information Officer
Office of the Secretary
Department of Commerce

William N. Bryan
Director
Critical Infrastructure Protection
Department of Defense

Kenneth P. Moran
Acting Bureau Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

James A. Williams
Commissioner
Federal Acquisition Service
General Services Administration

Gregory Garcia
Assistant Secretary
Cyber Security and Telecommunications
Department of Homeland Security

Awaiting Signature

Department of Justice

John Kneuer
Assistant Secretary
National Telecommunications and
Information Administration

Connie O. Hughes
Commissioner
New Jersey Board of Public Utilities

Chair,
David Barron
BellSouth

Vice Chair,
J. Michael Hickey
Verizon

Secretary,
Dan Bart
TIA

To Contact CSCC:
DBart@tiaonline.org

www.commscc.org

December 20, 2006

The Honorable Robert B. Stephan
Assistant Secretary for Infrastructure Protection
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Mr. Assistant Secretary:

Letter of Coordination

The National Infrastructure Protection Plan (NIPP) endeavors to provide a unifying structure for the integration of critical infrastructures and key resources (CI/KR) protection efforts into a single national program. The NIPP provides an overall framework to integrate programs and activities currently under way in the various sectors, as well as new and developing CI/KR protection efforts. The NIPP includes seventeen sector-specific plans (SSPs) that detail the application of the overall risk management framework to each specific sector.

The Communications SSP (CSSP) describes a collaborative effort among the private sector, Federal government, and state and local governments to protect the Nation's communications infrastructure. It is hoped that this collaboration will result in assessments of risk to the communications architecture and its functions in a way that will help better prioritize protection initiatives and investments within the sector and aid the identification of critical assets against specific threats.

The signing of this letter does not commit the Communications Sector Coordinating Council (CSCC), its members, or their companies to follow or implement specific measures as related to the CSSP. By signing this letter, the CSCC members acknowledge that they:

- Support, in general, CSSP concepts and will continue to work, as appropriate, with the National Communications System (NCS) and other security partners to develop and implement the CSSP;
- Have had an opportunity to provide insights and guidance on the unique needs, concerns, and perspectives of their organizations or members;
- Will maintain partnerships, as appropriate, to foster better CI/KR protection with relevant Federal, state and local government entities, and other private sector entities; and
- Will continue to work with the Department of Homeland Security and the

NCS to consider suitable mechanisms, such as proprietary marking and non-disclosure agreements, for possible sharing of CI/KR protection-related information.

Thank you for your continued support of the Communications Sector as we mobilize our constituencies around critical infrastructure protection. We look forward to working in this partnership and to future interaction with the other Sector Coordinating Councils both bilaterally and via the Partnership for Critical Infrastructure Security (PCIS).

Respectfully submitted,

Communications Sector Coordinating Council

By: David M. Barron
David M. Barron
Chair

J. Michael Hickey
Vice Chair

Dan Bart
Secretary

And the CSCC Executive Committee:
David Barron, BellSouth Corporation
Dan Bart, Telecommunications Industry Association
Jim Bugel, Cingular Wireless
Guy Copeland, Computer Sciences Corporation
Kate Dean, U.S. Internet Service Provider Association
J. Michael Hickey, Verizon Communications
Rick Kemper, CTIA – The Wireless Association
John Stogoski, Sprint-Nextel
Harry Underhill, AT&T

CSCC Members:

Alcatel-Lucent
Americom -GS
Association of Public Television Stations
AT&T
BellSouth Corporation
Boeing
Cincinnati Bell
Cingular Wireless
Cisco Systems
COMCAST
Computer Sciences Corporation
CTIA – The Wireless Association
Hughes Network Systems

Internet Security Alliance
Intrado
Level 3 Communications
McLeodUSA
Nortel
Qwest Communications
Rural Cellular Association
Satellite Industry Association
SAVVIS
Sprint-Nextel
Telcordia Technologies
Telecommunications Industry Association
United Telecom Council (UTC)
U.S. Internet Service Provider Association
USTelecom Association
Verizon Communications Inc.
VeriSign Inc.

Table of Contents

Executive Summary **1**

Background 2

Going Forward 2

Introduction **5**

Intersection With Other Homeland Security Initiatives 6

A National Communications Sector-Specific Plan 7

CSSP Structure 8

1. Sector Profile and Goals **9**

1.1 Sector Profile 9

1.2 Security Partners 11

1.2.1 Relationships With Private Sector Owner/Operators and Organizations 12

1.2.2 Federal Relationships 14

1.2.3 State and Local Relationships 16

1.2.4 International Relationships 18

1.3 Sector Security Goals 19

1.3.1 Vision Statement 19

1.3.2 Process to Establish Sector Security Goals 19

1.3.3 Sector Security Goals and Objectives 20

1.4 Value Proposition 23

2. Identify Assets, Systems, Networks, and Functions **25**

2.1 Defining Data Parameters 27

2.2 Collecting Infrastructure Information 27

2.2.1 Collecting Architectural Infrastructure Information 27

2.2.2 Collecting Specific Infrastructure Information 28

2.2.3 National Asset Database 28

2.2.4 Regulatory Requirements 29

2.3 Verifying Infrastructure Information 29

2.4 Updating Infrastructure Information 29

2.5 Protecting Infrastructure Information 29

3. Assess Risks **31**

3.1 Risk Assessments in the Sector 31

3.1.1 Industry Self-Assessments 32
3.1.2 Government-Sponsored Assessments 32
3.1.3 Government-Sponsored Cross-Sector Dependency Analyses 33
3.2 Government-Sponsored Risk Assessment Components 34
3.2.1 Infrastructure Screening and Consequence Assessment 34
3.2.2 Vulnerability Assessments 35
3.2.3 Threat Analysis 35
4. Prioritize Infrastructure 39
4.1 Communications Architecture Prioritization 39
4.1.1 National Prioritization 39
4.1.2 Industry Self-Prioritization 40
4.2 Cross-Sector Interdependency Analysis 40
5. Develop and Implement Protective Programs 43
5.1 Protection Roles and Responsibilities 44
5.1.1 Industry Customer Outreach 45
5.1.2 Shared Asset Protection 45
5.2 Existing Programs 45
5.2.1 Government-Sponsored Programs 45
5.2.2 Industry Protective Measures and Initiatives 47
5.3 Protective Program Identification Process 48
5.4 Protective Program Development and Implementation 49
5.5 Government Protective Program Performance 49
6. Measure Progress 53
6.1 CI/KR Performance Measurement 54
6.1.1 Communications Sector Metric Development 54
6.1.2 Information Collection and Verification 60
6.1.3 Reporting 60
6.2 Implementation Actions and Monitoring Performance 60
6.3 Challenges and Continuous Improvement 66
7. CI/KR Protection Research and Development 67
7.1 R&D Collaboration 67
7.1.1 Industry Coordination 68
7.1.2 Interagency Coordination 68
7.2 Identification of R&D Requirements 69
7.3 Analysis of Gaps 70
7.4 Establishment of R&D Priorities 72
7.4.1 Modeling and Simulation Requirements 74

8. Manage and Coordinate SSA Responsibilities **75**
8.1 Program Management Approach 75
8.2 Processes and Responsibilities 76
8.2.1 SSP Maintenance and Update 76
8.2.2 Annual Reporting 77
8.2.3 Resources and Budgets 77
8.2.4 Training and Education 77
8.3 Implementing the Sector Partnership Model 78
8.3.1 Coordinating Structures 78
8.4 Information Sharing and Protection 79
8.4.1 Information-Sharing Mechanisms 79
8.4.2 Data Protection Mechanisms 82
Appendix 1: List of Acronyms and Abbreviations **83**
Appendix 2: Glossary of Key Terms **87**
Appendix 3: Authorities **91**
3.1 Broad Communications Infrastructure Protection Policies 91
3.2 SSA Authorities 91
3.3 Coordinating Agency Authorities 92
3.4 Other Guidance 93
Appendix 4: Sector Profile **95**
4.1 Wireline Infrastructure 95
4.2 Wireless Infrastructure 98
4.3 Satellite Infrastructure 99
4.4 Cable Infrastructure 100
4.5 Broadcasting Infrastructure 101
Appendix 5: Existing Protective Programs **103**
5.1 Protective Actions 103
5.2 Preparedness Actions 104
5.3 Internet Security Programs 106
Appendix 6: Communications Sector Best Practices **109**
Appendix 7: R&D Initiatives **111**

List of Figures

Figure S-1. NIPP Risk Management Framework 3
Figure S-2. Communications Sector Security Goals 3
Figure I-1. NIPP Risk Management Framework 6
Figure I-2. Chapter Overview 8
Figure 1-1. Communications Sector Relationship Map 12
Figure 2-1. Communications Architecture and Risk Assignments 26
Figure 3-1. Improving Communications Resiliency 34
Figure 6-1. Communications Sector Performance Measurement Framework 55
Figure 7-1. R&D Process 67
Figure 8-1. Communications Sector Information Flow 81
Figure A4-1. Wireline Network Architecture 96
Figure A4-2. SS7 and Wireline Network Architecture 96
Figure A4-3. Next Generation Networks 97
Figure A4-4. VoIP Networks 97
Figure A4-5. Submarine Cable Architecture 98
Figure A4-6. Internet Architecture 98
Figure A4-7. Wireless Network Architecture 99
Figure A4-8. Satellite Network Architecture 100
Figure A4-9. Cable Network Architecture 101

List of Tables

Table 1-1. Communications Sector Partnerships 14
Table 1-2. Communications Sector Federal Relationships and Key Entities 15
Table 1-3. Emergency Response Organizations 17
Table 1-4. Chapter 1 Roles and Responsibilities 24
Table 2-1. Chapter 2 Roles and Responsibilities 30
Table 3-1. Communications Sector Consequences of Concern 35
Table 3-2. Chapter 3 Roles and Responsibilities 37
Table 4-1. Examples of CI Interdependencies With Communications 40
Table 4-2. Chapter 4 Roles and Responsibilities 42
Table 5-1. Associating Protective Programs With Goals and Risks 44
Table 5-2. Communications Sector Protective and Preparedness Programs 46
Table 5-3. Chapter 5 Roles and Responsibilities 50
Table 6-1. Potential Communications Sector Measurement Areas 57
Table 6-2. Communications Sector Metric Template 58

Table 6-3. Metrics Development Timeline 59
Table 6-4. Implementation Actions 61
Table 7-1. National CI/KR Protection R&D Themes 70
Table 7-2. Illustrative Maturity Chart 71
Table 7-3. Risk Management Approach 72
Table 8-1. Program Management Responsibilities 76
Table 8-2. Chapter 8 Roles and Responsibilities 82
Table A6-1. NRIC Best Practices Categories 110
Table A7-1. R&D Initiatives 111

Executive Summary

The terrorist attacks of September 11, 2001, and the unprecedented impact of Hurricane Katrina on the communications infrastructure significantly redefined the Communications Sector threat environment. The importance of communications to the Nation's health and safety, economy, and public confidence cannot be overstated.

To address the pre-existing threat environment of natural disasters, while factoring in the new threat of terrorism, the Department of Homeland Security (DHS) released the National Infrastructure Protection Plan (NIPP). The plan provides a comprehensive risk management framework that defines critical infrastructure protection roles and responsibilities for all levels of government and private industry. The DHS recognizes that a successful risk assessment framework requires cooperation and coordination among Federal departments and agencies; State, local, and tribal governments; private sector owners and operators; and international partners.

To implement the NIPP, Sector-Specific Agencies (SSAs) for each of the 17 critical infrastructure and key resources (CI/KR) sectors are partnering with State, local, and tribal governments, and industry to create and implement Sector-Specific Plans (SSPs). The National Communications System (NCS), within the DHS, serves as the SSA for the Communications Sector.

The SSPs are intended to ensure that each of the CI/KR sectors effectively coordinate with their security partners, other sectors, and the DHS to enhance protection and resiliency in an all-hazards environment. These plans are designed to evolve over time as threats change and protective programs are implemented.

The development and implementation of the Communications SSP provides an opportunity for industry and government sector security partners to take advantage of the infrastructure protection framework it provides. For government partners, the processes outlined in this plan support their missions to execute command, control, and coordination, to provide national, economic, and homeland security, and to ensure public health and safety. For private sector partners, the protection of critical infrastructure is important for the security of their employees, assets, business continuity, and services provided to customers.

This Communications SSP (CSSP) results from a close collaboration among the NCS, the Communications Sector Coordinating Council, and the Communications Government Coordinating Council (GCC). It provides a framework for industry and government partners to develop a coordinated protection strategy. Private sector companies have existing protection efforts, which are aimed at limiting risk to the business and maintaining operational capabilities. Business leaders have a board-level responsibility to direct these efforts and ensure they are implemented effectively. The Federal Government has a responsibility to develop and execute a national plan, which protects the overall security of the Nation.

The vision developed within the CSSP utilizes both public and private resources to establish a single strategic framework for protecting the Nation's critical communications infrastructure. This framework builds upon already strong corporate capabilities, unique government resources, and coordination capabilities beyond what business can provide. This combined capacity will help to maximize Communications Sector efforts to protect critical assets against natural and manmade threats.

Background

The communications companies that own, operate, and supply the Nation's communications infrastructure have historically factored natural disasters and accidental disruptions into network resiliency architecture, business continuity plans, and disaster recovery strategies. The interconnected and interdependent nature of these service provider networks has fostered crucial information sharing and cooperative response and recovery relationships for decades. Since one service provider network problem nearly always impacts the networks owned and operated by other network providers, the community has a long-standing tradition of cooperation and trust—even in today's highly competitive business environment.

Private sector owners and operators have enjoyed a close working relationship with the NCS since it was first created in 1963. This relationship was further enhanced by the establishment of the National Coordinating Center (NCC) in 1984. The NCC serves as a joint industry-government operations center with a clear mission of advancing information sharing and coordination. Under the aegis of the NCC, many member companies participated in the design and execution of the Local Exchange Carrier Mutual-Aid Agreement. This agreement was subsequently adopted in Canada and used for cross-border mutual aid.

Public and private sector collaboration within the Communications Sector has been advanced through other channels, including the President's National Security Telecommunications Advisory Committee (NSTAC). The NSTAC provides advice to the President in matters pertaining to national security and emergency preparedness (NS/EP) communications. This advice has led to and assisted in the development of the NS/EP programs for priority telecommunications services, later described in this document. Such services include Government Emergency Telecommunications Service (GETS), Telecommunications Service Priority (TSP), and Wireless Priority Service (WPS).

Over a decade ago, the NCS created joint industry and government Nwtwork Security Information Exchanges to further strengthen the information-sharing and threat analysis capacity of public and private sector partners. The NCS currently sponsors six of these exchanges annually.

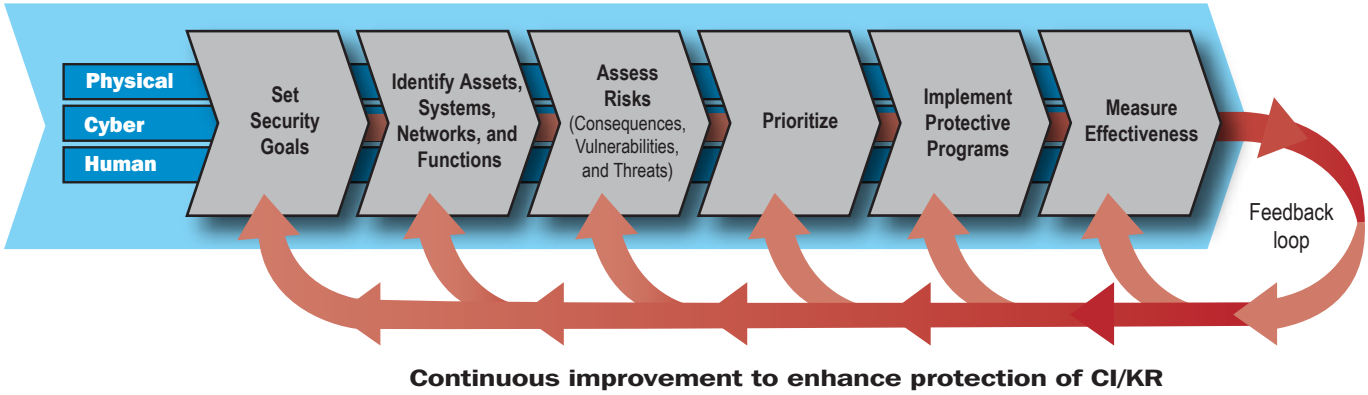
Going Forward

The Communications Sector's security strategy is to ensure the Nation's communications networks and systems are secure, resilient, and rapidly restored after an incident. The approach outlined in the CSSP includes:

- Utilizing industry and government partnerships to protect the communications infrastructure by leveraging corporate capabilities and government programs;
- Adopting an architectural approach to infrastructure identification and risk assessment processes;
- Coordinating with other CI/KR sectors and customers on communications infrastructure dependencies and solutions for mitigating risk; and
- Working closely with the DHS to integrate plan outcomes into national CI/KR products.

The NIPP established a common risk management framework for use by the 17 individual sectors. Within this framework, goals are established, risks are assessed, and priority programs are defined to enhance critical infrastructure protection. Figure S-1 illustrates the framework that provides the foundation for this plan.

Figure S-1: NIPP Risk Management Framework



The Communications Sector security goals are illustrated in figure S-2. CSSP partners considered existing programs and best practices when setting the sector's goals for securing physical, cyber, and human assets. The goals identified in the plan focus on protecting the overall health of national communications backbone; response and recovery during and after an attack or disaster; information sharing, awareness, and education in the context of current and potential future threats; and cross-sector coordination to address critical interdependencies.

National critical architecture elements are networks, systems, or functions that—if destroyed, disrupted, or exploited—would seriously threaten national security, result in catastrophic health effects or mass casualties, weaken the economy, or damage public morale and confidence.

Figure S-2: Communications Sector Security Goals

Goal 1: Protect the overall health of the national communications backbone.

Goal 2: Rapidly reconstitute critical communications services after national and regional emergencies.

Goal 3: Plan for emergencies and crises by participating in exercises and updating response and continuity of operations plans.

Goal 4: Develop protocols to manage the exponential surge in utilization during an emergency situation and ensure the integrity of sector networks during and after an emergency event.

Goal 5: Educate stakeholders on communications infrastructure resiliency and risk management practices in the Communications Sector.

Goal 6: Ensure timely, relevant, and accurate threat information sharing between the law enforcement and intelligence communities and key decisionmakers in the sector.

Goal 7: Establish effective cross-sector coordination mechanisms to address critical interdependencies, including incident situational awareness, and cross-sector incident management.

The CSSP focuses the Communications Sector's risk management process on identifying and protecting nationally critical architecture elements; ensuring overall network reliability; maintaining "always-on" services for critical customers; and quickly restoring critical communications functions and services following a disruption.

The framework's risk assessment process analyzes threats and vulnerabilities to better understand associated risks to the infrastructure. The CSSP discusses three levels of risk assessment activity, which include:

- Industry self-assessments;
- Government-sponsored risk assessments; and
- Government-sponsored cross-sector dependency analyses.

The first level of activity addresses the historically significant internal measures taken by private sector owners and operators to ensure the reliability of their services. Private sector owners and operators infuse business continuity and contingency planning principles into standard operating business practice. Risks associated with networks, products, and services are assessed routinely to improve business practice and better meet customer expectations. Lessons learned from incidents that occur during the normal course of business are analyzed, and solutions are incorporated into ongoing business operations.

The second level of activity addresses the need to assess national communications architecture. The Nation's communications infrastructure is a complex system of systems that incorporates multiple technologies and services with diverse ownership. The infrastructure includes wireline, wireless, satellite, cable, and broadcasting capabilities, and includes the transport networks that support the Internet and other key information systems. Defining an agreed-upon architecture will provide a common risk assessment lens for government and private sector participants. The assessment of the Nation's communications architecture by industry and government review and analysis will yield a comprehensive picture of risk.

The third level of activity provides a vehicle for the other 16 critical infrastructure sectors to assess cross-sector communications risks and solutions. There is a need to address how private sector and government customers utilize available communications services to support their critical missions and processes. Customers need to understand how the infrastructure operates and the associated levels of risks for a given design solution. This knowledge enables customers to determine what is required to sustain their critical functions during times of crisis. Enhanced facilities, modified business practices, or alternative solutions may be required to provide the level of assurance needed for the continuity of business operations.

Once the national risk assessment is completed, the Communications Sector will determine what initiatives may be needed to strengthen infrastructure protection and to secure the necessary resources to address priorities. This effort may necessitate the enhancement of existing protective programs and the creation of new programs, as necessary. New programs will be evaluated using defined sector goals to ensure alignment with the CSSP framework.

The development and implementation of the CSSP encourages public and private sector security partners to enhance the Nation's communications infrastructure protection framework. For government partners, the processes outlined in this plan support their missions to execute command, control, and coordinate; to provide national, economic, and homeland security; and to ensure public health and safety. For private sector partners, enhanced security and critical infrastructure protection is crucial for safeguarding physical, cyber, and human assets, systems, and networks, ensuring continuity of business operations, and enhancing shareholder value. The Sector Partnership Model supporting the NIPP and the CSSP also provides an opportunity for cross-sector collaboration on a scale that has not previously existed. Such collaboration brings value during incident response, when working with other CI/KR sectors becomes crucial to response and recovery efforts.

Introduction

The threat of terrorist attacks and catastrophic natural disasters brings to the forefront the need to focus our national attention on protecting the Nation's critical infrastructures and making them more resilient. The events of September 11, 2001, and the hurricanes of 2005 highlighted the importance of communications to public health and safety, to the economy, and to public confidence. At the same time, these disasters proved the overall resiliency of the national communications network. Despite the enormity of these incidents, the network backbone remained intact.

The *Homeland Security Act* of 2002 and subsequent Presidential strategies[1] provided the authority and direction for what must be done to protect critical infrastructures. Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*, issued by the President on December 17, 2003, provided the direction on how to implement the strategic vision.

HSPD-7 required the Department of Homeland Security (DHS) to lead the development of a National Infrastructure Protection Plan (NIPP). The NIPP provides a structure to unify existing and future critical infrastructure and key resources (CI/KR) protection efforts under a single national program. The NIPP draws on a risk management framework that aims to mitigate risk in the context of an all-hazards environment.

HSPD-7 recognizes that CI/KR sectors possess unique characteristics and operating models, and assigns critical infrastructure protection responsibilities for each sector to individual Federal Sector-Specific Agencies (SSAs), with guidance to be provided by the DHS. To implement HSPD-7, SSAs were tasked with developing Sector-Specific Plans (SSPs) in partnership with public and private stakeholders. These SSPs are expected to follow and support the risk management approach (illustrated in figure I-1) and key steps as outlined in the NIPP:

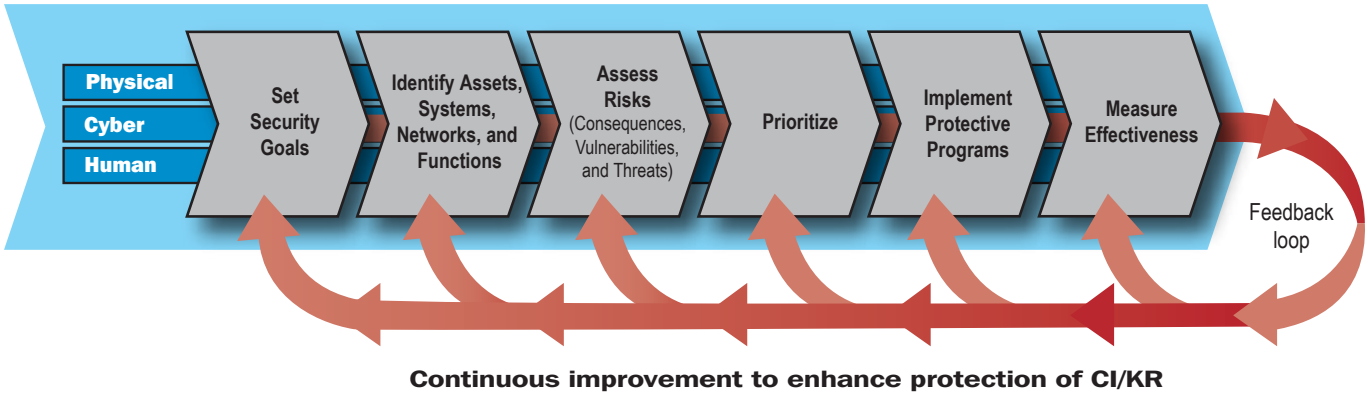
Setting sector-specific security goals;

- Identifying the sector's assets, networks, systems, and functions;
- Identifying and assessing risk for the sector, based on an analysis of vulnerabilities and potential threats and consequences;
- Prioritizing infrastructure based on risk assessments and normalization of data;

[1] The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (February 2003), and The *National Strategy to Secure Cyberspace* (February 2003).

- Developing protective measures to protect critical infrastructure and implementing these programs effectively and efficiently; and
- Using metrics to measure and communicate the effectiveness of the SSP and associated sector protective measures.

Figure I-1: NIPP Risk Management Framework



The ultimate objective of the SSPs is to have Federal, State, and local agencies, and the private sector work with SSAs to develop and implement sector plans in a way that is consistent, sustainable, effective, and measurable.

Intersection With Other Homeland Security Initiatives

Implementing CI/KR protection requires partnerships, coordination, and collaboration among all levels of government and the private sector. Homeland security plans and strategies at the Federal, State, local, and tribal levels of government address CI/KR protection within their respective jurisdictions. Similarly, private sector owners and operators have responded to the post-9/11 environment by instituting a range of CI/KR protection-related plans and programs, including business continuity and resiliency measures. The NIPP and the National Response Plan (NRP) together provide a comprehensive, integrated approach to the homeland security mission. The NIPP establishes the overall risk-based approach that defines the Nation's CI/KR steady-state protective posture, while the NRP provides the approach for domestic incident management.

In most instances, State and local agencies take the lead on preparedness and response. Under the NRP, the Federal role is to support the activities of these agencies. At the national level, Communications Sector preparedness activities are coordinated primarily through the National Coordinating Center (NCC). In the NCC, industry and governments experts jointly plan and work to support a more endurable national communications system.

During an event, the NCC coordinates the initiation and reconstitution of national security and emergency preparedness (NS/EP) communications services and facilities. As the operational arm of the NCS, the NCC carries out Emergency Support Function (ESF) #2 (Communications) responsibilities under the NRP. The NCC's all-hazard response approach relies on the flexible application of resources to meet crises. When a Cyber Incident of National Significance[2] occurs, the DHS National Cyber

[2] A Cyber Incident of National Significance is induced directly through cyber means, with cyber or physical results that cause or are likely to cause harm to mission-critical functions across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threaten public health or safety, undermine public confidence, have a negative effect on the national economy, or diminish the security posture of the Nation.

Security Division (NCSD) coordinates with the NCS through the National Cyber Response Coordination Group (NCRCG)[3] and supports the Joint Telecommunications Resources Board (JTRB)[4].

A National Communications Sector-Specific Plan

The communications infrastructure is a complex system of systems that incorporates multiple technologies and services with diverse ownership. The infrastructure includes wireline, wireless, satellite, cable, and broadcasting, and provides the transport networks that support the Internet and other key information systems. With a strong and well-refined focus on risk management, long-established processes and procedures for network security and rapid response and recovery under all hazards assure the continued operation of vital communications services. Focused risk management and infrastructure protection are integral to the sector's business continuity planning and network design processes. These network level protective strategies and individual owner/operator protective measures are tested, implemented, and used daily to rapidly restore outages caused not only by those with malicious intent (e.g., cyber attacks) but also by accidental or natural incidents such as flooding, earthquake, hurricanes, or tornados. The resiliency built into the communications infrastructure increases the availability of service to its customers and reduces the impact of outages. In addition, priority service programs, including Government Emergency Telecommunications Service (GETS), Telecommunications Service Priority (TSP), and Wireless Priority Service (WPS) provide capabilities to assure critical communications to support response, restoration, and assurance of critical services and functions.

Communications Sector owners and operators focus on ensuring overall reliability of the networks, maintaining "always on" capabilities for certain critical customers, and quickly restoring capabilities following a disruption. The sector mitigates cascading effects of incidents by designing and building resilient and redundant communications systems and networks to ensure disruptions remain largely localized and do not affect the national communications backbone.

While the sector focuses on ensuring network level systems are resilient and secure, customers must ensure their own critical systems and operations are supported by diverse primary and backup communications capabilities. Although the Communications Sector industry partners maintain and protect the core backbone and shared assets and systems portion of the network (e.g., public switched telephone network (PSTN) switches, asynchronous transfer mode (ATM) switches, video servers for video on demand, Internet Protocol (IP) routers for Internet providers) and the facilities connecting these assets to the customer premises, customers must understand the risk inherent in the access portion of their network and develop and employ mitigation strategies accordingly. As both an owner of communications assets and a customer of commercial communications services, all levels of government have the responsibility to understand and mitigate their own risk through continuity of operations (COOP) planning.

This plan outlines the infrastructure protection activities in which the Communications Sector industry and government partners will individually and cooperatively mitigate risks to national communications infrastructure assets and services that, if exploited, would have a national impact. The Communications Sector-Specific Plan (CSSP) is the result of a collaborative infrastructure protection planning process through the NCS, the Communications Sector Coordinating Council (CSCC), and the Communications Government Coordinating Council (CGCC).

The CSSP is supported through strong industry and government partnerships with NCS as the SSA for the Communications Sector. For almost 25 years, industry and government have worked closely together on NS/EP communications issues through the NCC, the President's National Security Telecommunications Advisory Committee (NSTAC), and Network Security Information Exchanges (NSIE).

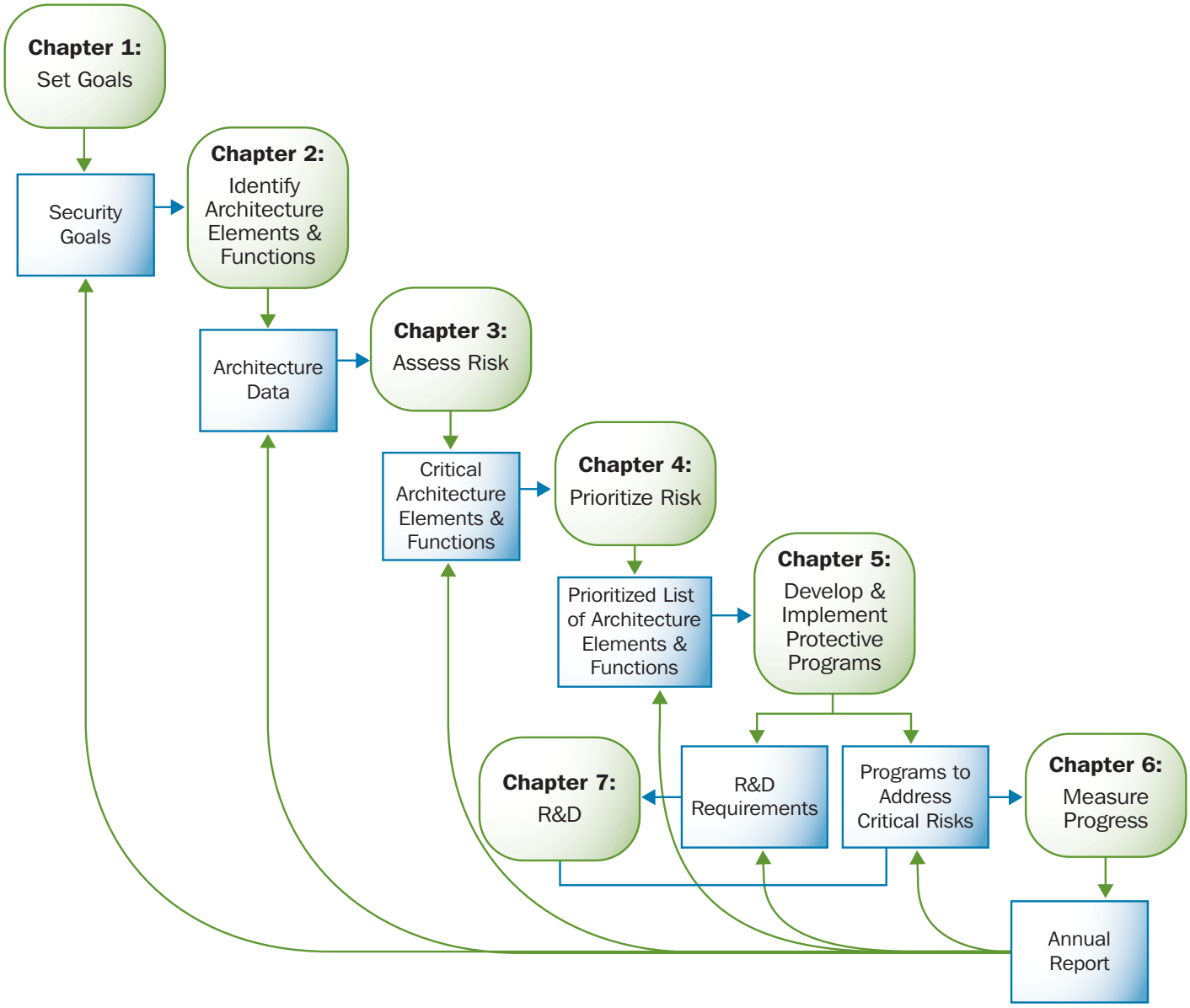
[3] The NCRCG is an interagency group that facilitates Federal efforts to prepare for, respond to, and recover from cyber incidents and physical attacks that have significant cyber consequences.

[4] The JTRB is an interagency forum that deliberates during major crises, resolves competing demands for communications services, and monitors the performance of the national communications infrastructure during emergencies.

