

# **National Security/Emergency Preparedness Telecommunications Applications Study**

**July 2002**



GSA Federal Technology Service  
Office of Information Assurance and Critical Infrastructure Protection



National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table of Contents**

## EXECUTIVE SUMMARY

A comprehensive review of Telecommunications and Information Technology (IT) Services in the context of National Security/Emergency Preparedness (NS/EP) applications<sup>1</sup> is critical in order to design and build network architectures or contract for services capable of supporting NS/EP activities. This review is especially important in a telecommunications environment in which traditional circuit-switched (CS) time division multiplex (TDM) services are migrating, i.e., “converging”, to packet- and cell-based networks. This study is designed to identify Telecommunications and IT Services that relate to the fourteen NS/EP Telecommunication Services Functional Requirements<sup>2</sup> and, thereby, could be used to support NS/EP activities.

This study examines the following three Telecommunications and IT Technology Service Groups and indicates the functions and features that meet the NS/EP Functional Requirements for each of the services in these Groups.<sup>3</sup>

- a. Wireline Services,
- b. Non-Wireline Services,
- c. IT Systems and Services.

Information in this compilation permits an NS/EP user to determine the set of functions and features to procure from its Telecommunications and IT Service providers in order to meet the Functional Requirements of its NS/EP missions. Furthermore, the study identifies any limitations or constraints that would affect the intended operation of the NS/EP Telecommunications and IT Services.

This study may be considered to be a reference. In order to most easily use the information contained herein, the following set of tables has been created that relates the Functional Requirements to the functions and features available with various Telecommunications and IT Services. Links and section references have been included in each row of the tables. These section references link to descriptions of the functions and features in the study.

To make the best use of the information in this study, the reader is encouraged to pursue the following approach.

---

<sup>1</sup> For the purposes of this study, the term “applications” is defined as: “Those existing or proposed telecommunications and information technology (IT) services, systems, and technologies which serve to enhance the NS/EP Functional Requirements of NS/EP users, end-to-end, through the public and private switched networks and communications systems.”

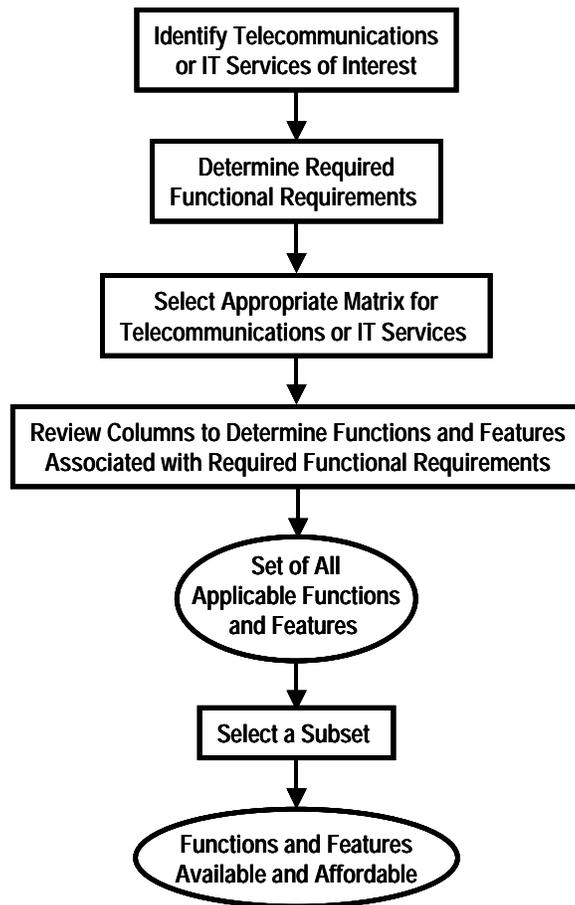
<sup>2</sup> The fourteen Functional Requirements are listed in Table A-1 of Appendix A.

<sup>3</sup> The NS/EP Telecommunication Services Functional Requirements are being used for IT services as well as for Telecommunications Services. No Functional Requirements for IT services have been officially defined.

### Executive Summary

1. Determine how Telecommunications or IT Services could support the activities associated with the NS/EP event of interest.
2. Determine which Functional Requirements are necessary to support the activities associated with the NS/EP event.
3. From the appropriate matrix below, associate the Functional Requirements with the functions and features available for the Telecommunications or IT Services chosen in Step 1. (This step will identify the set of all functions and features for the Telecommunications or IT Services that could be applied to meet the necessary Functional Requirements.)
4. From this set of functions and features, select a subset which best meets the user's needs.

The flow of these steps is illustrated in Figure ES-1 below.



**Figure ES-1 – Function and Feature Selection Approach**

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table 1 - Relationship of Functional Requirements to Wireline Services**

Legend:

1. Enhanced Priority Treatment
2. Secure Networks
3. Non-Traceability
4. Restorability
5. International Connectivity
6. Interoperability
7. Mobility
8. Ubiquitous Coverage
9. Survivability/Endurability
10. Voice Band Service
11. Broadband Service
12. Scaleable Bandwidth
13. Affordability
14. Reliability/Availability

Wireline Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13	14
<b>CSVS</b>	<a href="#">2.1.1</a>	X		X	X	X	X		X	X	X			X	X
Priority Dial Tone	<a href="#">2.1.2.1</a>	X													
Priority Call Setup Message	<a href="#">2.1.2.2</a>	X													
Exemption From Restrictive Network Controls	<a href="#">2.1.2.3</a>	X								X					
Attendant Override	<a href="#">2.1.2.4</a>	X													
User Verification	<a href="#">2.1.2.5</a>	X	X												
Authorization Codes	<a href="#">2.1.2.6</a>	X	X												
Automated Verification of Authorization Codes	<a href="#">2.1.2.7</a>	X	X												
Call Pickup	<a href="#">2.1.2.8</a>			X											
Suppression of Calling Number Delivery	<a href="#">2.1.2.9</a>			X											

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table 1 - Relationship of Functional Requirements to Wireline Services (Continued)**

Wireline Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Route or Path Avoidance	<a href="#">2.1.2.10</a>		X							X					X
Route or Path Diversity	<a href="#">2.1.2.11</a>				X					X					X
Dedicated Transmission	<a href="#">2.1.2.12</a>		X							X					X
Call Forwarding	<a href="#">2.1.2.13</a>	X													
Make Busy Arrangement	<a href="#">2.1.2.14</a>												X		
Call Screening	<a href="#">2.1.2.15</a>	X													
Class of Service and Restrictions	<a href="#">2.1.2.15.1</a>	X													
Traveling Classmark	<a href="#">2.1.2.15.2</a>	X													
Code Block	<a href="#">2.1.2.15.3</a>		X										X		
Security Procedures	<a href="#">2.1.2.16</a>		X												
Toll Free Calling	<a href="#">2.1.2.17</a>													X	
Routing Control for Toll Free Numbers	<a href="#">2.1.2.17.1</a>									X				X	X
Time of Day Routing for Toll Free Calling	<a href="#">2.1.2.17.2</a>												X	X	
Day of Week Routing for Toll Free Calling	<a href="#">2.1.2.17.3</a>												X	X	
Percentage Routing for Toll Free Calling	<a href="#">2.1.2.17.4</a>												X	X	
NPA/NXX Routing for Toll Free Calling	<a href="#">2.1.2.17.5</a>									X				X	X
ANI-Based Routing for Toll Free Calling	<a href="#">2.1.2.17.6</a>									X				X	X
Command Routing for Toll Free Calling	<a href="#">2.1.2.17.7</a>				X					X			X	X	X
Cascade Routing for Toll Free Calling	<a href="#">2.1.2.17.8</a>				X					X			X	X	X
Network Call Distributor Routing for Toll Free Calling	<a href="#">2.1.2.17.9</a>				X					X			X	X	X
Network Queuing for Toll Free Calling	<a href="#">2.1.2.17.10</a>	X												X	

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table 1 - Relationship of Functional Requirements to Wireline Services (Continued)**

Wireline Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Agency Based Routing Database for Toll Free Calling	<a href="#">2.1.2.17.11</a>				X					X			X	X	X
Call Redirection for Toll Free Calling	<a href="#">2.1.2.17.12</a>			X										X	
Dialed Number Identification for Toll Free Calling	<a href="#">2.1.2.17.13</a>		X											X	
Call Prompter Routing for Toll Free Calling	<a href="#">2.1.2.17.14</a>			X										X	
Call Prompter Routing - Electronic Access for Toll Free Calling	<a href="#">2.1.2.17.15</a>								X					X	
Call Status Report for Toll Free Calling	<a href="#">2.1.2.17.16</a>		X												X
Caller Profile Report for Toll Free Calling	<a href="#">2.1.2.17.17</a>		X												X
Caller Information Report for Toll Free Calling	<a href="#">2.1.2.17.18</a>		X										X		X
Caller Response Report for Toll Free Calling	<a href="#">2.1.2.17.19</a>		X												
Real-Time Call Status for Toll Free Calling	<a href="#">2.1.2.17.20</a>		X												X
Operator Connect Bridging for Toll Free Calling	<a href="#">2.1.2.17.21</a>			X											
Basic ATB Rerouting for Toll Free Calling	<a href="#">2.1.2.17.22</a>				X					X			X	X	X
Service Assurance Rerouting for Toll Free Calling	<a href="#">2.1.2.17.23</a>									X					X
Service Level Agreements	<a href="#">2.1.2.18</a>				X					X					X
<b>CSDS</b>	<a href="#">2.2.1</a>				X	X	X		X	X	X	X	X	X	X
Priority Dial Tone	<a href="#">2.2.2.1</a>	X													
Priority Call Setup Message	<a href="#">2.2.2.2</a>	X													
Exemption From Restrictive Network Controls	<a href="#">2.2.2.3</a>	X								X					

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table 1 - Relationship of Functional Requirements to Wireline Services (Continued)**

Wireline Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13	14
User Verification	<a href="#">2.2.2.4</a>	X	X												
Authorization Codes	<a href="#">2.2.2.5</a>	X	X												
Automated Verification of Authorization Codes	<a href="#">2.2.2.6</a>	X	X												
Suppression of Calling Number Delivery	<a href="#">2.2.2.7</a>			X											
Route or Path Avoidance	<a href="#">2.2.2.8</a>		X							X					X
Route or Path Diversity	<a href="#">2.2.2.9</a>				X					X					X
Dedicated Transmission	<a href="#">2.2.2.10</a>		X							X					X
Call Screening	<a href="#">2.2.2.11</a>	X													
Class of Service and Restrictions	<a href="#">2.2.2.12</a>	X													
Traveling Classmark	<a href="#">2.2.2.12.1</a>	X													
Code Block	<a href="#">2.2.2.12.2</a>		X										X		
Security Procedures	<a href="#">2.2.2.13</a>		X												
Toll Free Calling	<a href="#">2.2.2.14</a>													X	
Routing Control for Toll Free Numbers	<a href="#">2.2.2.14.1</a>									X				X	X
NPA/NXX Routing for Toll Free Calling	<a href="#">2.2.2.14.2</a>									X				X	X
ANI-Based Routing for Toll Free Calling	<a href="#">2.2.2.14.3</a>									X				X	X
Command Routing for Toll Free Calling	<a href="#">2.2.2.14.4</a>				X					X			X	X	X

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table 1 - Relationship of Functional Requirements to Wireline Services (Concluded)**

Wireline Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Cascade Routing for Toll Free Calling	<a href="#">2.2.2.14.5</a>				X					X			X	X	X
Network Queuing for Toll Free Calling	<a href="#">2.2.2.14.6</a>	X												X	
Agency Based Routing Database for Toll Free Calling	<a href="#">2.2.2.14.7</a>				X					X			X	X	X
Dialed Number Identification for Toll Free Calling	<a href="#">2.2.2.14.8</a>		X											X	
Call Status Report for Toll Free Calling	<a href="#">2.2.2.14.9</a>		X												X
Caller Profile Report for Toll Free Calling	<a href="#">2.2.2.14.10</a>		X												X
Caller Information Report for Toll Free Calling	<a href="#">2.2.2.14.11</a>		X										X		X
Real-Time Call Status for Toll Free Calling	<a href="#">2.2.2.14.12</a>		X												X
Basic ATB Rerouting for Toll Free Calling	<a href="#">2.2.2.14.13</a>				X					X			X	X	X
Service Assurance Rerouting for Toll Free Calling	<a href="#">2.2.2.14.14</a>									X					X
Service Level Agreements	<a href="#">2.2.2.15</a>				X					X					X
<b>PSDS</b>	<a href="#">2.3.1</a>	X		X	X	X	X		X	X	X	X	X	X	X
Dedicated Transmission	<a href="#">2.3.2.1</a>		X							X					X
Route or Path Avoidance	<a href="#">2.3.2.2</a>		X							X					X
Route or Path Diversity	<a href="#">2.3.2.3</a>				X					X					X
Security Procedures	<a href="#">2.3.2.4</a>		X												
Service Level Agreements	<a href="#">2.3.2.5</a>				X					X					X
Security Features	<a href="#">2.3.2.6</a>		X												

**Table 2 - Relationship of Functional Requirements to Non-Wireline Services**

Legend:

1. Enhanced Priority Treatment
2. Secure Networks
3. Non-Traceability
4. Restorability
5. International Connectivity and Interoperability
6. Mobility
7. Ubiquitous Coverage
8. Survivability/Endurability
9. Voice Band Service
10. Broadband Service and Scaleable Bandwidth
11. Affordability
12. Reliability/Availability

Non-Wireline Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12
<b>Wireless Services</b>	<a href="#">3.1.1</a>												
Wireless Priority Service (WPS) available NYC and Wash. DC; underdevelopment nationwide	<a href="#">3.2.1</a>	X											
Qualcomm's CONDOR™ Wireless Secure telecommunications System and GSM with authentication offer some security features; otherwise encrypt transmitted signal	<a href="#">3.3.1</a>		X										
Non-Traceability Unavailable	<a href="#">3.4.1</a>												
Use of TSP for wireline interconnections to MSOs; SLAs with service providers; backup equipment	<a href="#">3.5.1</a>				X								

**Table 2 - Relationship of Functional Requirements to Non-Wireline Services (Continued)**

<b>Non-Wireline Services and Functions/Features</b>	<b>Section</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>	<b>10</b>	<b>11</b>	<b>12</b>
Via commercial wireline voice and packet service providers; use of GSM under certain conditions; multimode handsets; use of SDR technology	<a href="#">3.6.1</a>					X							
Inherently mobile	<a href="#">3.7.1</a>						X						
“Nearly” Ubiquitous Coverage dependent upon the wireless equipment and system implementation	<a href="#">3.8.1</a>							X					
Robust designs and physical protection; back-up and replacement systems; radio frequency interference (RFI) prevention	<a href="#">3.9.1</a>								X				
Inherently	<a href="#">3.10.1</a>									X			
Available with 2.5G (using General Packet Radio Service), 3G, and potentially 4G	<a href="#">3.11.1</a>										X		
Rely on COTS services	<a href="#">3.12.1</a>											X	
Dependent upon equipment quality and system designs; adequate and uncorrupted radio frequency (RF) signals; WPS Program should help; rapid restoration a key element; need financially viable service providers	<a href="#">3.13.1</a>												X
<b>Paging and Short Text Services</b>	<a href="#">3.1.2</a>												
Enhanced Priority Treatment Unavailable	<a href="#">3.2.2</a>												
BlackBerry offers secure e-mail; otherwise encrypt and decrypt the data message itself	<a href="#">3.3.2</a>		X										
Generally unavailable except for e-mail sent with originating address removed	<a href="#">3.4.2</a>			X									
SLAs with service providers; backup equipment	<a href="#">3.5.2</a>				X								
Use of SMS for Interoperability	<a href="#">3.6.2</a>					X							
Inherently mobile	<a href="#">3.7.2</a>						X						
Nearly worldwide paging services available	<a href="#">3.8.2</a>							X					
Robust designs and physical protection; back-up and replacement systems; RFI prevention	<a href="#">3.9.2</a>								X				

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table 2 - Relationship of Functional Requirements to Non-Wireline Services (Continued)**

Non-Wireline Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12
Available only as a voice message	<a href="#">3.10.2</a>									X			
Broadband Service and Scaleable Bandwidth Unavailable	<a href="#">3.11.2</a>												
Rely on COTS services	<a href="#">3.12.2</a>											X	
Dependent upon equipment quality and system designs; adequate and uncorrupted RF signals; rapid restoration a key element; need financially viable service providers	<a href="#">3.13.2</a>												X
<b>LMDS and MMDS</b>	<a href="#">3.1.3</a>												
Enhanced Priority Treatment Unavailable	<a href="#">3.2.3</a>												
Encryption and decryption of the traffic only	<a href="#">3.3.3</a>		X										
Non-Traceability Not Applicable	<a href="#">3.4.3</a>												
SLAs with service providers; backup equipment	<a href="#">3.5.3</a>				X								
International Connectivity and Interoperability Not Applicable	<a href="#">3.6.3</a>												
May be considered "transportable"	<a href="#">3.7.3</a>						X						
Ubiquitous Coverage Not Applicable	<a href="#">3.8.3</a>												
Robust designs and physical protection; back-up and replacement systems; RFI prevention	<a href="#">3.9.3</a>								X				
Inherently	<a href="#">3.10.3</a>									X			
Available with free space optics and microwave implementations	<a href="#">3.11.3</a>										X		
Rely on COTS services	<a href="#">3.12.3</a>											X	
Dependent upon equipment quality and system designs; rapid restoration a key element	<a href="#">3.13.3</a>												X
<b>WLAN and PAN</b>	<a href="#">3.1.4</a>												
Enhanced Priority Treatment Unavailable	<a href="#">3.2.4</a>												

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table 2 - Relationship of Functional Requirements to Non-Wireline Services (Continued)**

Non-Wireline Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12
Use WEP protocol (part of WLAN IEEE 802.11b standard) or VPN on WLAN; PAN Bluetooth security not sufficient; UWB under development, and has some inherent security	<a href="#">3.3.4</a>		X										
Non-Traceability Unavailable	<a href="#">3.4.4</a>												
SLAs with service providers; backup equipment	<a href="#">3.5.4</a>				X								
International Connectivity and Interoperability Not Applicable	<a href="#">3.6.4</a>												
PANs are inherently mobile; certain applications of WLANs can be mobile	<a href="#">3.7.4</a>						X						
Ubiquitous Coverage Not Applicable	<a href="#">3.8.4</a>												
Care in physical location and physical protection; back-up and replacement systems; RFI prevention	<a href="#">3.9.4</a>								X				
Dependent on the WLAN and PAN usage	<a href="#">3.10.4</a>									X			
WLANs via IEEE 802.11b, a, and g standards; PANs via Bluetooth and UWB	<a href="#">3.11.4</a>										X		
Most WLAN and PAN implementations currently rely on COTS services; UWB under development but expected to be competitively priced	<a href="#">3.12.4</a>											X	
Dependent upon equipment quality and system designs; rapid restoration a key element; selection of viable service provider and long-lived technology	<a href="#">3.13.4</a>												X
<b>Satellite Services</b>	<a href="#">3.1.5</a>												
Enhanced Priority Treatment Unavailable	<a href="#">3.2.5</a>												
Encryption and decryption of the traffic	<a href="#">3.3.5</a>		X										
Non-Traceability Unavailable	<a href="#">3.4.5</a>												

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table 2 - Relationship of Functional Requirements to Non-Wireline Services (Continued)**

Non-Wireline Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12
Use of TSP for wireline interconnections between satellite earth stations and the terrestrial wireline network; SLAs with service providers; backup equipment	<a href="#">3.5.5</a>				X								
Interoperability via commercial wireline voice and packet service providers; International Connectivity by use of certain Satellite Services, such as Glocall SP or Iridium	<a href="#">3.6.5</a>					X							
Inherently mobile	<a href="#">3.7.5</a>						X						
“Nearly” Ubiquitous Coverage dependent upon the system	<a href="#">3.8.5</a>							X					
Robust designs and physical protection; back-up and replacement systems; RFI prevention	<a href="#">3.9.5</a>								X				
Inherently	<a href="#">3.10.5</a>									X			
Via services like Glocall SP, Two-way Direct Broadcast Satellite services, Starband, and DirecPC; Teledesic and SkyBridge in the future	<a href="#">3.11.5</a>										X		
Rely on COTS services	<a href="#">3.12.5</a>											X	
Dependent upon equipment quality and system designs; rapid restoration a key element; selection of viable service provider	<a href="#">3.13.5</a>												X
<b>Land Mobile Radio and Two-Way Mobile Radio Services</b>	<a href="#">3.1.6</a>												
For some LMR systems, channels can be reserved for priority treatment	<a href="#">3.2.6</a>	X											
Encryption and decryption of the voice and traffic	<a href="#">3.3.6</a>		X										
Only if no identification is ascribed to particular transmissions	<a href="#">3.4.6</a>			X									

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table 2 - Relationship of Functional Requirements to Non-Wireline Services (Concluded)**

Non-Wireline Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12
SLAs with service providers; backup equipment	<a href="#">3.5.6</a>				X								
Interoperability via SDR technology; through projects like AGILE and Project SafeCom	<a href="#">3.6.6</a>					X							
Inherently mobile	<a href="#">3.7.6</a>						X						
Relocation of mobile equipment can provide Ubiquitous Coverage	<a href="#">3.8.6</a>							X					
Robust designs and physical protection; back-up and replacement systems; RFI prevention	<a href="#">3.9.6</a>								X				
Inherently Unavailable	<a href="#">3.10.6</a>									X			
Many implementations rely on COTS products; systems employing SDR may be more expensive unless user base grows	<a href="#">3.12.6</a>											X	
Dependent upon equipment quality and system designs; rapid restoration a key element; selection of viable service provider and long-lived technology	<a href="#">3.13.6</a>												X

**Table 3 - Relationship of Functional Requirements to IT Services**

Legend:

1. Enhanced Priority Treatment
2. Security
3. Audit Trails and Non-Traceability
4. Interconnectivity and Interoperability
5. Mobility
6. Restorability
7. Survivability/Endurability
8. Reliability/Availability
9. Voice Band Service
10. Broadband Service
11. Scaleable Bandwidth
12. Affordability
13. Ubiquitous Coverage

IT Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13
<b>Information Repository Systems</b>	<a href="#">4.1.1</a>													
Prioritize data access and transactions; place critical information/data in cache memory; deny system access to non-critical users	<a href="#">4.2.1</a>	X												
Implement Security policies, procedures, and practices via a Security Management Program; permit system interaction by only authorized personnel; limit system access; continuously update security patches; conduct frequent virus scanning; take measures for prevention of DoS, DDoS, and DRDoS attacks; employ encryption	<a href="#">4.3</a>		X											

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table 3 - Relationship of Functional Requirements to IT Services (Continued)**

IT Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13
Use Audit Trails to track personal accountability; monitor problems in real-time; reconstruct events; identify attempts to penetrate a system; log events; determine trends	<a href="#">4.4</a>			X										
Use common standardized data formats and languages, such as SQL, SNMP, X.400, X.500, UCA, HTTP, FTP, SMTP, and TCP/IP;	<a href="#">4.5.1</a>				X									
Maintain operations while in motion using large vehicle like FEMA's MATS ; also consider "transportable" systems	<a href="#">4.6.1</a>					X								
Availability and use of a comprehensive disaster recovery plan; maintain backup copies of standard or customized software with periodic checks of medium's quality; perform regular frequent system backups; log database management systems and associated transactions; consider implementing "mirroring"; maintain a "hot" or "cold" backup site	<a href="#">4.7.1</a>						X							

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table 3 - Relationship of Functional Requirements to IT Services (Continued)**

IT Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13
Provide resistance to attacks by: 1) restricting physical access, hardening the physical site, employing user authentication, using access controls, data encryption, message filtering at system boundary, functional isolation among systems, maintaining stringent requirements on system development and testing practices and quality control of software; 2) intrusion detection, performing system audits, using baseline checksum or cryptographic signatures for periodic comparison to the current data contents; 3) implement mechanisms for rapid system restoration; 4) developing systems capable of evolving in response to user requirements for new functions and intruders' increasing knowledge of system structure and behavior	<a href="#">4.8</a>							X						

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table 3 - Relationship of Functional Requirements to IT Services (Continued)**

IT Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13
In general, employ system design architecture with redundant critical components and high Reliability and Availability of the individual components; perform regular system backups; maintain alternate storage sites for databases; conduct periodic drills on the recovery procedures; maintain continuity of operations, concept of operation, and disaster recovery plans; perform regression and integration testing of changes and updates; employ a Configuration/Change Control Board to review and approve system changes or updates; employ SLAs and Performance Based Contracting for outsourced functions; follow "best practices" for software development such as those published by the SEI, the SA-CMM and the SRE Service; specifically for Information Repository Systems, log all transactions; create backup databases; limit which data fields may be updated and the personnel authorized to do so; employ multi-level security authentication techniques	<a href="#">4.9</a> and <a href="#">4.9.1</a>								X					
Telecommunications facilities capable of Voice Band Service would be able to handle transfers of small amounts of data via permanent low data rate or dial-up connections to the Information Repository; voice messages can be recorded and the message files entered into and retrieved from these repositories	<a href="#">4.10.1</a>									X				
Telecommunications facilities capable of Broadband Service would handle data transfers to and from the repositories	<a href="#">4.11.1</a>										X			

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table 3 - Relationship of Functional Requirements to IT Services (Continued)**

IT Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13
Telecommunications facilities capable of Scaleable Bandwidth may be required to connect to the repository depending upon traffic load into and out of the system	<a href="#">4.12.1</a>											X		
Ways to manage Affordability are: consider the Total Cost of Ownership and any necessary modifications to COTS hardware and software; minimize the duplicate IT System stovepipes that exist within organizations by promoting use of a components-based enterprise architecture; following best practices, like those from the SEI; possibly outsource certain IT functions; compare results of a risk analysis against cost to implement system functions	<a href="#">4.13</a>												X	
Ubiquitous Coverage Not Applicable	<a href="#">4.14</a>													
<b>Monitor and Control Systems</b>	<a href="#">4.1.2</a>													
Prioritize acquisition and processing of signal input and output (I/O); prioritize data handling by Telecommunications Systems between agents and managers	<a href="#">4.2.2</a>	X												
Same as for Information Repository Systems	<a href="#">4.3</a>		X											
Audit trails same as for Information Repository Systems; Use Non-Traceability to hide origination or destination of sensory/control data for Monitor and Control Systems	<a href="#">4.4</a>			X										
Use common standardized data formats and languages, such as UCA and SNMP between a manger and its agents. For Telecommunications Systems, refer to Interoperability in Section 2 for Wireline Services	<a href="#">4.5.2</a>				X									

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table 3 - Relationship of Functional Requirements to IT Services (Continued)**

IT Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13
Agents may be mobile; use GPS to track agents monitoring various types of resources; connect agents to manager via Non-Wireline technology	<a href="#">4.6.2</a>					X								
Use same approaches as for Information Repository Systems; in addition, use rapid automatic switchovers to redundant network agent and manager equipment; use redundant or alternate telecommunications paths between an agent and manager	<a href="#">4.7.2</a>						X							
Same as for Information Repository Systems; additionally planning for agent redundancy and continued operation assuming some loss of some agents; maintaining robust Telecommunications System(s) between agents and manager by employing diverse routing or redundant telecommunication facilities	<a href="#">4.8</a> and <a href="#">4.8.1</a>							X						
Same techniques as for Information Repository Systems plus maintaining the Reliability and Availability of the Telecommunications System between the agents and managers; employ “out of band” management to determine the state of the network element, determine the nature of the failure, and attempt restoration to the normal state; log events	<a href="#">4.9</a> and <a href="#">4.9.2</a>								X					

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table 3 - Relationship of Functional Requirements to IT Services (Continued)**

IT Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13
Telecommunications facilities capable of Voice Band Service would be used as a permanent low bandwidth data connection between agents and managers or as an alternative link in the event of a failure of the primary telecommunications facilities; voice communication may be used by individuals to verbally communicate information between agents and their managers	<a href="#">4.10.2</a>									X				
Telecommunications facilities capable of Broadband Service to handle communications between agents and their manager and between managers and the control center	<a href="#">4.11.2</a>										X			
Telecommunications facilities capable of Scaleable Bandwidth may be needed depending upon traffic load requirements between the agents and managers	<a href="#">4.12.2</a>											X		
Same as for Information Repository Systems	<a href="#">4.13</a>												X	
Ubiquitous Coverage Not Applicable	<a href="#">4.14</a>													
<b>E-Commerce Systems</b>	<a href="#">4.1.3</a>													
Prioritize NS/EP-related transactions in CPU; implement strong SLAs	<a href="#">4.2.3</a>	X												
Same as for Information Repository Systems	<a href="#">4.3</a>		X											
Audit Trails same as for Information Repository Systems;	<a href="#">4.4</a>			X										
Use common standardized data formats and languages, such as XML; use GUIs for human interface; use COTS software and servers; establish interrelationships among E-Commerce components	<a href="#">4.5.3</a>				X									

National Security/Emergency Preparedness Telecommunications Applications  
 Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table 3 - Relationship of Functional Requirements to IT Services (Concluded)**

IT Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13
E-commerce systems are likely to be Mobile; they could be made Transportable	<a href="#">4.6.3</a>					X								
Use same approaches as for Information Repository Systems	<a href="#">4.7.3</a>						X							
Same as for Information Repository Systems	<a href="#">4.8</a>							X						
Same techniques as for Information Repository Systems plus SEI best practices; employing specialized implementations to "isolate" and duplicate major E-Commerce System components; providing redundant or backup components and telecommunications facilities	<a href="#">4.9</a> and <a href="#">4.9.3</a>								X					
Voice Band Telecommunications Services connected to E-Commerce Systems may be adequate to provide the necessary connectivity to the systems	<a href="#">4.10.3</a>									X				
Broadband Telecommunications Services connected to E-Commerce Systems may be needed to provide the necessary connectivity to the systems	<a href="#">4.11.3</a>										X			
Scaleable Bandwidth may be needed to connect to the E-Commerce System depending on the varying telecommunications traffic loads	<a href="#">4.12.3</a>											X		
Same as for Information Repository Systems	<a href="#">4.13</a>												X	
Ubiquitous Coverage Not Applicable	<a href="#">4.14</a>													

# 1 INTRODUCTION

A comprehensive review of Telecommunications and Information Technology (IT) Services in the context of National Security/Emergency Preparedness (NS/EP) applications is critical in order to design and build network architectures or contract for services capable of supporting NS/EP activities. This review is especially important in a telecommunications environment in which traditional circuit-switched (CS) time division multiplex (TDM) services are migrating, i.e., “converging”, to packet- and cell-based networks. This study is designed to identify Telecommunications and IT Services that relate to the fourteen NS/EP Telecommunication Services Functional Requirements<sup>4</sup> and, thereby, could be used to support NS/EP activities.