CSSP Structure

The CSSP helps provide a common understanding of the national strategy for critical infrastructure protection in the Communications Sector. The plan provides a consistent path for industry and government partners to follow, minimizing divergent courses that might otherwise have been taken. The CSSP is organized into eight chapters. The first seven chapters outline risk management from the goal-setting process to measuring progress. The output of each chapter and relationships with other chapters is illustrated in figure I-2. The final chapter discusses SSA responsibilities and management of the risk management and infrastructure protection process.

Figure I-2: Chapter Overview



1. Sector Profile and Goals

This section provides a characterization of the Communications Sector, including an overview of sector assets and a review of governing authorities. This section also provides an overview of security partner interactions within the Communications Sector between private sector companies and organizations; the Federal Government; State, local, and tribal governments; foreign governments; and international organizations. It portrays the complexity of this sector and illustrates how a network of individual companies, organizations, and governments come together to protect the infrastructure. Finally, this chapter describes the sector's goals and desired long-term security posture.

1.1 Sector Profile

Developments in the policy, economic, technology, and threat arenas have positioned the Communications Sector at a critical juncture. Over the past 20 years, the sector has evolved from a predominantly closed and secure wireline telecommunications network focused on providing equipment and voice services, into a diverse, open, highly competitive, and interconnected industry with wireless, satellite, and cable service companies providing many of those same services. Although market competition and standardization have helped lower prices and spurred the development of new services, these developments also have presented new challenges to protecting critical communications assets for NS/EP purposes.

Two key policy events helped shape the modern-day communications industry. The first event was the 1984 court-ordered breakup of AT&T, which controlled the majority of the local and long distance markets. The second event was the passage of the *Telecommunications Act of 1996*, which, as the Telecommunications Act conference report states, aimed "to provide for a pro-competitive, de-regulatory national policy framework designed to accelerate rapidly private sector deployment of advanced telecommunications and information technologies and services to all Americans by opening all telecommunications markets to competition." As a result, instead of one company controlling and protecting the entire communications network, hundreds of wireline and wireless companies, including cellular and satellite, provide communications services today.

The industry continued to expand in concert with the economic boom of the late 1990s, which spurred a network-building binge within the Communications Sector. Large investments were made in new fiber facilities, helping modernize the communications infrastructure and deliver advanced Internet services to home and business users. As the Nation began to experience an economic downturn at the turn of the century, the communications industry saw an oversupply of capacity and a drop in prices. Capital spending declined, jobs were cut, and seasoned communications industry players and new competitors filed for bankruptcy.

In addition to these sweeping regulatory and economic changes, technological convergence has also had a profound impact on the communications industry. Whereas the public network had consisted primarily of the narrowband, mature PSTN, it is now rapidly evolving toward wideband packet-based next-generation networks (NGNs). In addition to the complexity associ-

ated with convergence, the Nation's communications system is characterized by the diversity of technology and the intra-sector dependencies.

Telecommunications is defined as: "(1) Any transmission, emission, or reception of signs, signals, writing, images, and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems; or (2) any transmission emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems," in American National Standard T1.523-2001, Telecommunications—Telecom Glossary 2000. In addition, industry organizations, such as the Alliance for Telecommunications Industry Solutions (ATIS) and the Telecommunications Industry Association (TIA), consider the Communications Sector as "including the (tele)communications service providers, network operators, regulators, manufacturers and suppliers, subscribers, and users."

The Communications Sector is integrally linked with the Information Technology (IT) Sector, which is composed of entities—often owners and operators and their respective associations—who produce and provide hardware, software, IT systems and services, including development, integration, operations, communications, and security. These IT Sector products are employed across other critical infrastructures and the government. The IT Sector also can be considered the "IT Industrial Base." In a cooperative effort, the Communications and IT Sectors will hold a joint meeting twice annually to address issues of interest to both sectors and discuss potential areas for collaboration. The Communications Sector has an indelible linkage, shared responsibilities, and interdependencies with the IT Sector (e.g., the Internet, routers, Internet points of presence (POP), Internet peering points); however, certain boundaries exist between the two sectors. Because of this linkage, the two sectors will collaborate on areas spanning the scope of this SSP. Examples of joint activities include the following:

- Identifying synergies and gaps between Communications and IT security partners, and collaborating whenever possible on partner outreach;
- Working closely on assessing and addressing shared Internet architecture elements; and
- Cooperatively addressing areas of convergence, such as those identified in the NSTAC Report to the President on the NCC, including developing an approach for a long-term regional communications and IT coordinating capability that serve all regions of the Nation, convening a conference to focus on cyber issues, and exploring ideas for a multi-industry coordinating center.

Driven by 21st century technology transformation and convergence, the Communications and the IT sectors will become more closely aligned over time. The Communications Sector includes not only physical properties such as wireline, wireless, satellite, cable, and broadcasting but also services such as the Internet, information services, and cable television networks. In addition, publicly and privately owned cyber/logical assets are inextricably linked with these physical communications structures. Brief descriptions of each component follow. Detailed descriptions of each component are provided in appendix 4.

- **Wireline:** The wireline component consists primarily of the PSTN, but also includes cable networks and enterprise networks. Traditionally it has been divided between interexchange carriers (IXC) and local exchange carriers (LEC), which are defined in appendix 4; however, following passage of the *Telecommunications Act of 1996*, new competitive local exchange carriers (CLEC) entered the local, long distance, and data services markets, as did some traditional cable television providers. Today, many larger carriers operate in various areas of the Nation in all of the capacities listed above. Wireline networks also are being redefined by NGNs, which are high-speed converged circuit-switched and packet-switched networks capable of transporting and routing a multitude of services, including voice, data, video, and multimedia, across variant platforms. The wireline component also includes the Internet, and submarine cable infrastructure;
- **Wireless:** The wireless component consists primarily of cellular telephone, paging, personal communications services, high-frequency radio, unlicensed wireless, and other commercial and private radio services—including numerous law enforcement, public safety, and land mobile radio systems;

- **Satellite:** Satellite communications systems use a combination of terrestrial and space components to deliver various communications, Internet data, and video services. Three different types of satellite services exist: fixed, broadcast, and mobile. Fixed Satellite Services (FSS) generally support voice, data, and video broadcast services, as well as Internet backbone connectivity. Broadcast Satellite Services (BSS) support video programming (i.e., DirecTV) and digital radio services. Mobile Satellite Services (MSS) support voice, voice band data, and broadband data service;
- **Cable:** Cable television (CATV) networks are wireline networks offering television, Internet, and voice services that interconnect with the PSTN through end offices. Primary CATV network components include headends and fiber optic and/or hybrid fiber cables (HFC). Since the CATV network was designed primarily for downstream transmission of television signals, most of the existing network is being refitted to support two-way data transmissions; and
- **Broadcasting:** Broadcasting elements consist of all parts of a radio or television station transmission system. These elements have a direct and fundamental effect on the station's ability to remain on the air and to provide news and emergency information to the public. Much of the broadcasting infrastructure overlaps with the other subsectors of the Communications Sector, especially satellites that are used widely for transmission.

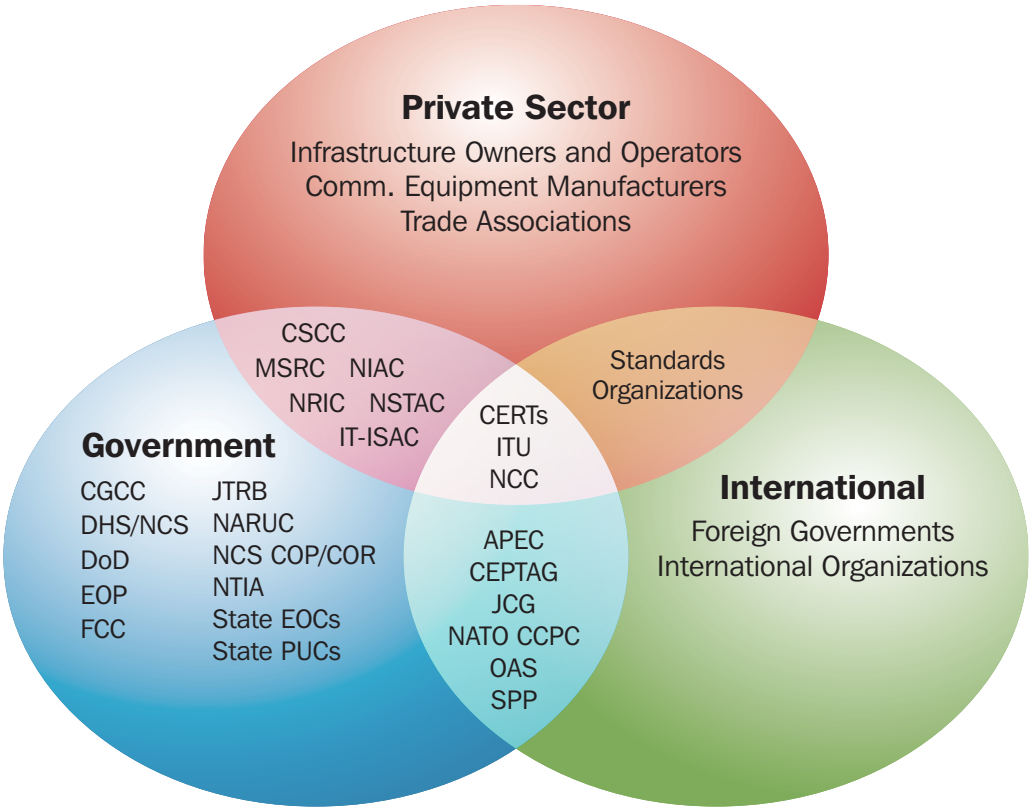
While the private sector owns more than 85 percent of critical infrastructure, government and public safety agencies own and operate communications systems that support their critical missions, including defense, law enforcement, and public safety. The Department of Defense, for example, owns and operates communications systems in at least four of the components. Public safety agencies are heavily vested in wireless communications (e.g., land mobile radio) for disaster response.

1.2 Security Partners

Relationships in the Communications Sector span a magnitude of private sector, government, and international organizations. This subsection describes the current relationships between the variety of sector partners. Figure 1-1 illustrates the complexity of the Communications Sector and the numerous government agencies that have a role in communications infrastructure protection. The NCS leads these protective efforts, with particular support from the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA). The National Association for Regulatory Utility Commissioners (NARUC) serves as the coordinator between Federal efforts and State and local governments.

The Communications Sector focuses its protective strategies and response efforts through such partnerships as the NSTAC, the NCC, the NSIEs, and the NCS Committee of Principals (COP). These partnerships have proven effective during many natural disasters and events such as 9/11. In addition, the CSCC and CGCC also provide leadership to the sector and builds on efforts to increase assurance and resilience. The NCS has coordinated the development of the CSSP with all of these partners and will work with them to implement the plan.

Figure 1-1: Communications Sector Relationship Map



Note: Please see appendix 1 for definitions of acronyms.

1.2.1 Relationships With Private Sector Owner/Operators and Organizations

Inter-Company Sector Relationships

The Communications Sector is composed of wireline and wireless communications carriers, cable, Internet Service Providers (ISPs), CLECs, network service providers, equipment manufacturers and suppliers, and software providers. In addition, numerous trade associations represent broad industry perspectives on several issues such as security and assurance.

Because of the interconnectivity and interoperability aspects of networks, sector partners have broad requirements to collaborate in numerous areas, such as network interconnection, collocation, equipment and software standards, and response planning. For example, companies collaborated through ATIS on the National Diversity Assurance Initiative to create a framework and process for studying circuit diversity. Companies work together regularly at all levels during response activities, from high-level executives to emergency operations centers (EOC) to field offices. The NCC, described below, facilitates many of these coordination activities, coalescent with Federal efforts. Overall, industry has built resiliency and redundancy into their systems, providing a high level of assurance that the Communications Sector will continue to operate and support critical infrastructures and systems during emergencies.

Industry-Government Relationships

Industry and government have worked closely together on communications issues since the breakup of AT&T and the Bell System in the early 1980s. Today, various industry partnerships and forums advise government on communications issues, share information about vulnerabilities and threats, and develop best practices for securing the infrastructure. The success of many of these partnerships rests on the ability to establish a trusted environment where sensitive information can be shared.

Brief descriptions of the key industry and government communications partnerships, including each group's focus and membership, are provided below.

Critical Infrastructure Partnership Advisory Council (CIPAC)

The CIPAC represents a partnership between government and CI/KR owners and operators and provides a forum in which they can engage in a broad spectrum of activities to support and coordinate critical infrastructure protection. CIPAC membership includes both Sector Coordinating Council (SCC)-member CI/KR owner/operator institutions and their designated trade or equivalent organizations, and Government Coordinating Council (GCC)-member representatives from Federal, State, local, and tribal governmental entities. CIPAC activities, managed and coordinated by the DHS, include planning, coordination, security program implementation, and operational activities related to critical infrastructure protection security measures, including incident response, recovery, and reconstitution. (See chapter 8 for more discussion on the SCC and GCC.)

President's National Security Telecommunications Advisory Committee (NSTAC)

The NSTAC provides industry-based advice and expertise on issues related to the implementation of NS/EP communications policy. The NSTAC includes up to 30 chief executive officers from various components of the Communications Sector: communications service providers, software and hardware manufacturers, information systems security providers, major information users, the aerospace industry, and trade associations. Through its working body, the Industry Executive Subcommittee, the NSTAC studies topics related to infrastructure protection, including vulnerability analyses, protective methods, technological convergence, and infrastructure interdependencies. Studies and recommendations that are approved by the NSTAC are forwarded to the President for consideration.

National Coordinating Center (NCC)

Managed by the NCS, the NCC includes government agencies, major communications carriers (wireline and wireless), equipment manufacturers, software vendors, network services providers, select CLECs and ISPs, and major communications trade associations.

The NCC provides two important infrastructure protection functions. Its primary mission is to assist in the initiation, coordination, restoration, and reconstitution of NS/EP communications services under all conditions, crises, or emergencies. Composed of industry and government representatives, NCC members also work together during day-to-day operations and produce emergency response plans and procedures to be used during real-world events. Designated the Telecommunications Sector Information Sharing and Analysis Center (ISAC) in January 2000, the NCC facilitates voluntary collaboration and information sharing among its participants, and the gathering of information on vulnerabilities, threats, intrusions, and anomalies from the communications industry, government, and other sources. In 2006, the ISAC was renamed the Communications ISAC (C-ISAC).

Network Security Information Exchanges (NSIEs)

The NCS, in coordination with the NSTAC, established the NSIEs in 1991 as a structure for fostering an informal, collegial exchange on network security issues regarding the PSTN. The NSIE consists of two forums—the government NSIE and the NSTAC NSIE. Members of the government NSIE represent agencies that have research, standards, regulatory, law enforcement, or intelligence functions related to the Public Network, or are major communications users. NSTAC NSIE members include representatives from communications service providers, equipment vendors, systems integrators, and major users. The NSIEs meet jointly about every 2 months to exchange information and views on threats and incidents affecting the public network's software elements, vulnerabilities, and their remedies. In addition, the NSIEs periodically conduct an assessment of the risk to the PSTN from electronic intrusion.

Network Reliability and Interoperability Council (NRIC)

The NRIC is a Federal advisory body chartered by the FCC created to facilitate enhancement of emergency communications networks, homeland security, and best practices across the telecommunications industry. Participants include executives from major communications carriers and equipment manufacturers, ISPs, representatives from the public safety community, Federal and State regulators, the NCS, NTIA, and the Office of Science and Technology Policy (OSTP).

Other industry and government communications partnerships, including each group's focus and membership, are described in table 1-1.

Table 1-1: Communications Sector Partnerships

Name	Description
The Internet Disruption Working Group (IDWG)	The IDWG is a strategic partnership between public and private sector entities formed in response to concerns surrounding the dependency of critical communications, operations, and services on Internet functions. The IDWG is focused on identifying actions that government and other security partners can take in the near term to prepare for, protect against, and mitigate nationally significant Internet disruptions. The NCS and NCSD are co-leads of the IDWG.
ISAC Council	The ISAC Council is composed of senior CI/KR sector leaders representing the major ISACs, including the NCC. In ensuring the security of the Nation's physical and cyber/logical CI/KR, the council supports exchange among ISACs and with government. The council works closely with the DHS to strengthen information-sharing relationships and practices.
Media Security and Reliability Council (MSRC)	The MSRC is an FCC Federal advisory committee focused on assuring the optimal reliability, robustness and security of the broadcast and multichannel video programming distribution (MVPD) industries in emergency situations, the MSRC mission is to develop comprehensive national strategies for securing and sustaining broadcast and MVPD facilities during all crises nationwide. Members include major broadcasters, cable and satellite television providers, and trade associations.
National Infrastructure Advisory Council (NIAC)	The NIAC provides the President with advice on the security of the critical infrastructure sectors and their information systems. The council is composed of a maximum of 30 members, appointed by the President from private industry, academia, and State and local government.
Partnership for Critical Infrastructure Security (PCIS)	The PCIS is made up of representatives from each SCC, including the CSCC. Working closely with the DHS, the PCIS coordinates cross-sector initiatives to support CI/KR protection by identifying legislative issues that affect such initiatives and by raising awareness of issues in CI/KR protection.
TSP Oversight Committee	The TSP Oversight Committee is chartered to identify and review any problems developing in the TSP program and recommend actions to correct or prevent reoccurrence.

1.2.2 Federal Relationships

The NCS has a long history of coordinating NS/EP communications with agencies throughout the Federal Government. As the critical infrastructure protection lead for the Communications Sector within the Federal Government, the NCS is responsible for coordinating activities with numerous DHS offices, as well as other departments and agencies with Communications Sector responsibilities. The NCS coordinates many of its critical infrastructure protection efforts with other offices within the department, including the NCSD on cyber security issues and the Office of Infrastructure Protection (OIP) on cross-sector critical infrastructure and risk management issues. Table 1-2 provides descriptions of formal Communications Sector relationships with other Federal Government entities.

Table 1-2: Communications Sector Federal Relationships and Key Entities

Name	Description
CIO Council	The CIO Council is an interagency forum for improving practices around the use of Federal Government agency information resources. Its role includes developing recommendations for information technology management policies, standards, and procedures; identifying opportunities to share information resources; and addressing the needs of the Federal Government's IT workforce.
Executive Office of the President (EOP)	The OSTP, National Security Council (NSC), Homeland Security Council (HSC), and Office of Management and Budget (OMB) are all stakeholders of the NCS. All these EOP entities work closely with the DHS, through the NCS, on planning the NS/EP-related missions and activities.
Federal Communications Commission (FCC)	The FCC regulates interstate and international communications by radio, television, wire, satellite, and cable. The Public Safety and Homeland Security Bureau (Bureau) is responsible for all FCC activities pertaining to public safety, homeland security, national security, emergency management and preparedness, disaster management, and other related issues. In particular, the Bureau manages the FCC's efforts with respect to critical communications infrastructure protection, and provides representatives to serve on key committees and working groups.
Federal Partnership for Interoperable Communications (FPIC)	The FPIC serves as a coordination body to address technical and operational activities within the Federal wireless communications community. The FPIC mission is to address Federal wireless communications interoperability by fostering intergovernmental cooperation and identifying and leveraging common synergies.
Joint Telecommunications Resources Board (JTRB)	JTRB provides a forum for immediate deliberation in the event of major crises, resolves competing demands for communications services, and monitors the performance of the national communications infrastructure during emergencies. Membership is made up of senior Federal Government officials and is chaired by the Director of OSTP.
National Cyber Response Coordination Group (NCRCG)	The NCRCG facilitates the Federal Government's efforts to prepare for, respond to, and recover from cyber incidents and physical attacks that have significant cyber consequences. As a member agency, the NCS brings subject matter expertise, established relationships with private industry, and other capabilities to the NCRCG's efforts.

Name	Description
National Telecommunications and Information Administration (NTIA)	The NTIA serves as the manager of Federal Government use of the radio frequency electromagnetic spectrum under all conditions. Among other things, the NTIA advises and assists the President in administering a system of radio spectrum priorities for those spectrum-dependent communications resources of the Federal Government that support NS/EP functions.
NCS Committee of Principals (COP)/ Council of Representatives (COR)	As a Presidentially designated interagency group, the COP provides advice and recommendations on NS/EP communications to the EOP, as well as the Manager, NCS, and its Executive Agent (the Secretary of Homeland Security). The COP consists of 23 high-level Government officials representing Federal operational, policy, regulatory, and enforcement organizations. The COR is a permanent subordinate group of the COP. COR members participate in working groups to conduct studies and make recommendations to the COP on matters of concern.
SAFECOM Executive Committee (EC)	The SAFECOM EC serves as the steering group for the SAFECOM Program and evaluates the guidance and recommendations for SAFECOM as developed by the Advisory Group. It is comprised of representatives from State and local public safety and government associations representing key public decisionmakers as well as contributing Federal agencies with significant, vested interest in public safety.
White House Communications Agency (WHCA)	WHCA is an operational unit of the White House Military Office and is a "special mission" component of the Defense Information Systems Agency (DISA). It provides communications and related support to the President, Vice President, White House staff, NSC, U.S. Secret Service, and others as directed by the White House Military Office (consistent with statutory, regulatory, and budgetary requirements).

1.2.3 State and Local Relationships

Relationships with State and local agencies in the Communications Sector focus primarily on regulatory issues with State Public Utility Commissions (PUC), State and local emergency operation centers, and emergency response activities with first responders and 911 emergency centers. Since 2001, Federal entities have been coordinating homeland security initiatives by establishing information-sharing relationships within the Federal Government and with States and cities, and conducting vulnerability assessments of their communications networks.

Regulatory

State and local agencies have jurisdiction over communications providers within their boundaries regarding individual requirements related to providing service and constructing networks. The State PUC is the primary authority for implementing these regulations. Individual communications carriers work directly with State PUCs regularly to address regulatory issues. As noted in the authorities section, some States have requirements for communications carriers related to CI/KR protection, such as providing critical infrastructure asset information. State regulators and other agencies have working relationships with the sector that far exceed their regulatory role in the sector. For example, in States with hundreds of local telephone companies, regulators are well positioned to play an important role in providing the interface between government support and utility activity on protection and preparedness.

NARUC functions as the Federal Government's main interface with State regulators. NARUC's membership includes State and local government agencies that regulate utilities and certain carriers, including communications. NARUC serves the public interest by improving the quality and effectiveness of public utility regulation. NARUC established an Ad Hoc Committee

on Critical Infrastructure, which focuses on identifying the proper role for PUCs with respect to the security of the Nation's electric, natural gas, communications, and water infrastructures from threats of terrorism.[5] The Ad Hoc Committee acts as the primary point of contact (POC) for Federal agencies on CI/KR protection issues related to States' public utilities. In addition, through the Ad Hoc Committee, NARUC member Commissions have partnered with Federal agencies and engaged in analysis, coordination, and institutional network-building programs that facilitate CI/KR protection and improved emergency response. NARUC also is represented in numerous Federal and private sector partnerships, including NRIC, Department of Transportation's E-911 working group, FCC-State E-911 Working Group, and GCC for the Energy Sector.

Emergency Response

Another set of State and local relationships involves emergency responders, including firefighters, police, emergency medical services, emergency management agencies, and 911 centers. Overall, Federal relationships focus on national organizations, such as the ones listed in table 1-3, representing the interests of the different groups. The NCS and other Federal agencies work closely with these organizations in numerous capacities, such as promoting the adoption of Federal programs, discussing communications requirements, and developing standards.

In addition to working with emergency response organizations on communications requirements and service issues, the NCS conducts emergency response training seminars with Federal, State, and local emergency responders. These seminars provide an overview of the NRP and priority communications service offerings and include a facilitated group discussion on regional disaster response scenarios.

Other relations involving State and local players revolve around technology sharing issues, such as Project SAFECOM that focuses on improving interoperability of wireless communications between Federal, State, and local responders.

Table 1-3: Emergency Response Organizations

Name	Description
Association of Public-Safety Communications Officials (APCO) International	APCO International is a professional association dedicated to the enhancement of public safety communications.
International Association of Fire Chiefs (IAFC)	The IAFC is a network of more than 12,000 chief fire and emergency officers. In addition to career enhancement for its membership, the IAFC works with the Federal Government on key issues and serves as a liaison with other fire service organizations.
International Association of Chiefs of Police (IACP)	The IACP is an organization of more than 20,000 police executives in more than 89 different countries. IACP's leadership consists of the operating chief executives of international, Federal, State, and local agencies of all sizes.

[5] The FCC and the DHS are also members of the Ad Hoc Committee.

Name	Description
International Association of Emergency Managers (IAEM)	The IAEM is a nonprofit organization dedicated to promoting the goals of saving lives and protecting property during emergencies and disasters.
National Association of State 911 Administrators (NASNA)	NASNA represent 32 States that currently have a central 911 planning or program administration. NASNA helps the FCC educate the public safety community on the TSP Program.
National Emergency Management Association (NEMA)	NEMA is nonprofit association dedicated to enhancing public safety by improving the Nation's ability to prepare for, respond to, and recover from all emergencies, disasters, and threats to our Nation's security.
National Emergency Number Association (NENA)	NENA's mission is to foster the technological advancement, availability, and implementation of a universal emergency telephone number system. In carrying out its mission, NENA promotes research, planning, training, and education. Among other activities, such as measuring the performance of 911 services, NENA works with the U.S. Department of Transportation, APCO, NASNA, and other stakeholders on the implementation of the Enhanced 911 (E-911) service.

1.2.4 International Relationships

Communications networks are global in scope; hence, it is important that infrastructure protection activities for the sector extend beyond U.S. borders. Industry and government are actively involved in international organizations and multilateral/bilateral relationships to share lessons learned, discuss best practices, and set standards.

The NCS leads U.S. government efforts on international NS/EP in the Communications Sector. In cooperation with the DHS and the Department of State, the NCS actively assesses the work of multilateral organizations such as the United Nations (UN), the European Union (EU), the Organization of American States (OAS), and Asia-Pacific Economic Cooperation (APEC). The NCS also works closely with the International Telecommunication Union (ITU), an organization within the United Nations, where governments and the private sector coordinate global communications networks, services, and standards.

Bilaterally, the NCS has a strong working relationship with Canada on NS/EP and critical infrastructure protection issues. The United States and Canada created the Civil Emergency Planning Telecommunications Advisory Group (CEPTAG) in 1988 to address shared communications concerns, as well as to facilitate cross-border cooperation and mutual assistance in the event of an emergency. The NCS also enjoys a well-developed bilateral relationship with the United Kingdom, which is pursued primarily through the Joint Contact Group (JCG). The principal NCS task under the JCG is to develop government-to-government priority routing capability for emergency communications. The NCS will continue to collaborate with government and industry partners to strengthen these and other key bilateral relationships.

The NCS is also involved in the implementation of the U.S./Mexico/Canada Security and Prosperity Partnership (SPP). The SPP was launched in 2005 as a dual bi-national effort to increase security and enhance prosperity in North America. The NCS leads several initiatives within the SPP as part of the larger effort to develop and implement a common approach to critical infrastructure protection and plans for response to cross-border terrorist incidents and natural disasters. The NCS also represents the U.S. Government within the North Atlantic Treaty Organization's (NATO) Civil Communications Planning Committee (CCPC).

The CCPC works to assess existing and future civil postal and telecom systems, networks, and other resources relative to civil emergency planning and critical infrastructure protection in response to natural and manmade disasters. The NCS International Affairs Advisor leads the U.S. delegation to the CCPC along with an NCC industry representative and colleagues from the U.S. Postal Service.

As the SSA, the NCS will continue to work with the 23 Federal departments and agencies represented on its Committee of Principals, as well as with private industry, to advance the international Communications Sector goals. It will also work closely with the international components of NCSD, OIP, FEMA, and other elements of the department to build effective international critical infrastructure protection and emergency response partnerships to address interdependencies.

1.3 Sector Security Goals

With the wide range of companies, technologies, and government interests that make up the Communications Sector, it is important to find common ground in establishing sector security goals. The goals represent specific outcomes, conditions, end points, and performance targets for the sector, and provide a framework for the remainder of the SSP, guiding the sector's focus on resources and protective measures and giving the sector a means by which to evaluate its progress and performance.

Vision Statement for the Communicationss Sector

The Communications Sector acknowledges the Nation's critical reliance on assured communications. The Communications Sector will strive to ensure that the Nation's communications networks and systems are secure, resilient, and rapidly restored after a natural or manmade disaster.

1.3.1 Vision Statement

Based on the sector's characteristics and risk management approach, the sector developed the following vision statement to reflect its desired security posture:

The desired security posture will be achieved through the application of the following principles:

- Protective programs will principally focus on response and recovery strategies;
- Communications Sector industry partners are responsible for employing prevention and protection strategies, except when industry may request government assistance for protection of critical communications facilities during extraordinary events, such as Hurricane Katrina and 9/11;
- Customers are responsible for protecting their own assets and access points, and providing for diverse and assured communications that support their specific essential functions;
- Government programs will support the availability of communications services for NS/EP users and protection of government communications assets;
- Communications Sector industry partners will continue to work with government through the NCC on NS/EP, threat dissemination, subject matter expertise, analytic support, information sharing, and contingency planning and response; and
- The Communications Sector recognizes that other critical infrastructures are highly dependent upon communications for basic operations.

1.3.2 Process to Establish Sector Security Goals

A collaborative process for setting sector security goals, for the industry and government components of the sector, was necessary to ensure that the goals accurately reflect the security posture and priorities of all sector security partners. The NCS began the process with a facilitated offsite meeting to draft a set of security goals where participants included a small group of industry partners and NCS representatives.[6] This dialogue was continued during a series of meetings where industry and government partners further refined sector security goals. A broader distribution of security partners had subsequent opportunities to comment on and revise the goals during numerous comment periods.

The goals developed considered the many dimensions of the protective spectrum. In many cases, security partners referenced existing programs and best practices to set the sector goals for securing physical, cyber, and human assets. Within this structure, the sector security goals cover the following categories:

- Protection;
- Response and Recovery;
- Awareness; and
- Cross-Sector Coordination.

Although all these are critical, preserving the overall health of the communications backbone[7] is the sector's first priority at a national level. The sector acknowledges that resiliency and its ability to withstand disruptions is critical; however, the integrity and security of the backbone is the sector's main focus from a protection standpoint.

The goals established in this document will be reviewed and updated regularly, as the sector's infrastructure protection planning and implementation evolves. The NCS plans to host annual joint CGCC/CSCC meetings to discuss the goals, report on progress, and make modifications to goals, as necessary.

1.3.3 Sector Security Goals and Objectives

Protection

Goal 1: Protect the overall health of the national communications backbone.

The Communications Sector recognizes that other critical infrastructures are highly dependent on its services for basic operations. The overall architecture of the Communications Sector incorporates various technologies and services and has diverse ownership. Interconnection, interoperability, and security are achieved through technology standards, regulation, carrier agreements, and intercarrier cooperation, enabling the communications infrastructure to operate effectively and rapidly restore networks after a disaster. Resiliency is achieved through the technology, redundancy, and diversity employed in the network design and by customers who plan for and employ diverse and resilient primary and backup communications capabilities.

Industry and government will work together to conduct a national sector risk assessment, identify network high critical vulnerabilities, and develop and implement the necessary security measures to provide for the health and security of the communications backbone. Communications Sector industry partners are encouraged to participate in NRIC and its focus groups to develop industry best practices for addressing communications infrastructure vulnerabilities. Other protective measures may include continued research and development (R&D) to decrease communications dependency on commercial power (e.g., backup sources such as batteries, generators, and fuel cell technology), and coordination with governments on cross-border communications infrastructure protection.

[6] The first meeting was held July 28-29, 2005.

[7] The communications backbone is inclusive of the core wireline network and Internet backbone. "Backbone" will primarily be used in future references throughout this document to the Core Network/Internet Backbone.

Response and Recovery

Goal 2: Rapidly reconstitute critical communications services after national and regional emergencies.

Industry and government will continue to improve processes and procedures to respond rapidly to all crises to restore critical communications services. The NCS, as lead for ESF #2 (Communications), will support industry's response and recovery effort in collaboration with States to assist with obtaining necessary resources (e.g., fuel, security), getting access to disaster areas, and setting restoration priorities. The NCS will maintain the NCC and enhance its suite of priority service programs in support of restoration and recovery process. In coordination with service providers, operators, and communications equipment manufacturers, the NCS will develop next-generation priority service programs to meet the evolving requirements of critical communications customers in a converged communications environment. The NSTAC will continue to review national policy implications related to communications emergency response and service restoration, including analysis of new threats and evolving technologies.

In addition, the sector will continue to pursue the implementation of a standardized screening process for personnel with regular and continued unescorted access to critical communications assets; relevant access control best practices to protect against unauthorized access (e.g., credentialing during incidents); relevant human resources best practices to protect against intentional and unintentional insider threats; and measures to protect cyber/logical assets identified as high risk.

Goal 3: Plan for emergencies and crises through participation in exercises, and update response and continuity of .

To achieve this goal, the NCS will employ the most likely threat scenarios provided by the Intelligence Community or natural disaster scenarios to evaluate existing contingency and reliability plans. Based on these threat scenarios, Federal and State governments and the private sector will jointly plan and participate in emergency response training and exercises that address a spectrum of threats and hazards. The NCS also will support Federal Government continuity planning efforts to put measures in place to ensure service continuity and availability for National Essential Functions and associated Priority Mission Essential Functions requiring communications within identified Maximum Allowable Outage (MAO) periods. The dynamic nature of the communications industry and developing technology necessitates that industry and government remain flexible and diligent in the review of their COOP planning. Maintaining regularly updated plans will allow for faster decisionmaking and real-time collaboration during emergencies and crises.

State agencies will continue to work together regionally and nationally, and with the Federal community, to develop coordinated approaches to preparedness. Through NARUC, State regulators will continue disseminating information on preparedness; participating in exercises; engaging in analysis on key CI/KR issues, including information protection, interagency communications, and regional coordination; and developing regional partnerships and harmonized policies. Coordination with international partners, particularly Canada and Mexico, also is essential to ensure a robust response capability for disasters near the U.S. border.

Coordination of industry and government preparedness and relief efforts before, during, and after a disaster will significantly enable a response targeted at emergency needs and relief efforts for the maximum benefit of the public in a time of crisis.

Goal 4: Develop protocols to manage the exponential surge in utilization during an emergency situation, and ensure the integrity of sector networks during and after an emergency event.

To achieve this goal, the NCS and Communications Sector industry partners will coordinate with the international community in the development of protocol standards and technologies to better manage the exponential surge in calls that can occur during emergency situations. The NCS, in collaboration with the FCC and NARUC, also will continue to conduct outreach at conferences and trade shows on priority service programs (e.g., TSP, WPS, and GETS) to ensure necessary users and facilities are appropriately registered. The NCS will coordinate with the DHS Science and Technology Directorate to promote R&D to improve priority service programs and to explore ways of preserving the integrity of sector networks during and after an

attack or natural disaster. In addition, the NCS and the Communications Sector will conduct an outreach program with the Federal, State, and local governments to help them better understand the eligibility requirements and the capabilities of these programs. NARUC and the FCC will continue outreach to States and local governments to facilitate widespread adoption of TSP, GETS, and WPS and to State regulators regarding barriers related to TSP that these regulators can help overcome. In addition, the NCS will work with Canada, the United Kingdom, and other partners to develop government-to-government priority communications services.

Awareness

Goal 5: Educate stakeholders on communications infrastructure resiliency and risk management practices in the Communications Sector.

Awareness and education on communications infrastructure resiliency and risk management practices are critical for stakeholders to maintain their critical operations. The NCS, in partnership with industry, will seek to develop education mechanisms to work with public and private critical infrastructure users to coordinate protection and response strategies to assist customers in employing existing methods and capabilities more effectively. The NCS and industry will partner with other government agencies to analyze and prioritize the full spectrum of critical government and private sector functions that depend on the Communications Sector. Finally, in partnership with NCSD, the NCS and industry will identify and assess critical operational cyber/logical functions for potential impact if a communications infrastructure element is lost.

Goal 6: Ensure timely, relevant, and accurate threat information sharing between the law enforcement and intelligence communities and key decisionmakers in the sector.

Information sharing is an important component of improving awareness and preventing an event or minimizing its impact. To achieve this goal, it is important that information sharing be mutual (two-way) and provide specific and actionable information. The sector will work to obtain the necessary security clearances to receive actionable information and to assist in intelligence and threat analysis as appropriate. The NCC will serve as the focal point for sharing information to and from relevant State and local authorities for the sector, and implement industry-government information-sharing processes to ensure that consistent and accurate information is provided from a centralized source. Industry and government will need to increase threat and vulnerability information sharing to implement the appropriate threat-based security measures and risk management programs. Industry partners should proactively report suspicious activities (e.g., death, injury, illness, and trespassers) internally and to appropriate authorities so patterns and security risks can be identified.

Cross-Sector Coordination

Goal 7: Establish effective cross-sector coordination mechanisms to address critical interdependencies, including incident situational awareness and cross-sector incident management.

To fully understand and determine an acceptable level of risk, all sectors must understand their dependency on and interdependency with the communications infrastructure. The NCS will work with industry and all levels of government to identify cross-sector critical dependencies by leveraging existing industry and government cross-sector groups, task forces, and other mechanisms. NCC members will continue to work with existing sector coordination groups (e.g., ISACs, SCCs) on procedures for cross-sector incident management and sharing situational awareness information during incidents. The NCS will also coordinate with other SSAs to conduct diversity assessments for high-risk critical infrastructure and NS/EP user facilities.

To develop further the capabilities required to address these cross-sector dependencies, industry and government will continue to plan and participate in emergency response training and exercises that address a spectrum of threats across sectors, and test the coordination mechanisms, situational awareness, and incident management.

Regulators, emergency managers, and other State agencies and their government and Sector counterparts will continue to build contact lists, establish networks, and engage in dialogue to develop coordinated approaches to COOP planning, regional coordination, access, and credentialing, among other issues.

1.4 Value Proposition

The full engagement of the Communications Sector—industry and government—is essential for the CSSP to achieve its goals and support the NIPP. The services offered or performed by the Communications Sector are critical components of the business and government processes that are fundamental to our way of life, including electricity, banking and finance, emergency services, and government continuity of operations.

The Communications Sector brings value to the community and its citizens through measures employed to better protect against and more rapidly recover from any event, catastrophic or otherwise, that could potentially damage, disrupt, or destroy its critical assets, systems, networks, and functions. The Communications Sector uses robust business continuity plans that combine threat and vulnerability assessments and countermeasures with sound business practices, subject to relevant Federal regulation, to guide the ownership and management of critical infrastructures under its control. Industry's extensive experience protecting, restoring, and reconstituting the communications infrastructure is invaluable in enabling the Federal Government to predict, anticipate, and understand how communications failures affect the national leadership's ability to communicate during times of crisis, impact the operations of other infrastructures, and affect response and recovery efforts.

The development and implementation of the Communications SSP provides an opportunity for industry and government sector security partners to take advantage of the infrastructure protection framework it provides. For government partners, the processes outlined in this plan support their missions to execute command, control, and coordination; to provide national, economic, and homeland security; and to ensure public health and safety. For private sector partners, the protection of critical infrastructure is important for the security of their employees, assets, business continuity, and services provided to customers. Table 1-4 lists chapter 1 roles and responsibilities.

The following specific benefits to the private sector result from active participation in the public-private partnerships supporting the protection of the Nation's critical infrastructure.

- **Access to General, Sector-Specific, or Site-Specific Threat Information.** Threat information will help partners prepare for crisis situations, alerting them of potential problems/attacks. Information sharing is an important component of improving awareness and preventing an event or minimizing its impact.
- **Support for Security Best Practices over Additional Regulation.** Best practices are derived from insights from either the historic technical support experience of individual companies or, since September 11, 2001, from proactive efforts to address communications infrastructure vulnerabilities. Through the risk management strategies outlined in the CSSP, industry and government will be able to create new best practices and further confirm the value of existing best practices, while simultaneously improving network reliability and potentially mitigating the need for additional reliability regulation by creating a working environment that is mutually beneficial to industry and government.
- **Potential Access to Resources for the Protection of Certain Critical Assets or Protective Programs for the Sector.** The partnerships will provide priority communications services that assure the communications infrastructure's ability to meet NS/EP requirements under all circumstances. The key partners and users of these priority services and programs are those responsible for minimizing loss of life and restoring order and critical services following a major disaster. These groups include not only national, State, and local government leaders but also senior leadership of the Nation's critical infrastructures and key communications and information technology industries and organizations. Access to these programs will help facilitate priority status for restoration of services (e.g., power) and result in better direction of recovery efforts in terms of personnel and assets.

- **Potential Government Support for Necessary R&D Initiatives.** The CSSP process will help identify and prioritize R&D initiatives related to the Communications Sector. To accomplish this effort, government will review Federal R&D initiatives with the potential to meet the communications challenges identified in the CSSP, conduct a gap analysis, identify which could fill the sectors technology gaps, and produce a report summarizing the initiatives.

Table 1-4: Chapter 1 Roles and Responsibilities

Entity	Activity
NCS	Host annual joint CGCC/CSCC meeting to revisit and revise security goals.
NCS CGCC CSCC	Hold joint Communications and IT Sectors meeting twice annually to address issues of interest to both sectors and discuss potential areas for collaboration.
NCS CGCC CSCC	Identify synergies and gaps between Communications and IT security partners, and collaborate whenever possible on partner outreach.
NCS CGCC CSCC	Cooperatively address with the IT Sector areas of convergence, such as those identified in the NSTAC Report to the President on the NCC, including developing an approach for a long-term regional communications and IT coordinating capability that serves all regions of the Nation, convening a conference to focus on cyber issues, and exploring ideas for a multi-industry coordinating center.
NCS DOS	Work with Canada, Mexico, and other international partners to identify international interdependencies.
NCS DOS	Work with Canada, the United Kingdom, and other partners to develop government-to-government priority communications services.

2. Identify Assets, Systems, Networks, and Functions

The CSSP's highest priority is to identify and protect nationally critical architecture elements, ensure overall reliability of the networks, maintain "always on" capabilities for certain critical customers, and quickly restore essential communications services following a disruption. Nationally critical elements are assets, networks, systems, or functions that, if destroyed, disrupted, or exploited, would seriously threaten national security, result in catastrophic health effects or mass casualties, weaken the economy, or damage public morale and confidence.

As a result of the overall resiliency and the dynamic nature of communications technology, the Communications Sector adopted a high-level architectural approach to concentrate on nationally critical elements. Physical communications assets become critical based on the role the asset plays in the continued operation of the network backbone, or based on that asset being essential to a critical service or mission of another critical infrastructure sector. Logical elements, which are defined by the relationship of different assets or networks, also may be designated as critical, depending on the function they provide to end users in an affected area and the MAO before impacting user missions.

The identification of sector high-level architecture elements is an important theme of the CSSP. For example, one of the sector's security goals is to have a secure and resilient national communications backbone because of its primary function to carry national and international traffic between primary network nodes. Analysis of the backbone system will be focused on identifying the primary architecture elements of those networks, rather than all of the specific assets in the network and their individual owners. Over the next year, the Communications Sector will collaborate with the IT Sector on the identification of Internet architecture elements. The Internet architecture information will be compiled and used in specific components of the national risk assessment process.

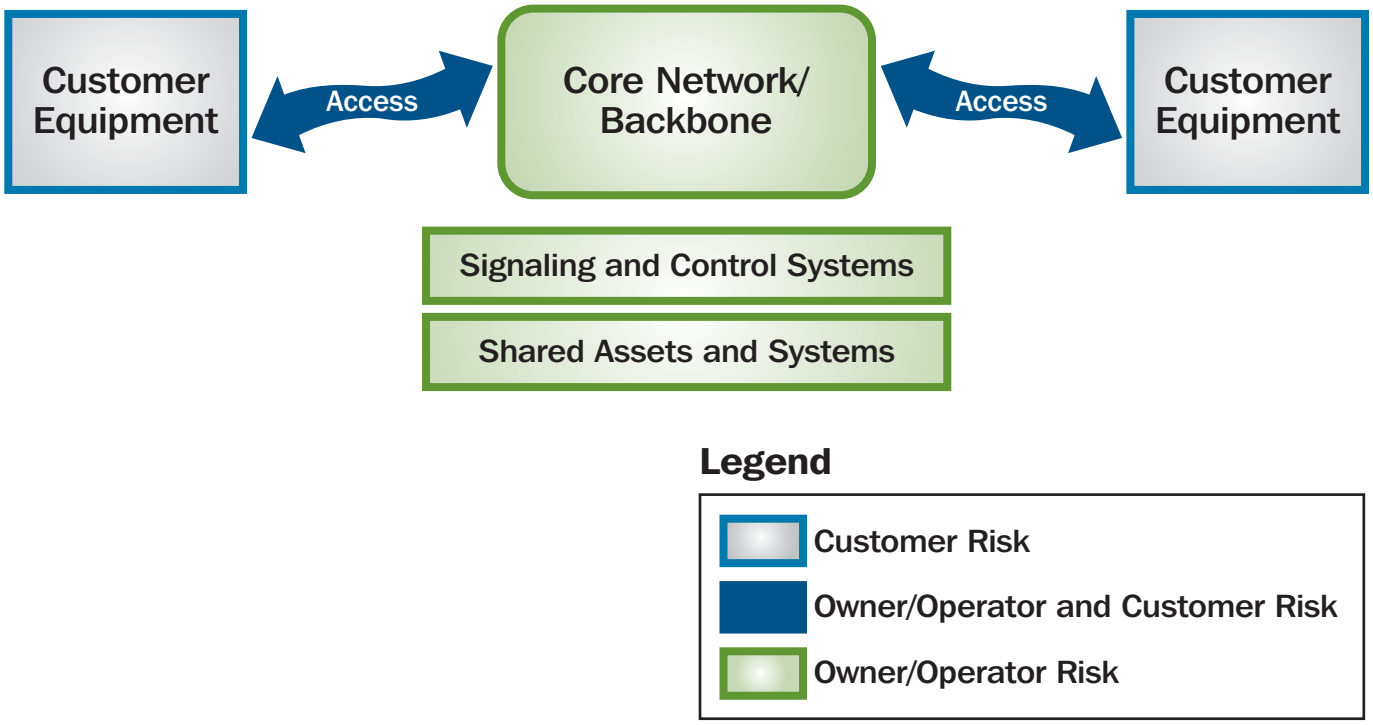
The Communications Sector's high-level architecture approach will factor in the individual responsibilities for addressing risk, which fall into three categories: owner/operator risk, owner/operator and customer risk, and customer risk.

- **Owners and operators** are responsible for mitigating risk to the communications backbone and signaling and control systems related to the operations of the communications infrastructure. They also share the responsibility for mitigating risk to assets and systems shared by multiple operators.
- **Owner/operators and customers** share the responsibility for the access portion of the network, particularly in that the access arrangement is significantly influenced by the location and characteristics of the customer premises. Although owners and operators accept responsibility for maintaining the access portion of the network and restoring/reconstituting it in a timely manner after an event, customers must accept the risk that the access portion of the network may be disrupted and should adopt mitigation strategies, as appropriate. Large customers often negotiate service level agreements to guarantee service availability or quality of service as a measure to reduce risk. Customers may mitigate the access risk by locating their mis-

sion-critical functions in at least two geographically diverse locations, dual-homing those locations, providing for dual cable entrances, and procuring diverse primary and backup services.

- **Customers** are responsible for accepting and mitigating risk to their own communications assets and systems. Customer enterprise infrastructure is as much of a limiting factor during incidents as the commercial communications capacity. Without proper planning, enterprise network users may not have reliable access to their internal systems.

Figure 2-1: Communications Architecture and Risk Assignments



Federal and State governments play multiple roles in mitigating risk to the Communications Sector: infrastructure protection planning, enabling response and recovery operations, assisting with risk assessments, participating in cross-sector assessments, and implementing national protective programs. These activities are described throughout the CSSP. Overall, Federal and State governments can fall into more than one of the risk assignment groups shown in figure 2-1. For example, the Federal, State, local, and tribal governments and end users of the communications services are considered customers who have the responsibilities for risk assigned as "customer risk." Likewise, some departments and agencies also have responsibilities as owners and operators of specific government communications infrastructure.

The Communications Sector recognizes the importance of addressing cross-sector dependencies on communications. In terms of responsibility for risk, other CI/KR sectors usually are considered customers. Communications Sector industry and government partners are committed to working with other CI/KR sectors to address cross-sector dependencies, through customer relationships as well as through other SSAs and sector partnerships.

This chapter describes the processes used in the Communications Sector for identifying high-level architecture infrastructure as part of the overall risk management effort. Steps involved in sector identification are defining data parameters and collecting, verifying, updating, and protecting infrastructure information.

2.1 Defining Data Parameters

The complexity of sector assets, indepth corporate security programs, technology, and the numerous systems composing the communications infrastructure help reduce the likelihood of a significant national level network failure. For example, resiliency is achieved through the technology and redundancy employed in designing networks, and by encouraging customers to employ diverse primary and backup communications capabilities. Communications network architects employ technology and protocols (e.g., Synchronous Optical Network (SONET) rings, routing protocols), creating effective "self-healing" networks, and helping to mitigate risk at the design stage. Sector owners and operators focus on ensuring overall network reliability, maintaining "always on" capabilities for customers, and quickly restoring capabilities following a disruption.

Data parameters for the sector will be defined primarily by the architecture elements of assets, systems, networks, and functions. The following architectural elements in the Communications Sector will be explored:

- **Assets:** Shared assets and systems owned and operated by multiple companies. Includes facilities in which equipment is collocated and systems shared by network operators, and equipment owned and operated by the end user or located at the end user's facility. Customers include individuals, organizations, businesses, and government.
- **Systems:** Signaling and control systems that exchange information about establishing a connection and control the management of the network; and access, primarily, the local portion of the network connecting end users to the backbone that enables users to send or receive communications. Access includes equipment and systems such as PSTN switches, ATM switches, video servers for video on demand, and IP routers for ISPs.
- **Networks:** Core network/Internet backbone elements of the communications network that represent high-capacity network elements servicing regional, nationwide, and international connectivity.
- **Functions:** As defined in the NIPP, service, process, capability, or operations performed by specific infrastructure assets, systems, or networks.

2.2 Collecting Infrastructure Information

Although information about the sector's architecture elements may be available, significant challenges are associated with collecting information about network access architecture and functions at the customer level. Monitoring customer use of the communications infrastructure is extremely difficult, particularly when customers move parts of their organization geographically, change the use of particular architecture elements as they are associated with particular missions, or merge with other organizations. The dynamic nature of communications technology further complicates the process. As a result, identification of customer-level critical assets must rely on each customer to provide that information to sector owners and operators and the DHS.

Collecting CSSP infrastructure information falls into three categories: (1) architectural infrastructure information, (2) specific infrastructure information, and (3) National Asset Database (NADB) information.

2.2.1 Collecting Architectural Infrastructure Information

For the collection of architectural infrastructure information, the NCS will work with industry to examine sector infrastructure elements to include the backbone, signaling and control systems, shared assets and systems, access, and customer equipment. Understanding the changing nature of the Communications Sector is critical to identifying and validating sector architectural elements. Industry and government will work closely to develop a deeper understanding of these architectural elements and their associated assets, systems, networks, and functions. This process also will consider the dependencies and interdependencies of the architectural elements with physical and cyber/logical infrastructure not owned by the sector.

The Communications Sector will examine the architectural elements of each type of communications carrier (e.g., wireline, wireless, satellite, cable, and broadcasting) and classify it into one of the proposed five major architectural element categories. As section 2.1 discussed, the Communications Sector will identify asset/system categories within each architectural element, as well as their respective functions. A majority of the sector cyber/logical infrastructure identified falls within the signaling and control systems category; however, there also will be asset/system categories within the other elements. This high-level architecture view will structure the analysis and management of risk throughout the CSSP process.

2.2.2 Collecting Specific Infrastructure Information

Through well-established relationships with individual carriers, the NCS will request specific asset information on an as-needed basis, particularly during incidents of national significance or in preparation for NSSEs (National Special Security Event). The NCC is the main industry POC for asset information. In response to the DHS's requests for sector asset information, the NCC will work with industry to clarify the instances in which asset data will be collected. The NCC periodically will test this process to ensure procedures work in a timely manner. The NCC will develop a formal process in which the National Operations Center (NOC) will work with the NCC to identify specific sector assets related to an explicit, credible threat, during emergencies or in preparation for NSSEs. In these cases, the NCS will establish arrangements with the NCC industry members whereby the NCS may acquire relevant asset data from their corporate operations centers. The information then will be passed back to the NOC and appropriate State and local agencies.

The NCS collects data for the NCS Network Design and Analysis Capability (NDAC) using commercial and private databases, such as the Local Exchange Routing Guide (LERG), and contractually obtained information. Communications Sector industry partners maintain stringent proprietary control over the dissemination of infrastructure-related information for competitive and security reasons. Based on the trusted and longstanding working relationship with the NCS, however, industry partners traditionally have provided selected proprietary information directly to the NCS on a case-by-case basis. As the ESF #2 lead, the NCS has also created a deployable disaster communications asset database to assist in tracking assets for incident response. This information is employed for operational analysis, program development, and operations, some of which is integrated into the NDAC.

2.2.3 National Asset Database

The Communications Sector is committed to working with the DHS to ensure that the communications infrastructure is accurately and appropriately represented in the National Asset Database (NADB). Currently, the NCS is using the LERG to populate the Communications Sector portion of the NADB to provide some representation of sector assets in the database. The LERG includes information on LEC switching entities, including their geographic locations, operating companies, and equipment used, among other routing information. This addresses only a small portion of today's communications infrastructure and excludes segments such as wireless, satellite, and cable.

Because of the blended physical and logical nature of Communications Sector assets, efforts generally have been directed at systemic risk assessments. The NIPP framework calls for the sector to conduct a National Sector Risk Assessment. As part of the assessment process, the sector will validate corresponding entries in the NADB and make the appropriate updates so that the DHS can work with owners and operators to afford appropriate protective measures.

In addition, industry partners may voluntarily submit information or, as described in section 2.2.2, industry partners will work with the NCS to fulfill specific requests for purposes of NSSE planning, response to a specific threat, or response to a natural disaster.

2.2.4 Regulatory Requirements

Currently, Federal regulatory requirements for providing infrastructure information in the sector vary by subsector. At present, wireless and broadcasting infrastructure owners are required to file information with the FCC detailing information on the equipment location and type. Wireline infrastructure operators submit data annually to the FCC to allow for the measurement of competition and service quality. Information required in these filings includes a summary of infrastructure (e.g., number of access lines), service quality, and financial data. Further, the FCC requires wireline, wireless, and satellite carriers to report network outages. The Commission maintains an expert staff of engineers and statisticians to analyze this data in an attempt to reveal troublesome trends in network reliability and security. For example, the Commission's reports are designed to provide information on the extent to which industry best practices developed by NRIC are being applied. The reports also include detailed information about the causes of network outages and methods used to restore service. With this information in hand, the Commission works with industry bodies like the Network Reliability Steering Committee (NRSC)[8] and NRIC to improve communications reliability and security. Resulting improvements are documented in revised or new best practices so they can be applied more broadly across the industry.

2.3 Verifying Infrastructure Information

In addition to the procedures and processes employed by the Communications Sector industry partners to verify the ongoing accuracy and completeness of their own infrastructure information, industry also participates in NCS efforts to maintain strong, trusted partnerships with various government agencies. The trust and productivity of these relationships require strong policies and procedures for collecting, handling, storing, and disseminating information; a common understanding of the ultimate use of that data; and a process for ensuring compliance and enforcement to protect the interests of the government and its private sector partners.

The NCS verifies data through multiple sources, primarily through interviews with carriers. Each carrier is given an opportunity to verify data and the network topology. Such interviews may identify the need for more indepth analysis by the carrier, in which case contractual relationships may be required to reimburse the carrier's cost. The NCS addresses incomplete and incorrect data by re-engaging the owners and operators of the related assets to ensure the information is accurate and comprehensive.

2.4 Updating Infrastructure Information

Maintenance of communications infrastructure databases is a continual effort undertaken by a host of sector partners. Information collected by the NCS, depending on the source of information, license agreements, and contractual obligations, is updated daily, monthly, quarterly, or annually. Updated infrastructure data also will be re-verified using these sources. For purposes of the NADB, the NCS will provide updates on data sets as permitted.

2.5 Protecting Infrastructure Information

The Communications Sector industry partners recognize the well-intended desire of government to understand the scope of a broad range of critical infrastructures and to be prepared for an incident. A comprehensive listing of communications architecture elements, absent a need to address a specific threat, may provide some level of value to governments in their decisionmaking processes. On the other hand, the existence of such aggregated communications elements within a government entity creates risks to the communications industry. With so many organizations having varying degrees of legal nondisclosure

[8] The NRSC is a subcommittee of the Alliance for Telecommunications Industry Solutions, whose objective is to monitor and improve communications network reliability.

protection in possession of this sensitive information, inadvertent or unauthorized public disclosure might become a potential blueprint for terrorism.

Wherever possible, industry data shared with the NCS will be protected by "commercial proprietary" markings and contractor nondisclosure agreements (NDA). The Protected Critical Infrastructure Information (PCII) Program is another mechanism available to submit CII information to the Federal Government. PCII protection applies to information offered directly and indirectly to the DHS through the PCII Program Office. The Final Rule, issued on September 1, 2006, identifies procedures for indirect submission to the DHS through the DHS field representatives and other Federal agencies. Federal agencies other than the DHS may be designated to receive CII on behalf of the DHS, but only the PCII Program Manager is authorized to make the decision to validate a submission as PCII. Only the PCII Program Manager or the PCII Program Manager's designees are authorized to acknowledge receipt of information being submitted for consideration of protection under the Act. The PCII Program Manager will authorize personnel in Federal Government entities other than the PCII Program Office to accept a submission on behalf of the Program Office, but only after such personnel are trained to ensure compliance with the requirements of this final rule.[9] The NCS will become a registered designee and be able to accept submissions on behalf of the Program Office.

State regulators often collect information for regulatory purposes from communications actors. Because of the transparency and public accountability requirements of the regulatory context, the States' ability to protect this information from widespread disclosure varies and is detailed in the NARUC report, *Critical Infrastructure Information Sharing Rules: Model Protocols for States.*[10] NARUC's Ad Hoc Committee on Critical Infrastructure Protection is developing additional analysis on information-sharing and protection issues and model approaches in the regulatory context for the Communications Sector and for interdependent sectors, to be finalized in early 2007. Table 2-1 lists chapter 2 roles and responsibilities.

Table 2-1: Chapter 2 Roles and Responsibilities

Responsible Entity	Activities
NCS	Identify sector architecture elements for each subsector, including cyber assets.
NCS (NCC)	Develop a formal process for the NOC and NCC to identify specific sector assets related to credible threats, during emergencies or in preparation for NSSEs.
NCS	Coordinate with the OIP to populate the NADB and validate existing entries.
NCS	Verify data and address incomplete or incorrect data.
NCS	Maintain the communications asset database and provide the DHS with asset data updates.
NCS CGCC CSCC	Collaborate with the IT Sector on the identification of Internet infrastructure elements.

[9] Protected Critical Infrastructure Information (PCII) Program, Final Rule on Procedures for Handling Critical Infrastructure Information, September 1, 2006.

[10] This paper is available online at www.naruc.org/cipbriefs.

3. Assess Risks

A risk assessment creates a comprehensive picture of the sector's overall exposure to risk. **Consequence** measures the cost or impact of an incident, which will be measured based on impact on human life and well-being, the economy, public confidence, and government's ability to function. **Vulnerability** assessments estimate the odds that a characteristic of, or flaw in, an infrastructure element could make it susceptible to destruction, disruption, or exploitation based on its design, location, security posture, processes, or operations. **Threat** considers the intent or capability of an adversary for a terrorist threat or the probability of occurrence for a natural disaster or accident.

3.1 Risk Assessments in the Sector

The Communications Sector will conduct a National Sector Risk Assessment. As part of this assessment, the sector will work with subject matter experts (SMEs) to identify critical functions provided by the Communications Sector and related architecture elements. Keeping the scope of the assessment at a high-level architectural and functional view, the assessment will consider the diverse technologies that make up the infrastructure, including wireline, wireless, satellite, cable, and broadcasting.

Related risk assessment efforts in the sector will focus on those areas that require specific priority focus based on the evaluation of consequences, vulnerabilities, and threats. Risk assessments will also guide three levels of protective efforts: (1) asset- or system-specific protective programs, typically coordinated by the owner or operator; (2) sector- or subsector-specific protective programs, typically coordinated by the SSA or other Federal agency; and (3) cross-sector protective programs, typically coordinated by the DHS or State and local governments.

The risk strategy outlined in the previous chapters drives risk assessment activities for the sector. Communications networks are designed to be resilient and redundant. The sector's built-in resiliency implies that few of its assets are nationally critical in and of themselves; therefore, the sector's approach focuses on risk to architectural elements and their functions, as well as assessing customer dependencies. Communications Sector owners and operators accept the responsibility for the risk associated with the communications backbone, as well as signaling and control systems. Owners and operators accept shared responsibility for shared systems/assets and the "access" portions of the network, and acknowledge that there will be possible disruption at the access points. The risk assessment approach for the CSSP includes three sets of activities.

- **Industry Self-Assessments:** Owners and operators of communications infrastructure conduct self-assessments of their critical assets and networks voluntarily. In addition, assessments are often done to assist in customer solutions.
- **Government-Sponsored Assessments:** The NCS and industry partners will assess the risk of the architectural elements, including the associated consequence, vulnerability, and threat. This effort may require contractual arrangements between the NCS and sector owner/operators.

- **Government-Sponsored Cross-Sector Dependency Analyses:** The NCS will work with other SSAs on communications dependencies for other sectors' critical assets, networks, systems, and functions.

One of the outputs of these activities is the development of a risk profile that summarizes the aggregate risk for the sector. While specific industry self-assessment information will not be collected by the government, vulnerabilities prevalent throughout the sector will be shared through the National Sector Risk Assessment development process. Additional government-sponsored risk assessments on specific architecture elements and cross-sector dependency analyses will further inform the risk profile. The sector risk profile will be compiled as part of the CI/KR Sector Annual Report, which is further described in section 8.2.2.

3.1.1 Industry Self-Assessments

The Communications Sector risk management approach focuses on resiliency, service reliability, response, and recovery. Risk assessment and management processes are by nature customer driven; owners and operators must offer reliable service and quickly respond to and restore service when an outage occurs. However, the diverse nature of the communications industry—wireless, wireline, satellite, cable and broadcasting—makes the creation of a common methodology for self-assessments impractical. As with engineering and operational activities, specific risk management methodologies used by companies are closely guarded. In general, changes to systems, processes, buildings, and the environment can have an impact on the level of security. Corporate self-assessments are conducted to verify compliance with policies, standards, contracts, and regulations. The assessment function recognizes the criticality of the facility as it relates to the specific company and its customer base. Depending on company resources, these assessments may be handled internally, outsourced, or a combination of both.

Most companies use a standard process methodology for developing assessments. For example, prior to conducting a risk assessment of a facility, personnel must first understand the function of the facility. If an onsite inspection is required, employee interviews are used to determine the effectiveness of security solutions and processes. Results are analyzed and recommendations are developed and presented to the appropriate management team to begin addressing the recommendations. Progress on implementation of the recommendations is monitored to ensure risks are addressed in a timely fashion. Furthermore, business relationships with vendors and business partners may require companies to perform regular assessments on another company's facility to ensure that their assets are not at increased risk and contract requirements are being met. Any issues that are discovered are discussed with the vendor or business partner, and a remediation plan is determined.

3.1.2 Government-Sponsored Assessments

The National Sector Risk Assessment serves as the basis for targeted sector risk assessments. This qualitative national assessment will identify:

- Consequences, vulnerabilities, and threats to the communications architecture;
- Architecture elements and functions that could be nationally critical based on HSPD-7 defined consequences;
- Specific assets related to an architecture element or function deemed to be at high risk; and
- Protective measures to mitigate risks.

This assessment effort will capitalize on expertise from CSCC, CGCC, NSTAC, NCC, and NSIE members, as well as other security partners. The primary role of industry partners will be to analyze vulnerabilities related to the functional view of the various architecture elements. Government will provide threat information based on available intelligence and knowledge of critical government dependencies. The government also will provide regional analyses for high-risk regions, including major facilities, dependencies, and associated connectivity. Industry and government will jointly assess potential consequences as

described in HSPD-7. The assessment process will draw on past sector vulnerability and risk assessment reports, including NSTAC reports, the NSIE risk assessment, and NRIC and NCS analyses.

The NCS and relevant industry partners will conduct detailed risk assessments on architecture elements or functions identified as high risk through the National Sector Risk Assessment. Architecture elements that may be identified for detailed risk assessments include shared databases, shared facilities, or other critical architecture elements or systems. The risk assessment methodology to support detailed risk assessments is currently under development. The methodology will document the partner roles, assumptions, key definitions, and thresholds to determine what constitutes high risk and will meet the NIPP baseline criteria as detailed in appendix 3 of the NIPP to ensure it is sound, complete, and defensible.

This sector risk assessment strategy relies on broad participation of Communications Sector industry and government partners. Although government can estimate potential impact based on its aggregate knowledge of U.S. communications networks and engineering principles, only industry can assess risk and the potential impact an event may have on its networks. Contractual relationships may need to be established with the sector operators to facilitate these indepth analyses.

3.1.3 Government-Sponsored Cross-Sector Dependency Analyses

For the Communications Sector, consequence and risk cannot be calculated accurately without considering what functions a particular asset, system, or network supports. Also, supporting critical functions performed by other critical infrastructures raises the level of risk for that asset, network, or system. Because owners and operators are not always aware of the dependencies with other critical infrastructures, the Communications Sector determined that it would focus a portion of its risk assessment strategy on cross-sector dependency analysis. The primary goal is to assist other sectors in the assessment of communications dependencies for high-risk infrastructure.

The NCS and CSCC will educate other sectors through the coordinating council framework on approaches for addressing communications dependencies. This effort will be expanded to educating State, local, and tribal governments. The education process will include diversity, redundancy, and recoverability issues (see figure 3-1).

Federal departments and agencies will be encouraged to ensure the availability of NS/EP mission essential communications through contingency and COOP planning. Departments and agencies are responsible for ensuring the continued availability of mission essential and NS/EP communications services.[11] Prescribed methods of ensuring availability include redundant and physically separate communications service entry points into federally owned buildings and physically diverse local network facilities. In addition, NARUC, in partnership with the DHS, NCS, the FCC, and the private sector, has an education initiative underway with State, local, and tribal governments to coordinate approaches that facilitate resiliency and protection of interdependent CI/KR.

For high-risk CI/KR, the NCS will facilitate communications dependency analyses for other critical infrastructure sectors by performing assessments that evaluate facilities' communications resiliency. These dependency analyses will require participation of other SSAs, States, and relevant industry partners from the Communications Sector and the other critical infrastructure sector. Results will provide an assessment of risk and suggested mitigation options.

[11] Executive Office of the President, Office of Management and Budget, Memorandum M-05-176: Regulation on Maintaining Telecommunication Services During a Crisis or Emergency in Federally Owned Buildings, June 30, 2005.