For the purposes of this study, the term “applications” is defined as, “Those existing or proposed Telecommunications and IT Services, systems, and technologies which serve to enhance the NS/EP Functional Requirements of NS/EP users, end-to-end, through the public and private switched networks and communications systems.”

This study examines the following three Telecommunications and IT Technology Service Groups and indicates the functions and features that meet the NS/EP Functional Requirements for each of the services in these Groups.<sup>5</sup> These relationships are summarized in the tables of the appendices so indicated.

- a. Wireline Services (Summary in Table B-1),
- b. Non-Wireline Services (Summary in Table C-1),
- c. IT Systems and Services (Summary in Table D-1).

Information in this compilation permits an NS/EP user to determine the set of functions and features to procure from its Telecommunications and IT Service providers in order to meet the Functional Requirements of its NS/EP missions. Furthermore, the study identifies any limitations or constraints that would affect the intended operation of the NS/EP Telecommunications and IT Services.

Most of the Telecommunications and IT Services, along with their functions and features, discussed in this study may be used for non-NS/EP applications in day-to-day operations as well as for NS/EP applications. What makes these functions and features applicable to supporting NS/EP applications is the manner in which they relate to the Functional Requirements. Any function or feature which in no manner relates to a Functional Requirement may be considered unsuitable for NS/EP applications. If a function or feature relates to only a subset of the Functional Requirements, it may be suitable for

---

<sup>4</sup> The fourteen Functional Requirements are listed in Table A-1 of Appendix A.

<sup>5</sup> The NS/EP Telecommunication Services Functional Requirements are being used for IT services as well as for Telecommunications Services. No Functional Requirements for IT services have been officially defined.

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

some NS/EP applications. The suitability must be determined by the NS/EP user on a case-by-case basis.

Some of the information contained in this study was derived from interviews conducted with individuals having experience in conducting certain NS/EP activities. The names of the individuals interviewed and their responses are indicated.

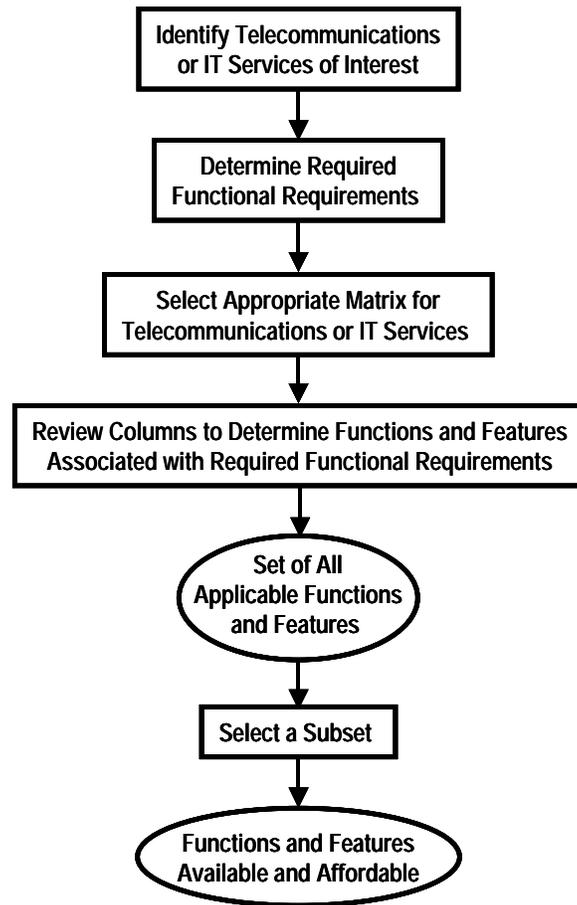
Products or services specifically discussed in this study are mentioned only as examples. No recommendations for these products or services is intended.

This study may be considered to be a reference., In order to most easily use the information contained herein, the set of tables in the Executive Summary has been created that relates the Functional Requirements to the functions and features available with various Telecommunications and IT Services. Links and section references have been included in each row of the tables. These section references link to descriptions of the functions and features in the study.

To make the best use of the information in this study, the reader is encouraged to pursue the following approach.

1. Determine how Telecommunications or IT Services could support the activities associated with the NS/EP event of interest.
2. Determine which Functional Requirements are necessary to support the activities associated with the NS/EP event.
3. From the appropriate matrix below, associate the Functional Requirements with the functions and features available for the Telecommunications or IT Services chosen in Step 1. (This step will identify the set of all functions and features for the Telecommunications or IT Services that could be applied to meet the necessary Functional Requirements.)
4. From this set of functions and features, select a subset which best meets the user's needs.

The flow of these steps is illustrated in Figure -1 below.



**Figure -1 – Function and Feature Selection Approach**

## **2 WIRELINE SERVICES**

For the purposes of this study, Wireline Services are those Telecommunications Services which are delivered end-to-end employing transmission technologies operating over copper wire and cable as well as over fiber optic cable. The Telecommunications Services delivered using Wireline Services are:

1. Circuit-Switched Voice,
2. Circuit-Switched Data,
3. Packet Switched Data, including multimedia, such as voice, video, graphics, and imagery.

Of course, other technologies, such as satellite, microwave, free space optics (FSO), and wireless, may be used to deliver the three services listed above, but, for the purposes of this study, these three services are considered to be part of the Wireline Services Technology Service Group. Other Technology Service Groups will address similar Telecommunications Services in other sections of this study.

Table B-1, in Appendix B, relates the NS/EP Functional Requirements to these three Wireline Services and to the services' functions and features.

### **2.1 Circuit-Switched Voice Services**

The Public Switched Telephone Network (PSTN) forms the basis for public Circuit-Switched Voice Services (CSVs) in the United States. CSVs includes those Telecommunications Services employing TDM technology and CS networks to deliver voice and voice band data services, such as analog modem, facsimile, and low baud rate TeleTYpewriter (TTY)<sup>6</sup> transmissions.

The PSTN supports the connection mode of operation, in which an end-to-end path is established for the communication to transit upon entry of the address, or telephone number, of the destination terminal. Once a connection is established, the call effectively is "hard-wired" in the form of a CS connection.

#### **2.1.1 Functional Requirements Inherently Available with CSVs**

For the support of NS/EP activities, Circuit-Switched Voice Services continue to be of major use. Inherently, CSVs supports the following Functional Requirements:

---

<sup>6</sup> A TTY is a typewriter-style device for communication alphanumeric information over telecommunications networks.

### **2.1.1.1 Enhanced Priority Treatment**

The mostly widely available solution for providing Enhanced Priority Treatment for CSVS is the Government Emergency Telecommunication Service<sup>7</sup> (GETS). The events of September 11 have indicated the success of GETS in providing Enhanced Priority Treatment in the form of priority queuing for CSVS domestic calls within the PSTN and international calls to and from the PSTN. Completion rates exceeding 95% were achieved during these events.

Among the individuals interviewed for this study, only Mr. Art McLemore, from General Service Administration's (GSA's) Region 10, indicated that a GETS call did not complete during a recent emergency event. This instance of non-completion, and others reported to the Office of the Manager National Communications System (OMNCS), are being investigated by the OMNCS to determine the cause(s). In fact, the use of GETS was so successful for NS/EP operations following the September 11 attacks that the OMNCS will be distributing additional GETS cards. GETS is currently provisioned for 250,000 calls, but to date only about 53,000 cards have been distributed.

### **2.1.1.2 Non-Traceability**

CSVs calls are traceable unless specific actions are taken to limit the traceability. Non-Traceability in the PSTN, is achieved through the Special Routing Arrangement Service (SRAS), which is a federal government Telecommunications Service that provides enhanced call completion and lower occurrence of call blocking, blocking of caller identification, and suppression of origination and destination information. SRAS is currently implemented by only one interexchange carrier (IXC), i.e., AT&T.

### **2.1.1.3 Restorability**

Because of the design of the PSTN, many redundant and alternative paths are available to enable quick restoration of service. Hence, if a failure occurs on one connection path, in many instances an alternative path is available from either the same service provider or from a different service provider. Network architectures permit automatic and nearly instantaneous alternative routing to redundant backup transmission paths. Many service providers have bi-lateral transmission facility sharing agreements permitting them to share another service provider's fiber optic cable plant during emergencies with automatic cutover capability in place.

In addition, restoration to required service levels on a priority basis is achieved via the Telecommunications Service Priority (TSP) System. "The TSP Report and Order, which

---

<sup>7</sup> GETS provides priority establishment and routing of telephone calls through the PSTN specifically for authorized users. GETS priority is obtained through software enhancements in the PSTN, including trunk queuing, exemption from network management control (NMC), and alternate carrier routing. GETS is implemented under contracts with major Local Exchange Carriers, Interexchange Carriers, and switch manufacturers. Access to GETS requires the dialing of a universal access number and a personal identification number. While GETS calls receive priority for next available path, they do not preempt existing calls.

establishes the TSP System, allows telecommunications service vendors to provide priority treatment to NS/EP Telecommunications Services and ensures that such vendors are not violating Title II, Section 202 of the Communications Act of 1934 when doing so.<sup>8</sup> The TSP System operates primarily within the circuit switched network environment...”<sup>9</sup> TSP is a system whereby orders for adds and changes to existing wireline circuits can be expedited within a service provider’s network. TSP processes also apply to priority restoration of failed wireline circuits. TSP traditionally has been applied to physically identifiable circuits and equipment.

#### **2.1.1.4 International Connectivity**

Networks supporting the PSTN are inherently designed to, and do, interconnect with foreign networks equivalent to those of the PSTN. This interconnectivity is achieved via service providers’ adherence to international standards developed and publicized by the International Telecommunications Union (ITU).

#### **2.1.1.5 Interoperability**

The PSTN is comprised of interconnected and interoperable CS TDM networks operated by numerous local and interexchange carriers. Interoperability is achieved by service providers’ adherence to a set of standards developed and publicized, in part, by the American National Standards Institute (ANSI), Committee T1 of the Alliance for Telecommunications Solutions (ATIS), and best practices published by Telcordia Technologies, the successor to Bellcore.

#### **2.1.1.6 Ubiquitous Coverage**

The PSTN is widely deployed in North America, and public telephone networks worldwide offer CSVS. Consequently, the PSTN, in conjunction with the international networks with which it interoperates, offers “nearly ubiquitous” coverage for NS/EP purposes. For locations in which the PSTN or its equivalents are unavailable, alternative forms of communications usually are available for substitution, such as Satellite Services.

#### **2.1.1.7 Survivability/Endurability**

The PSTN is comprised of numerous interconnected CS TDM networks with many redundant and alternative paths available to make connections. Hence, a failed connection path, in many instances, may be substituted by an alternative path that is available from either the same service provider or from a different service provider. Synchronous Optical Network (SONET) ring architectures inherently provide alternative routing for damaged transport facilities. Also, the routing possibilities available via the interconnected PSTN afford multiple routes for completing CSVS calls if alternative routing is implemented. Finally, service providers’ Network Operations Centers (NOCs) provide constant monitoring of traffic loads within their networks such that disruptions in

---

<sup>8</sup> *TSP Report and Order*, 3 FCC Rcd 6650 (1988).

<sup>9</sup> *NSTAC Network Security/Vulnerability Assessment Task Force Report*, March 2002

service can be lessened by manual traffic rerouting. Therefore, the PSTN is generally considered to be a survivable and enduring network.

### **2.1.1.8 Voice Band Service**

By definition, Circuit-Switched Voice Services provide voice band service.

### **2.1.1.9 Affordability**

In today's environment, CSVS represents a commercially available commodity as offered by local and long distance service providers. Service providers frequently offer their customers discounted pricing arrangements or special pricing packages dependent upon the customer's usage of the CSVS. Besides price, other parameters for determining Affordability are the service's reliability, availability, maintainability, and ease of implementation and operation. All these parameters affect the service's Affordability to the subscriber and should be determined on a case-by-case basis dependent upon the subscriber and its requirements. In general, CSVS is considered an affordable commodity.

### **2.1.1.10 Reliability/Availability**

The PSTN is well known for its Reliability and Availability. An historical availability percentage of 99.999% is the bench mark against which other technologies and their networks are compared.

Under extreme conditions, the PSTN may not always be available for support of NS/EP activities. In such cases, alternative forms of communications usually are available for substitution. For instance, if the wireline connection with the PSTN is lost in a location suffering substantial physical damage, such as in the World Trade Center (WTC) attack, alternative point-to-point microwave and laser, or FSO systems<sup>10</sup>, may be employed for short distances to connect to the PSTN. Such connections bypass any damaged PSTN infrastructure.

Mr. Rex Whitacre, of the Federal Emergency Management Agency (FEMA), indicated FEMA uses point-to-point FSO links. The links can support DS-1s for data or video. Qwest provided such an FSO link between two buildings in New York City shortly after the attack on the WTC to bypass the damaged wireline infrastructure. The links connected FEMA in New York City with FEMA's Mount Weather site in Bluemont, Virginia. FEMA also uses Tsunami point-to-point microwave links operating in the 2.4 gigahertz (GHz) band and capable of simultaneously providing two DS-1s and a 10 megabits per second (Mbps) link.

## **2.1.2 CSVS Features Meeting Certain Functional Requirements**

Besides the inherent Functional Requirements, numerous functions and features associated with CSVS and the PSTN can support NS/EP activities. The following

---

<sup>10</sup> FSO systems have the potential to offer data rates up to 1.25 gigabits per second.

paragraphs describe these functions and features along with an indication of the Functional Requirements they could support.

#### **2.1.2.1 Priority Dial Tone<sup>11</sup>**

This feature prioritizes the provision of dial tone to permitted lines only. Call attempts from such designated lines are placed in a priority queue and are handled before non-priority calls. No call marking is required.