Figure 3-1: Improving Communications Resiliency

- Critical infrastructures and their communications capabilities should be able to withstand natural or manmade hazards with minimal interruption or failure. The communications infrastructure is by design resilient; however, other critical infrastructures are responsible for achieving communications resiliency by having an appropriate mix of diversity, redundancy, and recoverability, based on a risk-based cost-benefit assessment.
- Diversity: Facilities should have diverse primary and backup communications capabilities that do not share common points of failure. Diversity solutions may include diverse data links (e.g., PSTN, satellite, microwave), having local loops terminate at different central offices, obtaining services from different providers with certifiable diverse routes, or using alternative transport mechanisms (e.g., wireless, satellite);
- Redundancy: Facilities should use multiple communications capabilities to sustain business operations and eliminate single points of failure that could disrupt primary services. Redundancy solutions include having multiple sites where a function is performed, multiple communications offices serving sites, and multiple routes between each site and the serving central offices; and
- Recoverability: Plans and processes should be in place to restore operations quickly if an interruption or failure occurs. Recoverability of network services could include network management controls, automatic service recovery technologies, and manual transfer to alternate facility routes.

3.2 Government-Sponsored Risk Assessment Components

As noted previously, a risk assessment should address three components: consequence, vulnerability, and threat. The following subsections describe how each component is addressed as part of the government-sponsored risk assessment process. As discussed in section 3.1.1, industry's self-assessment methodologies vary by company, but generally include an assessment of a facility's criticality as it relates to the specific company and its customers.

3.2.1 Infrastructure Screening and Consequence Assessment

The infrastructure screening and consequence assessment step will narrow the scope of the risk assessment process to those communications architecture elements having the greatest impact if disrupted, destroyed, or exploited. The analysis done in this step will include an evaluation of the dependencies and interdependencies of the sector's physical and cyber/logical architecture elements. The National Sector Risk Assessment will narrow the scope of sector risk assessments to those architectural elements that are nationally critical. National criticality will be based on consequences of primary concern to the Communications Sector. Table 3-1 provides examples of systems and missions that, if disrupted, destroyed, or exploited, could have a national impact. These concerns are also the focus of the NCS operational analysis process that assesses impact of an incident on the Nation's communications infrastructure.

Table 3-1: Communications Sector Consequences of Concern

HSPD-7 Consequence	Consequences of Primary Concern to Communications Sector
Human Impact. Effect on human life and physical well-being (e.g., fatalities, injuries)	• Emergency communications (e.g., public safety answering points, first responders) • Hospitals and other public health facilities
Economic Impact. Direct and indirect effects on the economy	• Financial markets • Communications supporting CI/KR response and recovery (e.g., transportation, electric power) • Core network and Internet backbone (national communications connectivity) • Distributed Controls Systems
Impact on Public Confidence. Effect on public morale and confidence in national economic and political institutions	• Communications supporting CI/KR response and recovery • Core network and Internet backbone (national communications connectivity)
Impact on Government Capability. Effect on the government's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions	• NS/EP communications • COOP/Continuity of Government (COG) communications • Law enforcement communications

3.2.2 Vulnerability Assessments

Vulnerabilities typically are identified through internal assessments and information sharing with customers, vendors, and suppliers. This vulnerability information will support the National Risk Assessment and asset-focused risk assessments.

The NCS will lead the government-sponsored risk assessment of architecture elements identified as critical through the consequence screening process with assistance from private sector and government SMEs. A vulnerability assessment methodology will be developed as part of the complete CSSP risk assessment methodology. The methodology will examine physical, cyber/logical, and human vulnerabilities and will consider relevant national preparedness threat scenarios. The process may vary depending on the architecture elements being studied, and may include SME interviews, site visits, and modeling and analysis. The vulnerability assessment methodology will meet the NIPP baseline criteria detailed in appendix 3 of the NIPP.

3.2.3 Threat Analysis

The DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) conducts sector threat assessments. HITRAC conducts integrated threat analysis for all CI/KR sectors, bringing together intelligence and infrastructure specialists to ensure a complete understanding of the risks to U.S. CI/KR. HITRAC works in partnership with the U.S. intelligence and law enforcement communities to integrate and analyze available threat information. HITRAC also partners with the SSAs and owners and

operators to ensure that their expertise on infrastructure operations is integrated into threat analysis. Threat assessments also are conducted through public-private partnerships such as the NSIE and the C-ISAC.

Threat Environment

The number and high profile of international and domestic terrorist attacks during the last decade underscore the determination and persistence of terrorist organizations. Analysis of terrorist strategies points to domestic and international CI/KR as prime targets for terrorist attacks. As security for more predictable targets increase, terrorists will shift their focus to softer targets. Future terrorist attacks against CI/KR across the United States could seriously threaten national security, result in mass casualties, weaken the economy, and damage public morale and confidence. Terrorist attacks on CI/KR are expected to achieve three general types of effects:

- **Direct Infrastructure Effects:** Disruption or arrest of critical functions through direct attacks on an asset, system, or network.
- **Indirect Infrastructure Effects:** Cascading disruption and financial consequences for the government, society, and economy through public and private sector reactions to an attack. An operation could reflect an appreciation of interdependencies between different elements of CI/KR, as well as the psychological importance of demonstrating the ability to strike effectively inside the United States.
- **Exploitation of Infrastructure:** Exploitation of elements of a particular infrastructure to disrupt or destroy another target or produce cascading consequences. Attacks using CI/KR elements as a weapon to strike other targets, allowing terrorist organizations to magnify their capabilities far beyond what could be achieved using their own limited resources.

Risk-mitigation measures must address each of the elements of CI/KR—physical, cyber, and human. Physical attacks represent the attack method most frequently used by terrorists. Terrorists also may use the cyber domain as a platform to attack America's CI/KR, either alone or simultaneously with a physical attack. Because of the interconnected nature of the cyber elements of CI/KR, cyber attacks can spread quickly and could have a substantial impact on the Nation's essential services and functions. Credible information on specific adversaries or cyber attack methods is difficult to obtain. However, rapidly changing technology and the relatively easy access to powerful cyber tools raises the likelihood that adversaries can develop the capability to conduct cyber attacks against CI/KR. Cyber threats are addressed in unclassified documents such as cyber threat assessments produced by HITRAC and through classified intelligence community threat assessments.

A third important aspect in this element of risk is the long-standing threat posed by insiders, or persons who have access to sensitive information and facilities. Access to, or information about, CI/KR can result from intentional actions such as extortion or terrorist infiltration of the organization, or by exploitation or manipulation of unwitting employees. Insiders can intentionally compromise the security of CI/KR through espionage, sabotage, or other harmful acts motivated by the rewards offered to them by a terrorist or other party. Others may provide unwitting assistance to an insider threat through lack of awareness of the need for or methods to protect assets or employees (e.g., by leaving security badges and uniforms in open areas). Damage caused by an insider threat may include, but is not limited to, the introduction of viruses, worms, or Trojan horses; the theft of corporate secrets or money; or the corruption or deletion of data.

Sector Threat Assessment

The Communications Sector faces both natural and manmade threats. The terrorist events of September 11, 2001, as well as the unprecedented impact that Hurricane Katrina had on the communications infrastructure, have solidified the existence of a new all-hazards threat environment. HITRAC produces sector-specific threat assessments that provide an overall review of potential terrorist threats posed to the sector and an analysis of how these threats relate to sector vulnerabilities. These assessments include known specific and general terrorist threat information, as well as relevant background information such as possible terrorist objectives and motives as they apply to the sector.

For the Communications Sector, the sector threat assessment produced by HITRAC identified few direct threats and vulnerabilities. With relatively few attacks to communications facilities or infrastructures worldwide, the threat to the Communications Sector is low. However, the risk for the sector as a residual target is high due to the sector's interdependencies on other critical infrastructure.

HITRAC also produced a cyber threat assessment. The assessment concluded that cyber/logical vulnerabilities are compounded by today's dynamic business environment, which is characterized by reliance on open system protocols and commercial off-the shelf products to manage networks and the interconnection of management networks through the Internet and with enterprise networks. Specific categories of cyber-related threats include the following: hacking, "cyber" warfare (e.g., modular malicious code, bot networks, phishing, etc.), outsourcing, hacktivists, insider threat, and NGNs incorporating both data and voice communications.

DHS Threat Scenarios

The DHS produces attack-specific threat scenarios across the sectors. The scenarios are detailed vignettes of specific methods, techniques, and actions terrorists are likely to use to attack specific types of U.S. CI/KR. The scenarios are based on HITRAC analysis of known terrorist capabilities or on their stated intent as derived from intelligence and the study of terrorist tactics, techniques, and capabilities. Threat scenarios are specific enough to be used by corporate or facility-level security officers to support operational security planning.

NSIE Assessments and Partnership Input

Threat is an important component of discussion and analysis by many of the Communications Sector's public-private partnerships (e.g., NSIEs, C-ISAC). The NSIEs produce risk assessments biannually that focus on SME opinions of perceived threat. The C-ISAC participants also regularly share threat information during weekly meetings that will be considered during the overall risk management process. Table 3-2 lists chapter 3 roles and responsibilities.

Table 3-2: Chapter 3 Roles and Responsibilities

Responsible Entity	Activities
Owner/Operators	Voluntarily conduct self-assessments of critical assets, networks, and systems.
NCS CGCC CSCC	Collaborate with industry SMEs on the development of a National Sector Risk Assessment for the Communications Sector to identify critical architecture elements for further assessment.
NCS	Facilitate risk assessments on critical architecture elements identified in National Sector Risk Assessment in collaboration with industry.
NCS CGCC CSCC	Collaborate with the IT Sector on the risk assessment of the Internet infrastructure.
HITRAC	Produce sector threat assessments.

Responsible Entity	Activities
NCS CGCC CSCC HITRAC	Collaborate with the IT Sector on cyber threat assessments affecting the Internet.
NCS	Assist other SSAs in performing risk assessments that evaluate communications dependencies for high-risk assets.
NARUC	Work with State, Territorial, and local governments on education and coordinated approaches that facilitate resiliency and protection of interdependent CI/KR assets.

4. Prioritize Infrastructure

To ensure that resources are directed to protect the country's most at-risk infrastructure, a need to normalize and prioritize assets, networks, and systems exists across sectors to the maximum extent possible. This chapter focuses on the process that the Communications Sector uses to calculate and normalize risk assessment results in a way that can be compared with other sectors and then prioritizes the infrastructure for purposes of protective program requirements.

4.1 Communications Architecture Prioritization

4.1.1 National Prioritization

The current prioritization process primarily considers consequence-related metrics and functions performed by a particular asset, system, or network to determine criticality. As the risk assessment process matures and ample data has been collected, the sector will move toward a process that prioritizes infrastructure based on the results of the full risk assessment process. Because the Communications Sector has focused its risk assessments on communications architecture elements and not specific assets, systems, and networks, the results will reflect that approach. At the conclusion of a risk assessment, the sector will validate corresponding entries in the NADB and make the appropriate updates so that the DHS can work with owners and operators to develop and implement appropriate protective measures.

Additionally, communications infrastructure elements become critical based on incident location and the specific effects on end users in the incident impact area. To determine which assets, systems, and networks are most critical during situational impact analyses, infrastructure elements supporting the following missions are identified:

- NS/EP;
- COOP/COG missions;
- Public health and safety (e.g., public safety answering points, hospitals);
- Law enforcement;
- Core Network/IP Backbone (i.e., national communications connectivity);
- Financial markets; and
- CI/KR supporting response/recovery (e.g., transportation, electric power).

During incidents, industry and government work together through the NCC to identify priorities for restoration and re-provisioning. The FCC TSP Report and Order (FCC 88-341) dictates priorities for circuits registered as critical for NS/EP.

4.1.2 Industry Self-Prioritization

The diverse nature of the communications industry makes the creation of a common methodology for prioritization complex. Companies independently determine what constitutes appropriate priority of their assets relative to their own needs and circumstances. Companies need to adopt or employ practices based on their factual situations, the practicality and effectiveness of particular actions, and economic and technological feasibility. In making this determination, companies consider all information that might be relevant. Companies also consult with legal counsel to ascertain whether their actions comply with relevant Federal, State, and local laws, which vary by the type of communications company. For example, as part of the business continuity and business impact analysis function, partners of the Communications Sector routinely assess what aspects of the business are essential for determining levels of resiliency in the event of a manmade or natural disaster. However, how a company gets to this point and what is considered critical will vary by company.

4.2 Cross-Sector Interdependency Analysis

The NCS will conduct the government-sponsored risk assessments discussed in chapter 3. Using common scales for consequences, vulnerabilities, threats, and overall risk can normalize results of these assessments and enable their comparison across sectors to the extent that is possible. Because the DHS-provided risk assessment methods/tools are not always naturally suitable for the Communications Sector, the NCS will work closely with the DHS and collaborate with the CSCC to determine methods of assigning qualitative and quantitative ratings. The DHS OIP will be responsible for aggregating the results with other sectors and prioritizing across sectors.

The centralized normalization process performed by the DHS OIP will allow for further evaluation of cross-sector interdependencies. This is important because SSAs often do not have the data to assess consequences accurately based on these interdependencies, which in turn can affect overall risk. To assist in this process, the DHS OIP will collaborate with the Communications Sector to develop a general list of interdependencies with other sectors—an effort the NCS has begun with the development of the sample list shown in table 4-1. When requested, the NCS also will assist the DHS OIP and the National Infrastructure Simulation and Analysis Center (NISAC) with cross-sector interdependency analyses, reaching out to additional Communications Sector security partners as appropriate. Table 4-2 lists chapter 4 roles and responsibilities.

Table 4-1: Examples of CI Interdependencies With Communications

Responsible Entity	Interdependency Example
Banking and Finance	The Banking and Finance Sector is dependent on communications for electronic transactions, the operation of domestic and world financial markets, and other communications needs. Any disruption of communications, especially in major financial services hubs (e.g., New York City, Chicago), would have a cascading impact on the sector's operations. The NCS has worked closely with the sector to address vulnerabilities and discuss mitigation strategies.
Chemical	The Chemical Sector is dependent on communications, largely for its control systems; thus, communications outages would have a cascading impact on the Chemical Sector.

Responsible Entity	Interdependency Example
Defense Industrial Base	The Defense Industrial Base is dependent on communications to carry out much of its mission, including the ability of Secretary of Defense to carry out National Command authority functions, intelligence functions, and communication with commanders. Thus, any widespread outages of communications may have a cascading impact on Department of Defense (DOD) operation, to include transportation and manufacturing.
Drinking Water and Water Treatment	Water systems rely on communications for its control systems; thus, communications outages would have a cascading impact on the Water Sector.
Emergency Services	Responders (police, fire, and medical) rely heavily on communications for various regular operations. In addition, emergency services coordinates response through radio, telephone, and wireless communications between the Incident Command elements, EOCs, and response agencies involved at the scene. As the lead for ESF #2 (Communications), the NCS works closely with the Emergency Services Sector and the NCC to meet emergency responders' communications needs and coordinate recovery during emergencies.
Energy (Electric Power, Oil and Gas, Nuclear Power)	Numerous interdependencies exist between the Energy and Communications Sectors. The Energy Sector relies on communications for its control systems, coordination of maintenance and repair, and for public health and safety as in the case of the Nuclear Regulatory Commission. The Communications Sector also requires energy to operate its systems, even though systems have backup generators. During blackouts, cell sites and teleports require additional fuel supplies for their generators after a certain period of time.
Information Technology	The IT and Communications Sectors have numerous interdependencies and shared critical assets. The IT Sector's communications and cyber systems ride on the communications backbone, while the Communications Sector operations are dependent on the hardware, software, and services supplied by the IT Sector. In addition, the IT Sector and the Communications Sector have a shared responsibility of protecting and maintaining the Internet. The NCS collaborates closely with the NCSD on numerous programs and CI/KR protection.
Postal and Shipping	The Postal and Shipping Sector relies on communications for its control systems and tracking shipments, as well as regular communications requirements; thus, any disruption in communications services may have cascading effects on the sector.
Public Health, Healthcare, Food and Agriculture	Any outage of communications would have a cascading impact on Public Health, Healthcare, and Food and Agriculture sectors on a localized or regional basis.
Transportation	The Transportation Sector is heavily dependent on communications. Control systems for pipelines systems and communication and data transmission systems for the National Airspace System are critically dependent on communications. Loss of communications services would have a significant cascading effect on the Nation's transportation system.

Table 4-2: Chapter 4 Roles and Responsibilities

Responsible Entity	Activities
NCS CGCC CSCC	Collaborate on the prioritization of communication architecture elements.
NCS CGCC CSCC	Collaborate to determine methods of assigning qualitative and quantitative ratings for normalizing and prioritizing architecture elements.
DHS NCS CSCC	Collaborate on the development of a general list of interdependencies with other sectors.
NCS	Assist the DHS during its cross-sector interdependency analyses when requested.

5. Develop and Implement Protective Programs

As discussed in chapter 1, the Communications Sector security strategy is to focus on ensuring the Nation's communications networks and systems are secure, resilient, and rapidly restored after an incident. Sector partners should collectively develop programs that help industry and government prevent and prepare for a potential incident; detect a potential attack on the sector; mitigate the impact and/or respond to a major disruption to critical communications services; and recover and restore essential communications assets, services, and infrastructure after an incident. This chapter presents an overview of the sector strategy and processes for developing and implementing protective programs. It takes into account the sector's mature set of protective measures and partnerships, including various government initiatives as well as those that have been put in place by industry.

The protective program development and implementation process builds on the sector security goals, and their affiliated and prioritized high-risk infrastructure, as determined by the processes described in previous chapters. Government-sponsored protective programs enable industry to better work together to address issues that it normally would not address collectively due to competitive reasons. As illustrated through examples in table 5-1, protective programs will be linked directly to goals and related risks. For example, congestion of the Nation's communications backbone during an incident has the potential for impacting the Nation by further exacerbating the situation at the national level. Protective programs that currently operate to mitigate that risk include a set of priority communications programs geared toward the NS/EP user group. Companies also mitigate this risk through network design processes.

The protective program development and implementation process will ensure that government protective programs are logically linked to specific goals and critical risks to justify costs. Industry is encouraged to undertake similar processes to justify its protective programs.

Table 5-1: Associating Protective Programs With Goals and Risks

Goal	Risk	Government Program	Risk Reduction
Backbone health	Overload of access networks	Priority services (e.g., GETS, WPS, Special Routing Arrangement Service (SRAS))	Improves access to communications for critical user groups
Rapid restoration of critical communications services	Delays in restoration of critical circuits; impact on public health/safety, national/economic security	TSP	Provides for priority restoration and provisioning of critical circuits
Plan for emergencies/crises	Delay in response resulting in impact on public health/safety and public confidence	NCC	Improves coordination of industry and government responders
Educate stakeholders on communications infrastructure resiliency	Government customers' critical communications disrupted; impact on national security	Route Diversity Project	Determines risk to a Federal agency's communications systems; applies route diversity mitigation solutions
Cross-sector coordination	Lack of knowledge and understanding of interdependencies increases risk	NCC	Improves situational awareness through the sharing of situation reports; provides mechanism to resolve cross-sector issues

5.1 Protection Roles and Responsibilities

Infrastructure owners, following proven business continuity and contingency planning practices, are responsible for protecting their internal assets. To protect those assets during either manmade or natural disasters, infrastructure owners must be provided a thorough and accurate picture of the terrorist threat; possess a clear understanding of government infrastructure protection and recovery priorities; coordinate with the Federal Government, when necessary, to obtain necessary resources and assistance relative to the protection, sheltering, and credentialing of employees and access to fuel and energy sources; and have the ability to restore the sector without the constraints of overly burdensome regulations and governmental requirements and procedures that delay recovery efforts.

The NCS has numerous programs and responsibilities for the Communications Sector, spanning the spectrum of protective and preparedness activities. As detailed in appendix 5, the NCS manages the NCC; leads ESF #2 (Communications) planning, response, and recovery efforts; develops and maintains numerous priority services; conducts training and exercises; and performs operational analyses. In addition, the NCS, with assistance from the FCC and NARUC, will continue its priority services

outreach activities to ensure that critical NS/EP circuits are registered with TSP and that key officials have access to GETS and WPS. Throughout all these activities, the NCS mission is to be responsive to NS/EP needs of the Federal Government.

States also have protective program responsibilities for the Communications Sector. Current multi-State initiatives include development of not only multi-sector, multi-State access and credentialing procedures, but also POC networks to be used for incident management.

5.1.1 Industry Customer Outreach

Industry partners regularly work with enterprise customers to educate them on risks and mitigation strategies. In addition to joint outreach activities conducted through the coordinating council framework, Communications Sector industry partners will continue to conduct customer outreach. These outreach activities will educate customers on the CSSP and on the risk variables that customers need to consider as part of their own business continuity practices as well as resiliency best practices. The Communications Sector will collaborate with the IT Sector on outreach and education to customers on their reliance on Communications and IT infrastructures and corresponding security roles and responsibilities. Future outreach should also include educating customers on the results of risk assessments relevant to the customer.

As addressed in previous chapters, customers also have responsibility for protecting the communications infrastructure. Customers need to assist in mitigating risk by developing communications backup plans and implementing resiliency measures (e.g., geographic diversity). Industry does not always know how, when, and where its customers are using their assets and what critical business functions they may be running on communications assets. Communications Sector industry partners plan to engage with customers on their responsibilities and provide information on the preparedness and protective actions that customers can take to mitigate risks.

5.1.2 Shared Asset Protection

Many assets within the national communications architecture are shared by multiple providers. Typically, owners and operators have agreements in place that address protection, repair, or restoration of those assets. Agreements often stipulate that the provider that reaches the asset first will either restore the asset or have a schedule identifying which provider is responsible at any given time. TSP restoration priorities, as defined in the FCC TSP Report and Order (FCC 88-341), dictate priorities for circuits registered as critical for NS/EP.

5.2 Existing Programs

5.2.1 Government-Sponsored Programs

The Communications Sector, through an established self-management process, is responsible for supporting numerous protective programs that are either sponsored by government or are owned by government. The existing protective programs:

- Help stakeholders prepare for crisis situations, alerting them of potential problems/attacks;
- Mitigate vulnerabilities;
- Provide priority communication services;
- Facilitate the recovery of critical communications assets for Federal, State, local, and tribal governments; and
- Address interdependencies with other sectors.

The continued success and evolution of these programs will help ensure the security of the communications infrastructure and delivery of services. Although these programs are focused largely on response and recovery measures within the sector, the following protective programs (see table 5-2) have been developed, and owner/operators are active participants. These programs are described in more detail in appendix 5.

Table 5-2: Communications Sector Protective and Preparedness Programs

Category	Program
Protective Actions[12] Deter Devalue Detect Defend	National Coordinating Center (NCC)/NCC Watch National Security Telecommunications Advisory Committee (NSTAC) Network Reliability and Interoperability Council (NRIC) Media Security and Reliability Council (MSRC) Network Security Information Exchanges (NSIEs)
Preparedness Actions Mitigate Respond Recover	NCC NCS Emergency Response Training Government Emergency Telecommunications Service (GETS) Wireless Priority Service (WPS) Telecommunications Service Priority (TSP) Special Routing Arrangement Service (SRAS) Hotline System Shared Resources (SHARES) High Frequency Radio Program Regional Coordinating Capability Route Diversity Project COOP/COG Support

In addition to formal programs, Communications Sector industry and government partners regularly work together on ad hoc projects to improve the sector's preparedness and protective posture. Although most programs focus on physical and cyber elements, two recent initiatives address the human element of risk.

- **Pandemic Flu Planning:** The NCS and the Communications Sector have participated in multiple aspects National Pandemic Flu Planning. During the initial phases of planning, the NCS participated in preparing the DHS OIP's IP Contingency Plan. The plan identified nine major actions to be taken at various stages of a pandemic outbreak in the world and transfer to the U.S. mainland. These actions were subsequently written up as an appendix to the NCS COOP Plan. Work with industry involves two aspects. First, the NCS, with cooperation from industry, is conducting ongoing modeling of the infrastructure to determine the impacts of substantial surges in telework in the event of a pandemic. Reports are presented to the DHS

[12] Government-sponsored protective actions emphasize coordination between industry and government to promote information sharing, development of best practices, and operational planning. Infrastructure owners, following proven business continuity and contingency planning practices, are responsible for protecting their assets, networks, and systems.

Office of Cyber Security and Telecommunications and the DHS leadership as information changes. Modeling and analysis will continue as new information regarding potential impacts are changed by the Department of Health and Human Services. The second aspect is to plan jointly for corporate actions required to maintain network operations and fulfill new service requests. The infrastructure owners and operators, in part through these efforts, have instituted significant planning efforts in their individual operations; and

- **Access and Credentialing Pilot Program:** Industry and government have been working with State and local jurisdictions in the Southeastern and Gulf Coast regions to pilot a credentialing program to improve access for private sector responders to be permitted into restricted areas to restore infrastructure. These pilot programs have been distributed widely through the NCC, CSCC, State Homeland Security Advisors, NARUC, the National Emergency Management Association, and emergency management officials. Access was the subject of a NARUC-sponsored workshop and was exercised in regional ESF #2 exercises. Communications companies and State and local government organizations have been advised to work closely with each other to establish access protocols. ESF #2 will monitor access in future national emergencies and take immediate action to facilitate access for communications responders.

Specific programs, highlighted below, also are in place that address Internet security and communications and IT cross-sector issues (see appendix 5 for full descriptions).

- **United States Computer Emergency Readiness Team (US-CERT):** A team that coordinates defense against and responses to cyber attacks nationwide;
- **Internet Disruption Working Group (IDWG):** A strategic partnership between public and private sector entities formed in response to concerns surrounding the dependency of critical communications, operations, and services on Internet functions;
- **National Cyber Response Coordination Group (NCRCG):** a group that facilitates the Federal Government's efforts to prepare for, respond to, and recover from cyber incidents and physical attacks that have significant cyber consequences; and
- **NetGuard:** A DHS-led initiative set up to bring together the public sector with the State and local community following an incident that impacts information systems and communications networks.

5.2.2 Industry Protective Measures and Initiatives

Industry efforts to protect their assets include, but are not limited to, multi-billion dollar investments to improve redundancy and resiliency by adding generators, improving physical security at facilities, improving crisis management processes and protocols, and performing audits to increase the level of protection. Industry also supports a number of organizations that share common knowledge in the development of industry standards. Three such organizations are the International Organization for Standardization (ISO), ITU, and ATIS.

- **ISO:** An international standards-setting body composed of representatives from national standards bodies that produces world-wide industrial and commercial standards, called ISO standards. An example of an ISO security management standard that is widely recognized within the communications industry is ISO 17799. This standard provides high-level recommendations for enterprise security in the areas of information security policy for the organization, creation of information security infrastructure, asset classification and control, personnel security, physical and environmental security, communications operations management, access control, system development and maintenance, business continuity, and compliance.
- **ITU:** An international organization established to standardize and regulate international radio and telecommunications. Its main tasks include standardization, allocation of the radio spectrum, and organizing interconnection arrangements between different countries to allow international phone calls.

- **ATIS:** Develops and promotes technical and operations standards for the communications industry. ATIS members include more than 300 companies representing communications service providers, equipment manufacturers, and related industry segments.

Protective measures implemented by infrastructure owners and operators vary depending on a company's risk management and security practices. Appendix 6 describes the sector's approach to best practices. Typically, companies have in place a suite of physical, cyber, and human security measures.

- **Physical Security:** These measures will vary depending on the characteristics of the asset's location, function in the architecture, and customer requirements. Types of assets typically include data centers, switch sites, POP sites, warehouses, call centers, retail stores, and general office buildings. For example, transmission lines that are omnipresent cannot receive the same level of security as an end office or a teleport. Similarly, an end office in a rural area will likely not have the same security level as one in an urban area. Furthermore, physical security assessments are conducted based on the criticality of the asset to verify compliance with policies, standards, contracts, and regulations (see section 3.1.1, Industry Self-Assessments).

- **Cyber/Logical Security:** These measures are a critical security element for the infrastructure provider. Communication companies have created extensive cyber security programs designed to protect their networks from malicious attacks and unauthorized activity. The risk management strategies used by communications companies are consistent with, and can be mapped to, the IT SSP.

  Similar to the other security elements, they will vary; however, some common practices exist throughout the sector. For example, two common practices carriers take to ensure the signaling and control planes are:

  – **Access Control Lists (ACL):** Filtering IP packets destined to the router in specific IP address and protocol ranges to protect the router management plane and router control plane;

  – **Reverse Path Forwarding:** Checking the source IP address to protect against spoofing and denial of service attacks and dropping packets when the source address does not match the packet's origin path.

- **Human Security:** These elements also vary depending on a company's human resources policies. Companies may screen employees to confirm their backgrounds and provide assurance of necessary trustworthiness; rotate assignments to reduce the chance of fraud and misuse of resources; enforce separation of duties and least- privilege policies; conduct periodic security awareness training; implement password and account management policies and practices; log, monitor, and audit employee online activity; monitor and respond to suspicious or disruptive behavior; and deactivate access following termination. The purpose of these procedures is to mitigate the threat posed by insiders and a company's reliance of individual employees. The Communications Sector also uses robust business continuity plans assessing threats, vulnerabilities, and countermeasures with sound business practices to develop and maintain an appropriate state of resiliency and preparedness within the company.

5.3 Protective Program Identification Process

In recognition of the shared protective responsibilities between industry and government, the Communications Sector will coordinate the development of protective measure strategies as part of the risk analysis process and prioritization of risk assessment results. Based on prioritization of risks, the SSA, CGCC, and CSCC will meet to determine if a new government protective program is necessary. The decisions on which risks to address will consider the following factors:

- Impact on the entire communications infrastructure;

- Imminence of threat;

- Magnitude of vulnerability;
- Cost-benefit analysis;
- Available funding; and
- Effectiveness of existing or potential protective measures in reducing risk.

In the event that a new government protective program is necessary, the process will conclude with identifying appropriate partners (e.g., CSCC, CGCC, IT Sector) and assigning roles and responsibilities for developing agreed-on protective measures. Partners may include select owner/operators, equipment manufacturers, trade associations, and appropriate government agencies for programs focused on the communications infrastructure. For programs geared at addressing dependencies with other critical infrastructure, the NCS will engage appropriate SSAs.

To help guide and validate protective programs, the NCS also will continue to consult two of its trusted partners—the NCS COP and NSTAC—to identify shortfalls and weaknesses in the NS/EP communications infrastructure and recommend appropriate action. Through the COP process, the NCS provides NS/EP communications recommendations to the EOP. The NSTAC provides crucial advice and recommendations to the President and the Secretary of Homeland Security on the development and execution of NS/EP communications programs.

Funding is a major issue affecting all security and protective initiatives, including those within the communications industry. Implementation of sector protective measures will be determined by the availability of resources.

5.4 Protective Program Development and Implementation

New protection priorities identified through the risk assessment process may require additional protective programs. These protective programs are likely to fall into three categories: private sector initiatives, Federal Government programs, and State government projects.

- **Private Sector Initiatives:** Typically require a business case for justification to implement the initiative. These initiatives may be developed by owners and operators to voluntarily respond to specific vulnerabilities identified during risk assessments. These initiatives may be in the form of voluntary best practices, standards, or individual company protective measures. Individual owners and operators or trade associations will develop, implement, and maintain these initiatives.
- **Federal Government Programs:** May be developed if there is a risk to NS/EP users that could be mitigated by a national-level program or enhancements to an existing program. Upon obtaining funding, the NCS will lead the development, implementation, and maintenance of these programs. A relationship will be maintained with relevant service providers and operators and with equipment manufacturers throughout the process.
- **State Government Projects:** Allow State agencies to coordinate with one another and with their Federal and private sector counterparts. NARUC and States have begun to work with the FCC and others to develop emergency POC networks in PUCs, emergency management agencies, Governors' offices, and others to facilitate regional coordination and mitigate effects on interdependent sectors, when appropriate.

5.5 Government Protective Program Performance

Once government programs have been developed and implemented, the NCS will conduct followup risk assessments on government protective programs to measure their success in reducing overall risk after about 2 years of full implementation. When a program overlaps the Communications and IT Sectors, there will be a joint program review. This evaluation process will include the following steps:

- Program briefing with program manager;
- Followup interviews with program users (if relevant);
- Site assessment (if relevant),
- Update of risk assessment of relevant architectural element(s);
- Cost-benefit analysis; and
- Program performance evaluation.

The performance evaluation will assess the program's effectiveness and make recommendations for future funding and potential changes or enhancements. With the high rate of technological advances in the Communications Sector, these performance evaluations will need to consider changes in technology, which may lead to the enhancements in some programs, while discontinuing others that are no longer relevant.

The NCS will discuss successes and lessons learned from protective program performance in the CI/KR Sector Annual Report. The annual report will be shared with sector security partners to ensure that partner security decisions are informed by the current activities. Table 5-3 lists chapter 5 roles and responsibilities.

Table 5-3: Chapter 5 Roles and Responsibilities

Responsible Entity	Activity
NCS Private Sector	Coordinate the development of protective measure strategies.
NCS	Work with NCSD to avoid duplication of efforts.
NCS FCC NARUC	Continue priority services outreach to ensure that critical NS/EP circuits are registered with TSP and key officials have ready access to GETS and WPS.
FCC NARUC	Voluntarily develop and implement POC networks and engage in regional coordination on preparedness.
Private Sector	Continue customer service outreach to educate customers on the CSSP and risk.
NCS	Manage numerous protective programs for the Communication Sector in close partnership with the private sector.
NCS	Develop and implement operational plans and procedures for the DHS to assist the Communications Sector in incident prevention, detection, mitigation, response, and recovery.

Responsible Entity	Activity
NCC	Coordinate joint industry-government efforts to initiate, restore, and reconstitute critical communications services.
NCC	Work with industry representatives to support communications emergency response.
NCS CGCC CSCC	Determine necessary protective measures for high-risk assets, networks, and systems.
NCS	Validate protective initiatives with COP/COR and NSTAC.
Private Sector	Voluntarily develop and implement protective measures for its high-risk assets and networks.
NCS	Develop and implement national-level protective measures to mitigate risks to nationally critical systems supporting NS/EP.
NCS	Conduct followup risk assessments and performance evaluations of government-sponsored programs to measure success of protective measures.
NCS	Report on protective measure successes and lessons learned in the sector's annual report.
NCS	Collaborate with the IT Sector on outreach and education to customers on their reliance on Communications and IT infrastructures and security roles and responsibilities.
NCS	Conduct joint discussions with the IT Sector on protective program effectiveness and requirements for new protective programs.

6. Measure Progress

Industry and government partners in the Communications Sector will measure their collective success based on progress achieved against CSSP goals. These goals will evolve over time according to changes in the sector's risk and business environments. In this CSSP, the Communications Sector is establishing a framework to help identify, monitor, and evaluate its successes in sector-wide risk management efforts.

This framework and the specific measures contained in this document will be reviewed by industry and government annually and in the aftermath of major events. It will be revisited, as necessary, as the sector's risk mitigation activities mature. Although industry's participation in this process is voluntary, it will help ensure accuracy in performance measurement. With performance results, industry and government can make more informed decisions on protective investments and process improvements.

This performance measurement process requires close industry and government collaboration in monitoring sector progress in critical infrastructure protection, response and recovery, awareness, and cross-sector coordination. To assess its progress, the Communications Sector will use three levels of performance measurement, including:

- **Core NIPP Metrics:** Measures that are common to all sectors and used to demonstrate how each sector contributes to overall NIPP critical infrastructure risk mitigation efforts;
- **Specific Communications Sector Metrics:** Measures that demonstrate how Communications Sector industry and government partners are performing against explicit sector requirements and goals; and
- **Protective Programs Metrics:** Measures that assess the performance of government protective programs, outlined in section 5.4 of this CSSP.

Performance measures will promote Communications Sector awareness of the status of sector risk mitigation activities and the progress of related programs and activities. This awareness will help spur corrective action to address sector vulnerabilities and to help leverage sector sound practices. Sector metrics also provide quantifiable snapshots of performance trends over time. Trend analysis will facilitate benchmarking sector success in meeting goals and cataloging the impacts of sector progress.

6.1 CI/KR Performance Measurement

The implementation of Communications Sector performance measures will depend on the quality of collaboration between the NCS and its industry and government partners to develop, track, and report on sector-specific metrics. Through such collaboration, the NCS and its security partners will work together to accomplish the following:

- Develop sector-specific metrics;
- Collect responses to core and sector-specific metrics from the sector;
- Ensure the accuracy of the information collected;
- Report metrics to the DHS; and
- Ensure that metrics meet the DHS's needs for monitoring performance across the Communications Sector.

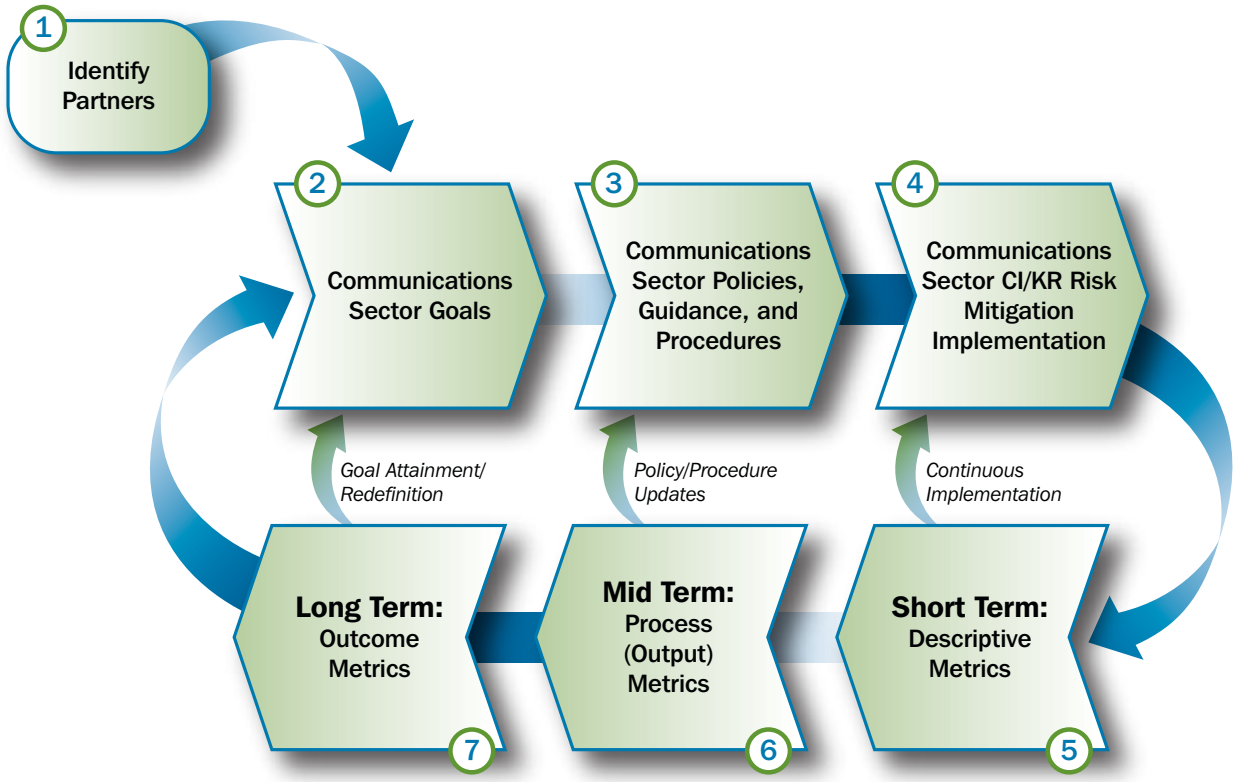
6.1.1 Communications Sector Metric Development

Metrics are tools designed to facilitate decisionmaking, performance improvement, and accountability through the collection, analysis, and reporting of relevant performance data. To ensure that metrics are useful for tracking performance, directing resources, and facilitating performance improvement, the metrics must:

- **Be Based on Performance Goals:** Sector goals for industry and government partners are identified and prioritized to ensure that performance measures correspond with the operational priorities of the Communications Sector.
- **Yield Quantifiable Information:** Metrics should produce the data necessary for making comparisons, applying formulas, and tracking changes using the same points of reference. When quantifiable information is unavailable, meaningful qualitative indicators will be substituted.
- **Be Obtainable and Repeatable:** Data for calculating metrics needs to be easily obtainable and repeatable (i.e., obtainable on a regular basis) to enable analysis of performance trends over time.

To adhere to these fundamental aspects of sound performance measurement, the Communications Sector will use the Performance Measurement Framework depicted in figure 6-1 to develop its sector-specific metrics. As figure 6-1 illustrates, the Communications Sector will use a time-phased approach to performance measurement, using different types of metrics to assess sector performance as the sector metric efforts mature. Steps 1 through 3 include identifying sector-specific partners, and applicable goals and policies that govern the sector. Steps 4 through 7 measure the sector's progress in achieving goals and compliance with applicable policies and procedures through a maturing series of measurement indicators. Feedback mechanisms will be used to update and amend the measurement framework over time.

Figure 6-1: Communications Sector Performance Measurement Framework



Step 1 of the Communications Sector Performance Measurement Framework involves identifying Communications Sector partners. Partners should be involved in each step of metrics development to ensure sector-wide buy-in to the concept of measuring sector performance. Partner involvement will also ensure that a sense of ownership of the metrics exists throughout the sector to encourage success in mitigating sector risks. Initial partners in this process include the following:

- NCS representatives;
- CSCC members; and
- CGCC members.

The number and mix of Communications Sector industry and government partners in this process will evolve over time.

Step 2 involves identifying Communications Sector goals that will guide performance by industry and government partners. These goals serve as performance objectives and will frame the measurement process. These goals are defined in chapter 1.

Step 3 involves examining applicable sector-specific policies and procedures for securing and assuring the resiliency of Communications Sector infrastructure. These policies and procedures describe the key activities and responsibilities of industry and government partners in the Communications Sector. They are intended to serve as a framework for establishing performance measures. Only those policies and procedures with a direct impact on CI/KR that lend themselves to measurement will be used. Specific sector policies, authorities, directives, and orders are explained in detail in appendix 3.

The overarching critical infrastructure protection policies that deal with Communications Sector availability, resiliency, and security include:

- HSPD-7 (December 2003);
- *The Homeland Security Act of 2002* (November 2002);
- *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* (July 2002); and
- *The National Strategy to Secure Cyber Space* (July 2002).

These high-level policies will be combined with sector goals to establish the measurement process for industry and government partners within the Communications Sector. As sector measurement activities mature, other policies and procedures may be incorporated into the measurement framework to provide a more robust view of sector CI/KR risk mitigation performance.

In addition, Executive Orders, National Security Decision Directives, Presidential Decision Directives, Presidential War Emergency Powers for Telecommunications, NTIA policy, and Federal, State, and local authorities all drive the Communications Sector. These authorities, directives, and orders discussed in appendix 3 may contribute to sector metrics formulation. All metrics developed by industry and government partners will be intended to support these policies and to evaluate the sector's progress in reducing risk by adhering to these authorities.

Step 4 involves establishing measures to assess the sector's performance against its goals, policies, and procedures from Steps 2 and 3. Performance measures will help determine the effectiveness of risk mitigation efforts and whether specific activities and programs need to be continued, modified, or cancelled to best meet sector goals. Specific metrics will be mapped to sector goals to provide a robust assessment of sector performance. This will allow partners to determine which goals are not being met and what corrective actions may be necessary.

As the sector matures, new metrics may be used in subsequent steps of the Performance Measurement Framework to assess performance. For instance:

- **Short-Term Descriptive Metrics:** May be used initially to assess sector risk mitigation and protection program and activity implementation. An example of a short-term descriptive metric is: "Total number of COP/COR meetings hosted during fiscal year."
- **Mid-Term Process and Output Metrics:** May be used as the sector matures to determine if the risk mitigation and protection activities and programs outlined in this SSP are working as planned. An example of a process metric is: "Percentage of protective program milestones met."
- **Long-Term Outcome Metrics:** May be used as the sector reaches maturity to assess the impact of sector risk mitigation activities and programs. Where possible, outcome metrics will assess not only risk mitigation effectiveness but also the financial efficiency of risk mitigation activities. Examples of outcome metrics are: "Cost per Communications Sector partner trained in government-sponsored infrastructure resiliency and risk management" and "Percentage of sector networks with protocols in place to protect integrity in the event of usage surge."

Metrics will be designed to support and demonstrate progress against Communications Sector goals. Table 6-1 illustrates the sector goals and the potential areas of measurement for each goal. The measurement areas will be used to help create and approve relevant metrics. All industry and government partners will be involved in the metric creation and approval process. The NCS, together with the Communications Sector Measurement Working Group participants, will develop metrics based

on the measurement areas for each goal. Each metric will be documented in a standard template to help ensure consistency. Table 6-2 illustrates the metric template.[13]

Table 6-1: Potential Communications Sector Measurement Areas

Responsible Entity	Activity
Goal 1: Protect the overall health of the communications backbone	• Implementation of security processes and best practices to protect the backbone: • Standardized screening process for relevant personnel with access to communications assets; • Access control best practices; • Insider threat mitigation best practices; and • Industry and government threat and vulnerability information sharing.
Goal 2: Rapidly reconstitute critical communications services after national and regional emergencies	• Implementation of processes and procedures to rapidly respond to crises affecting the communications infrastructure; • COOP during crises; and • Ability to meet evolving communications requirements in austere environments.
Goal 3: Plan for emergencies and crises through participation in exercises, and update response and COOP plans	• Development of and participation in threat simulations and exercises; and • Implementation of processes to ensure continuity and availability of National Essential Functions and Priority Mission Essential Functions.
Goal 4: Develop protocols to manage the exponential surge in calls during an emergency and ensure the integrity of sector networks during and after an emergency event	• Development of increased surge capacity protocols to allow for increased traffic during emergencies; • Participation in conferences, trade shows, and outreach activities on priority service programs; • Research and development on priority service programs; and • Development of POC networks in State government to facilitate regional coordination.
Goal 5: Educate stakeholders on communications infrastructure resiliency and risk management practices in the Communications Sector	• Development of educational programs on communications technologies and their potential points of failure during emergencies; • Prioritization of critical private and public sector capabilities and functions that depend upon the communications infrastructure; and • Continuation of NARUC education programs for State regulators and others on the role of State agencies in building resiliency, facilitating response, and considering interdependencies.

[13] The metrics template aligns with the metric template contained in NIST Special Publication 800-55, ***Security Metrics Guide for Information Technology Systems***, October 2002.

Responsible Entity	Activity
Goal 6: Ensure timely, relevant, and accurate threat information sharing between the law enforcement and intelligence communities and key decision-makers in the sector	• Implementation of policies to enable appropriate industry partners to get necessary security clearances; and • Development of procedures for getting input from industry and State and local officials into threat assessments.
Goal 7: Establish effective cross-sector coordination mechanisms to address critical interdependencies, including incident situational awareness, and cross-sector incident management	• Development of and participation in cross-sector threat exercises; and • Development of and participation in cross-sector working groups.

Table 6-2: Communications Sector Metric Template

Metric Component	Description
Performance Goal	Communications Sector goal that the metric supports
Purpose	Overall functionality obtained by collecting the metric, what insights are hoped to be gained from the metric, regulatory or legal reasons for collecting a specific metric if such exist, or other similar items
Implementation Evidence	Implementation evidence is used to calculate the metric, provides indirect indicators that validate that the activity is performed, and identifies causation factors that may point to the causes of unsatisfactory results for a specific metric
Frequency	Time periods for data collection
Formula	Calculation to be performed that results in a numeric expression of a metric
Data Source	Location of the data to be used in calculating the metric and parties responsible for reporting the data
Indicators	Information about the meaning of the metric and its performance trend; possible causes of trends; possible solutions to correct the observed shortcomings; performance target, if it has been set for the metric; and indication of what trends would be considered positive in relation to the performance target

Once developed, metrics will be shared with sector partners for review and comment. Feedback will be incorporated into the metric template, and the metrics will become official and tracked for data analysis and reporting purposes according to their frequency, as indicated in the metric template. As Steps 5 through 7 of the Performance Measurement Framework indicate, various metrics will yield different results and provide different indicators for Communications Sector industry and government partners as the CSSP process matures.

Step 5 begins the metric data collection process for the sector. It features short-term descriptive measures to assess the implementation of planned sector activities and programs and their subsequent resource requirements. The descriptive metrics are used to understand sector resources and activities; they do not reflect CI/KR protection performance.

The Communications Sector Measurement Working Group will develop and advance descriptive measures with Communications Sector partners. Once agreement is reached, each metric will be formally documented in the template presented in table 6-3. As the sector continues to evolve, metrics will change and mature to continually meet the evolving measurement requirements of industry and government partners.

The Communications Sector is currently working to define and implement its metrics methodology. The Communications Sector expects to begin descriptive metrics identification, collection, and reporting within a year of SSP approval, collecting output and outcome metrics only for existing programs. Furthermore, the sector anticipates reliance on descriptive and qualitative metrics for the first 2 years of CSSP implementation, with qualitative and outcome metrics being implemented by fiscal year (FY) 2009. Table 6-3 shows key milestones in the Communications Sector metric development effort.

Table 6-3: Metrics Development Timeline

Activity	Days After SSP Approval			
	90 Days	180 Days	365 Days	Specific Date
Submit Final SSP				FY 2007
Finalize specific descriptive metrics	+			
Begin collecting descriptive metrics data		+		
Educate stakeholders on communications infrastructure resiliency		+		FY 2009
Cross-sector coordination				FY 2009

Step 6 shifts from a descriptive metrics focus to an output metrics focus. Output measures help partners determine whether specific activities are performing as planned by tracking the progression of a task, reporting on the output of a process such as inventorying assets, or showing progress toward performing the activities necessary to achieve Communications Sector goals. They also build on descriptive metrics by helping to build a comprehensive picture of Communications Sector CI/KR protection status and activities. As the sector matures, the Communications Sector Measurement Working Group will develop output metrics for review and comment for sector partners using the same process as the descriptive metrics.

Step 7 moves from an output metrics focus to an outcome metrics focus. Outcome metrics track progress toward reaching the sector's strategic goals by evaluating beneficial results rather than implementation or activity levels. This, in turn, indicates progress toward reaching sector-specific goals. As the Communications Sector continues to mature, the Communications Sector Measurement Working Group will develop outcome metrics for review and comment for sector partners utilizing the same process as the descriptive and output metrics.

As figure 6-1 illustrates, feedback loops are built into the performance measurement framework. As the Communications Sector continues to mature, feedback loops will ensure that goals, policies, and procedures are updated, as necessary.

6.1.2 Information Collection and Verification

Consistent data collection, verification, analysis, and reporting are crucial to a successful performance measurement effort. The Communications Sector will rely on a structured metric information collection and verification strategy.

As identified in figure 6-3, each metric has specific data sources, parties responsible for reporting metric data, and metric reporting frequencies. Because each metric will have different data sources and responsible parties, the NCS Customer Service Division will be used as a centralized conduit for the NCS and its industry and government partners to report metric data. The NCS Customer Service Division, in conjunction with its industry and government partners, will employ an online or automated tool with an easy-to-use front end for partners to report data and a data repository back-end to store and validate data fields for analysis and reporting purposes. The NCS Customer Service Division can then transfer appropriate information to the NIPP online metrics portal.

6.1.3 Reporting

The primary means of Communications Sector reporting will be the CI/KR Sector Annual Report. This report is submitted to the DHS and describes the sector security goals, priorities, programs, and related funding requirements, as well as a catalogue of progress that has been made in sector CI/KR protection. By collecting and reporting metrics results, the Communications Sector will be able to establish a performance baseline and then show progress against the baseline in ensuing years. In addition, metric performance data against each goal will allow industry and government partners to identify under-performing areas for the sector quickly and prioritize funding, resources, and activities accordingly to improve sector performance.

Furthermore, as discussed in section 6.1.2, the NCS Customer Service Division will serve as a clearinghouse for sector metrics reporting from industry and government partners. The NCS Customer Service Division will collect sector-reported information, report it to the NIPP online metrics portal, and aggregate data for the sector annual report. Further information on reporting is detailed in section 8.2.2.

6.2 Implementation Actions and Monitoring Performance

Table 6-4 illustrates the milestones outlined in this CSSP, milestone start dates, and parties responsible for milestone completion. New milestones may be added as the CSSP is implemented and the sector matures.

Table 6-4: Implementation Actions

Activity	Milestone					Security Partner					
	Ongoing	90 Days After SSP Approval	180 Days	365 Days	Specific Date	DHS	SSA	Other Federal Agency	State or Territory	Local and Tribal	Private Sector
Communications SSP 1. Sector Profile and Goals											
Host Annual Joint CGCC/CSCC meeting to revisit and revise security goals				+		O	X	O	O	O	O
Hold joint Communications and IT Sectors meeting twice a year to address issues of interest to both sectors and discuss potential areas for collaboration	+		+			O	X	X	O	O	X
Identify synergies and gaps between Communications and IT security partners, and collaborate whenever possible on partner outreach	+					O	X	X	O	O	X
Cooperatively address with the IT Sector areas of convergence, such as those identified in the NSTAC Report to the President on the NCC, including developing an approach for a long-term regional communications and IT coordinating capability that serves all regions of the Nation, convening a conference to focus on cyber/logical issues, and exploring ideas for a multi-industry coordinating center	+		X			O	X	X	O	O	X
Work with Canada, Mexico, and other international partners to identify international interdependencies	+		X			O	X	X			O
Work with Canada, the United Kingdom, and other partners to develop government-to-government priority communications services	+					O	X	X			O
Communications SSP 2. Identify Assets, Systems, Networks, and Functions											
Identify sector architecture elements for each subsector, including cyber/logical assets			+				X				O
Develop a formal process for the NOC and the NCC to identify specific sector assets, related to credible threats, during emergencies or in preparation for NSSEs			+			X	X				O
Coordinate with the OIP to populate the NADB and validate existing entries	+					X	X				
Verify data and address incomplete or incorrect data	+						X				O

Activity	Milestone					Security Partner					
	Ongoing	90 Days After SSP Approval	180 Days	365 Days	Specific Date	DHS	SSA	Other Federal Agency	State or Territory	Local and Tribal	Private Sector
Maintain the communications asset database and provide the DHS with asset data updates	+		+			X	X	O	O	O	O
Collaborate with the IT Sector on the identification of Internet infrastructure elements				+		O	X	X	O	O	X
Communications SSP 3. Assess Risks											
Voluntarily conduct self-assessments of critical assets, networks, and systems	+										X
Collaborate with industry SMEs on the development of a National Sector Risk Assessment for the Communications Sector to identify critical architecture elements for further assessment				+			X	X	O		X
Facilitate risk assessments on critical architecture elements identified in National Sector Risk Assessment in collaboration with industry	+			+		O	X	O	O	O	O
Collaborate with the IT Sector on the risk assessment of the Internet infrastructure				+		O	X	X	O	O	X
Produce sector threat assessments	+					X	X				
Collaborate with the IT Sector on cyber threat assessments impacting the Internet	+					X	X	X	O		X
Assist other SSAs in performing risk assessments that evaluate communications dependencies for high-risk assets	+			+		X	X	X	O	O	O
Work with State, Territorial, and local governments on education and coordinated approaches that facilitate resiliency and protection of interdependent CI/KR assets	+					O	O	X	O	O	O
Communications SSP 4. Prioritize Infrastructure											
Collaborate on the prioritization of communication architecture elements					FY 2008	X	X	O	O		O
Collaborate to determine methods of assigning qualitative and quantitative ratings for normalizing and prioritizing architecture elements					FY 2008	X	X	O	O		O

Activity	Milestone					Security Partner					
	Ongoing	90 Days After SSP Approval	180 Days	365 Days	Specific Date	DHS	SSA	Other Federal Agency	State or Territory	Local and Tribal	Private Sector
Collaborate on the development of a general list of interdependencies with other sectors				+		X	X	O	O	O	O
Assist the DHS during its cross-sector interdependency analyses when requested											
Communications SSP 5. Develop and Implement Protective Programs											
Coordinate the development of protective measure strategies	+					X	X		O		X
Work with NCSD to avoid duplication of efforts	+	+				X	X				
Continue priority services outreach to ensure that critical NS/EP circuits are registered with TSP and key officials have ready access to GETS and WPS	+						X	X	X		
Voluntarily develop and implement POC networks and engage in regional coordination on preparedness	+					O	O	X	X	O	
Continue customer outreach to educate customers on the CSSP and risk	+								O		X
Manage numerous protective programs for the Communications Sector in close partnership with the private sector	+						X	O	O		
Develop and implement operational plans and procedures for the DHS to assist the Communications Sector in incident prevention, detection, mitigation, response, and recovery	+					O	X	X			X
Coordinate joint industry-government efforts to initiate, restore, and reconstitute critical communications services	+					O	X	O	O		X
Work with industry representatives to support communications emergency response	+					O	X		O		X
Determine necessary protective measures for high-risk assets, networks, and systems					As Needed	O	X	X			X
Validate protective initiatives with COP/COR and NSTAC Voluntarily develop and implement protective measures for its high-risk assets and networks					As Needed	X	X	X			X

Activity	Milestone					Security Partner					
	Ongoing	90 Days After SSP Approval	180 Days	365 Days	Specific Date	DHS	SSA	Other Federal Agency	State or Territory	Local and Tribal	Private Sector
Voluntarily develop and implement protective measures for its high-risk assets and networks	+										X
Develop and implement national-level protective measures to mitigate risks to nationally critical systems supporting NS/EP					As Needed	O	X				O
Conduct followup risk assessments and performance evaluations of government-sponsored programs to measure success of protective measures					FY 2008		X		O		
Report on protective measure successes and lessons learned in the sector's annual report			+				X	O			O
Collaborate with the IT Sector on outreach and education to customers on their reliance on Communications and IT infrastructures and security roles and responsibilities	+			+		X	X	X	O		X
Conduct joint discussions with the IT Sector on protective program effectiveness and requirements for new protective programs	+					X	X	X	O		X
Communications SSP 6. Measure Progress											
Establish Communications Sector measurement working group		+									
Finalize specific descriptive metrics		+					X	X	O		X
Begin collecting descriptive metrics data			+				X	X	O		X
Report descriptive metrics data				+			X	X	O		X
Finalize output and outcome metrics					FY 2009		X	X	O		X
Begin collecting output and outcome metrics					FY 2009		X	X	O		X
Develop Communications Sector online or automated metrics tool			+			X	X				
Develop Communications CI/KR Sector Annual Report			+			O	X	O	O		O

Activity	Milestone					Security Partner					
	Ongoing	90 Days After SSP Approval	180 Days	365 Days	Specific Date	DHS	SSA	Other Federal Agency	State or Territory	Local and Tribal	Private Sector
Communications SSP 7. CI/KR Protection Research and Development											
Coordinate requirements collection with the NCO/NITRD and the NSTC CIIP-IWG annually				+		O	X	O			O
Set cyber/logical-related R&D requirements				+		X	X				O
Work with the DHS Science and Technology Directorate partners to review Federal R&D initiatives with the potential to meet telecommunication CI/KR protection challenges				+		X	X				
Solicit gap analysis of communications R&D needs and current initiatives and write a report summarizing and prioritizing the most important gaps in the sector				+		X	X				
Solicit candidate R&D initiatives to identify which could fill the sector's technology gaps and produce a report summarizing these initiatives and identifying remaining gaps				+		X	X				O
Conduct R&D Exchange Workshop to stimulate and facilitate dialog among industry, government, academia, and international partners on emerging security technology R&D activities	+						X				X
Publish the results of the R&D Exchange Workshop in a proceedings document	+						X				X
Coordinate with the IT Sector on overlapping R&D critical infrastructure protection priorities	+					X	X	X	O	O	X
Communications SSP 8. Manage and Coordinate SSA Responsibilities											
Conduct an annual review of the CSSP and on a tri-ennial basis conduct a complete review of the CSSP in conjunction with the update of the NIPP Base Plan. In addition, revisit the CSSP after any incident that has a major impact on the sector				+		X	X	X	X	O	X
Coordinate closely with the IT Sector on the development of the next version of the CSSP					FY 2009	X	X	X	X	O	X

Legend
X = Primary responsibility
+ = Milestone indicator
O = Support responsibility
FY = Fiscal Year

6.3 Challenges and Continuous Improvement

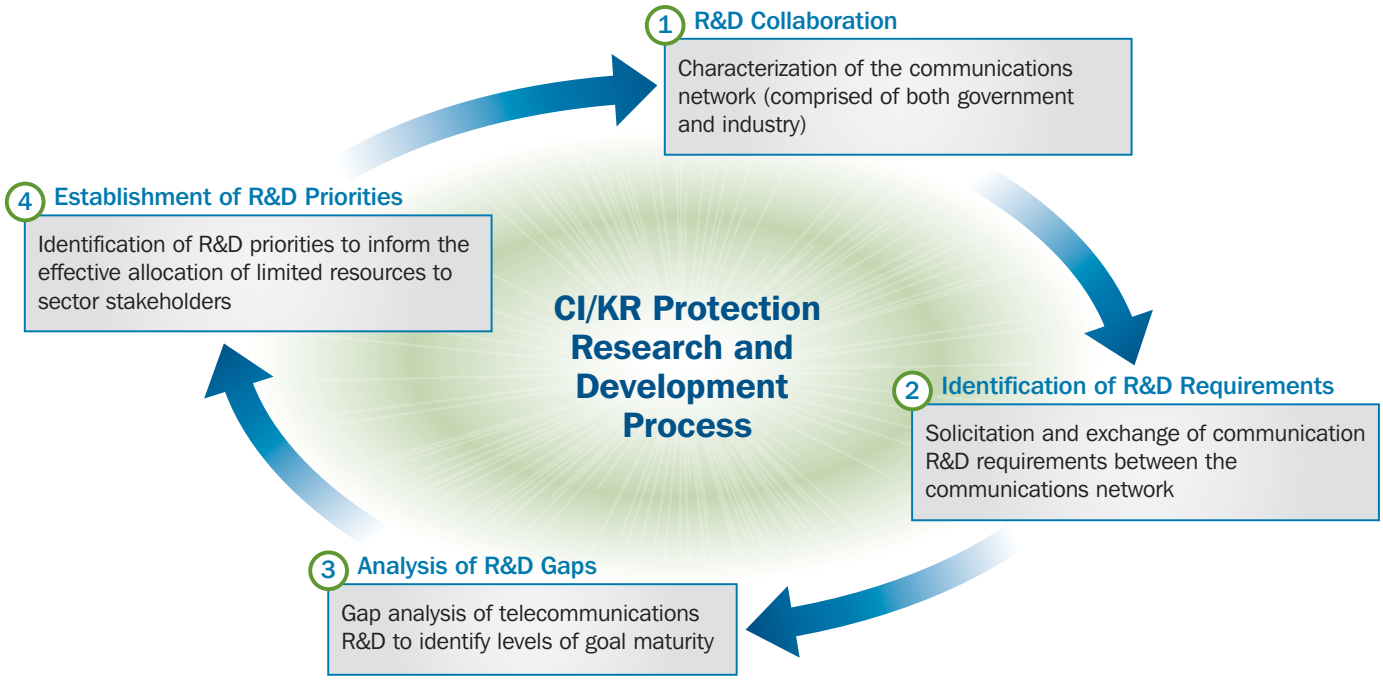
As figure 6-1 demonstrates, the Communications Sector will use a time-phased approach to performance measurement, using descriptive, process, and outcome measures as sector measurement activities mature to examine sector performance in mitigating CI/KR risk. Throughout the measurement process, feedback mechanisms will help update and amend the framework, as needed, to accommodate sector change and maturity. Feedback between initial descriptive measures and sector protection initiatives and programs will help guide protection implementation activities. Process metrics will help reexamine sector policies and procedures. Outcome measures will measure sector goal attainment.

The measurement process is an important part of the overall risk management framework because it gauges industry and government partner progress and gaps in meeting sector goals and, in turn, informs resource decisions, protective program improvements, and changes to risk management processes. When gaps are identified, the NCS will review them with industry and government partners to determine useful corrective actions. Outcomes could include revising sector security goals to account for changes in the threat environment; addressing protective programs; and/or calling for a new or operationalizing an existing R&D initiative. As detailed in section 8.2.3, the NCS Customer Service Division will work with the NCS Plans and Resources Division to track and manage the aspects of the NCS budget that are related to infrastructure protection. The performance measurement process will be used to prioritize resource requests to ensure the budget is aligned towards effective programs.

7. CI/KR Protection Research and Development

Many of the new challenges facing the Communications Sector call for innovations in science and technology, making R&D initiatives essential to sector CI/KR protection. As a result, one of HSPD-7's requirements is the development of an R&D plan on CI/KR protection. This section addresses the R&D planning processes (summarized in figure 7-1) for the Communications Sector, which calls for not only hard science but also people-oriented R&D.

Figure 7-1: R&D Process



7.1 R&D Collaboration

This section characterizes the network of partners from Federal, State, local, and tribal governments and industry that collaborate to collect and develop R&D priorities for the Communications Sector. To facilitate and coordinate communications-related

R&D initiatives, the NCS participates in interagency working groups and actively seeks input from industry as well as State, local, and tribal officials.

Coordination with industry and government partners helps the NCS remain up-to-date on technology developments, enabling the incorporation of these advancements into sector activities, where appropriate.

7.1.1 Industry Coordination

Historically, public research had been the primary driver for technology innovation and development in the United States. With the onset of the digital age, private deployment of resources for R&D began to equal and exceed government investment. Recent innovations and advancements in networked information systems have brought about dynamic change, driven primarily by commercial forces. The government depends on private companies, in their role as owners, operators, and innovators, to share responsibility for increasing the resiliency of CI/KR. In today's environment, communications companies are relied on to assure physical resiliency for their critical assets, including backup power reserves and hardened facilities, as well as to control access in the physical and cyber realms. Thus, collaboration in setting an R&D agenda and identifying priorities is critical.

The NSTAC provides a direct connection to this vital industry insight. Periodically, the Industry Executive Subcommittee (IES) Research and Development Task Force of the NSTAC conducts an R&D Exchange (RDX) Workshop to stimulate and facilitate dialogue among industry, government, and academia on emerging security technology R&D activities that impact the NS/EP posture of the Nation. The results of the RDX Workshop are published in a Proceedings document, which provides important input into the Federal Government's research agenda for NS/EP communications.

The NSTAC represents a significant connection to leading industry perspectives from the communications and information technology (IT) sectors. However, the sector also will coordinate overlapping R&D critical infrastructure protection priorities with the IT Sector through the IT SCC and GCC. To add to this source of input, the NCS routinely collaborates with additional industry partners across sectors to develop and identify further R&D priorities. The Partnership for Critical Infrastructure Security (PCIS) represents another means to facilitate this collaboration. Through participation in the PCIS, the sector gains access to industry representatives from other sectors and can better ascertain cross-sector R&D priorities.

7.1.2 Interagency Coordination

On an annual basis, the NCS coordinates requirements collection with more than 20 government agencies through the Subcommittee for Networking Information Technology R&D (NITRD) of the National Science and Technology Council (NSTC), which is part of the OSTP.[14] Joint participation in interagency working groups, information exchanges, and other outreach activities accelerate sector-specific technology transition. Specifically, the NITRD agencies' collaborative efforts increase the overall effectiveness and productivity of Federal investment in networking and information technologies, leveraging strengths, avoiding duplication, and increasing interoperability of R&D investments.

The NCS and NCSD participate in the Cyber Security and Information Assurance Interagency Working Group (CSIA IWG), a component of the NSTC. Involvement in this interagency process allows the NCS to collaborate on technical planning, coordinate investments, and assess the direction of research to improve the ability of information systems to prevent, resist, respond to, or recover from actions or events that compromise or threaten to compromise the availability, integrity, or confidentiality of data, of the information systems themselves, or of related information services. The NCS also works closely with NCSD to coordinate communications and cyber R&D requirements for submission to the DHS Science and Technology (S&T) Directorate, the primary R&D arm of the DHS.