*Functional Requirement – Enhanced Priority Treatment*

#### **2.1.2.2 Priority Call Setup Message<sup>11</sup>**

This feature provides priority call setup messages through the signaling network with the high priority call (HPC) identifier. It requires call marking, a method of marking and identifying priority calls through networks. As the priority call progresses through the network, this identifier enables special routing and preferential treatment to ensure the higher probability of call completion.

*Functional Requirement – Enhanced Priority Treatment*

#### **2.1.2.3 Exemption From Restrictive Network Controls<sup>11</sup>**

This feature provides exemption from restrictive (network) controls, such as call gapping. It requires call marking. It provides a set of control measures used to prevent or control degradation of network service. For instance, since call gapping would be prevented with Exemption From Restrictive Network Controls, the feature would inhibit the limitation of calls to a particular station address or telephone number. If call gapping was implemented for a set of telephone numbers, then its inhibition for certain calls with Exemption From Restrictive Network Controls to that set of numbers could effectively result in priority treatment for those calls with Exemption From Restrictive Network Controls.

*Functional Requirements – Enhanced Priority Treatment and Survivability/Endurability*

#### **2.1.2.4 Attendant Override<sup>11</sup>**

This feature allows the terminal equipment operator to interrupt a call that is in progress. The ability of the operator to interrupt a call in progress is a form of Enhanced Priority Treatment since preference can be given to other calls in lieu of the interrupted call.

*Functional Requirement – Enhanced Priority Treatment*

#### **2.1.2.5 User Verification<sup>11</sup>**

This feature allows for the verification of the user authorized for priority handling of his/her calls. Personal Identification Numbers (PINs), line identification, authorization codes, or call-back facilities could be used to verify the call as being placed by an authorized party.

---

<sup>11</sup> This information was extracted from the draft version of International Telecommunication Union Recommendation E.106.

*Functional Requirements – Enhanced Priority Treatment and Secure Networks*

**2.1.2.6 Authorization Codes<sup>11</sup>**

This feature applies unique multi-digit codes, such as associated with a Personal Identification Number (PIN), to allow an authorized user privileged access to a network. If the code is validated, the call is allowed to proceed. An Authorization Code could be associated with a scheme to acquire Enhanced Priority Treatment for certain CSVS calls.

*Functional Requirements – Enhanced Priority Treatment and Secure Networks*

**2.1.2.7 Automated Verification of Authorization Codes**

This feature permits verification of an authorization code, when used for the service, to occur without involving an operator before the service is provided. Automated Verification of Authorization Codes could be associated with a scheme to acquire Enhanced Priority Treatment for certain CSVS calls.

*Functional Requirements – Enhanced Priority Treatment and Secure Networks*

**2.1.2.8 Call Pickup<sup>12</sup>**

This feature enables a connected extension to answer any ringing extension within an assigned call pickup group. This feature potentially could provide Non-Traceability by hiding the true identity of the individual being called and answering the phone in that the actual number being called is hidden from the caller.

*Functional Requirement – Non-Traceability*

**2.1.2.9 Suppression of Calling Number Delivery**

Based on the class of service (COS) of the originating station or calling card, the service provider would inhibit the delivery of the calling number, i.e., automatic number identification (ANI), by setting the Privacy Indicator at the originating end of the call and honoring it at the terminating end.

*Functional Requirement – Non-Traceability*

**2.1.2.10 Route or Path Avoidance**

This feature allows a customer to define a geographic location or route to avoid in the transmission path of its communications. For instance, this feature would permit the customer to prevent its service provider from routing the subscriber's communications over a microwave path in a geographical area with a high likelihood that the microwave signal could be intercepted and monitored by an unauthorized party. Also, this feature would permit the subscriber to prevent its service provider from routing the subscriber's communications over a portion of the network which may be susceptible to outages due to natural or man-made phenomenon.

---

<sup>12</sup> This information was extracted from the draft version of International Telecommunication Union Recommendation E.106.

*Functional Requirements – Secure Networks, Survivability/Endurability, and Reliability/Availability*

**2.1.2.11 Route or Path Diversity**

This feature permits the user to require its service provider to establish diverse routes which do not share any common telecommunications facilities or offices, including a common building entrance. The service provider should maintain a minimum separation (e.g., 30 feet) throughout all diverse routes, except for cable crossovers, between premises and buildings at certain permitted locations. However, for cable crossovers, the service provider should maintain a minimum vertical separation (e.g., two feet) with cables separately encased in appropriate steel or concrete conduits, for example.

The service provider should provide the capability for the real-time automatic switching of transmission from the primary route to one or more diverse route(s) and from the diverse route(s) to the primary route.

*Functional Requirements – Restorability, Survivability/Endurability, and Reliability/Availability*

**2.1.2.12 Dedicated Transmission**

This feature permits the service subscriber to order dedicated transmission facilities from its service provider. The dedicated transmission facilities may be ordered so as to avoid any active equipment, such as switching or digital cross connect (DXC) system equipment. The avoidance of such equipment would make the dedicated transmission facilities immune from disruption by failures of this equipment. These facilities should have a higher availability and should not be susceptible from unauthorized intrusion into the Signaling System 7 (SS7) signaling network or DXC control systems. However, the subscriber will be required to provide its own terminal equipment since the service provider is delivering only a digital pipe.

*Functional Requirements – Secure Networks, Survivability/Endurability, and Reliability/Availability*

**2.1.2.13 Call Forwarding**

This feature enables calls to be re-routed automatically from one line to another or to an attendant. If the original destination number has call forwarding initiated, the network will reroute and process an emergency call that has preferential treatment to the new destination. Call forwarding thus permits preferential emergency communications to be completed to an alternate destination number in case the primary number is busy. In this sense, call forwarding supports Enhanced Priority Treatment.

*Functional Requirement – Enhanced Priority Treatment*

**2.1.2.14 Make Busy Arrangement**

This feature permits the user to make one or more access lines within a service group appear busy by operation of user equipment (e.g., a terminal) located at the subscriber's

premises or, at the subscriber's option, by notification to the service provider (e.g., via telephone, e-mail, etc.). The service provider should provide the subscriber with the capability of busy-ing-out individual circuits within a trunk group or an entire trunk group. For example, this feature may be invoked should the user's private branch exchange (PBX) be overloaded with incoming calls during an emergency and the user desired to limit the load on the PBX.

*Functional Requirement – Scaleable Bandwidth*

#### **2.1.2.15 Call Screening**

Call screening comprises a set of features that determines a call's eligibility to be completed as dialed, based upon COS information associated with the user, the terminal device, or the trunk group.

*Functional Requirement – Enhanced Priority Treatment*

##### **2.1.2.15.1 Class of Service and Restrictions**

This feature permits the subscriber's service provider to establish a set of classes of service available to each user, terminal device, or trunk. The COS may be determined from ANI, authorization codes, traveling classmarks, or trunk groups. The COS derived from an authorization code may be set up to take precedence over that derived from other means. Hence, Enhanced Priority Treatment could result from the COS assigned.

*Functional Requirement – Enhanced Priority Treatment*

##### **2.1.2.15.2 Traveling Classmark**

This feature provides for the acceptance of traveling classmarks (TCOS) from all locations served by PBXs and Centrexes that are able to provide these classmarks, including calls extended by operators. Traveling classmarks should conform to the TCOS format (i.e., called number + TCOS). User calling characteristics and limitations may be determined from the traveling classmark.

*Functional Requirement – Enhanced Priority Treatment*

##### **2.1.2.15.3 Code Block**

This feature screens ineligible users, terminal devices, and trunks with certain COS access restrictions from calling specified area codes, exchange codes, and countries. Blocked calls could be intercepted to appropriate network recorded announcements. This feature can provide security by inhibiting calls to non-secure locations and telephone numbers.

*Functional Requirements – Secure Networks and Scaleable Bandwidth*

#### **2.1.2.16 Security Procedures**

Establishment of proper security procedures will permit the user to accomplish the following activities:

- a) Controlling access to user-related sensitive databases and information,
- b) Prevention of fraudulent use of user information or services, and
- c) Prevention of fraudulent use of calling cards, e.g., GETS cards.

*Functional Requirement – Secure Networks*

**2.1.2.17 Toll Free Calling**

This feature permits authorized users to dial certain numbers using service access codes<sup>13</sup>, such as 800, 888, 877, etc., to complete toll free and message unit-free (to the callers) directory numbers. A service provider would be responsible for furnishing toll free numbers. For domestic services, numbering should be consistent with 800, 888, and other toll free service access codes services. For non-domestic service, numbering should be consistent with requirements or practices in the host country or should be consistent with toll free domestic service when no standard exists. The toll free service provider should supply network intercepts to recorded announcements as an inherent network capability when a call cannot be completed.

Toll free calling is a method to enhance the Affordability for callers to contact the organization providing NS/EP services since the users can call for assistance, or other purposes, during a disaster or emergency without incurring any charges themselves. For instance, calls from users of NS/EP services may be placed from pay telephones without the need for coins or incurring calling card charges.

*Functional Requirement – Affordability*

**2.1.2.17.1 Routing Control for Toll Free Numbers**

This feature permits the subscriber to review, create, validate, change, or execute his/her call routing plans via a terminal located at the subscriber's premises. The service provider should provide adequate security procedures that would prevent unauthorized access to this feature. This feature permits the NS/EP subscriber to direct the toll free calls to certain locations of the subscriber's choosing. This flexibility permits the subscriber to provide better service to its users. In some cases, the routing flexibility could be employed to avoid locations that were damaged by an emergency or disaster. In this sense, the routing flexibility improves the availability and the survivability of the NS/EP services being provided by the subscribing organization in addition to the Affordability offered by toll free calling.

*Functional Requirements –Survivability/Endurability, Affordability, and Reliability/Availability*

---

<sup>13</sup> Service Access Codes are 3-digit codes which are part of the Numbering Plan Area (NPA) portion of the 10-digit North American Numbering Plan telephone address to identify generic services or provide access capability.

#### **2.1.2.17.2 Time of Day Routing for Toll Free Calling**

This feature permits calls to be routed to different subscriber specified locations depending on the time of day. This feature permits more equitable distribution of traffic loads on the subscriber's call centers and call response equipment. In this context, the feature provides Scaleable Bandwidth in addition to the Affordability offered by toll free calling.

*Functional Requirement – Scaleable Bandwidth and Affordability*

#### **2.1.2.17.3 Day of Week Routing for Toll Free Calling**

This feature permits calls to be routed to different subscriber specified locations depending on the day of the week. This feature permits more equitable distribution of traffic loads on the subscriber's call centers and call response equipment. In this context, the feature provides Scaleable Bandwidth in addition to the Affordability offered by toll free calling.

*Functional Requirement – Scaleable Bandwidth and Affordability*

#### **2.1.2.17.4 Percentage Routing for Toll Free Calling**

This feature permits calls to be distributed between two or more subscriber locations and/or service groups based on the subscriber's specified percentage distribution from zero percent to 100 percent in one percent increments. This feature permits more equitable distribution of traffic loads on the subscriber's call centers and call response equipment. In this context, the feature provides Scaleable Bandwidth in addition to the Affordability offered by toll free calling.

*Functional Requirement – Scaleable Bandwidth and Affordability*

#### **2.1.2.17.5 NPA/NXX Routing for Toll Free Calling**

This feature permits calls originating from within subscriber-selected geographic areas, defined by one or more Numbering Plan Area (NPA) codes and/or NPA/NXX<sup>14</sup> combinations, to be routed to a subscriber specified location. When an NPA/NXX is not available, calls are to be routed to a subscriber's default location. This feature permits a subscriber to automatically route toll free calls to other locations depending upon the availability or accessibility of the subscriber's call or response center(s). In a disaster or emergency, the default call or response center may be unavailable for use. This feature provides for Survivability of the Affordable toll free calling service as well as improving the Reliability and Availability of the service.

*Functional Requirements –Survivability/Endurability, Affordability, and Reliability/Availability*

---

<sup>14</sup> NXX is a generic designation for the digits of a 10-digit North American Numbering Plan telephone address. "N" represents any digit of 2-9 and "X" represents any digit of 0-9.

#### **2.1.2.17.6 ANI-Based Routing for Toll Free Calling**

This feature permits calls to be routed based on the full ANI of the callers. Default routing defined by the subscriber could be used if ANI were not available.

*Functional Requirements – Survivability/Endurability, Affordability, and Reliability/Availability*

#### **2.1.2.17.7 Command Routing for Toll Free Calling**

This feature permits a subscriber that has subscribed to one or more of the features supporting various types of Toll Free Call Routing to route calls differently (i.e., select a different predefined routing path alternative) on command at any time. As a consequence of this feature's applicability to the other Toll Free Call Routing features, it supports several Functional Requirements.

*Functional Requirements –Restorability, Survivability/Endurability, Scaleable Bandwidth, Affordability, and Reliability/Availability*

#### **2.1.2.17.8 Cascade Routing for Toll Free Calling**

This feature permits the destination of calls to be changed on a subscriber-defined predetermined basis based on the availability of egress circuits at the subscriber's original destination. As a function of the bandwidth (number of circuits) available in the egress circuits at the destination for toll free calls, the subscriber can prearrange alternate destination locations. This feature would be very useful in cases in which some of the egress lines to the subscriber's call or response centers were made unavailable due to an emergency or disaster.

*Functional Requirements – Restorability, Survivability/Endurability, Scaleable Bandwidth, Affordability, and Reliability/Availability*

#### **2.1.2.17.9 Network Call Distributor Routing for Toll Free Calling**

This feature provides call routing capabilities based on real-time information obtained from the subscriber's automatic call distributors. This feature would offer the same set of capabilities as the other routing features and, therefore, would meet the same Functional Requirements.

*Functional Requirements – Restorability, Survivability/Endurability, Scaleable Bandwidth, Affordability, and Reliability/Availability*

#### **2.1.2.17.10 Network Queuing for Toll Free Calling**

This feature is a hybrid routing/announcement feature that allows a caller to be held in queue in the service provider's network until a subscriber's terminating equipment becomes available to receive the call. Consequently, the incoming call is given a form of Enhanced Priority Treatment to ensure that it gets answered and not dropped.

*Functional Requirement – Enhanced Priority Treatment and Affordability*

#### **2.1.2.17.11 Agency Based Routing Database for Toll Free Calling**

This feature permits queries to a subscriber-provided call routing processor which will allow call-by-call routing based upon information returned from the subscriber's call routing processor. This feature provides capabilities similar to those mentioned above for other toll free calling features. Hence, it is associated with the same set of Functional Requirements.

*Functional Requirements – Restorability, Survivability/Endurability, Scaleable Bandwidth, Affordability, and Reliability/Availability*

#### **2.1.2.17.12 Call Redirection for Toll Free Calling**

This feature allows an incoming toll free call to be transferred by the called party to another toll free number or any PSTN number by utilizing, at the subscriber's discretion, any one of three modes of call transfer: (i) blind transfer, (ii) verification by the called party that the called number is not busy and then transfer, or (iii) three-way conference and then transfer. This feature could conceivably be employed for Non-Traceability of the called party in that the toll free number originally dialed need not be the final destination of the call since the call ultimately would be forwarded to the proper party with the original called party acting as only an intermediary.

*Functional Requirement – Non-Traceability and Affordability*

#### **2.1.2.17.13 Dialed Number Identification for Toll Free Calling**

This feature allows a user with multiple toll free numbers in the same service group to identify electronically the specific toll free number that was dialed by the calling party. This information could be useful in determining whether malicious calls are being dialed to overload the toll free call or response center(s) resulting in denial of service for legitimate callers in addition to the Affordability offered by toll free calling.

*Functional Requirement – Secure Networks and Affordability*

#### **2.1.2.17.14 Call Prompter Routing for Toll Free Calling**

This feature allows callers to be routed to various network locations by dialing, via dual tone multi-frequency (DTMF), digits or speaking specific route selection information. Once a caller has been connected, the network should provide a recorded announcement identifying one or more DTMF selection digits that will provide further routing of the call. This feature could provide capability similar to that in Call Redirection since the toll free number originally dialed need not be the final destination of the call because the call ultimately would be redirected to the proper destination.

*Functional Requirement – Non-Traceability and Affordability*

#### **2.1.2.17.15 Call Prompter Routing – Electronic Access for Toll Free Calling**

This feature permits callers with terminals designed for individuals who are deaf, hard of hearing, or have speech disabilities to have access to a toll free number and receive prompts and/or selection instructions displayed in electronic form and to enter desired

selections. This feature should support callers' terminals, e.g., Terminal Devices for the Deaf (TDDs), transmitting or receiving information in Baudot Code and/or American Standard Code for Information Interchange (ASCII) format. In a sense, this feature could be considered to provide ubiquitous coverage because it provides access to a larger user community for toll free services in addition to the Affordability offered by toll free calling.

*Functional Requirement – Ubiquitous Coverage and Affordability*

**Note:** The provision of access for individuals who are deaf, hard of hearing, or have speech disabilities is a requirement that transcends toll free service since it applies to basic CS voice service and toll free service as well.

**2.1.2.17.16 Call Status Report for Toll Free Calling**

This report provides the subscriber with information about the status of calls placed to each of its toll free numbers. This report provides statistics as to how the toll free services are performing and are being used. The statistics may be useful for determining whether call overload attempts are occurring and whether any malicious calls have impaired service. Therefore, the information could be applied to ensuring the Security of the service provider's network as well as assuring Reliability and Availability of the toll free service.

For any given toll free number, the subscriber may request its service provider to provide the following information within the reports:

- a) The number of calls from each area code that dialed the toll free number (i.e., call attempts),
- b) The number of calls and the percentage of all calls that encounter a busy signal (i.e., that are blocked):
  - a. In the service provider's network,
  - b. At the user's terminating access.
- c) The number of calls offered to the user's terminating access (i.e., egress trunk group),
- d) The number of calls received at each user's terminating access,
- e) The number of received calls at each user's terminating access that resulted in successful answerback supervision,
- f) The average duration of calls answered at each user's terminating access, and
- g) The average duration of all calls answered for a given toll free number at all users' terminating access serving the toll free number.

*Functional Requirement – Secure Networks and Reliability/Availability*

**2.1.2.17.17 Caller Profile Report for Toll Free Calling**

This report, with the following parameters, can provide useful information about the status of toll free calls into the network and to the subscriber's call or response centers.

As such, the statistics may be useful for determining whether call overload attempts are occurring, identifying the number(s) from which they originate, and whether the malicious calls have impaired service. Therefore, the information could be applied to ensuring the Security of the service provider's network as well as assuring Reliability and Availability of the toll free service.

The statistics that could be reported are:

- a) Lost Callers: The number of callers who never called back after an incomplete attempt during the reporting period.
- b) Average Number of Attempts Per Caller: The grand total number of call attempts divided by the number of first call attempts during the reporting period.
- c) Average Number of Contacts Per Caller: The number of attempts generated from each telephone number on average during the reporting period.
- d) 50 Percent of Successful Attempts Within 1,000 Calls: This statistic represents the number of attempts required to access the network for 50 percent of the callers who completed calls.
- e) 75 Percent of Successful Attempts Within 1,000 Calls: This statistic represents the number of attempts required to access the network for 75 percent of the callers who completed calls.

*Functional Requirement – Secure Networks and Reliability/Availability*

#### **2.1.2.17.18 Caller Information Report for Toll Free Calling**

This report provides information about the ANI of all callers to a given toll free number. ANI, although available in most cases, is not yet being universally provided. In those instances where ANI is not available, the NPA or NPA-NXX (as available) of the caller should be provided. Zeroes should be substituted in place of any missing digits. For any given toll free number, the subscriber may request its service provider to provide the following information within the reports:

- a) Date of call,
- b) Time of call (expressed using either a 24 hour clock or a 12 hour clock with an AM/PM indicator and indicating time zone),
- c) ANI of caller (if available),
- d) Dialed (i.e., destination) 10 digit number,
- e) Duration of call (to the nearest 6 seconds), and
- f) Disposition of call, i.e., using an alpha or numeric code, to include, at a minimum, the following:
  - a. Call blocked within service provider's network,
  - b. Call blocked at subscriber's terminating access,
  - c. Call completed to subscriber's terminating access, and
  - d. Other (e.g., call abandoned enroute to subscriber's terminating access, no answer back supervision received, etc.).

These statistics may be useful for determining whether call overload attempts are occurring, identifying the number(s) from which they originate, and whether the malicious calls have impaired service. Therefore, the information could be applied to ensuring the Security of the service provider's network. The information may also be applicable for determining the necessity of additional trunk (or bandwidth) capacity relative to Scaling the network's bandwidth and for determining the Reliability/Availability of the network.

*Functional Requirements – Secure Networks, Scaleable Bandwidth, and Reliability/Availability*

#### **2.1.2.17.19 Caller Response Report for Toll Free Calling**

The service provider should be able to retrieve, format, and provide caller-entered DTMF or speech messages and provide such information to the subscriber. This information may also be applied to determining if malicious use is being made of the toll free calling service.

*Functional Requirement – Secure Networks*

#### **2.1.2.17.20 Real-Time Call Status for Toll Free Calling**

This feature permits the subscriber of the toll free service to receive information about the status of toll free calls in progress on a near real-time (e.g., refreshed within a few minutes) basis. This information may be of use in determining if malicious calls are attempting to overload the subscriber's toll free call or response centers and for determining the Reliability/Availability of the network.

*Functional Requirement – Secure Networks and Reliability/Availability*

#### **2.1.2.17.21 Operator Connect Bridging for Toll Free Calling**

This feature permits toll free inbound calls to connect directly to the service provider's operator allowing the caller to speak with the operator (at any time, rather than continue to prompt through messages) based either on caller's prompt defined in the recorded announcement or announcement logic. The service provider's operator shall assist the caller in reaching a calling destination location based on pre-determined default routing. This feature may be applied to the Functional Requirement of Non-Traceability since establishing the connection through the operator may prevent called number identification to be recorded in the network or calling number known to the called party.

*Functional Requirement – Non-Traceability*

#### **2.1.2.17.22 Basic ATB Rerouting for Toll Free Calling**

This feature permits automatic rerouting of a toll free call to a predefined local PSTN number when an all trunks busy (ATB) condition at the destination egress trunks is encountered. This feature is similar to that of Cascade Routing. Therefore, it is associated with the same set of Functional Requirements.

*Functional Requirements – Restorability, Survivability/Endurability, Scaleable Bandwidth, Affordability, and Reliability/Availability*

#### **2.1.2.17.23 Service Assurance Rerouting for Toll Free Calling**

This feature permits inbound toll free calls to be routed to a predefined recorded announcement or defined telephone number, within five minutes, when a network problem(s) is encountered.

*Functional Requirements – Survivability/Endurability and Reliability/Availability*

#### **2.1.2.18 Service Level Agreements**

Service Level Agreements (SLAs) are contractual arrangements between service subscribers and service providers to provide incentives for the provider to meet specified and measurable performance levels. Although not a panacea for enlisting rapid restoration and maintaining the quality of service (QoS) of CSVS from service providers, SLAs, with severe penalties or advantageous incentives, could be negotiated with service providers to encourage them to quickly restore services under certain conditions and to maintain the QoS agreed upon. As a consequence of the SLA's terms, the service provider may install redundant equipment at diverse locations with rapid switch-over capability as well as configuring its network in such a manner to ensure QoS for CSVS services delivered.

*Functional Requirements – Restorability, Survivability/Endurability, and Reliability/Availability*

## **2.2 Circuit-Switched Data Services**

Circuit-Switched Data Services (CSDS) use TDM networks similar to those employed for the PSTN. However, these networks are designed for synchronous and full duplex data transmissions in increments of DS-0 levels. Similar to voice calls, data calls are placed via dialing. CSDS access may be provided to subscribers' locations via the Integrated Services Digital Network (ISDN) or "Switched 56 kilobits per second (kbps)" service. CSDS circuits may be used as temporary dial-backup circuits or circuits required for a short duration in place of a subscriber's normal packet- or cell-based service(s).

### **2.2.1 Functional Requirements Inherently Available with CSDS**

In today's telecommunications market, Circuit-Switched Data Services play a smaller role than they did about 15 years ago because they have been replaced by packet, i.e., Internet Protocol (IP) networks and cell networks such as frame relay (FR) and asynchronous transfer mode (ATM) networks. Nevertheless, in some instances CSDS may be useful to support NS/EP missions. Since CSDS networks are based on networks similar to those of the PSTN, CSDS can inherently support many of the same Functional Requirements as CSVS.

### **2.2.1.1 Restorability**

Like the PSTN, CSDS networks also rely on redundant and alternative paths, which may be employed to restore failed circuits. If a failure occurs on one connection path, in many instances, an alternative path is available from either the same service provider or from a different service provider. Network architectures allow very rapid automatic alternative routing to redundant backup paths.

Additionally, like with the PSTN, CSDS circuits are covered under TSP.

### **2.2.1.2 International Connectivity**

CSDS networks, like CSVS networks in the PSTN, are inherently designed to, and do, interconnect with foreign networks equivalent to those of the PSTN as implemented in North America. ITU standards are used. However, the digital hierarchy is different in North America from other parts of the world, e.g., Europe. Therefore, digital hierarchical conversion is needed for some International Connectivity arrangements.

### **2.2.1.3 Interoperability**

Analogous to CSVS networks in the PSTN, CSDS networks are comprised of interoperable CS TDM networks operated by numerous local and interexchange carriers. Interoperability is achieved by service providers' adherence to a set of standards, in part, from ANSI, Committee T1, and Telcordia.

### **2.2.1.4 Ubiquitous Coverage**

Since CSDS networks are widely deployed in North America and abroad, coverage is extensive and may be considered "nearly ubiquitous" for NS/EP purposes. Alternative forms of communications, such as satellite, usually are available for substitution.

### **2.2.1.5 Survivability/Endurability**

CSDS networks are generally considered to be Survivable and Enduring. Since they have the same architecture as the PSTN, their endurability results from the numerous interconnected CS TDM networks with many redundant and alternative paths available to make connections. A failed connection path, in many instances, may be substituted by an alternative path. Furthermore, NOCs constantly monitor and manage the operational health of CSDS networks.

### **2.2.1.6 Voice Band Service**

Circuit-Switched Data Services are not specifically designed for voice communications. However, these services do support Voice Band Service, such as in a video teleconference (VTC). In CS VTCs, voice information is transmitted using CSDS. The digitization (and compression) of the voice signal is performed in the terminal end equipment.

### **2.2.1.7 Broadband<sup>15</sup> Service**

Broadband service is available through CSDS because these services can be delivered in increments of DS-0 or DS-1 (E-1 for Europe, et al). Use of DS-0 and DS-1 inverse multiplexers<sup>16</sup> can aggregate individual DS-0 and DS-1 channels into much larger bandwidths.

### **2.2.1.8 Scaleable Bandwidth**

Since CSDS is offered in increments of DS-0 or DS-1, Scaleable Bandwidth is achievable. Subscribers may purchase the appropriate bandwidth for their purposes. With the use of inverse multiplexers, additional bandwidth may be aggregated as needed. An example is the need for variable bandwidth for a VTC. As the bandwidth requirement during a CS VTC grows beyond the baseline bandwidth set for the teleconference, additional DS-0 increments of bandwidth may be automatically dialed up, as required, and aggregated with existing DS-0 channels via the inverse multiplexer.

### **2.2.1.9 Affordability**

Like CSVS, CSDS is commercially available as commercial-off-the-shelf (COTS) services. Discounted pricing arrangements or special pricing packages, dependent upon the customer's usage of the CSDS, are available. Besides price, other parameters for determining Affordability are the service's reliability, availability, maintainability, and ease of implementation and operation. All these parameters affect the service's Affordability to the subscriber and should be determined on a case-by-case basis dependent upon the subscriber and its requirements. Hence, CSDS is considered an Affordable commodity.

### **2.2.1.10 Reliability/Availability**

Networks supporting CSDS are based on the same technologies as those which support the PSTN. Network architectures are also similar. For these reasons, CSDS has essentially the same Reliability and Availability as the PSTN. During periods of unavailability, alternative forms of communications usually are available for substitution.

## **2.2.2 CSDS Features Meeting Certain Functional Requirements**

Various functions and features associated with CSDS can be used to adapt these services to NS/EP uses and meet certain Functional Requirements. The following Subsections describe these functions and features along with an indication of the Functional Requirements they could support. Since CSDS is a dial-up service, some of the functions

---

<sup>15</sup> Broadband: 1. Synonym (in analog technology) wideband. 2. A descriptive term for evolving digital technologies that provide consumers a signal-switched facility offering integrated access to voice, high-speed data service, video-on-demand services, and interactive delivery services. (Glossary of Telecommunication Terms, <http://www.its.bldrdoc.gov/fs-1037>).

<sup>16</sup> Inverse multiplexers are telecommunication devices that split a single high-speed digital channel into multiple signals, transmitting each of the multiple signals over a separate facility operating at a lower data rate than the original signal, and then (at the terminating end) recombining the separately-transmitted portions into the original signal at the original rate.

and features mentioned for CSVS also apply, under certain conditions, to CSDS. However, other functions and features do not apply.

#### **2.2.2.1 Priority Dial Tone<sup>17</sup>**

This feature prioritizes the provision of dial tone to permitted lines only. Call attempts from such designated lines are placed in a priority queue and are handled before non-priority calls. No call marking is required.

*Functional Requirement – Enhanced Priority Treatment*

#### **2.2.2.2 Priority Call Setup Message<sup>17</sup>**

This feature provides priority call setup messages through the signaling network with the HPC identifier. It requires call marking.

*Functional Requirement – Enhanced Priority Treatment*

#### **2.2.2.3 Exemption From Restrictive Network Controls<sup>17</sup>**

This feature provides exemption from restrictive (network) controls, such as call gapping. It requires call marking. It provides a set of control measures used to prevent or control degradation of network service.