[14] The Subcommittee on NITRD also includes participants from the Department of Defense, Department of Energy, Department of Homeland Security, National Science Foundation, and National Institute for Standards and Technology, among other Federal departments and agencies.

The NCS routinely solicits information and analysis from these government agencies. NCS then summarizes this information into reports providing comprehensive insight on the communications environment. Although the NCS often leads such efforts, it relies heavily on the OSTP, NCSD, and other NITRD agencies for the specific R&D references within the reports.

7.2 Identification of R&D Requirements

In conjunction with industry and government partners across Federal, State, local, and tribal levels, the NCS determines requirements for future R&D to advance NS/EP communications. Requirements outline particular research topic areas within the Communications Sector that could benefit from technological advancements. The sector security goals, outlined in chapter 1, set the framework for the R&D requirements. However, some of the goals are focused on the development and improvement of processes (e.g., intelligence sharing and cross-sector coordination) rather than the hard sciences. To meet these goals, the sector needs to exercise response procedures repeatedly and strengthen established partnerships and networks.

The collection and development of R&D requirements is informed by the collaborative efforts described above and informed by several key documents, including the Federal Plan for CSIA R&D,[15] the National Plan for R&D in Support of Critical Infrastructure Protection,[16] and the *RDX Workshop Proceedings*. As the sector's risk assessment process matures, R&D requirements will be guided increasingly by calculations of risk.

The identification of requirements calls for a comprehensive assessment of the progress and impact of current initiatives and a forward-thinking perspective on future needs. As part of the R&D requirements process, the NCS monitors ongoing communications research investments through its industry outreach and its participation in interagency technical planning efforts. The NCS works in close coordination with NCSD to examine current and planned cyber R&D projects that have applications for the Communications Sector. The NCS also studies past gap analyses and previously published reports on Communications Sector R&D priorities to determine which identified technology gaps require further attention. After collecting these inputs and reviewing existing plans, the NCS explores areas for future technological progress in relation to sector security goals. The NCS relies on inputs from industry and interagency partners to assess the direction of future research, incorporating findings from the RDX Workshop and other advice from industry representatives into the requirements identification process. Having performed these information-gathering activities, the NCS is equipped to identify topic areas that require additional R&D. On an annual basis, the NCS formulates a list of research requirements for submission to OSTP and the DHS S&T to inform their investment decisions. Table 7-1 lists national CI/KR protection R&D themes.

[15] Interagency Working Group on Cyber Security and Information Assurance, National Science and Technology Council, *Federal Plan for Cyber Security and Information Assurance Research and Development*, April 2006.

[16] The Executive Office of the President, Office of Science and Technology Policy and Department of Homeland Security, Science and Technology Directorate, *The National Plan for Research and Development in Support of Critical Infrastructure Protection*, 2004.

Table 7-1: National CI/KR Protection R&D Themes

NCIP R&D Themes	Goal 1 Health of the Communications Backbone	Goal 2 Critical Communications Service Restoration	Goal 3 Response Plans and Exercise	Goal 4 Protocols for Network Integrity	Goal 5 Infrastructure Resiliency & Risk Mgmt. Education	Goal 6 Processes for Intel Sharing	Goal 7 Cross-Sector Coordination
Detection and Sensor Systems	✓	✓		✓	✓		
Prevention and Protection		✓	✓		✓	✓	
Entry and Protection Access Portals		✓	✓		✓		
Insider Threats					✓		
Analysis and Decision Support Sys.				✓	✓		
Response, Recovery, and Reconstitution				✓		✓	✓
New and Emerging Threats and Tech.	✓	✓			✓		
Advanced Infrastructure Architecture and Systems	✓			✓	✓		
Human and Social Issues			✓		✓	✓	✓

7.3 Analysis of Gaps

To better understand future R&D needs and priorities, an assessment of the current state of research initiatives and investments is required to ascertain gaps and shortfalls. The input received during the requirements identification process is the basis for a more comprehensive gap analysis.

The NCS reviews current Federal R&D initiatives related to communications, in light of the sector security goals and national infrastructure protection priorities. Access to data from Federal partners about ongoing research projects is critical to assess their capacity to contribute to increased sector security. The NCS reviews these individual projects and determines their relevance to the sector and then classifies them according to security goal. Furthermore, they rely on input from OSTP, the DHS S&T, NCSD, and other NITRD agencies to augment their understanding of current communications R&D priorities. Formal and informal interactions with communications companies give the NCS trusted insight and valuable information on the R&D

activities and expenditures in the private sector. In addition, the planning documents listed above and other publications, such as the Information Security Research Council's Hard Problems List,[17] enhance the NCS's understanding of the current state of communications R&D.

Based on this study, the NCS is able to assign a maturity level (immature, mature, very mature) to each current R&D priority, describing the relative maturity of research initiatives addressing a particular priority, as follows:

- **Immature:** Few research initiatives; projects are in early developmental stages;
- **Mature:** Many research initiatives; project fully developed, testing/trials with modification as necessary; and
- **Very Mature:** Numerous research initiatives; projects fully developed; project deployment or pilot programs well advanced with assessments, analysis, and review.

Table 7-2 illustrates a maturity chart. An informal analysis was limited to R&D initiatives funded by the government and excluded projects and expenditures by industry and academia.

Table 7-2: Illustrative Maturity Chart

Goal	Communications R&D Priority Areas	Immature	Mature	Very Mature
Communication Backbone	Identity Management	■	■	
	Insider Threat	■	■	
	Interoperability Testing	■	■	
	Ipv6 Transition	■		
	Network Forensics	■		
	Protocol Security-BGP and DNS	■	■	
	Secure Network Element Technology	■		
	Threat Definition and Analysis	■	■	■
Communication Restoration	Next Generation Priority Services	■		
	Situational Awareness	■	■	■

[17] INFOSEC Research Council (IRC). Hard Problems List, November 2005.

Comparing the maturity of current priorities with R&D requirements, discussed in the previous section, gives the NCS a basic understanding of gaps and shortfalls. The NCS solicits input from industry regarding findings from its gap analysis. Based on these inputs, the NCS develops a report summarizing the maturity of current R&D priorities and identifying technology gaps that must be addressed through the requirements identification process in the future to help achieve sector security goals. Although the NCS leads this gap analysis effort on behalf of the sector, input from interagency and industry partners is critical to the accuracy of its findings.

7.4 Establishment of R&D Priorities

Following the completion of the gap analysis, the NCS solicits information on proposed R&D initiatives from all partners to determine whether these initiatives could fill the identified technology gaps. The NCS collaborates with the NSTAC's RDTF and the CSCC, among other partners, on its analysis of relevant findings and candidate R&D initiatives. Those research areas associated with high-risk communications infrastructure and identified technology gaps will be given the highest priority (e.g., immature + high risk = high priority). The NCS produces a separate report describing R&D priorities, which refers to the gap analysis and discusses potential mission impact if gaps are left unfilled. In combination with the gap analysis, this report on R&D priorities informs the requirements identification process for the following year. This cyclical approach will result in the most effective allocation of limited resources to address the identified gaps.

Table 7-3 illustrates this risk management approach. Following the establishment of sector goals (listed below) and investigation into the maturity of R&D initiatives to address these goals, partners can identify technology gaps (maturity analysis) that exist across the sector. The risks (of inaction) from the identified gaps are also listed below. From this analysis, the partners can make informed decision on future R&D investments to fill the associated gaps.

These R&D initiatives were developed or funded (e.g., National Science Foundation grants) largely by government, a majority of which are neither sponsored nor directed by the NCS. Clearly, they represent only a fraction of the expansive R&D occurring in the Communications Sector; however, they symbolize some of the cutting-edge development in the sector by government. Forthcoming analysis will incorporate input from industry more effectively.

Table 7-3: Risk Management Approach

Goal Components	Risks of Inaction	Goal Priorities	Selected Examples of R&D Initiatives
Overall Health of the Communications Backbone	• Unauthorized access to critical communication infrastructure/assets • High risk cyber assets (i.e., wireless modes) • Uncoordinated and un-standardized response and recovery efforts • Communication congestion; unmanageable amounts of information to sensor and detect • Slow and inaccurate recognition/interpretation of intrusion alerts (i.e., false/nuisance alarms) • Increasingly sophisticated (internal and external) intruders • Limited availability of portal systems to infer actions/intent to control/direct outcomes in varied security situations • Insider degradation of systems and services	• Identity Management • Insider Threat • Interoperability Testing • IPv6 Transition • Network Forensics • Protocol Security • Secure Network Technology • Threat Def. Analysis	• Development of digital fingerprint authentication tool • Evaluation/development of automatic remote identification system • Development of scalable threat warning and tactical collection systems • Creation of web-based architecture allowing a single workstation to access multiple security networks • Development of automated methods to assess hostile user intent in a cyber security domain • Creation of large-scale end-to-end wireless testbed for mobile voice and data communications • Piloting the use of biometric smart cards into a multi-agency Public Key Infrastructure system • Prototyping cross-layer communication to accommodate a dynamic environment

Goal Components	Risks of Inaction	Goal Priorities	Selected Examples of R&D Initiatives
Rapid Reconstitution of Critical Communications Services	• Limited infrastructure capacity • Inability to sustain optimal detection capabilities under varied/changing conditions • Lack of public confidence due to sector inabilities • Evolving requirements of networks and stakeholders • Delays in efficient and quick restoration/ replacement of damaged CI networks • Inability to detect and tract people during and following an incident	• Next Generation Priority Services • Situational Awareness	• Development of integrated tracking and monitoring capability enabling real-time protection of CI • Improve network intrusion defense to lessen response time, provide automatic capabilities and improve collaboration • Development of framework allowing vertical and horizontal info. sharing to reduce time-required for event based decision-making • Improvement upon mobile ad-hoc networks to provide interconnection w/o stationary infrastructure • Creation of tech-enabled security with goal of monitoring, preventing, and recovering from disaster
Plan for Emergency and Crises	• Communications service discontinuity or service interruption • Uncoordinated response or decision-making and potential overlap	• Mitigation and Recovery Methodologies	• Focused on the development and improvement of processes rather than specific R&D initiatives
Protocols for Network Integrity	• System failure or breakdown during emergency due to an inability to handle the exponential surge in calls • Federal, State, and local governments unaware of respective eligibility and capability requirements	• International coordination for exponential call surge during emergencies	• Development of wireless systems adaptable to changes in connectiviity and bandwidth • Exploration into and establishment of regional priority services (process)
Stakeholders Awareness of Communication Infrastructure Resiliency	• Uneducated stakeholders on the status of communications infrastructure • Failure to understand the functions and potential points of breakdown in the national comm. network • Unavailability of real-time effective monitoring of CI at all response levels • Lacking auto-response and self-healing systems	• Infrastructure Resiliency Assessments • Risk Management Practices	• Delivery of cyber security assessment methodology • Develop software for CI interdependency modeling • Fielding of early warning systems • Investigation of explosives and their effects on CI • Development of threat assessments to better understand impact of CI failures • Investigation on the cultural aspects of info sharing
Processes for Intelligence Sharing	• Inability of the Intelligence Community to utilize sector expertise due to inadequate or untimely communications (and vice-versa) • Inability to immediately recognize points of contact during an emergency	• Timely, relevant, accurate threat reporting from and to Intel Community	• Focused on the development and improvement of processes rather than specific R&D initiatives
Cross-sector Coordination	• Lack of knowledge and understanding of interdependencies • Unnecessary duplication of service/product • Dynamic movements of massive amounts of information	• Collaborative Testbeds • CI Dependencies and Interdependencies • Metrics, Benchmarks, Best Practices	• Development of networked collaborative environment capable of monitoring, detection, protection, and remediation of threats to CI ops • Demonstration of scalable, rapid, secure integrated capability to retrieve, store and share massive amounts of info among global users in real-time • Creation of an integrated security service for dynamic management (multiple domains and interests) • Development of a model of infrastructure transactions on communication infrastructure • Development of interdependency modeling for the susceptibility of high reliability requirements

Appendix 7 provides details of select R&D initiatives. Table 7-4 lists chapter 7 roles and responsibilities.

Responsible Entity	Activity
NCS	Coordinate requirements collection with the NCO/NITRD and NSTC CIIP-IWG annually.
NCS NCSD	Set cyber-related R&D requirements.
NCS	Work with the DHS Science and Technology Directorate partners to review Federal R&D initiatives with the potential to meet telecommunication CI/KR protection challenges.
NCS	Solicit gap analysis of communications R&D needs and current initiatives and write a report summarizing and prioritizing the most important gaps in the sector
NCS	Solicit candidate R&D initiatives to identify which could fill the sector's technology gaps and produce a report summarizing these initiatives and identifying remaining gaps.
NSTAC	Conduct RDX Workshop to stimulate and facilitate dialog among industry, government, and academia on emerging security technology R&D activities.
NSTAC	Publish the results of the R&D Exchange workshop in a proceedings document.
NCS CSCC CGCC	Coordinate with the IT Sector on overlapping R&D critical infrastructure protection priorities.

7.4.1 Modeling and Simulation Requirements

Modeling and simulation is an especially important requirement in the CI/KR protection process because it assists in identifying weaknesses in the infrastructure, analyzing potential impacts of threat scenarios, and assessing cross-sector interdependencies. The NCS has the NDAC, which includes a collection of asset databases and analytical capabilities used to identify, analyze, and help mitigate threats and vulnerabilities to the U.S. communications infrastructure. The NCS has invested many years establishing strong working relationships with commercial carriers and government departments and agencies, and developing PSTN modeling methodologies, tool sets, and unique databases that include proprietary data from the major carriers. The NDAC serves as a tool to conduct studies that cover multiple communications areas such as wireline, wireless, and the Internet.

One of the main challenges in performing modeling and simulation of the communications infrastructure is the availability of complete data sets. The NCS continues to work with industry partners to provide more complete data; however, companies are generally unwilling to release detailed infrastructure information because of its proprietary nature. In addition, industry partners have concerns that their data can be misinterpreted easily due to the complexity of the networks and routing protocols. Because of the proprietary nature of the information compiled in the NDAC, its asset databases cannot be shared for other modeling and simulation activities.

8. Manage and Coordinate SSA Responsibilities

This chapter presents an overview of the processes established by the NCS to support its responsibilities as SSA. Specifically, this section discusses the NCS program management approach, implementation of the sector partnership model, and information-sharing mechanisms. The NCS will manage and coordinate the processes of the SSP, which include SSP maintenance, resources and budgets, and training and education. While all SSA responsibilities will be managed through the NCS, most activities will involve extensive industry and government partner collaboration.

8.1 Program Management Approach

The NCS approach to managing risk and associated CI/KR protection efforts within the sector requires the NCS to support and strengthen industry and government partnerships continually and to ensure that resiliency and redundancy are built into the Nation's communications infrastructure. The existing structure of the NCS supports its current mission to "Assist the President, the National Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget in (1) the exercise of the communications functions and responsibilities, and (2) the coordination of the planning for and provision of [NS/EP] communications for the Federal Government under all circumstances, including crisis or emergency, attack and recovery and reconstitution." To date, this mission has been met through establishing and maintaining robust industry partnerships and programs. Because the NCS mission already is aligned with its infrastructure protection and NS/EP communications responsibilities, and its preferred approach for executing those responsibilities, it is most appropriate for the NCS to assimilate its NIPP-related responsibilities into its existing structure.

The NCS will manage its responsibilities as the Communications SSA primarily through the NCS Customer Service Division, although specific responsibilities may be allocated to other offices within the NCS as appropriate. The NCS Customer Service Division will manage most of the key processes and partnerships associated with the implementation of the NIPP Framework. This effort will allow the NCS to ensure that the NIPP-related responsibilities always are conducted by the most appropriate entity and will allow it to leverage continually the existing institutionalized relationships with industry. In addition, the NCS will maintain an active dialogue with the CGCC and CSCC to monitor the execution of these responsibilities. Table 8-1 identifies primary task responsibilities for specific divisions of the NCS.

Table 8-1: Program Management Responsibilities

Task	Responsible NCS Division(s)
Infrastructure Identification	NCS Technology and Programs Division
Risk Assessments	NCS Critical Infrastructure Protection Division
Protective Program Development	NCS Technology and Programs Division
Protective Program Maintenance	NCS Technology and Programs Division
Training and Education	NCS Critical Infrastructure Protection Division
Partnerships	NCS Customer Service Division
SSP Maintenance and Updates	NCS Customer Service Division
Resources and Budget	NCS Plans and Resources Division

8.2 Processes and Responsibilities

8.2.1 SSP Maintenance and Update

The NCS Customer Service Division, in its role as overall manager of NCS SSA-related responsibilities, is responsible for maintaining the SSP. The SSP will be reviewed annually to ensure that it reflects current sector processes, as well as the continuously evolving nature of the risk environment. This annual review will occur as part of the sector's annual reporting process. As the NCS works with its security partners to produce this annual report, it will also work with them to identify any changes in process or sector characteristics that may have occurred over the preceding year. During this annual review, the SSP will be updated as appropriate. On a triennial basis, a complete review of the SSP will be conducted in conjunction with the update of the NIPP Base Plan. The plan also will be reviewed after any incident or exercise event that has a major impact on the sector. In addition, the Communications Sector will coordinate closely with the IT Sector to develop the next version of the CSSP.

In addition to conducting these periodic reviews, the NCS Customer Service Division will be responsible for identifying any changes in processes associated with the NIPP Framework or in the characteristics of the sector. In the case of a major change to an element of the SSP, a decision may be made to update the SSP outside the normal annual review cycle. In all cases, revisions to the SSP will be coordinated with sector security partners and will be reviewed by the CGCC and CSCC.

8.2.2 Annual Reporting

As directed in HSPD-7, and further described in the NIPP Base Plan, CI/KR Sector Annual Reports are produced by each sector annually to identify, prioritize, and coordinate CI/KR protection progress and requirements in their respective sectors. This report is submitted to the DHS and describes the sector's CI/KR protection goals, priorities, programs, and related funding requirements, as well as a catalogue of progress that has been made in sector CI/KR protection.

The production of the Communications CI/KR Sector Annual Report will be managed by the NCS Customer Service division but will involve input from all security partners in the Communications Sector. The process used to gather input from security partners is the same used to produce the SSP. When appropriate, the CGCC and CSCC will meet to provide input to the annual report and to ensure that the report's data accurately reflects CI/KR protection activities sector-wide. In addition, CGCC and CSCC members will review the annual report before it is submitted to the DHS to ensure that all relevant data are included. Other security partners will also contribute to the production of the annual report, including State and local entities.

8.2.3 Resources and Budgets

Given the highly distributed, diverse, interdependent nature of the Communications Sector, and the sector's overall approach to CI/KR protection, a risk management approach is the most appropriate method for decisions regarding the allocation of limited security resources. To align resource decisions with the overall approach to conducting CI/KR protection activities, the NCS Customer Service Division will work with the Plans and Resources Division to track and manage the aspects of the NCS budget that are related to infrastructure protection. Because the SSA's CI/KR protection resources are distributed across the NCS, all divisions will support this process, and the NCS Plans and Resources Division will work with appropriate entities within the agency to apply resources based on a risk management approach.

As described in chapters 4 and 5, the NCS will work with industry and government security partners to identify those initiatives and programs to which funding should be directed. These decisions will be based on the results of risk assessments and on an assessment of how certain protective programs will reduce overall risk. Included in this assessment will be the results of the prioritization process described in chapter 4 and of program performance evaluations (for new and existing programs) described in chapter 5. These efforts will be coordinated between various divisions within NCS, depending on the stage of this process and the program involved.

Once investment priorities have been identified, actions must be taken to ensure that these decisions are reflected in the annual NCS budget. The NCS Customer Service Division will work with the Plans and Resources Division, along with individual program managers, to identify those aspects of the agency budget that are related to sector CI/KR protection efforts, and to ensure that sector priorities are effectively being addressed. Information about how resources are being directed to meet the Communications Sector's CI/KR protection priorities, and about the risk-reduction programs these resources support, will be relayed to the DHS in the sector annual report.

8.2.4 Training and Education

The NCS recognizes the need for training and education in all areas of the NIPP Framework. A large portion of this training is targeted to NCS staff members, who are responsible for implementing the processes outlined in the SSP. This includes specialized training on risk management methodologies, related to physical and cyber security risk assessments, for those responsible for this task, or in cost-benefit analysis, for those responsible for ensuring that limited resources are effectively applied. Often, this training is available through traditional employee training, although as the SSP is implemented, there will be a need for expertise in areas where it does not exist. As this need arises, NCS will seek appropriate avenues for providing this training to ensure that all necessary capabilities are adequately developed.

In addition to individual employee training and education, education for providers and users of NS/EP communications is a critical factor in the success of the implementation of this SSP. As such, the NCS facilitates and participates in various programs that are aimed at building awareness or educating a greater community about the problem of critical infrastructure assurance and the availability of NCS programs and activities. For example, the Route Diversity Forum periodically helps educate NCS member departments and agencies about improving communications resiliency. The NCS will build on this effort or initiate new ones to ensure proper scope and reach. Overall, a key first step in implementing a successful protection strategy is elevating national awareness. Toward that end, the NCS will intensify its efforts to market, conduct outreach, and develop industry and government partnerships, which have proved vital for protecting the communications infrastructures. The NCS will continue to develop a strategic program for marketing the NCS and its products and services to its Federal customers, the broader NS/EP community at the State, local, and tribal levels, and the private sector.

The NCS also will work with other sectors to improve their communications resiliency. To reach out to the broadcast industry, NCS will work through the FCC, trade associations, and the FCC's MSRC, which is developing best practices to ensure optimal reliability, robustness, and security of broadcast facilities. The NCS also is reaching out to other sectors with which it shares interdependencies and is assisting them in reviewing how their plans address communications interdependencies.

8.3 Implementing the Sector Partnership Model

8.3.1 Coordinating Structures

The NCS, as the SSA for the Communications Sector, is responsible for coordinating the development and implementation of the sector's GCC and SCC. This subsection describes the CI/KR protection-related coordinating structures and mechanisms used within the Communications Sector. It also highlights the role of State and local entities in sector operations and the potential interconnectedness of U.S. CI/KR with foreign countries.

NIPP Coordination Councils

Communications Government Coordinating Council. The CGCC helps coordinate the implementation of the NIPP and the corresponding Communications SSP across government and between government and the Communications Sector. Membership in the CGCC includes the DHS (NCS and NCSD), Department of Commerce, DOD (Office of the Secretary of Defense/Networks and Information Integration), FCC, GSA, NTIA, Department of Justice, and NARUC. The NCS is the chair of the CGCC.

Communications Sector Coordinating Council. The CSCC, an industry-only body with more than 25 communications companies and trade associations, assists in implementing the SSP and provides input on critical infrastructure protection and sector-related policies and programs. The CSCC is not operational, but focuses on input to critical infrastructure protection policies and plans. As such, it will not take on all responsibilities that NIPP designates to SCCs. The NCC will continue to coordinate operational issues.

State, Local, and Tribal Government Entities. Through the CIPAC process, NCS can facilitate improved coordination among State, local, and tribal authorities and the communications industry on CI/KR protection initiatives. The NCS will develop a process to facilitate coordination among State and local authorities and the communications industry on CI/KR protection initiatives, including collecting critical sector asset listings and vulnerability or impact assessments. Through NARUC, the NCS will work to build on outreach to States on key issues (e.g., pandemic preparedness, access, and credentialing) and provide POCs to the NARUC/FCC communications assurance emergency POC network.

Coordinating these groups on collection of critical asset listings and vulnerability/impact assessments, among other initiatives, will help improve assessments, protection of critical infrastructure information, and reduce the burden on industry by minimizing the duplication of efforts.

International

The NCS participates in international organizations and bilateral discussions with other countries regarding the NCS model for Communications Sector coordination and infrastructure protection. These partnerships are described below.

U.S./Canada Civil Emergency Planning Telecommunications Advisory Group. CEPTAG was established in 1988 to provide a forum for addressing concerns and enabling cross-border cooperation and mutual assistance during an emergency. Among other tasks, the group maintains an active dialogue on CI/KR protection issues, identifies and studies cross-border CI/KR protection requirements such as priority service and emergency preference schemes, and evaluates the capability of existing and planned facilities to meet the planning, mitigation, and response requirements associated with CI/KR protection.

Security and Prosperity Partnership. The SPP, launched in June 2005, builds on existing relationships among the United States, Canada, and Mexico, by providing a framework to advance collaboration. The SPP created architecture to enhance further the security of North America while simultaneously promoting its citizens' economic well-being.

The three governments have established numerous goals and initiatives, with corresponding deadlines, as well as various working groups to address cross-border issues.

The NATO Civil Communications Planning Committee. The NATO CCPC is responsible for ensuring the continued availability of civil communications during crises and war, for civil and military purposes. The CCPC provides for the maintenance of communication services for political, economic, and military purposes, including communications and postal facilities/services. The Committee creates work programs based on comprehensive political and ministerial guidance and works to advance the civil emergency planning and response capabilities of the alliance.

U.S./U.K. Joint Contact Group. Initiatives of the U.S./U.K. NS/EP communications relationship are pursued primarily through the JCG. The NCS leads the Communications Sector work, and its primary partner is the U.K.'s Central Sponsor for Information Assurance (CSIA). The principal NCS/CSIA task being conducted under the auspices of the JCG is the development of government-to-government priority routing capability for emergency communications. The goal of the initiative is to address requirements for secure and resilient communications at times of crisis, emergency, or other disruptive challenges.

International Telecommunication Union. The NCS represents U.S. government interests at the ITU. The ITU, under the auspices of the United Nations, has 189 member States and more than 650 industry sector members. The ITU serves as the world's principal communications standards organization and explores topics such as NGNs and international emergency preference schemes.

8.4 Information Sharing and Protection

8.4.1 Information-Sharing Mechanisms

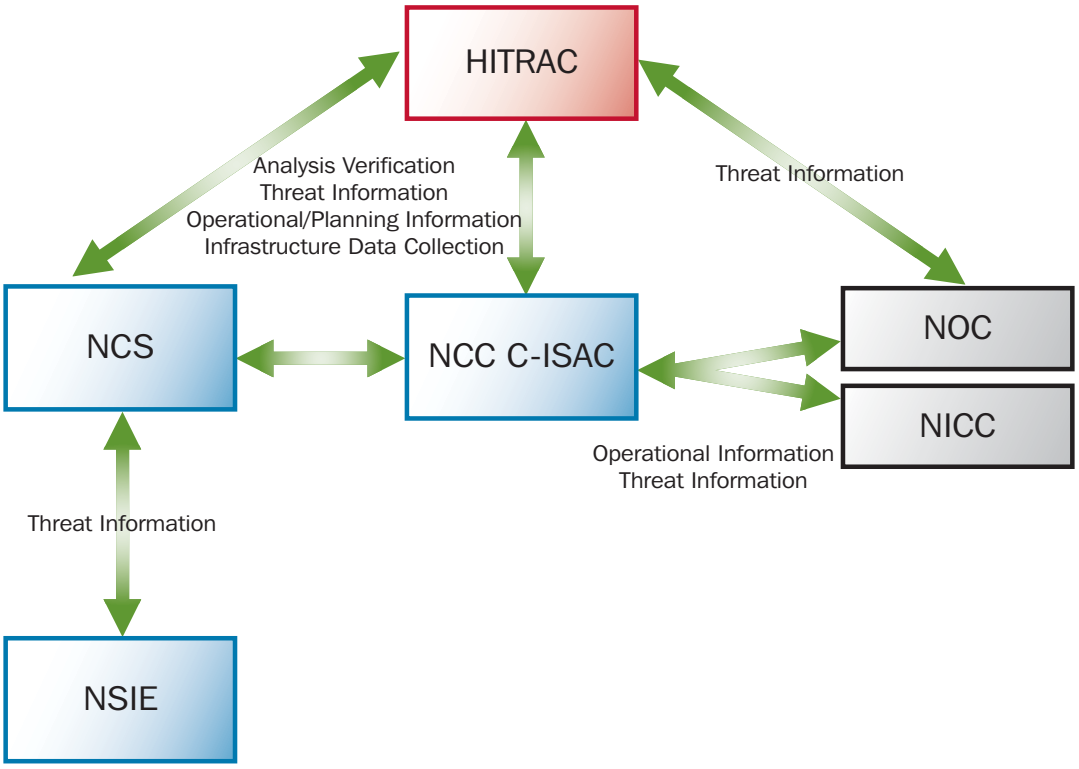
The effective implementation of the NIPP is predicated on active participation by industry and government security partners in robust multidirectional information sharing. When owners and operators are provided with a comprehensive picture of threats or hazards to CI/KR and participate in ongoing multidirectional information flow, their ability to assess risks, make prudent security investments, and take protective actions is enhanced substantially. Similarly, when the government is equipped with an understanding of industry information needs, it can adjust its information collection, analysis, synthesis, and dissemination activities accordingly.

The NIPP information-sharing approach constitutes a shift from a strictly hierarchical to a networked model, allowing distribution and access to information both vertically and horizontally, as well as the ability to enable decentralized decisionmaking and actions. The information-sharing process is designed to communicate both actionable information on threats and incidents and information pertaining to overall CI/KR status (e.g., plausible threats, vulnerabilities, potential consequences, incident situ-

ation, and recovery progress) so that owners and operators, States, localities, tribal governments, and other security partners can assess risks, make appropriate security investments, and take effective and efficient protective actions. Information sharing in the Communications Sector occurs largely through established channels among the NCS, including NCC C-ISAC, HITRAC, NOC, and National Infrastructure Coordinating Center (NICC). Figure 8-1 illustrates the relationships and information flow among these entities.

- **NCS/NCC C-ISAC:** The NCC assists the NCS in the initiation, coordination, restoration, and reconstitution of NS/EP communications services or facilities under all conditions of crisis or emergency. The NCC regularly monitors the status of communications systems. It collects situational and operational information on a regular basis, as well as during a crisis, and provides information to the NCS. The NCS, in turn, shares information with the White House and other DHS components. ISACs provide an example of an effective private sector information-sharing and analysis mechanism. ISACs are sector-specific entities that advance physical and cyber CI/KR protection efforts by establishing and maintaining frameworks for operational interaction between and among members and external security partners.
- **NSIEs:** Industry and government NSIE representatives meet bimonthly to share information about incidents they are seeing in their organizations, such as viruses, vulnerabilities, hacker incidents, insider incidents, or fraud, and discuss solutions. In addition, they periodically conduct "Birds of a Feather" exercises that include discussions on security technologies, policy issues, and response activities related to the specific subject being addressed.
- **HITRAC:** HITRAC is responsible for integrating CI/KR specific vulnerability and consequence data with threat information to produce actionable risk assessments used to inform CI/KR risk-mitigation activities at all levels. HITRAC analysts work closely with CI/KR sector SMEs to ensure that these products address the individual requirements of each sector and help actuate corresponding security activities. HITRAC analyzes and integrates threat information and works closely with components of the Federal Infrastructure Node (i.e., the DHS, SSAs, and other Federal departments and agencies that gather and receive threat, incident, and other operational information to generate and disseminate threat warning products to security partners).
- **NOC:** The NOC, formerly known as the Homeland Security Operations Center, serves as the Nation's hub for domestic incident management operational coordination and situational awareness. The NOC is a standing 24/7 interagency organization fusing law enforcement, national intelligence, emergency response, and private sector reporting. The NOC facilitates homeland security information sharing and operational coordination among Federal, State, local, tribal, and private sector partners, as well as select members of the international community. As such, it is at the center of the NIPP information-sharing network.
- **NICC:** The NICC is a 24/7 watch/operations center that maintains ongoing operational and situational awareness of the Nation's CI/KR sectors. As a CI/KR-focused element of the NOC, the NICC provides a centralized mechanism and process for information sharing and coordination between the government, SCCs, GCCs, and other industry partners. The NICC receives situational, operational, and incident information from the CI/KR sectors, in accordance with information-sharing protocols established in the NRP. The Homeland Security Information Network (HSIN) is the NICC's primary system used for disseminating information to the CI/KR sectors. The NICC also disseminates products originated by HITRAC that contain all-hazards warning, threat, and CI/KR protection information.

Figure 8-1: Communications Sector Information Flow



The NIPP supports the broad concept of a multidirectional networked information-sharing approach. This information-sharing network consists of components that are connected by a national Web-based communications platform, known as the HSIN-Critical Sectors (HSIN-CS), so that security partners can obtain, analyze, and share information. When fully deployed, the HSIN-CS will constitute a robust and significant information-sharing system that supports NIPP-related steady-state CI/KR protection and NRP-related incident management activities, as well as serving the information-sharing processes that form the bridge between these two homeland security missions. HSIN-CS is used for two-way and multidirectional information sharing among the DHS; the Federal Intelligence Community; Federal departments and agencies; State, local, and tribal jurisdictions; and the private sector. The connectivity of the network also allows these partners to share information and coordinate among themselves (e.g., intrasector coordination). The Communications Sector is in the process of working with OIP on the development of the HSIN-CS Communications Sector Portal.

In addition to sharing information through already established channels, Communications Sector industry and government partners regularly work together on ad hoc projects and protective programs, offering further opportunities for successful information sharing. Specific programs in place that address Internet security and communications and IT cross-sector issues are US- CERT, IDWG, NCRCG, and NetGuard. These information-sharing mechanisms are described in section 5.2.

8.4.2 Data Protection Mechanisms

Wherever possible, information shared among any entities will be protected through appropriate mechanisms. In cases in which information is shared among government entities, data will carry appropriate classification markings and will be handled accordingly. In cases in which data are exchanged between industry and government, it will receive similar protections where possible (e.g., "commercial proprietary" markings or contractor NDAs). Once the NCS becomes an authorized PCII Program Manager designee, information provided to the NCS will be covered by the PCII Program. This serves as another avenue for information protection available to industry partners. Table 8-2 lists chapter 8 roles and responsibilities.