*Functional Requirements – Enhanced Priority Treatment and Survivability/Endurability*

#### **2.2.2.4 User Verification<sup>17</sup>**

This feature allows for the verification of the user authorized for priority handling of his/her calls. PINs, line identification, authorization codes, or call-back facilities could be used to verify the call as an authorized priority call. This feature may not be applicable for instances in which CSDS circuits are dialed up without human intervention, such as with automatic dialing using an inverse multiplexer.

*Functional Requirements – Enhanced Priority Treatment and Secure Networks*

#### **2.2.2.5 Authorization Codes<sup>17</sup>**

This feature applies unique multi-digit codes to allow an authorized user privileged access to a network. If the code is validated, the call is allowed to proceed.

*Functional Requirements – Enhanced Priority Treatment and Secure Networks*

#### **2.2.2.6 Automated Verification of Authorization Codes**

This feature permits verification of an authorization code, when used for the service, to occur without involving an operator before the service is provided.

*Functional Requirements – Enhanced Priority Treatment and Secure Networks*

---

<sup>17</sup> This information was extracted from the draft version of International Telecommunication Union Recommendation E.106.

#### **2.2.2.7 Suppression of Calling Number Delivery**

Based on the COS of the originating station or calling card, the service provider would inhibit the delivery of the calling number, i.e., ANI, by setting the Privacy Indicator at the originating end of the call and honoring it at the terminating end.

*Functional Requirement – Non-Traceability*

#### **2.2.2.8 Route or Path Avoidance**

This feature is equivalent to the same feature under CSVS. It allows a subscriber to define a geographic location or route to avoid in the transmission path of its communications.

*Functional Requirements – Secure Networks, Survivability/Endurability, and Reliability/Availability*

#### **2.2.2.9 Route or Path Diversity**

This feature is equivalent to the same feature under CSVS. It allows the user to require its service provider to establish diverse routes which do not share any common telecommunications facilities or offices, including a common building entrance. The service provider should provide the capability for the real-time automatic switching of transmission from the primary route to the one or more diverse route(s) and from the diverse route(s) to the primary route.

*Functional Requirements – Restorability, Survivability/Endurability, and Reliability/Availability*

#### **2.2.2.10 Dedicated Transmission**

This feature permits the user to order dedicated transmission facilities from its service provider. The dedicated transmission facilities may be ordered so as to avoid any active equipment, such as switching or DXC equipment. These facilities should have a higher availability and should not be susceptible from unauthorized intrusion into the SS7 signaling network or DXC control systems. However, the subscriber will be required to provide its own terminal equipment since the service provider is delivering only a digital pipe.

*Functional Requirements – Secure Networks, Survivability/Endurability, and Reliability/Availability*

#### **2.2.2.11 Call Screening**

Call screening comprises a set of features that determine a call's eligibility to be completed as dialed, based upon COS information associated with the user, the terminal device, or the trunk group.

*Functional Requirement – Enhanced Priority Treatment*

#### **2.2.2.12 Class of Service and Restrictions**

This feature permits the subscriber's service provider to establish a set of classes of service available to each user, terminal device, or trunk. The COS may be determined from ANI, authorization codes, traveling classmarks, or trunk groups. The COS derived from an authorization code may be set up to take precedence over that derived from other means.

*Functional Requirement – Enhanced Priority Treatment*

##### **2.2.2.12.1 Traveling Classmark**

This feature provides for the acceptance of traveling classmarks from all locations served by PBXs and Centrexes that are able to provide these classmarks, including calls extended by operators. Traveling classmarks should conform to the TCOS format (i.e., called number + TCOS). User calling characteristics and limitations may be determined from the traveling classmark.

*Functional Requirement – Enhanced Priority Treatment*

##### **2.2.2.12.2 Code Block**

This feature screens ineligible users, terminal devices, and trunks with certain COS access restrictions from calling specified area codes, exchange codes, and countries. Blocked calls could be intercepted to appropriate network recorded announcements.

*Functional Requirement – Secure Networks and Scaleable Bandwidth*

#### **2.2.2.13 Security Procedures**

Establishment of proper security procedures will permit the user to accomplish the following activities:

- a) Controlling access to user-related sensitive databases and information,
- b) Prevention of fraudulent use of user information or services.

*Functional Requirement – Secure Networks*

#### **2.2.2.14 Toll Free Calling**

This feature permits authorized users to dial certain numbers using service access codes, such as 800, 888, 877, etc., to complete toll free and message unit-free (to the callers) directory numbers. In a manner similar to voice calls, toll free calling can support CSDS. The toll free service provider may, or may not, supply network intercepts to recorded announcements as a network capability when a call cannot be completed. For NS/EP purposes, a subscriber could provide toll free CSDS calling to certain locations.

An example of such usage would be to connect personnel in the field, via dial-up connections, with a home location to access databases or other information sources. These calls could be made via toll free numbers in order to avoid having the field personnel pay the connection costs.

*Functional Requirement – Affordability*

**2.2.2.14.1 Routing Control for Toll Free Numbers**

This feature permits the subscriber to review, create, validate, change, or execute his call routing plans via a terminal located at the subscriber's premises. This feature permits the NS/EP subscriber to direct the toll free calls to certain locations of the subscriber's choosing. This flexibility permits the subscriber to provide better service to its users. In some cases, the routing flexibility could be employed to avoid locations that were damaged by an emergency or disaster. In this sense, the routing flexibility improves the Availability and the Survivability of the NS/EP services being provided by the subscribing organization in addition to the Affordability offered by toll free calling.

*Functional Requirements –Survivability/Endurability, Affordability, and Reliability/Availability*

**2.2.2.14.2 NPA/NXX Routing for Toll Free Calling**

This feature permits calls originating from within subscriber-selected geographic areas, defined by one or more NPA codes and/or NPA/NXX combinations, to be routed to a subscriber specified location. When an NPA/NXX is not available, calls are to be routed to a subscriber's default location. In a disaster or emergency, the default destination location(s) may be unavailable for use. This feature provides for Survivability of the Affordable toll free calling service as well as improving the Reliability and Availability of the service.

*Functional Requirements –Survivability/Endurability, Affordability, and Reliability/Availability*

**2.2.2.14.3 ANI-Based Routing for Toll Free Calling**

This feature permits calls to be routed based on the full ANI of the callers. Default routing defined by the subscriber could be used if ANI is not available.

*Functional Requirements –Survivability/Endurability, Affordability, and Reliability/Availability*

**2.2.2.14.4 Command Routing for Toll Free Calling**

This feature permits a subscriber that has subscribed to one or more of the above toll free routing features to route calls differently (i.e., select a different predefined routing path alternative) on command at any time. As a consequence of this feature's applicability to the other toll free routing features, it supports several Functional Requirements.

*Functional Requirements – Restorability, Survivability/Endurability, Scaleable Bandwidth, Affordability, and Reliability/Availability*

**2.2.2.14.5 Cascade Routing for Toll Free Calling**

This feature permits the destination of calls to be changed on a subscriber-defined predetermined basis based on the availability of egress circuits at the subscriber's original

destination. As a function of the bandwidth (number of circuits) available in the egress circuits at the destination for toll free calls, the subscriber can prearrange alternate destination locations. This feature would be very useful in cases in which some of the egress lines to the subscriber's default destination locations were made unavailable due to an emergency or disaster.

*Functional Requirements – Restorability, Survivability/Endurability, Scaleable Bandwidth, Affordability, and Reliability/Availability*

#### **2.2.2.14.6 Network Queuing for Toll Free Calling**

This feature is a hybrid routing/announcement feature that allows a caller to be held in queue in the service provider's network until a subscriber's terminating equipment becomes available to receive the call. Consequently, the incoming call is given a form of Enhanced Priority Treatment to ensure that it gets answered and not dropped. This queue hold would have to be compatible with the subscriber's terminal data equipment and inverse multiplexer.

*Functional Requirement – Enhanced Priority Treatment and Affordability*

#### **2.2.2.14.7 Agency Based Routing Database for Toll Free Calling**

This feature permits queries to a subscriber-provided call routing processor which will allow call-by-call routing based upon information returned from the subscriber's call routing processor. This feature provides capabilities similar to those mentioned above for other toll free calling. Hence, is associated with the same set of Functional Requirements.

*Functional Requirements – Restorability, Survivability/Endurability, Scaleable Bandwidth, Affordability, and Reliability/Availability*

#### **2.2.2.14.8 Dialed Number Identification for Toll Free Calling**

This feature allows a user with multiple toll free numbers in the same service group to identify electronically the specific toll free number that was dialed by the calling party. This information could be useful in determining whether malicious calls are being dialed to overload the subscriber's system resulting in denial of service for legitimate callers in addition to the Affordability offered by toll free calling.

*Functional Requirement – Secure Networks and Affordability*

#### **2.2.2.14.9 Call Status Report for Toll Free Calling**

This report provides the subscriber with information about the status of calls placed to each of its toll free numbers. This report provides statistics as to how the toll free services are performing and are being used. The statistics may be useful for determining whether call overload attempts are occurring and whether any malicious calls have impaired service. Therefore, the information could be applied to ensuring the Security of the service provider's network as well as assuring Reliability and Availability of the toll free service.

For any given toll free number, the subscriber may request its service provider to provide the following information within the reports:

- a) The number of calls from each area code that dialed the toll free number (i.e., call attempts),
- b) The number of calls and the percentage of all calls that encounter a busy signal (i.e., that are blocked):
  - a. In the service provider's network,
  - b. At the user's terminating access.
- c) The number of calls offered to the user's terminating access (i.e., egress trunk group),
- d) The number of calls received at each user's terminating access,
- e) The number of received calls at each user's terminating access that resulted in successful answerback supervision,
- f) The average duration of calls answered at each user's terminating access, and
- g) The average duration of all calls answered for a given toll free number at all users terminating access serving the toll free number

*Functional Requirement – Secure Networks and Reliability/Availability*

#### **2.2.2.14.10 Caller Profile Report for Toll Free Calling**

This report, with the following parameters, can provide useful information about the status of toll free calls in the network. As such, the statistics may be useful for determining whether call overload attempts are occurring, identifying the number(s) from which they originate, and whether the malicious calls have impaired service. Therefore, the information could be applied to ensuring the Security of the service provider's network as well as assuring Reliability and Availability of the toll free service. The statistics that should be reported are:

- a) Lost Callers: The number of callers who never called back after an incomplete attempt during the reporting period.
- b) Average Number of Attempts Per Caller: The grand total number of call attempts divided by the number of first call attempts during the reporting period.
- c) Average Number of Contacts Per Caller: The number of attempts generated from each telephone number on average during the reporting period.
- d) 50 Percent of Successful Attempts Within 1,000 Calls: This statistic represents the number of attempts required to access the network for 50 percent of the callers who completed calls.
- e) 75 Percent of Successful Attempts Within 1,000 Calls: This statistic represents the number of attempts required to access the network for 75 percent of the callers who completed calls.

*Functional Requirement – Secure Networks and Reliability/Availability*

#### **2.2.2.14.11 Caller Information Report for Toll Free Calling**

This report provides information about the ANI of all callers to a given toll free number. For any given toll free number, the subscriber may request its service provider to provide the following information within the reports:

- a) Date of call,
- b) Time of call (expressed using either a 24 hour clock or a 12 hour clock with an AM/PM indicator and indicating time zone),
- c) ANI of caller (if available),
- d) Dialed (i.e., destination) 10 digit number,
- e) Duration of call (to the nearest 6 seconds), and
- f) Disposition of call (i.e., using an alpha or numeric code to include, at a minimum, the following:
  - a. Call blocked within service provider's network,
  - b. Call blocked at subscriber's terminating access,
  - c. Call completed to subscriber's terminating access, and
  - d. Other (e.g., call abandoned enroute to subscriber's terminating access, no answer back supervision received, etc.)

These statistics may be useful for determining whether call overload attempts are occurring, identifying the number(s) from which they originate, and whether the malicious calls have impaired service. Therefore, the information could be applied to ensuring the Security of the service provider's network. The information may also be applicable for determining the necessity of additional trunk (or bandwidth) capacity relative to Scaling the network's bandwidth and for determining the Reliability/Availability of the network.

*Functional Requirements – Secure Networks, Scaleable Bandwidth, and Reliability/Availability*

#### **2.2.2.14.12 Real-Time Call Status for Toll Free Calling**

This feature permits the subscriber of the toll free service to receive information about the status of toll free calls in progress on a near real-time (e.g., refreshed within five minutes) basis. This information may be of use in determining if malicious calls are attempting to overload the subscriber's toll free call or response centers and for determining the Reliability/Availability of the network.

*Functional Requirement – Secure Networks and Reliability/Availability*

#### **2.2.2.14.13 Basic ATB Rerouting for Toll Free Calling**

This feature permits automatic rerouting of a toll free call to a predefined local PSTN number when an ATB condition at the destination egress trunks is encountered. This feature is similar to that of Cascade Routing. Therefore, it is associated with the same set of Functional Requirements.

*Functional Requirements – Restorability, Survivability/Endurability, Scaleable Bandwidth, Affordability, and Reliability/Availability*

#### **2.2.2.14.14 Service Assurance Rerouting for Toll Free Calling**

This feature permits inbound toll free calls to be routed to a predefined recorded announcement or defined telephone number, within five minutes, when a network problem(s) is encountered. This feature may be useful for CSDS, but the presence of human intervention to establish the call is needed.

*Functional Requirements –Survivability/Endurability and Reliability/Availability*

#### **2.2.2.15 Service Level Agreements**

Service Level Agreements (SLAs) are contractual arrangements between service subscribers and service providers to provide incentives for the provider to meet specified and measurable performance levels. Although not a panacea for enlisting rapid restoration and maintaining QoS of CSDS services from service providers, SLAs, with severe penalties or advantageous incentives, could be negotiated with service providers to encourage them to quickly restore services under certain conditions and to maintain the QoS agreed upon. As a consequence of the SLA's terms, the service provider may install redundant equipment at diverse locations with rapid switch-over capability as well as configuring its network in such a manner to ensure QoS for CSDS services delivered.

*Functional Requirements – Restorability, Survivability/Endurability, and Reliability/Availability*

### **2.3 Packet-Switched Data Services**

Packet-Switched Data Services (PSDS) comprise the set of services provided via packet- (or cell-based) digital networks. These types of networks provide various connectionless and connection-oriented paths through the network over which individual packets or cells travel. All packets created for a particular session are reassembled at the destination into the original communication transmitted from the origination point. Packet technology in modern networks is supported primarily by the Internet Protocol. Hence the term "IP networks". Cell networks are based on FR and ATM.

PSDS networks are beginning to replace both CSVS and CSDS networks as part of the "convergence" phenomenon. Telecommunications services formerly supported by CSVS and CSDS are now evolving into services supported solely on PSDS networks, in large part by IP networks or IP-enabled FR and ATM networks.

#### **2.3.1 Functional Requirements Inherently Available with PSDS**

The migration of services from traditional CS TDM networks onto these packet (or cell) networks has caused some concern in the NS/EP community since some of the key Functional Requirements, like Enhanced Priority Treatment, need to be adopted to these new networks. For instance, GETS is designed to work on only the PSTN. A different

approach is needed when telephone calls requiring priority treatment will be handled by packet (or cell) networks in the future.

PSDS can inherently support the following Functional Requirements.

### **2.3.1.1 Enhanced Priority Treatment**

In the context of PSDS, protocols have been developed in order to minimize latency for packet delivery in IP networks. Instead of forwarding packets on a “best effort” basis alone, as is done in normal packet traffic handling, priorities can be assigned to packets or network bandwidth can be reserved.

For example, Differentiated Services, or DiffServ, is a protocol by which the priority of packets can be set before they are forwarded through the network. The Differentiated Services marker in the packet header places the packet ahead in the routing queue of other packets not so marked. However, with current implementations, individual packet services can not be tagged for end-to-end priority treatment. This situation arises because each domain that the packet travels through may classify and treat the packet differently, making completely reliable end-to-end priority routing nearly impossible. Until interdomain quality of service is achieved, end-to-end packet priority will not be completely feasible.<sup>18</sup>

A technique to reserve bandwidth in the network is the use of the Resource Reservation Protocol (RSVP). Through RSVP, a user’s QoS requests are propagated to all routers along the packets’ path. This protocol establishes flows through the network.

Within an ATM or FR network, packet Virtual Circuits (VCs) could be designated. A higher priority VC would receive preferential treatment over a lower priority VC in terms of delay and guarantee of delivery (if a possibility of discard exists) during network congestion. Higher priority traffic would be delivered ahead of lower priority traffic and would be discarded only after all lower priority traffic had been discarded.

Although protocols and VCs can provide individual packets and cells with routing priorities or networks with reserved bandwidths, the call setup for a priority voice over IP (VoIP) call, in a manner similar to that established for PSTN calls via GETS, does not yet exist. In this sense, the Functional Requirement of Enhanced Priority Treatment is not met using PSDS. Such implementations remain to be developed.

To this end, the Internet Engineering Task Force (IETF) is developing a plan for prioritizing voice and data communications sent via the Internet in the event of a disaster. The IETF body looking into these issues is the Internet Emergency Preparedness Working Group. The Working Group's goal is to determine how the Internet can give Enhanced Priority Treatment to NS/EP communications in a manner similar to that

---

<sup>18</sup> *National Security Telecommunications Advisory Committee (NSTAC) Legislative and Regulatory Task Force Report*, March 2002

provided by GETS. The Working Group will create three standards documents that outline the requirements for emergency communications over the Internet, a framework for meeting those requirements, and advice for using Internet protocols to handle emergency communications. The Working Group expects the documents to be completed by August 2002. Members of the IETF's Emergency Preparedness Working Group say they can meet the GETS requirement by tapping existing signaling standards such as the Session Initiation Protocol (SIP), which is used to initiate VoIP calls, and Differentiated Services which can differentiate among classes of network traffic.<sup>19</sup>

One other approach to provide priority treatment to packets is the use of Multi-Protocol Label Switching (MPLS). MPLS integrates the capabilities of Layer 3 routing and Layer 2 switching. Packet priorities can be assigned via the labels. MPLS simplifies packet forwarding by decoupling packet forwarding from routing control, permitting routing to occur without affecting the packet forwarding hardware. MPLS extends the IP control plane to connection-oriented technology by integrating Layer 2-type traffic engineering into the scalability and flexibility afforded by IP traffic routing. MPLS is designed to eliminate the need to look up IP addresses in every node along the path. MPLS can be used for explicit routing, fast rerouting, "hard" quality-of-service constraints, and for routing with non-unique addresses, such as in setting up private user groups in Virtual Private Networks (VPNs)<sup>20</sup>. This technology helps deliver highly scalable, differentiated end-to-end IP services with simplified configuration, management, and provisioning.

The fundamental concept of MPLS is to add a fixed-length, short label to each packet with switching devices performing table lookups to determine where the data should be forwarded. An edge Label Switch Router (LSR), located at the edge of the network, does a complete analysis of the Layer 3 header, maps the header into a fixed label, and then for each of the down-stream routers across the network, only the label is examined in the inbound packet (or cell) as it traverses across the network (i.e., no routing protocol translation is needed) over a Label Switched Path (LSP). At the other end of the network, an edge LSR converts the label back into the appropriate header data linked to that label. This approach allows routing to be achieved through a single look-up table using a label as a table index and makes it feasible for routers and switches to determine forwarding paths based on multiple destination addresses. Many different headers can map to the same label, as long as those headers always result in the same choice of next hop.<sup>21</sup>

Results of interviews conducted for this study indicate interest in establishing priority treatment for PSDS. The position of Mr. Howard Foltz of the OMNCS is that NS/EP

---

<sup>19</sup> *IETF Plans Emergency System for Internet*, Carolyn Duffy Marsan, Network World Fusion, March 20, 2002

<sup>20</sup> A virtual private network is a private data network that makes use of the public telecommunications infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

<sup>21</sup> The description of MPLS is extracted from the article, *Internet Protocol Over Optics: A Robust and Simplified Network of the Future*, by Louis J. Ansaldi in *The Telecommunications Review* (2001) copyright 2001 Mitretek Systems.

priorities must, in some way, be implemented on the Internet. Such priorities would support VoIP and other multimedia priority calling. Mr. Bernard Farrell of the National Coordinating Center (NCC) for Telecommunications strongly recommends that Enhanced Priority Treatment be made available for all technologies supporting NS/EP activities.

### **2.3.1.2 Non-Traceability**

Although not applicable to all PSDS, Non-Traceability can be achieved for e-mail services. The address of the originator of the e-mail message may be hidden by passing the message through an e-mail service provider which strips off the originating address and then forwards the message to the intended recipient.

### **2.3.1.3 Restorability**

PSDS networks are comprised of redundant and alternative transport paths which may be employed to restore failed circuits. At the transport circuit level of PSDS networks, alternative paths are available from either the same service provider or from a different service provider. As with CSVS and CSDS, PSDS network architectures allow very rapid automatic alternative routing to redundant transport backup paths.

While TSP could apply to services that use the PSDS network cloud for transmission, such as the case with FR<sup>22</sup>, priority treatment within the network cloud is difficult under the methods envisioned in the TSP rules. This situation creates uncertainty as to whether the rules can be, or practically need to be, applied to the converging and Next Generation Network (NGN) environments using PSDS. Current TSP rules mandate only that common carriers provide TSP services. However, those non-common carrier service providers who elect to participate in the TSP Program may consent to be bound by the TSP Priority requirements.<sup>23</sup>

In addition, the packet- and cell-based technologies are inherently designed to offer alternative routing paths to packets and cells. Hence, if one portion of the network is inoperative, a high likelihood exists that packets and cells can automatically be rerouted around the inoperative portion. Although performance may be impaired, such as would be evidenced by increased packet or cell latency, communications can still be accomplished. However, this inherent capability for rerouting may be negated if permanent virtual circuits (PVCs) are established and routed over the damaged portion of the network. Unless the affected PVCs can be rerouted around the damaged network portion, PSDS may remain unavailable.

As a result of interviews, Mr. John Jolicoeur, Senior Emergency Response Coordinator of the Nuclear Regulatory Commission (NRC), said TSP will be different but still critical

---

<sup>22</sup> In the case of Frame Relay, TSP is provided on the physically identifiable portions of the circuit. If problems occur with the equipment within the cloud, that equipment is replaced or the permanent virtual circuit is rerouted.

<sup>23</sup> NSTAC Legislative and Regulatory Task Force draft report, *January 14, 2002*

for the converged packet- and cell-based networks. By this comment, he meant that TSP procedures need to be applied to the packet transport circuits supporting the converged data network services, as is currently being done for the PSTN circuits. Similarly, Mr. Bernard Farrell said that TSP must be included in the requirements for NS/EP priorities on the Internet.

#### **2.3.1.4 International Connectivity**

International Connectivity among PSDS networks has been extensively implemented. The Internet is a principal example. IP network interconnections are made at Network Access Points (NAPs), such as Metropolitan Area Exchange (MAE) East and MAE West, as well as directly between IP service providers. Consequently, packet-based voice, video, and data services can seamlessly interoperate across many countries' borders. Limitations on interconnectivity, however, may result by deliberate blockage of these interconnections for political, and not technical, reasons.

#### **2.3.1.5 Interoperability**

As with International Connectivity, Interoperability of PSDS networks has been extensively implemented. NAPs and bilateral interconnection arrangements, i.e., "peering" and "transit" arrangements, accomplish Interconnectivity and Interoperability.

"Peering" is an agreement between Internet Service Providers (ISPs) to carry traffic for each other and for their respective customers. Peering is usually a bilateral business and technical arrangement, in which two providers agree to accept traffic from one another and from one another's customers (and thus from their customers' customers). Peering does not include the obligation to carry traffic to third parties.<sup>24</sup>

"Transit" is an agreement in which an ISP agrees to carry traffic on behalf of another ISP or end user. In most cases, transit will include an obligation to carry traffic to third parties. Transit is usually a bilateral business and technical arrangement, in which one provider (the "transit provider") agrees to carry traffic to third parties on behalf of another provider or an end user (the "customer").<sup>25</sup>

#### **2.3.1.6 Ubiquitous Coverage**

As with networks supporting CSVS and CSDS networks, PSDS networks are widely deployed in many countries, including extensive deployment in the US. Therefore, PSDS may be considered to be "nearly ubiquitous". For locations in which wireline PSDS is not available, alternative forms of communications, such as satellite and third generation (3G) wireless services, are available for substitution.

---

<sup>24</sup> *Service Provider Interconnection for Internet Protocol Best Effort Service*, Network Reliability and Interoperability Council V, Focus Group 4: Interoperability, Annex B

<sup>25</sup> *Service Provider Interconnection for Internet Protocol Best Effort Service*, Network Reliability and Interoperability Council V, Focus Group 4: Interoperability, Annex B

### **2.3.1.7 Survivability/Endurability**

Packet- and cell-based data networks supporting PSDS are extensive and interconnected, thereby promoting the Survivability and Endurability of PSDS. Wire and fiber optic cable plants afford diverse routing. Many service providers have bi-lateral agreements permitting them to share one another's cable plants during emergencies, with automatic cutover capability in place. Automatic, and nearly instantaneous, rerouting has been implemented in many of these networks, such as that available with SONET. By design, the Internet is a meshed network using packet routing protocols that automatically support diverse routing of packets from origination to destination. Hence, the loss of a particular section of the infrastructure does not necessarily inhibit packet transmissions. As with CS networks supporting CSVS and CSDS, service providers' NOCs can implement manual traffic rerouting.

### **2.3.1.8 Voice Band Service**

PSDS networks are increasingly being used to support voice band communications. VoIP and IP-based video teleconferencing are gaining popularity among enterprises and for use by the public over the Internet or private IP networks. Numerous switch manufacturers are now developing products employing an ATM network fabric for their tandem (Class 4) and end office (Class 5) softswitches. As service providers begin offering Voice Band Service via their PSDS networks, the functions and features now available in CS networks, such as the PSTN, must be implemented in these PSDS networks as well.

### **2.3.1.9 Broadband Service**

PSDS networks inherently have the capability to provide Broadband Service in increments of  $N \times 64$  kbps, in which  $1 < N \leq 24$ . PSDS networks can also support bandwidths in increments of DS-1, E-1, DS-3, and optical carrier (OC) levels.

### **2.3.1.10 Scaleable Bandwidth**

Since PSDS networks can provide service in various bandwidth increments, they inherently have the capability to provide Scaleable Bandwidth. For instance, an ATM service could support bandwidth-on-demand (BOD) capability by allocating incremental bandwidths in response to a user's demand for additional bandwidth. For the packet-mode of data transfer, BOD would be initiated automatically by sending an increased number of packets.

For PSDS networks, bandwidth can be supplied under various conditions, such as:

- a) Variable Bit Rate (VBR),
- b) Constant Bit Rate (CBR),
- c) Available Bit Rate (ABR),
- d) Unspecified (or Undefined) Bit Rate (UBR),
- e) Sustainable Cell Rate (SCR), and
- f) Committed Information Rate (CIR).

#### **2.3.1.11 Affordability**

Packet-Switched Data Services are COTS, readily available in the US, and, accordingly, Affordable. Besides price, other parameters for determining Affordability are the service's reliability, availability, maintainability, and ease of implementation and operation. All these parameters affect the service's Affordability to the subscriber and should be determined on a case-by-case basis dependent upon the subscriber and its requirements.

#### **2.3.1.12 Reliability/Availability**

The Reliability and Availability of commercial PSDS networks may not be as high as those of the PSTN. The subscriber may overcome this deficiency by owning and operating its own PSDS network which the subscriber designs to suitably high Reliability and Availability levels. Since the subscriber would have control over its own network, it could ensure sufficiently reliable operation.

If the PSDS network were not controlled by the subscriber, the subscriber may need to invoke enforceable SLAs in its contract with its PSDS service provider. Through SLAs, the subscriber could encourage its service provider to meet reliability, availability, and QoS levels necessary to meet the subscriber's NS/EP requirements. Such SLAs should be written such that the service provider would find supplying satisfactory service to be to its financial advantage via stringent penalties and advantageous incentives. However, no guarantee exists that a service provider would act in the public's best interest and give priority to NS/EP contracts over those for favored commercial customers.

### **2.3.2 PSDS Features Meeting Certain Functional Requirements**

Various functions and features associated with PSDS can be used to adapt these services to NS/EP uses and meet certain Functional Requirements. The following paragraphs describe these functions and features along with an indication of the Functional Requirements they could support.

#### **2.3.2.1 Dedicated Transmission**

This feature permits the service user to order dedicated transmission facilities from its service provider. For PSDS, dedicated transmission facilities could be used by the subscriber to construct its own PSDS network and avoid any common carrier's network. FR, IP, and ATM networks could be so constructed. Since the user would own, operate, and manage its own network, the reliability, availability, operational integrity, and security of the network may be higher than that from a common carrier or other service provider.

In addition, dedicated access facilities could be used to connect directly to a PSDS service provider's network. Such a connection would allow the subscriber to have a dedicated connection to the PSDS service provider and not use any public network facilities with the associated decrease in reliability, availability, and security.

Three varieties of dedicated transmission may be ordered:

- a) Point-to-Point: A dedicated connection between two points.
- b) Point-to-Multipoint: Connections from one point to three or more points.
- c) Multipoint: Connections among three or more points.
  - a. Branch-Off mode: A form of multipoint connection in which all points are treated as if they are in one shared medium with the ability of autonomous sending and receiving of data by each point. The customer premises equipment (CPE) application should ensure a master/slave mode of operation.
  - b. Drop-and-Insert: A form of multipoint connection in which channels of a channelized digital hierarchical signal, such as DS-1, DS-3, or SONET Optical Carrier Level 3 (OC-3)<sup>26</sup> or higher, should be able to be extracted and simultaneously new channels able to be inserted.