Table 8-2: Chapter 8 Roles and Responsibilities

Responsible Entity	Activity
NCS CSCC CGCC	Conduct an annual review of the CSSP and triennially conduct a complete review of the CSSP in conjunction with the update of the NIPP Base Plan. In addition, revisit the CSSP after any incident that has a major impact on the sector.
NCS	Coordinate closely with the IT Sector on the development of the next version of the CSSP.

Appendix 1: List of Acronyms and Abbreviations

APCO	Association of Public-Safety Communications Officials
APEC	Asia-Pacific Economic Cooperation
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
BSC	Base Switching Controller
BSS	Broadcast Satellite Service
CATV	Cable Television
CCPC	Civil Communications Planning Committee
CEPTAG	U.S./Canada Civil Emergency Planning Telecommunications Advisory Group
CGCC	Communications Government Coordinating Council
CI	Critical Infrastructure
CII	Critical Infrastructure Information
CIPAC	Critical Infrastructure Partnership Advisory Council
C-ISAC	Communications Information Sharing and Analysis Center
CI/KR	Critical Infrastructure and Key Resources
CLEC	Competitive Local Exchange Carrier
CMRS	Commercial Mobile Radio Service
COG	Continuity of Government
COOP	Continuity of Operations
COP	Committee of Principals
COR	Council of Representatives
CSCC	Communications Sector Coordinating Council
CSIA IWG	Cyber Security and Information Assurance Interagency Working Group
CSSP	Communications Sector-Specific Plan
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DPAS	Defense Priorities and Allocations System
DSL	Digital Subscriber Line
E-911	Enhanced 911
EAS	Emergency Alert System
EMF	Event Management Framework
E.O.	Executive Order
EOC	Emergency Operations Center
EOP	Executive Office of the President
EOT	Emergency Operations Team
ERT	Emergency Response Training
ESF	Emergency Support Function
FACS	First Aid for Computer Systems
FCC	Federal Communications Commission
FSS	Fixed Satellite Service
FY	Fiscal Year
GCC	Government Coordinating Council

GEO	Geostationary Earth Orbit
GETS	Government Emergency Telecommunications Service
HF	High Frequency
HFC	Hybrid Fiber Cable
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSC	Homeland Security Council
HSIN-CS	Homeland Security Information Network-Critical Sectors
HSPD	Homeland Security Presidential Directive
IACP	International Association of Chiefs of Police
IAEM	International Association of Emergency Managers
IAFC	International Association of Fire Chiefs
IDWG	Internet Disruption Working Group
IES	Industry Executive Subcommittee
IMA	Individual Mobility Augmentee Program
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
IXC	Inter-exchange Carrier
JCG	Joint Contact Group
JTRB	Joint Telecommunications Resources Board
LATA	Local Access Transport Areas
LEC	Local Exchange Carrier
LEO	Low Earth Orbit
LERG	Local Exchange Routing Guide
MAO	Maximum Allowable Outage
MCS	Mobile Switching Center
MEO	Middle Earth Orbit
MG	Media Gateway
MGC	Media Gateway Controller
MSC	Mobile Switching Center
MSRC	Media Security and Reliability Council
MSS	Mobile Satellite Service
MVPD	Multichannel Video Programming Distribution
NADB	National Asset Database
NAICS	North American Industry Classification System
NARUC	National Association of Regulatory Utility Commissioners
NASNA	National Association of State 9-1-1 Administrators
NATO	North Atlantic Treaty Organization
NCC	National Coordinating Center
NCRCG	National Cyber Response Coordination Group
NCS	National Communications System
NCSD	National Cyber Security Division
NDA	Nondisclosure Agreement
NDAC	Network Design and Analysis Capability
NDER	National Defense Executive Reserve
NEMA	National Emergency Management Association
NENA	National Emergency Number Association
NGN	Next Generation Network
NGPS	Next Generation Priority Service
NIAC	National Infrastructure Advisory Council
NICC	National Infrastructure Coordination Center
NIPP	National Infrastructure Protection Plan
NISAC	National Infrastructure Simulation and Analysis Center
NITRD	Networking Information Technology R&D
NOC	National Operations Center
NRIC	Network Reliability and Interoperability Council
NRP	National Response Plan
NSC	National Security Council
NS/EP	National Security and Emergency Preparedness

NSF	National Science Foundation
NSIE	Network Security Information Exchange
NSSE	National Special Security Event
NSTAC	National Security Telecommunications Advisory Committee
NSTC	National Science and Technology Council
NTIA	National Telecommunications and Information Administration
OAS	Organization of American States
OIP	Office of Infrastructure Protection
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
PBX	Private Branch Exchange
PCII	Protected Critical Infrastructure Information Program
PCIS	Partnership for Critical Infrastructure Security
PDD	Presidential Decision Directive
POC	Point of Contact
POP	Point of Presence
PSTN	Public Switched Telephone Network
PUC	Public Utilities Commission
R&D	Research and Development
RDM	Route Diversity Methodology
RDT&E	Research, Development, Test, and Evaluation
RDX	R&D Exchange
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SG	Signaling Gateway
SHARES	Shared Resources
SIC	Standard Industrial Classification
SME	Subject Matter Expert
SONET	Synchronous Optical Network
SPP	Security and Prosperity Partnership of North America
SRAS	Special Routing Arrangement Service
SS7	Signaling System 7
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
S&T	Science and Technology Directorate
STP	Signal Transfer Point
TIA	Telecommunications Industry Association
TSP	Telecommunications Service Priority
TT&C	Telemetry, Tracking, and Command
UN	United Nations
US-CERT	United States Computer Emergency Readiness Team
VoIP	Voice Over Internet Protocol
VSAT	Very Small Aperture Terminal
WHCA	White House Communications Agency
WPS	Wireless Priority Service

Appendix 2: Glossary of Key Terms

Asset. Contracts, facilities, property, electronic, and nonelectronic records and documents, unobligated or unexpended balances of appropriations, and other funds or resources.

Communications Architecture Elements. Assets, systems, and networks that make up the communications architecture. Following are sample categories of architecture elements.

- **Core Network/Internet Backbone:** The portion of the communications network that consists of high-capacity network elements servicing regional, nationwide, and international connectivity.
- **Signaling and Control Systems:** Systems that exchange information regarding the establishment of a connection and control the management of the network.
- **Shared Assets and Systems:** Assets and systems owned and operated by multiple companies. Includes facilities where equipment is collocated and systems are shared by network operators.
- **Access:** Primarily the local portion of the network connecting end users to the backbone that enables users to send or receive communications. Access includes equipment and systems such as Public Switched Telephone Network (PSTN) switches, asynchronous transfer mode (ATM) switches, video servers for video on demand, and Internet Protocol (IP) routers for Internet Service Providers (ISP).
- **Customer Equipment:** Equipment owned and operated by the end user or located at the end user's facility. Customers include individuals, organizations, businesses, and government.

Communications Sector. Private and public sector entities that have equities in the provisioning, use, protection, or regulation of communications networks and services. The Communications Sector is made up of four industry sectors:

- **Wireline:** Consists primarily of the PSTN but also includes enterprise networks. The PSTN is a domestic communications network accessed by telephones, key telephone systems, private branch exchange (PBX) trunks, and data arrangements. Despite the industry's transition to packet-based networks, the traditional PSTN remains the backbone of the communications infrastructure. Includes landline telephone, the Internet, and submarine cable infrastructure.
- **Wireless:** Refers to telecommunication in which electromagnetic waves (rather than some form of wire) carry the signal over part of or the entire communication path. Consists of cellular telephone, paging, personal communication services, high-frequency radio, unlicensed wireless, and other commercial and private radio services.
- **Satellite:** Is a space vehicle launched into orbit to relay audio, data, or video signals as part of a telecommunications network. Signals are transmitted to the satellite from earth station antennas, amplified, and sent back to earth for reception by other earth station antennas. Satellites are capable of linking two points, one point with many others, or multiple locations with other multiple locations. Uses a combination of

terrestrial and space components to deliver various communications, Internet data, and video services.

- **Cable:** Is a wireline network offering television, Internet, and voice services that interconnect with the PSTN through end offices. Primary CATV network components include headends and fiber optic and/or HFC. Since the CATV network was designed primarily for downstream transmission of television signals, most of the existing network is being refitted to support two-way data transmissions.
- **Broadcasting:** Is a signal transmitted to all user terminals in a service area. Refers to content carried over air waves, using these waves to distribute radio or television programs that are available for reception by the public. Much of the broadcasting infrastructure overlaps with the other subsectors of the Communications Sector, especially satellites that are widely used for transmission.

Critical Infrastructure. Assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters.[18]

Function. The service, process, capability, or operation performed by specific infrastructure assets, systems, or networks.

Information Sharing. A strategic partnering relationship between all parties involved, ideally characterized by a willingness to be open and to share forecasted strategic information. Although not all relationships are this successful, both parties involved should aim toward openness and follow a continuous improvement philosophy. This openness exists because of the high degree of trust earned through multiple successful interactions among all parties.

Interdependency. A reciprocal relationship between infrastructures that rely on each others' goods or services to remain operational.

Key Resources. As defined in the Homeland Security Act, "key resources" are publicly or privately controlled resources essential to the minimal operations of the economy and government.

Metrics. Quantifiable statements that support the performance measurement process by defining an element to be measured and indicating how that measurement will be taken. As used in regard to the document:

- **Descriptive Metrics:** Used to understand sector resources and activities; they do not reflect CI/KR protection performance.
- **Output (Process) Metrics:** Measure whether specific activities were performed as planned, track the progression of a task, or report on the output of a process (e.g., inventorying assets). Process metrics show progress toward performing the activities necessary for achieving CI/KR protection goals.
- **Outcome Metrics:** Track progress toward a strategic goal by beneficial results rather than level of activity, which indicates progress toward specific goals or objectives.

National Sector Risk Assessment. A process to collect and analyze consequences, vulnerabilities, and threats to the communications architecture to identify critical communications architecture elements at risk. The assessment is a collaborative effort with input from industry and government SMEs.

Nationally Critical Elements. Assets, networks, systems, or functions that if destroyed, disrupted, or exploited would seriously threaten national security, result in catastrophic health effects or mass casualties, weaken the economy, or damage public morale and confidence.

Owner/Operators. Those entities responsible for day-to-day operations and investment in a particular asset, system, network, or function.

Prioritization. The process of using risk assessment results to identify where risk-reduction or mitigation efforts are most needed and subsequently determine which protective action should be instituted to realize the greatest effect.

Resiliency. The ability to recover from or adjust easily to a disruption, destruction, or incapacitation. The communications infrastructure is by design resilient; however, other critical infrastructure sectors are responsible for achieving communications resiliency by having an appropriate mix of diversity, redundancy, and recoverability based on a risk-based cost-benefit assessment.

[18] As defined in the National Infrastructure Protection Plan.

- **Diversity:** Facilities should have diverse primary and backup communications capabilities that do not share common points of failure. Diversity solutions may include diverse data links (e.g., PSTN, satellite, microwave), having local loops terminate at different central offices, obtaining services from different providers with certifiable diverse routes, or using alternative transport mechanisms (e.g., wireless, satellite).
- **Redundancy:** Facilities should use multiple communications capabilities to sustain business operations and eliminate single points of failure that could disrupt primary services. Redundancy solutions include having multiple sites where a function is performed, multiple communications offices serving sites, and multiple routes between each site and the serving central offices.
- **Recoverability:** Plans and processes should be in place to restore operations quickly if an interruption or failure occurs. Recoverability of network services could include network management controls, automatic service recovery technologies, and manual transfer to alternate facility routes.

Risk. A measure of potential harm that encompasses threat, vulnerability, and consequence. In the context of the NIPP, risk is the expected magnitude of loss as a result of a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss.

- **Threat:** The intention and capability of an adversary to undertake actions that would be detrimental to CI/KR.
- **Vulnerability:** A weakness in the design, implementation, or operation of an asset, system, or network that can be exploited by a natural hazard or technological failure.
- **Consequence:** The effect of a terrorist attack or other hazard that reflects the level, duration, and nature of the loss resulting from the incident.

Risk Assessment. A study of vulnerabilities, threats, and likelihood, loss or impact (i.e., consequence), and the theoretical effectiveness of security measures. The process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations.

Risk Management Framework. A planning methodology that outlines the process for setting security goals; identifying assets, systems, networks, and functions; assessing risks; prioritizing and implementing protective programs; measuring performance; and taking corrective action. Public and private sector entities often include risk management frameworks in their business continuity plans.

Value Proposition. A statement that outlines the national and homeland security interest in protecting the Nation's CI/KR and articulates benefits gained by all security partners through the risk management framework and public-private partnership described in the NIPP.

Appendix 3: Authorities

Key authorities for the Communications Sector address the availability, resiliency, and security of the communications infrastructure and provide guidance on sector coordination and specific programs. Federal authorities requiring the private Communications Sector to conduct vulnerability assessments and implement protective measures do not exist; however, the sector continues to conduct such activities internally. This subsection gives brief summaries of the major authorities.

3.1 Broad Communications Infrastructure Protection Policies

- ***Homeland Security Presidential Directive 7 (HSPD-7) (December 2003):*** Assigns the DHS lead responsibility for coordinating the protection of national critical infrastructures, including the Communications Sector, which is considered synonymous with the private sector usage of Communications Sector. The Department has delegated to the NCS the responsibility for coordinating protection of the Communications Sector.
- ***The Homeland Security Act of 2002 (November 2002):*** Section 202 addresses the submission of CI vulnerability assessments to the DHS. Also under the act, the DHS has issued an interim rule on Procedures for Handling Critical Infrastructure Information (CII), which provides protection of such data that are voluntarily provided by the private sector.
- ***The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets (July 2002):*** Directs the DHS to work with the private sector to understand the risks associated with physical vulnerabilities of CI/KR, including the communications infrastructure.
- ***The National Strategy to Secure Cyberspace (July 2002):*** States that a top priority is to understand infrastructure interdependencies and improve the physical security of cyber systems and communications.

3.2 SSA Authorities

- ***Executive Order (E.O.) 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions (April 3, 1984):*** Establishes the NCS as the Federal interagency system for ensuring that the national telecommunications infrastructure is responsive to the NS/EP needs of the Federal Government, is capable of satisfying priority communications requirements, and is survivable under all circumstances. E.O. 12472 also establishes NCS as the focal point for joint industry-government NS/EP communications planning and directs the establishment of a national coordinating center.
- ***E.O. 12382, President's National Security Telecommunications Advisory Committee (NSTAC) (September 13, 1982):*** Establishes the NSTAC to provide top-level industry advice and expertise to the President on issues and problems related to implementing NS/EP communications policy.

- ***E.O. 12656, Assignment of Emergency Preparedness Responsibilities (November 18, 1988):*** Assigns Federal departments and agencies NS/EP responsibilities and directs them to develop plans and capabilities to ensure the continuity of essential operations.
- ***E.O. 13286, An Amendment of Executive Orders and Other Actions in Connection with the Transfer of Functions to the Secretary of Homeland Security (February 28, 2003):*** Amends several E.O.s, including E.O. 12472 and E.O. 12382, to account for the creation of the DHS.
- ***National Security Decision Directive 97, National Security Telecommunications Policy (June 13, 1983):*** Outlines coordination between the NCS, the White House's OSTP, and OMB to oversee the implementation of national security telecommunications policies. Also assigned specific responsibilities to the Manager of NCS, the NSTAC, and other Federal departments and agencies.
- ***Presidential Decision Directive (PDD) 67, (CLASSIFIED) (October 12, 1988):*** Relates to enduring constitutional government, COOP planning, and COG operations. In addition, PDD 67 requires Federal agencies to develop Continuity of Operations Plans for Essential Operations.
- ***National Homeland Security Strategy (July 2002):*** Directs the NCS to help facilitate the DHS's efforts to develop comprehensive emergency communications systems.

3.3 Coordinating Agency Authorities

- ***Federal Communications Commission (FCC):*** The Communications Act of 1934, as amended by the Telecommunications Act of 1996, is the principal statute governing Federal regulation of the Communications Sector. The Act directs the FCC to ensure that radio and wire communications effectively serve the public's interest in the safety of life and property and in the national defense. Additional FCC authorities and policies with network protection equities include the following:
  - ***E.O. 12472:*** Directs the FCC to review the policies, plans, and procedures of all entities licensed or regulated by the FCC that are developed to provide NS/EP communications services to assure they are consistent with the public interest.
  - ***Section 0.181, Title 47 of the Code of Federal Regulations:*** Sets out the duties of the FCC Defense Commissioner, including serving as the principal point of contact for the Commission on all NCS-related matters.
  - ***47 United States Code (U.S.C.) 308(a):*** Establishes the FCC's licensing procedures during emergencies.
  - ***FCC 2nd Report and Order, WT Docket 96-86:*** Establishes rules and requirements for the NCS Priority Access Service program.
  - ***FCC Report and Order 88-341:*** Establishes the regulatory, administrative, and operational framework for the TSP program, which involves the priority restoration and provisioning of any qualified NS/EP communications service. The Office of the Manager, NCS, administers the TSP Program.
  - ***FCC Report and Order, Notification by Common Carriers of Service Disruptions, CC Docket No. 91-273:*** Requires wireline carriers to report significant service disruptions to the FCC. Note: Since January 2005, the FCC outage reporting requirement was broadened to cover wireless, cable, and satellite outages.
  - ***FCC's National Reliability and Interoperability Council (NRIC):*** The original NRIC Charter was filed January 6, 1992. Subsequent charters address specific areas of communications beyond reliability and resilience issues to include interoperability, security, cyber, and emergency services. The charter also expanded to adapt to the changing scope of the sector, including wireless and public data networks, for example.
- ***Department of Commerce (DOC)/National Telecommunications and Information Administration (NTIA):*** The Communications Act of 1934 specifies that all Federal agencies will have their spectrum needs administered and authorized by a separate agency,

currently the NTIA. As tasked under E.O.s 12046, 12472, and 12656, the NTIA also serves as the telecommunications policy adviser to the President and as a member of the Joint Telecommunications Resources Board:

– ***The Defense Production Act:*** Authorizes the President to require the priority performance of contracts and orders necessary to promote national defense. It also authorizes the President to allocate materials and facilities as necessary to promote national defense. Pursuant to the Defense Production Act, regulations promulgated by the DOC in the Defense Priorities and Allocations System (DPAS) permit the assignment of "priority ratings" to equipment associated with NS/EP communications services warranting priority treatment, if they support authorized programs under Schedule I of the DPAS.

3.4 Other Guidance

- ***Presidential War Emergency Powers for Telecommunications:*** Section 706 of the Communications Act of 1934 (47 U.S.C. 606) authorizes the President to exercise certain emergency communications functions during a wartime emergency:

  – **E.O. 12472** designates the Director of OSTP, to be the Nation's telecommunications resource manager during a wartime emergency.

- ***State and Local Authorities:*** State and local officials have some jurisdiction over the communications providers within their State or local boundaries. In many instances, State regulatory authorities, such as PUCs, focus on securing the communications infrastructure, for example:

  – In Maine, the PUC has promulgated rules requiring communications carriers to file maps indicating key utility infrastructure with the Commission (Utility Service Area and Infrastructure Maps (chapter 140), Docket No. 2001-284).

  – In Texas, there are State councils and operations centers that coordinate efforts to restore communications after a natural or manmade disaster. Groups within the Texas Office of Homeland Security coordinate the efforts of the State of Texas and private industry in the protection of critical infrastructure and key resources. During major emergencies, such as Hurricane Rita and the crash of the Space Shuttle Columbia, the State Operations Center activates its Emergency Management Council to coordinate efforts within the State agencies, and with local jurisdictions and with critical infrastructures.

Appendix 4: Sector Profile

4.1 Wireline Infrastructure

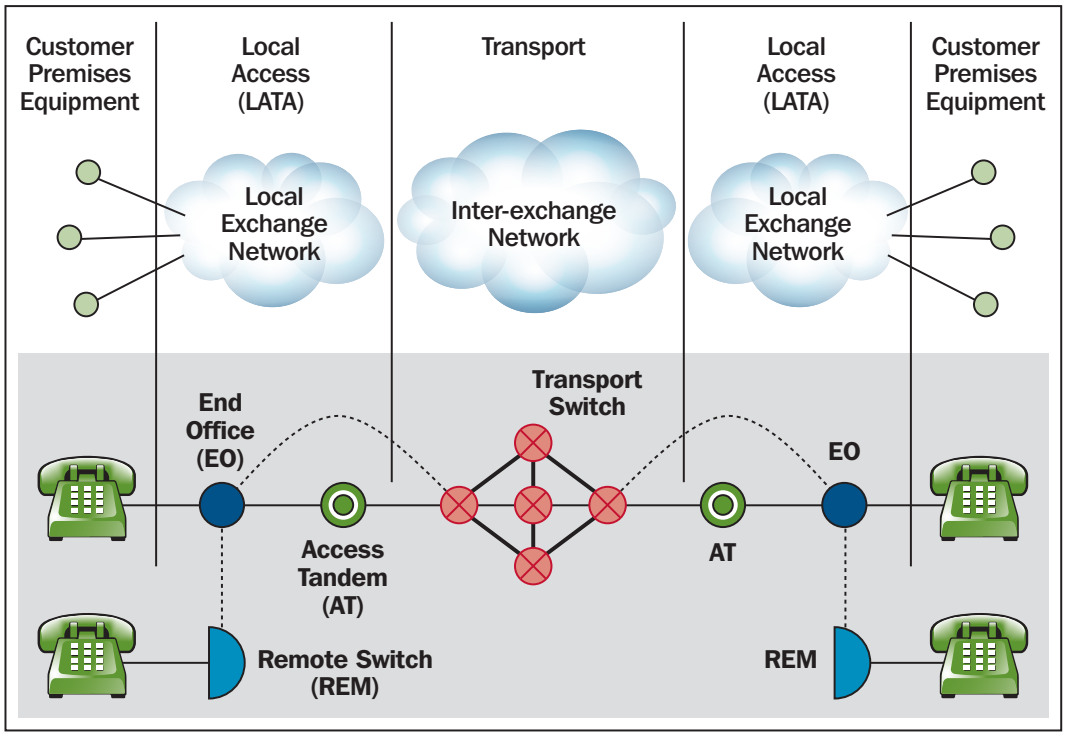
The wireline component primarily consists of the PSTN as well as enterprise networks. The PSTN is a domestic communications network accessed by telephones, key telephone systems, PBX trunks, and data arrangements. Completion of the circuit between the call originator and the call receiver requires network signaling in the form of dial pulses or multifrequency tones. These components are connected by nearly 2 billion miles of fiber and copper cable (physical), dedicated staff to ensure service (people), and IT systems that monitor and move the data (cyber). Despite the industry's transition to packet-based networks, the traditional PSTN remains the backbone of the communications infrastructure.

The wireline component has traditionally been divided between interexchange carriers (IXCs) and LECs. Local access transport areas (LATA) provide definition to the areas of provisioning responsibilities. Generally, the incumbent LEC companies provided local and intraLATA toll services, with the IXCs providing interexchange toll services. However, regulatory developments have blurred the lines between those providers. Now, many traditional LECs are evolving to provide long distance services, and more IXCs are becoming full service providers. In addition, following passage of the Telecommunications Act of 1996, new CLECs entered the local, long distance, and data services markets, as did some traditional cable television providers. Through their wireline networks, IXCs, LECs, and CLECs are also leading providers of Internet access and broadband services. Future providers may involve nontraditional platforms and infrastructures, such as broadband over power lines.

Key wireline network and transmission elements include the following, many of which are detailed in figure A4-1:

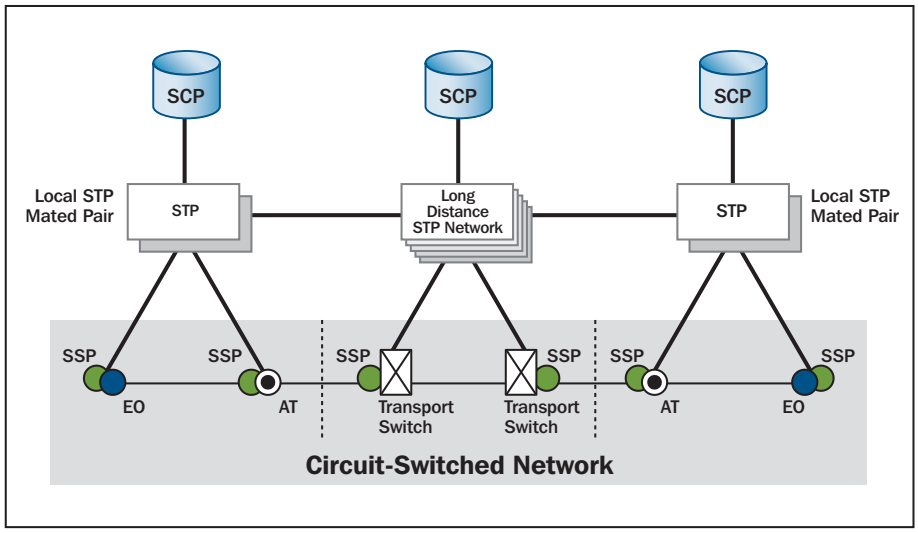
- **Local Exchange Switching:** The traditional local exchange network is a hierarchical structure with end-to-end connections using customer, local, and long distance networks. This, coupled with an ability to concentrate more traffic over fewer links, has lowered the cost of long distance traffic to the consumer. However, these same capabilities have resulted in more significant impacts when long distance links and node and link failures occur.
- **Interexchange Switching:** The traditional interexchange networks are independent mesh structures that incorporate direct point-to-point connections between nodes.
- **Transmission Links:** The physical unit of a subnetwork that provides the transmission connection between adjacent nodes.

Figure A4-1: Wireline Network Architecture



Signaling System Number 7 (SS7). SS7 is a communications protocol that provides signaling and control for various network services and capabilities. SS7 networks are medium-speed (56 or 64 kilobits per second), packet-switched networks that overlay the carriers' circuit-switched networks and provide network control functionality to the PSTN. SS7 is composed of a series of interconnected network elements (e.g., switches, databases, and routing nodes). The SS7 protocol also has significant cyber implications because it affords the interface from circuit-switched (traditional) networks to IP-based networks. Figure A4-2 illustrates how the SS7 connects to the wireline network.

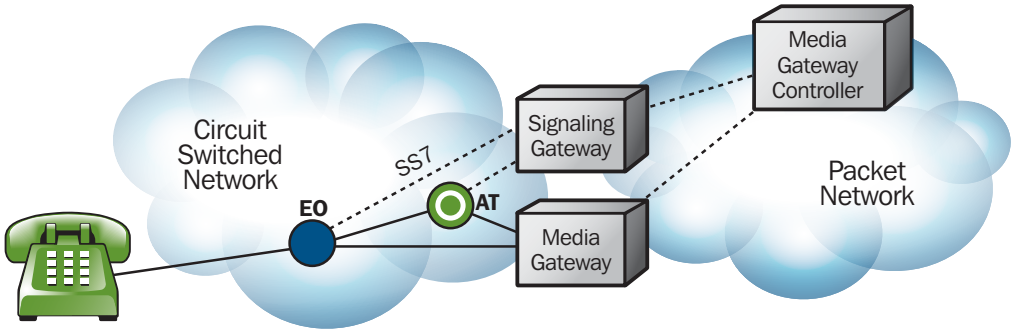
Figure A4-2: SS7 and Wireline Network Architecture



Next Generation Networks (NGNs). The concept of NGNs considers new realities within the communications industry and can be defined as a high-speed converged circuit-switched and packet-switched networks capable of transporting and routing a multitude of services, including voice, data, video, and multimedia, across variant platforms. NGNs leverage open architecture over a common transport network with an emphasis on optical networking and intelligent or NGN "aware" elements. NGNs seamlessly blend the PSTN and the packet switched data network and are also called converged networks because they integrate voice and data communications across traditionally divergent fixed and mobile platforms, to an increasing array of end-user devices.

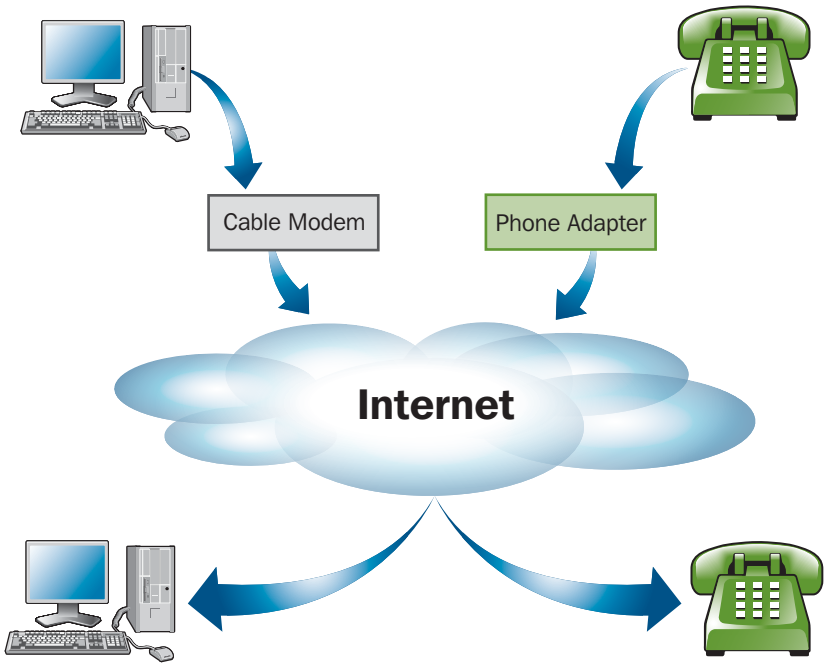
Key NGN functional elements (see figure A4-3) include: media gateway (MG), signaling gateway (SG), and media gateway controller (MGC).

Figure A4-3: Next Generation Networks



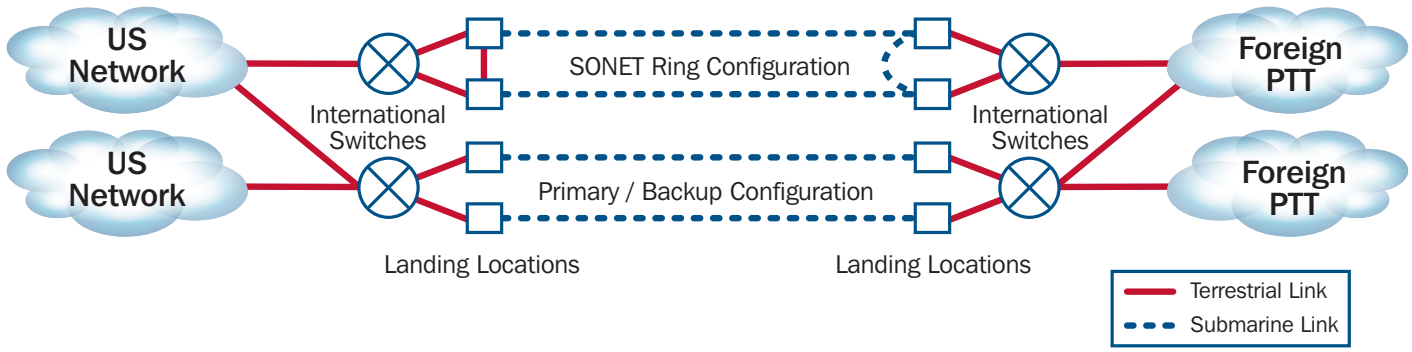
Voice over Internet Protocol (VoIP). VoIP uses the Internet or any other IP-based network to route calls rather than the PSTN with a packet-switched network being used rather than dedicated, circuit-switched telephony transmission lines. Figure A4-4 depicts the elements of a VoIP network configuration.

Figure A4-4: VoIP Networks



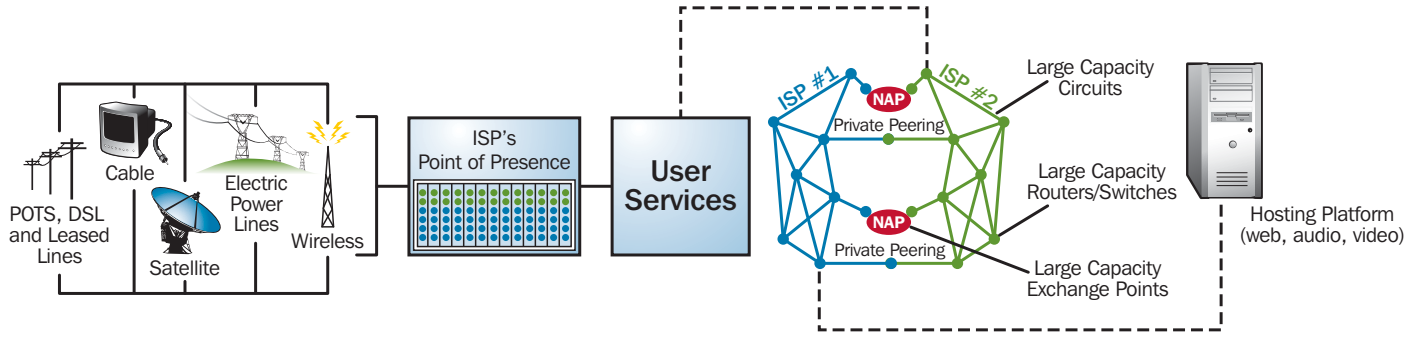
Submarine Cable Networks. Submarine cable networks are long-haul wireline networks constructed across major bodies of water to interconnect networks. Key submarine cable components (see figure A4-5) include landing locations/cable heads and switching centers.

Figure A4-5: Submarine Cable Architecture



The Internet. The Internet encompasses the global infrastructure of packet-based networks and databases that use a common set of protocols for communicating (see figure A4-6). The networks are connected by various transports. The most common examples of Internet access include ordinary telephone lines (dialup), broadband services such as Digital Subscriber Lines (DSL) and cable modems, Integrated Services Digital Network (ISDN), T1 and T3 lines, and interconnected wireless services, infrastructures, and devices.

Figure A4-6: Internet Architecture[19]



4.2 Wireless Infrastructure

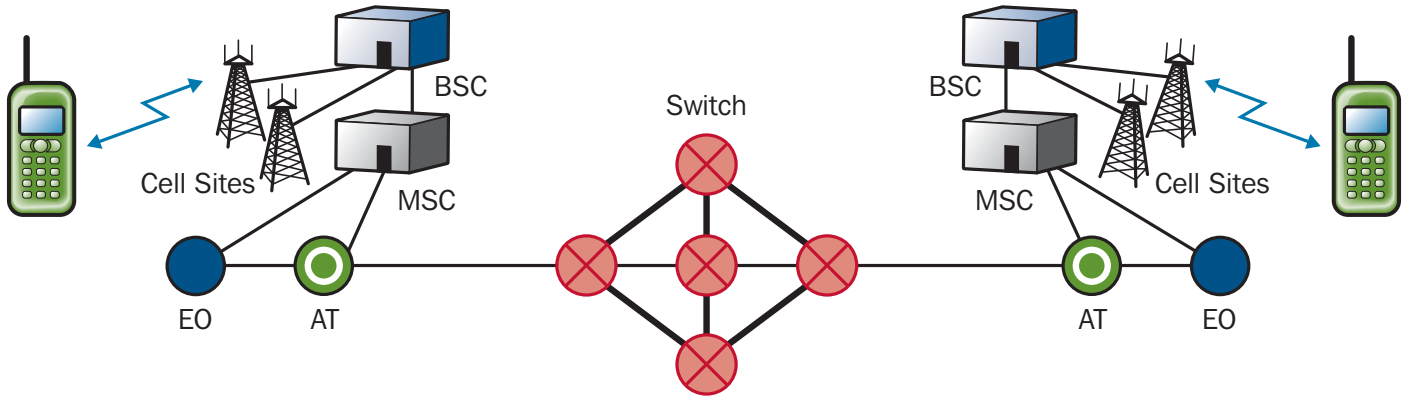
Wireless communications include cellular telephone, paging, personal communications services, high-frequency radio, unlicensed wireless, and other commercial and private radio services. Mobile wireless services have become indispensable for busi-

[19] Modified from: http://navigators.com/internet_architecture.html.

nesses and consumers, as well as for public safety needs. According to industry estimates, the U.S. mobile market penetration exceeded two-thirds in 2005, with greater levels in the largest metropolitan markets.[20]

Cellular-Type Wireless Communications System is an automated, high-capacity system of one or more multichannel base stations designed to provide radio communications services to users over a wide area in a spectrally efficient manner. A cellular-type architectural system operates by dividing a large geographical service area into cells and assigning the same channels to multiple, nonadjacent cells. This design allows channels to be reused, increasing spectrum efficiency. As a subscriber travels across the service area, the call is transferred (handed off) from one cell to another without noticeable interruption. Cellular-type wireless networks are composed of several elements (see figure D-7), including cell sites, mobile switching centers (MSC) and base switching controllers (BSC).

Figure A4-7: Wireless Network Architecture



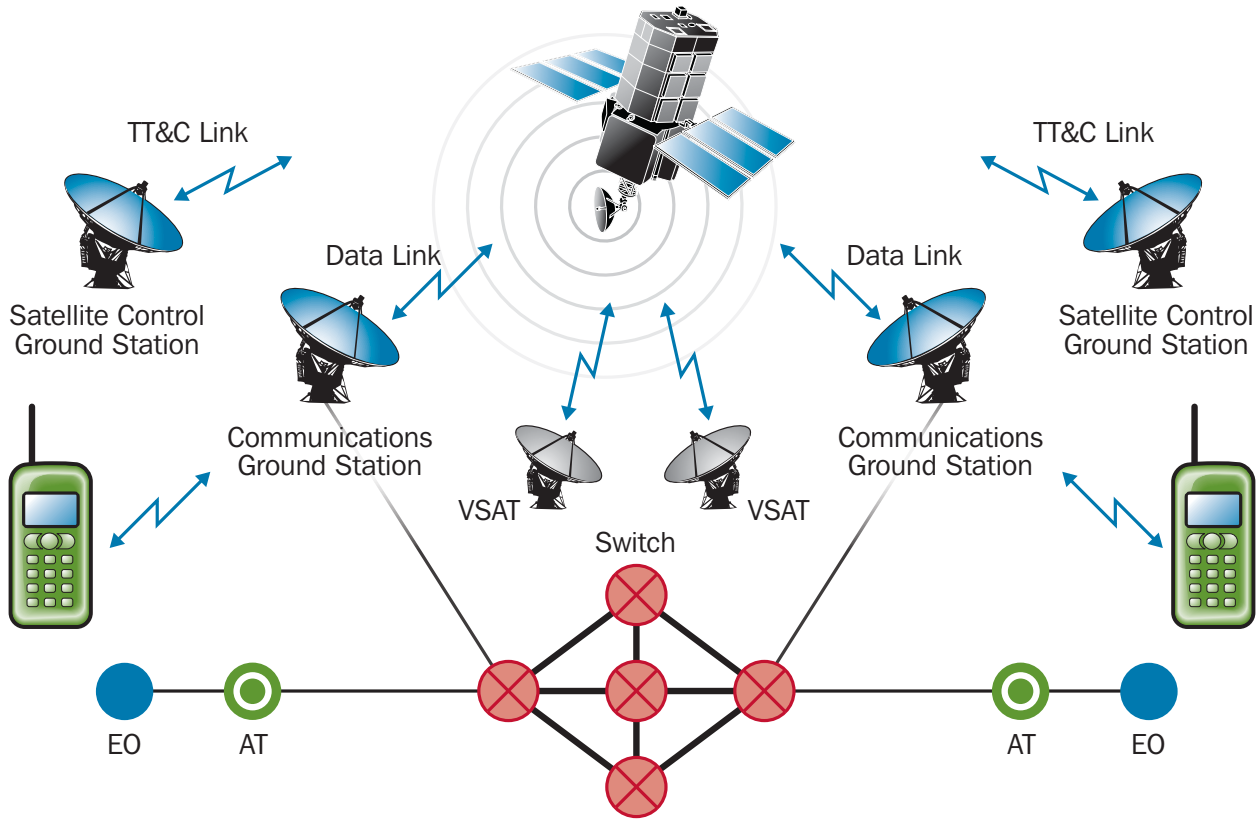
High-Frequency (HF) Radio (commonly known as shortwave radio) can be used for communication over great distances and between points separated by geographic barriers (e.g., mountains). An HF radio system consists of three basic components: transmitter/receiver unit (commonly called the transceiver), antenna, and power source.

4.3 Satellite Infrastructure

Satellite communication systems use a combination of terrestrial and space components to deliver various communications, Internet data, and video services. Geostationary Earth Orbit (GEO) systems typically require three satellites to have a global footprint. Non-geostationary Low Earth Orbit (LEO) and Middle Earth Orbit (MEO) require numerous satellites for global coverage. A group of satellites working in concert is thus known as a satellite constellation (see figure A4-8).

[20] Forbes.com, August 19, 2005.

Figure A4-8: Satellite Network Architecture



Three different types of satellite services exist: (1) FSSs support voice, data, and video broadcast services, as well as Internet backbone connectivity; (2) BSSs support video programming (i.e., DirecTV) and digital radio services; and (3) providers of MSSs support voice, voice band data, and broadband data service. MSS also is used to assist disaster recovery efforts and monitor U.S. infrastructure.

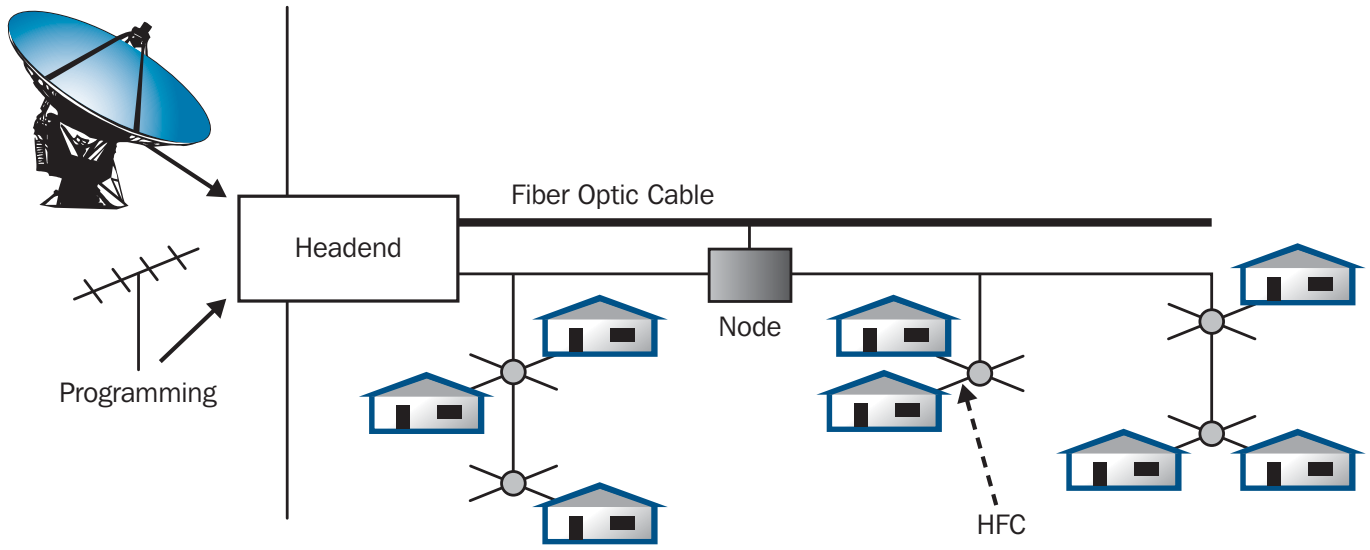
Important satellite network components include: ground stations, telemetry, tracking, and command links (TT&Cs), very small aperture terminals (VSATs), and data links (see figure D-8).

4.4 Cable Infrastructure

CATV networks are primarily wireline networks that use satellite/broadcasting infrastructure to receive programming. However, most CATV networks have transitioned from offering one-way transmission of video programming to support two-way video, data, and voice services. For data and voice services, the cable infrastructure interconnects with the PSTN through end offices. With the broader array of services, the cable infrastructure now supports both residential, commercial, and governments customers, which increases the criticality of its services.

Primary CATV network components (see figure A4-9) include satellites, headends, and fiber optic and/or HFC.

Figure A4-9: Cable Network Architecture



4.5 Broadcasting Infrastructure

Broadcasting elements consist of all parts of the radio or television station's transmission system. These elements include the studio, inclusive of the cameras and control boards, the antenna, and studio-transmitter links. These elements have a direct and fundamental effect on the station's ability to remain on the air and to provide news and emergency information to the public. If a station's transmitter fails, that station will be unable to broadcast. Fortunately, transmitters do not directly rely on computers for operation or control, and virtually all television stations and most radio stations have backup transmitters. Much of the broadcasting infrastructure overlaps with the other subsectors of the Communications Sector, especially satellites that are widely used for transmission.

Of particular importance, broadcast stations participate in the Emergency Alert System (EAS), which brings national, State, and local emergency messages to the public. All broadcast stations and cable systems are required to participate in EAS.

Appendix 5: Existing Protective Programs

Protective programs are grouped into two categories: protective actions and preparedness actions. **Protective actions** involve measures designed to prevent, deter, or mitigate threats, reduce vulnerability to an attack or disaster, or enable an efficient response and recovery in a post-incident situation. **Preparedness actions** involve activities that lessen the impact of an incident or improve the response and recovery after an attack or disaster.

Partnerships such as the NCC, the President's NSTAC, and the NSIEs are the basis for many protective programs as a result of their role in information sharing, protective program development, and response and recovery efforts. Communications Sector members are focused on meeting the needs of its sector and customers through protective and preparedness actions and operational plans and procedures to assist in the following:

- Preventing or delaying an incident;
- Determining the potential impact of an incident and detecting it when one occurs;
- Mitigating the impact of and/or responding to an incident in a manner that enables the sector asset to resume operations quickly; and
- Recovering from an incident.

5.1 Protective Actions

Protective actions include actions that contribute to the deterrence, devaluation, detection, or defense against attacks. At the owner/operator level, protective actions are implemented based on their business continuity requirements. Examples for each of the four categories of protective actions performed by owners and operators are as follows:

- **Deter:** Facility surveillance and facility and network access controls;
- **Devalue:** Backup network operations centers and synchronous optical network (SONET) ring networks;
- **Detect:** Facility alarm systems and network monitoring; and
- **Defend:** Buffer zones for critical facilities and firewalls on control system networks.

As an organized sector, partnerships serve as the mechanism for enhancing the protection provided by these protective activities. These partnerships foster the sharing of specific information on threats and vulnerabilities, which is crucial to understanding the risks to the sector. Industry shares important information that helps the government to understand the nature of the vulnerabilities and the potential impact if exploited and to report network anomalies. The following are examples of how these partnerships promote awareness and enhance protection.

- As part of its Information Sharing and Analysis (ISAC) function, the **NCC** collects and shares information about threats, vulnerabilities, intrusions, and anomalies;
- The **NSTAC** working groups regularly study vulnerabilities of the Communications Sector, often recommending new programs and mitigation techniques;
- **The NRIC** provides recommendations in the form of best practices that provide companies with guidance aimed at improving the overall reliability, interoperability, and security of wireless, wireline, satellite, cable, and public data networks; and
- In addition to sharing information on threats to the public network, the **NSIEs** periodically conduct a risk assessment of the public network.

In addition to improving overall sector risk awareness, the NCC plays a critical role in identify anomalies in the communications network and issue alerts and warnings through its 24x7 watch center. The NCS has developed programs that help provide government officials and communications owners with early warnings of potential threats and attacks on critical physical and cyber infrastructures. The NCC also coordinates and shares information with the NOC, the NICC, and other industry operation centers.

For the Federal Government, the NCS has undertaken protective activities to enhance the Federal Government's communications infrastructure protection. The NCS is conducting a study that evaluates Federal agencies' need for route diversity. The scope of the project includes identification of vulnerabilities of generic government facility communications network architectures, investigating technical mitigation solutions, and developing a route diversity methodology (RDM). The RDM includes an assessment methodology to determine risk to an agency's communications systems and apply route diversity mitigation solutions to reduce risk. The employment of route diversity solutions is a preventive strategy for Federal agencies to ensure availability communications during crises.

Overall, few Federal-level protective activities exist because the responsibility for protecting the critical infrastructure lies primarily with the private sector. Per the goals outlined in chapter 1, the private sector recognizes its responsibility for protecting its personnel and networks from attack. Operators and carriers voluntarily implement best practices (see appendix 6) for developing and implementing protective programs.

5.2 Preparedness Actions

Preparedness actions include actions that mitigate the consequences of an event. The Communications Sector is heavily focused on preparedness actions as a result of the exposure of the networks to natural disasters, as well as intentional or unintentional attacks. The Communications Sector has a solid record for its response and recovery efforts after incidents. Preparedness is coordinated at the company level, inter-company, and between industry and government. Examples of preparedness activities undertaken by industry include the following:

- **Mitigate:** Self-healing networks and redundant signaling systems.
- **Respond:** Emergency response plans, procedures and exercises.
- **Recover:** Business continuity plans and mutual-aid agreements.

In most cases, State and local agencies have been designated the leads for preparedness and response. Guiding authorities such as the NRP note that the Federal role is to support the activities of these agencies. At the national level, preparedness activities for the Communications Sector are primarily coordinated through the NCC. In the NCC, industry and government jointly plan and work to support a more endurable national communications system. These planning activities include the development and

maintenance of the ESF #2 Operations Plan and supporting standard operating procedures. ESF #2 provides for Federal communications support to State, local, and tribal government response elements, upon request.

In addition to planning, successful coordination requires training and exercises. The NCS Emergency Response Training (ERT) program ensures readiness, enhances partnerships between industry and government, coordinates communications operational planning among NCS elements, develops emergency response requirements, and provides skilled civilians and reservists during crises and emergencies. The NCS regularly conducts Telecommunications ERT seminars for emergency responders and planners that provide support to presidentially declared disasters and emergencies. The seminars provide an overview of current and future communication services and capabilities for use during disasters and emergencies, and aim to improve the ESF #2 (Communications) response and recovery structure. These training curricula address all hazards. The NCS also sponsors an annual Regional Managers Conference, for government only, to provide updated information on the evolving roles and responsibilities related to disaster planning and response operations.

The NCS conducts internal and external exercises for maintaining expert knowledge of, and proficiency in, the management, integration, and employ NS/EP communications resources. This effort includes accessing and evaluating NCS operational capabilities through the use of the Emergency Operations Team (EOT). The NCC also conducts several internal exercises annually. These exercises, typically 1 day long, are designed to test the NCC Watch Center, NCS staff, and EOT members and their operational procedures in response to the entire spectrum of emergencies and disasters. These exercises ensure that the NCS has a trained cadre of emergency response personnel and enable the NCC to test its standard operating procedures and operational readiness.

During an event, the NCC coordinates the initiation and reconstitution of NS/EP communications services and facilities. As the operational focus of the NCS, the NCC carries out ESF #2 (Communications) responsibilities under the National Response Plan. The NCC's all-hazard response approach relies on the flexible application of resources to meet crises. The NCC Initial Response Team is the first NCS organization to respond to a crisis, making an initial assessment and alerting the NCC Emergency Operations Team EOT staff, as necessary, to support the response.

To support response and recovery efforts, the NCS develops and administers a suite of priority service programs that provide for an enduring and effective communications infrastructure to fulfill NS/EP requirements under all circumstances. The key partners and users of NCS priority services and programs are responsible for minimizing loss of life and restoring order following a major disaster. These groups include those providing or supporting national security leadership, emergency warning and response, maintenance of public health and safety, maintenance of law and order, and maintenance of economic security. These groups include not only national, State, and local government leaders but also senior leadership of the Nation's critical infrastructures and key communications and information technology industries and organizations. In addition, the NCS Manager maintains an inventory of industry NGN capabilities that contribute to the reconstitution of NS/EP communications under ESF #2 of the NRP. The continued success of the programs, listed below, is essential to assuring the reliability and interoperability of the Federal Government's owned or commercially provided NS/EP communications resources.

- **Government Emergency Telecommunications Service (GETS):** Provides emergency access and priority processing in the local and long distance segments of the PSTN. This service increases the likelihood that NS/EP personnel can complete critical calls during periods of PSTN disruption and congestion resulting from natural or manmade disasters. GETS supports Federal, State, and local government, industry, and nonprofit organization personnel in performing their NS/EP missions. GETS uses three major types of networks: major long-distance networks, local networks, and government-leased networks.
- **Wireless Priority Service (WPS):** Provides priority Commercial Mobile Radio Service (CMRS) during and after emergencies for NS/EP personnel by ensuring WPS calls receive the next available radio channel during times of wireless congestion. WPS helps ensure that key NS/EP personnel can complete critical calls by providing priority access during times of wireless network congestion to key leaders and supporting first responders. In conjunction with GETS, it provides an end-to-end solution.

- **Special Routing Arrangement Service (SRAS):** Provides a vehicle for continuity of operations by providing survivable communications linkages to Federal and defense end users over the public network.
- **Next Generation Priority Service (NGPS):** Develops technology to provide priority service capabilities over the Internet, standardize the technology across industry through the commercial standards process, and migrate current priority service features to the technology.
- **Hotline System:** The NCS provides technical oversight of hotline systems to foreign countries for supporting national security and global security missions. The hotline supports the Secretary of State, Secretary of Defense, Nuclear Risk Reduction Center, and other DOD circuits and establishes international connectivity for robust, secure communications in critical situations.

In addition to the priority services programs that aid recovery efforts, the NCS administers the **Telecommunications Service Priority (TSP) Program**. This program provides the regulatory, administrative, and operational framework for priority restoration and provisioning of NS/EP communication circuits in the event of an emergency. Eligibility in the TSP program extends to Federal Government, State government, local government, private industry, or foreign governments that have communications services supporting an NS/EP mission.

The NCS also administers the **Shared Resources (SHARES) High Frequency (HF) Radio Program**, which enhances information sharing during an event. It provides a single, interagency emergency message handling system for the transmission of NS/EP information. The SHARES program brings together existing HF radio resources of Federal, State, and industry organizations when normal communications are destroyed or unavailable. SHARES also provides the Federal community a forum for addressing issues affecting HF radio interoperability.

The NCS must evolve its capabilities to continue providing NS/EP users with effective communications in an all-hazards environment. To meet national requirements and needs, the NCS will work with its public and private partners to improve these programs, particularly the WPS and NGN priority service capabilities, and to establish new services.

The NCS is also working with the OSTP and the NCS COP to develop an NS/EP continuity communications architecture that will reflect emerging threats and potential vulnerabilities arising from network convergence. The objects of the initiative are to develop an enterprise architecture that is: (1) secure, reliable, survivable, and enduring; (2) flexible, mobile, and interoperable; (3) consistent with converged network services and open standards; and (4) supported by the transformation of legacy circuit switched infrastructure to a service-oriented architecture.

To support COOP, the NCS also provides redundant operating sites to continue essential NS/EP communications functions. In its COG mission, the NCS supports the OSTP in its role to provide national-level policy and guidance to facilitate reconstitution of the Nation's communications infrastructure.

5.3 Internet Security Programs

Various government programs, as listed below, improve Internet security to prepare, mitigate against, and respond to cyber attacks.

- **United States Computer Emergency Readiness Team (US-CERT):** Coordinates defense against and responses to cyber attacks across the Nation. US-CERT collaborates with Federal agencies, private sector, the research community, State and local governments, and international entities. By analyzing incidents reported by these entities and coordinating with national security incident response centers responding to incidents on classified and unclassified systems, US-CERT disseminates actionable cyber security information to the public;
- **Internet Disruption Working Group (IDWG):** A strategic partnership between public and private sector entities formed in response to concerns surrounding the dependency of critical communications, operations, and services on Internet functions.

The IDWG is focused on identifying actions that government and other security partners can take in the near term to prepare for, protect against, and mitigate nationally significant Internet disruptions. The NCS and NCSD are co-leads of the IDWG;

- **National Cyber Response Coordination Group (NCRCG):** Facilitates the Federal Government's efforts to prepare for, respond to, and recover from cyber incidents and physical attacks that have significant cyber consequences. As a member agency, the NCS brings subject matter expertise, established relationships with private industry, and other capabilities to the NCRCG's efforts; and
- **NetGuard:** Brings together the public sector with the State and local community following an incident that affects information systems and communications networks. The intent of this DHS-led initiative is to create teams of volunteers from the private sector that could provide technical assistance and resources to the affected community. The program also acts as a clearinghouse for matching the needs of the local government and businesses with available resources in a timely manner.

Appendix 6: Communications Sector Best Practices

The Communications Sector supports the use of best practices to aid in the implementation of CI/KR protective measures. The NIPP encourages private sector owners and operators to adopt and implement those practices that are appropriate and applicable at the specific sector enterprise, individual facility, and system levels.

Best practices are derived from insights from historic technical support experience of individual companies to address communications infrastructure vulnerabilities. Best practices are presented to the industry only after sufficient rigor and deliberation over conceptual issue and particular wording of the practice. The goals developed throughout the CSSP consider the many dimensions of the protective spectrum. In many cases, security partners leverage existing programs and best practices to set the sector goals for securing physical, cyber/logical, and human elements. Industry partners support best practices processes, although due to the sector's diversity, true sector-wide risk management and sector-specific best practices are difficult to define.

The FCC has two industry advisory committees that develop best practices. The NRIC provides recommendations in the form of voluntary best practices that provide companies with guidance aimed at improving the overall reliability, interoperability, and security of networks. NRIC best practices result from broad industry cooperation that engages considerable voluntary resources, assembling vast industry expertise and experience. Table A6-1 lists NRIC best practices categories. The NRIC best practices can be found at https://svartifoss2.fcc.gov/nors/outage/bestpractice/BestPractice.cfm.

The MSRC has similar processes for developing voluntary best practices for the broadcasting industry. MSRC is an FCC Federal advisory committee focused on assuring the optimal reliability, robustness, and security of the broadcast and MVPD industries in emergency situations. MSRC best practices focus on physical security, backup power, redundant communications, and redundant facilities. MSRC best practices can be found at www.mediasecurity.org.

Use of NRIC and MSRC best practices remains voluntary, and they are not mandated by government. Not every recommendation will be appropriate for every company and circumstance.

Table A6-1: NRIC Best Practices Categories

Access Control	Facilities-Transport	Physical Security
Buildings	Fire	Fire
Business Continuity	Guard Force	Guard Force
Contractors and Vendors	Hardware	Hardware
Corporate Ethics	Human Resources	Human Resources
Cyber Security	Network Design	Network Design
Disaster Recovery	Network Elements	Network Elements
Documentation	Network Interoperability	Network Interoperability
Emergency Preparedness	Network Operations	Network Operations
Essential Services	Network Provisioning	Network Provisioning

Appendix 7: R&D Initiatives

Table A7-1: R&D Initiatives

Priority	Initiative Title	Initiative Description	Organization/ Agency	End Date
Goal 1: Health of the Communications Backbone				
Identity Management	Physical Security (Combating Terrorism Technology Support)	This project will evaluate next- generation biometric identification technologies for inclusion in integrated access control systems, field test an automatic remote identification system for vehicle drivers, and demonstrate a prototype integrated security system architecture.	Department of Defense (DOD) (Research, Development, Test, and Evaluation (RDT&E))	2008
Secure Network Element Technology; Protocol Security, Network Forensics	Location Specific Digital Fingerprint	This project will develop a digital authentication tool that destroys the capabilities of hacker tools by introducing physics into the computer security equation for wired and wireless networks and provides unpredictable random numbers that hackers cannot track. It provides an introduction of the strongest security and access control required by the government for use in national security systems.	DOD; Navy (RDT&E)	Unknown End Date
Building Scalable Secure Systems; Large-Scale Situational Awareness	Man-Portable Threat Warning System	Development of a small, lightweight, modular threat warning and tactical signals intelligence collection system that is rapidly scalable based on operational requirements. The individual body worn system will provide a display of threat and friendly force data, automated data analysis to permit hands-free operation, and reachback capabilities to access other operational or intelligence information available.	DOD (RDT&E) Advanced Concepts/ Joint Capabilities Technology Demonstration	2006

Priority	Initiative Title	Initiative Description	Organization/ Agency	End Date
Domain Name System/Border Gateway Protocol Authentication/ Security; Secure Network Element Technology	SECURE Kit	This component-based architecture will enable a user at a single workstation seat to access multiple security networks based on the user's access clearance and need to know. The Web architecture-based solution enables the user to access this information and eliminates the need to reconfigure networks and hardware when accessing one domain or another.	DOD; Navy (RDT&E)	2006
Collaborative Testbeds	A Testbed for Research and Development of Secure IP Multimedia Communication Services	This collaborative project will develop a testbed that enables research on understanding and analysis of vulnerabilities of Voice over IP (VoIP), investigates issues related to quality of service in VoIP, taking into account possible attacks, identity management, spamming, denial of service attacks, 911 emergency management, and high-availability.	NSF; Purdue University	2007
Collaborative Testbeds; NG Architectures	Next Generation Wireless Testbed	The cooperative effort will create a large-scale, end-to-end wireless testbed for independent testing of the next generation of integrated voice and data communications for mobile users; will support testing of wireless devices, technologies, and scenarios.	Department of Energy; Bechtel	2007
Holistic System Security	Surety Enhancement for Wireless Automated Control Networks	This research will create surety solutions, which directly address the vulnerabilities inherent in control systems that rely on the seamless interaction of wired and wireless communications; will identify the communication protocols used on the wireless and wired environments and investigate their interactions, balancing parameters such as bandwidth, latency, routing, power, and processing capabilities within a standards-based hybrid wired and wireless environment.	Department of Energy (DOE); Sandia National Laboratory	Unknown End Date 2001 (Startup Date)
Holistic System Security/Metric, Benchmarks, and Best Practices	Designing Next-Generation, Reliable Internet Servers	The focus of this research is to investigate the construction of a complex computer server system from simpler, separate computer systems. The effort will explore how to apply well-known (but seldom used) security engineering principles coupled with newer design features to produce highly secured components. The falling cost of IT hardware suggests that this latter approach may be more cost effective for secure system development.	NSF; Purdue University	2008

Priority	Initiative Title	Initiative Description	Organization/ Agency	End Date
Next-Generation Internet Infrastructure Architectures	An Evolvable Architecture for Next-Generation Internet Services	The proposed research program will develop and catalyze the core component of a next-generation Internet architecture that greatly increases the functional capabilities, robustness, flexibility, and heterogeneity of the Internet in the face of modern application requirements; architecture for the next generation of global networking infrastructure; and research infrastructure that allows discovery, evaluation, and deployment.	NSF; Princeton University	2006
Goal 2: Critical Communications Service Restoration				
Situational Awareness	Flexible Short-Range Communications Network	The end product of this research effort will be a set of small, independent, portable radio repeaters that will form a highly flexible short-range communications network. Most of the research effort will be involved with implementing the communications protocol. The repeaters will be low power, and run on common batteries. System goals will be high reliability, low cost, and low power.	DOE; Nevada Test Site	Unknown End Date 2002 (Start-up Date)
Situational Awareness	Analysis of Node Movement Models in Mobile Ad Hoc Networks	The project analyzes the characteristics of node movement in ad hoc networks to investigate the theoretical aspects of cooperative node movement to reduce the threats to emergency rescue personnel and to enhance the efficiency of their missions; capable of providing rapid inter-connection without any stationary infrastructure.	NSF; Indiana University	2008
Critical Infrastructure Dependencies/ Interdependencies	Event Management Framework (EMF)	EMF will provide 24/7 information search based on user criteria to protect the infrastructure of information; correlate incident information; provide analytical results for event assessment; and create database and engine servers to share information and analytical results.	DOD (RDT&E) Advanced Concepts/ Joint Capabilities Technology Demonstration	Unknown End Date 2006 (Startup Date)

Priority	Initiative Title	Initiative Description	Organization/ Agency	End Date
Goal 5: Infrastructure Resiliency and Risk Management Education				
Infrastructure Resiliency Assessment and Risk Management Practices; Critical Infrastructure Dependencies/ Interdependencies	Infrastructure Protection (Combating Terrorism Technology Support)	This initiative has produced a pocket guide on Supervisory Control and Data Acquisition (SCADA) systems and developed a software-based Virus Propagation Analysis Tool, available for download. It also includes field testing for a secure means of data communication between aircraft and air traffic controllers and creating a database on the effects of blast to critical infrastructure (CI), software tools for CI interdependency modeling, cyber security assessment methodology, a prototype early warning system for critical drinking water infrastructure.	DOD (RDT&E)	Unknown End Date
Infrastructure Resiliency Assessment and Risk Management Practices	Blast Effects and Mitigation (Combating Terrorism Technology Support)	The project will refine and provide critical blast information by performing experiments in a configurable urban city test facility, field laptop software system to aid in designing field fortifications at forward operating bases, promulgate engineering guidance and designs incorporating commercial technologies to protect CI, and investigate homemade terrorist explosive mixtures and their effects on buildings and infrastructure.	DOD (Research, Development, Test and Evaluation)	Unknown End Date
Risk Management Practices	Responding to the Unexpected	The long-term goals of this project are to radically transform the ability of organizations that respond to manmade and natural disasters to gather, process, manage, use, and disseminate information both within the emergency response agencies and to the public. This will be accomplished through scalable and robust information technology solutions that facilitate access to the right information, by the right individuals, at the right time.	NSF; University of California, San Diego	2008
Risk Management Practices	Instrumentation for Security Research and Training with Wireline and Wireless Information Networks	This project will augment capabilities for systematic analysis and evaluation of security vulnerabilities and developing new methodologies for prevention of security threats and attacks on information networks and networked systems. It aims at improving end-to-end security of information infrastructures and realizing various security applications.	NSF; University of Texas—Pan American	2008

Priority	Initiative Title	Initiative Description	Organization/ Agency	End Date
Infrastructure Resiliency Assessment	First Aid For Computer Systems (FACS)	FACS will be able to suspend or disable services and user accounts, and sequester files for forensic analysis. It will integrate these responses with local system policy so that the system administrator's knowledge of the resources and users available on the system is taken properly into account.	NSF; University of Southern California	2006
Goal 7: Cross-Sector Coordination				
Metrics Benchmarks Best Practices; Critical Infrastructure Dependencies/ Interdependencies	Combating Terrorism Technology Support	This project will evaluate virtual cyber security testing capability and publish a best practices guide and a notional architecture for infrastructure interdependency modeling, field of a prototype early warning system for critical drinking water infrastructure, and deploy a configuration-based network security technology.	DOD (RDT&E)	2007
Critical Infrastructure Dependencies; Holistic System Security	Supervisory Control and Data Acquisition System Interdependency Modeling	In collaboration with the NCS, provide applied research in security applications of supervisory control and data acquisition systems. The work will develop interdependency modeling to support and evaluate the susceptibility of high-reliability requirements. The vulnerabilities will be identified and addressed to reduce risk or downtime.	Department of Energy; NCS	2010
Situational Awareness	Pervasively Secure Infrastructures	This project addresses methods for monitoring, preventing, and recovering from natural and inflicted disasters. The project will create a novel technology-enabled security framework—Pervasively Secure Infrastructures—that will make use of such advanced technologies as smart sensors, wireless networks, pervasive computing, mobile agents, data mining, and profile-based learning in an integrated, collaborative, and distributed manner.	NSF; Penn State University	2006

Homeland Security