*Functional Requirements – Secure Networks, Survivability/Endurability, and Reliability/Availability*

#### **2.3.2.2 Route or Path Avoidance**

This feature is equivalent to the same feature under CSVS for dedicated PSDS transport circuits. This feature allows the subscriber to require its service provider to establish a geographic location or route to avoid in the transmission path of the subscriber's communications.

*Functional Requirements – Secure Networks, Survivability/Endurability, and Reliability/Availability*

#### **2.3.2.3 Route or Path Diversity**

This feature is equivalent to the same feature under CSVS for dedicated PSDS transmission circuits. It permits the subscriber to require its service provider to establish two or more diverse and physically separated routes which do not share any common telecommunications facilities or offices, including a common building entrance.

The service provider should provide the capability for the real-time automatic switching of transmission from the primary route to the one or more diverse route(s) and from the diverse route(s) to the primary route.

*Functional Requirements – Restorability, Survivability/Endurability, and Reliability/Availability*

#### **2.3.2.4 Security Procedures**

Establishment of proper security procedures will permit the user to accomplish the following activities:

---

<sup>26</sup> OC-3 has a bit rate of 155.52 Mbps.

- a) Controlling access to user-related sensitive databases and information and
- b) Prevention of fraudulent use of user information or services.

*Functional Requirement – Secure Networks*

**2.3.2.5 Service Level Agreements**

A contractual approach to provide incentives for the service provider to meet specified and measurable performance levels is to establish SLAs for the performance of interest. As mentioned for CSVS and CSDS, SLAs should be negotiated with the PSDS service provider to encourage the provider to quickly restore services under certain conditions and to maintain the QoS agreed upon.

*Functional Requirements – Restorability, Survivability/Endurability, and Reliability/Availability*

**2.3.2.6 Security Features**

PSDS networks need to have security features implemented within them in order to provide necessary security. Such networks are not inherently secure, especially those like the Internet which are accessible by the public. These networks are considered to be “untrusted”. Data security using public packet networks, like the Internet, requires special precautions to be taken.

Protection of private PSDS networks connected to public, untrusted PSDS networks can be achieved, in part, through “firewalls”. Firewalls should provide, as a minimum, the following capabilities.

- a) The ability to filter both incoming and outgoing traffic,
- b) A filter definition language consisting of a set of logging and reporting tools for per-port and per-socket management and administration,
- c) Provision of preconfigured checks for known methods of attack,
- d) Application specific forwarding capability (e.g., Telnet/File Transfer Protocol [FTP] only), and
- e) Support of encrypted tunneling.

Some level of security can be achieved via isolation from public access of a private and trusted PSDS network. This is the concept being investigated for the GovNet network. The extent of the isolation has an effect on the level of security attainable.

A solution to obtain some degree of security within an untrusted network is to create VPNs. VPNs may be created within IP, FR, and ATM networks. The IP Security (IPSec)<sup>27</sup> protocol may be employed with these VPNs.

---

<sup>27</sup> IPsec is designed to provide interoperable, high quality, cryptographically based security. These services are provided at the IP layer, offering protection for IP and/or upper layer protocols.

Additional security can be achieved via encryption of the communications at its origination and destination locations. Such encryption may require the handling of security keys and certificates, thereby increasing the administrative load on the organization employing these security techniques.

Finally, private PSDS networks can have their security enhanced by limiting access to the networks by organizations and individuals outside of and inside the organization(s) operating the networks. Statistics have shown that many security breaches of networks occur from within the organizations operating the networks. Therefore, restricting the number and categories of individuals accessing the network's controls should statistically reduce the risk of security breaches.

*Functional Requirement – Secure Networks*

### **3 NON-WIRELINE SERVICES**

Non-Wireline Services include all Telecommunications Services comprised in whole or in part of free space radio frequency (RF) or optical radiation. Although most of the systems supporting these Telecommunications Services also have a wireline component, the distinction between them and Wireline Services is made because the RF or optical component represents a significant difference in how information is transported.

The Non-Wireline Services discussed in this section are separated into the following categories:

1. Wireless, also termed Cellular and Personal Communications Service (PCS),
2. Paging and Short Text Services (as a separate and distinct component of Wireless Services),
3. Local Multipoint Distribution System (LMDS) and Multipoint Multichannel Distribution System (MMDS),
4. Wireless Local Area Network (WLAN) and Personal Area Network (PAN),
5. Satellite Services, and
6. Land Mobile Radio (LMR) and Two-Way Mobile Radio Products and Services.

For each Functional Requirement, the study discusses how the Functional Requirement is met, or not met, by that particular Non-Wireline Service category.

#### **3.1 Description of Non-Wireline Service Categories**

##### **3.1.1 Wireless Services**

Wireless Services have proven indispensable for support of NS/EP events. Typically, they are the first Telecommunications Service called upon if the wireline PSTN infrastructure is damaged or destroyed.

The first generation, or “1G”, of wireless voice telephone services used the analog Advanced Mobile Phone System (AMPS) technology. Due to a growing user base and the constraints AMPS placed on the number of simultaneous voice calls the system could handle, a set of second generation, or “2G”, Wireless Services evolved using various digital technologies.<sup>28</sup> In addition to voice calling, 2G services support limited data transmission rates of between 9.6 kbps and 19.2 kbps. “2.5G” Wireless Services are an extension of the current 2G services and, in addition to voice calling, offer data transmissions between 57.6 kbps and 115.2 kbps. The next generation, i.e., third generation “3G”<sup>29</sup>, wireless networks promise data speeds of about 384 kbps when a device is stationary or moving at pedestrian speed, 128 kbps in a car, and 2 Mbps in fixed

---

<sup>28</sup> The digital technologies were Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), and Global System for Mobile Communications (formerly Groupe Speciale Mobile) or GSM.

<sup>29</sup> 3G networks will be based on Wideband Code Division Multiple Access (WCDMA), which is an evolution of GSM, and CDMA 2000.

applications. 3G-based services will supply Internet and extranet access for data as well as supporting voice, video, and multimedia applications.

### **3.1.2 Paging and Short Text Services**

Paging services may be delivered via Satellite and Wireless Services. Certain Satellite Services provide two-way paging. Iridium Global Paging Service, for instance, offers global paging and messaging services via satellite. Similarly, certain Wireless Services can also deliver pages to their wireless customers. Motient offers paging and messaging services through its two wireless products, eLink and Blackberry. Often short text messages can accompany pages, whether they are delivered via Satellite or Wireless Services.

Narrowband Personal Communications Services (NPCS) provide terrestrial advanced messaging and paging services and operate in the 900 Megahertz (MHz) band. With the lowering cost of broadband PCS phones and services that have Short Message Service (SMS), paging services are no-longer as widely utilized as they were several years ago. Two principal NPCS providers are Mtel and PageNet, which have already built sizeable domestic networks.

### **3.1.3 LMDS and MMDS**

LMDS was originally intended as a “wireless loop” technology. The service could be used for point-to-point access between geographically closely located points. During an emergency, this technology could be applied to temporarily bypass damaged or destroyed wireline or other wireless infrastructures to provide connectivity to the PSTN or packet networks. As an example, WinStar<sup>30</sup>, a Competitive Local Exchange Carrier (CLEC), offered LMDS as a means to bypass the local Incumbent Local Exchange Carrier (ILEC) in many major markets. In New York City, this service was used after the attacks on the WTC to bypass the destroyed wireline telephone infrastructure.

LMDS can be provided based on microwave (in the 24-38 GHz band) or on the newer free space optics, i.e., laser, technology. Canon offers their free space optics Canobeam product with data rates achievable from 10 Mbps to 1.25 Gigabits per second (Gbps) with operational distances ranging from 500 meters to 2 kilometers, depending on the product. Terabeam<sup>™</sup> offers a point-to-multipoint product with a 1 mile range. AirFiber<sup>®</sup> offers a product operating at 622 Mbps that can be incorporated into a multipoint-multipoint mesh network with a 1500 ft range. Microwave, in this context, is used as a point-to-point replacement for wireline connectivity. Telecommunications carriers use microwave transmission paths extensively where wireline facilities are not readily available. Current technology allows for microwave links to operate at speeds of up to OC-3. Multiple links can be implemented to handle higher capacity requirements.

---

<sup>30</sup> WinStar’s assets have been purchased by IDT after WinStar declared bankruptcy.

MMDS offers a similar technology for bi-directional data, video, and voice services at speeds of up to 10 Mbps. It is used for point-to-multipoint in a broadcast mode or for two-way communications in a point-to-point mode. As such, it is sometimes referred to as “wireless cable”. Sprint and WorldCom have acquired licenses in the 2.5 GHz band to provide high speed fixed Wireless Services in competition with technologies such as Digital Subscriber Line (DSL) and cable. The first generation of MMDS operated as line of sight (LOS), but the next generation will not require LOS. As with LMDS, MMDS has an application during emergencies as a means to provide temporary high bandwidth telecommunications if the permanent telecommunications infrastructure is unavailable.

When LMDS and MMDS operate in the microwave band, they can experience range limitations due to signal absorption effects from vegetation (trees and foliage), obstructions (buildings and terrain), and precipitation (rain and snow). When LMDS operates using laser technology, signal attenuation can be experienced due to precipitation and LOS (visual) blockage.

#### **3.1.4 WLAN and PAN**

Current WLANs primarily use the IEEE 802.11b standard, which offers data rates up to 11 Mbps and operate in the 2.4 GHz band. Coverage is limited to about 100 meters but may be less due to walls and floors. The IEEE 802.11a standard using the 5 GHz band and 802.11g standard using the 2.4 GHz band are anticipated to provide data rates up to 54 Mbps.

WLAN technology can be quite useful when employed in support of NS/EP activities. For instance, a WLAN could be configured relatively quickly for a Disaster Field Office (DFO). Networked equipment could be interconnected using a WLAN much more easily than having to run cables throughout the DFO. A WLAN would be very convenient if the DFO consisted of separate distributed enclosures in a small campus setting. Local Area Network (LAN) cabling among the enclosures could be avoided.

The advantage of PANs is that they eliminate the need for short-distance hardwire connections. One technology for PANs utilizes a protocol stack called “Bluetooth”. This RF technology is designed to connect electronic devices which are no more than 10 meters apart. For instance, Bluetooth would be used to connect a personal digital assistant (PDA) or laptop to a mobile phone without the use of cables. Bluetooth employs radio frequency hopping among 79 channels 1,600 times per second in the 2.45 GHz band. Bluetooth operates in three different power ranges, i.e., 1) Class 1 with a power up to 100 milliwatt (mW) and a range up to 100 meters, 2) Class 2 with 1 – 2.5 mW for a 10 meter range, and 3) Class 3 with 1 mW for a range of 0.1 - 10 meters. The theoretical maximum data rate is 1 Mbps. Bluetooth can be used to form “ad hoc”<sup>31</sup> networks of several (up to eight) devices, called “piconets”.

---

<sup>31</sup> “Ad hoc” means that the networks are formed “on-the-fly” without a fixed infrastructure.

PANs also employ the Infrared Data Association (IrDA) standard, which allows PDAs to send and receive applications from other devices using infrared signals. PANs using the IrDA standard operate just like the remote controls for a television or video cassette recorder. Signals can bounce off walls and direct line of sight is not required. These devices are very low power and operate over a very short distances (tens of feet).

A new technology called Ultra-Wideband (UWB) was approved for limited commercial use by the Federal Communications Commission (FCC) in February 2002. UWB is permitted to operate between 3.1 and 10.6 GHz as well as in the 24 GHz RF spectrum. Its very short pulses (on the order of picoseconds, or  $10^{-12}$  second) create an “ultra-wide”, emission bandwidth ranging in width between 1 and 3 GHz. This wide bandwidth permits UWB to transport high data rates up to 100 Mbps using very low power, i.e., about 100 mW. UWB technology falls between WLAN and Bluetooth technologies. UWB communications devices have a low probability of detection because of the very low power output, which could be interpreted as RF noise. Commercially available products are expected to begin appearing in the second half of 2002.

PAN technology could be used, along with WLAN technology, in a DFO. As an example, a PAN could be used to connect a PDA with the WLAN. The WLAN, in turn, would be used to connect a number of desktop computers together on the LAN.

### **3.1.5 Satellite Services**

Satellite Services serve various purposes. They can provide communications links in locations lacking any terrestrial infrastructure. Two-way Direct Broadcast Satellite services are available at moderately high uplink speeds of 100 kbps and high speed downlinks at 600 kbps utilizing Transmission Control Protocol/Internet Protocol (TCP/IP) at the ground interface<sup>32</sup>. Satellite Services are also useful for data transfers and video broadcast transmissions using Motion Picture Experts Group (MPEG)-1 and MPEG-2 video compression. For voice transmissions, a satellite terminal can be combined with a wireless cellular handset and operate in a dual-mode configuration.

ORBCOMM provides global data services similar to two-way paging or e-mail via Low Earth Orbiting (LEO) satellites and a ground infrastructure through a data-only service with no voice service available. Because of the ORBCOMM network’s characteristics, i.e., a relatively high message latency of 6 to 15 minutes, ORBCOMM itself does not recommend its use for emergency response applications.<sup>33</sup> Qualcomm’s Globalstar is a satellite phone system based on LEO technology. The system can be accessed using a Qualcomm Globalstar GSP-1600 Portable Tri-Modal Phone that works like a cellular

---

<sup>32</sup> TCP/IP is not actually used over the RF transmission path due to timing issues associated with the RF propagation time between the satellite and earth station(s). Instead, the Satellite Service provider provides a proprietary protocol over the RF path and converts this protocol to TCP/IP at the ground interface with the wireline IP network.

<sup>33</sup> If latencies of 6 to 15 minutes could be tolerated and if communications from remote locations were necessary, ORBCOMM could be useful for NS/EP purposes.

phone when cellular service is available and will switch to Globalstar satellite mode when the user is out of cellular range. Motient Satellite Communications Services provides satellite coverage for the continental United States, Alaska, Hawaii, and the Caribbean. It can accommodate dispatch, data, telephone, and fax transmissions and would be suitable for NS/EP applications. Iridium and Inmarsat Satellite Services are also widely used world-wide.

Besides using Satellite Services for communications, they also provide global positioning. The Global Positioning System (GPS) is a constellation of 24 active satellites arranged in 3 orbital plains orbiting the earth every 12 hours. GPS provides specially coded telemetry signals that can be processed in a GPS receiver, thereby enabling the receiver to compute position, velocity, and time. Because GPS provides navigational as well as timing services to the military and civilian organizations, it may be an invaluable aid in support of NS/EP activities. GPS receivers are being installed in some commercial wireless handsets to facilitate identifying the physical location of the caller. This use of GPS is part of the technology required for mobile phone systems to meet the automatic location identification requirements of Enhanced 911 (E911).

Mr. Rex Whitacre of FEMA IT Engineering Disaster Response, in an interview, explained how his agency utilized bandwidth on a Ku-band satellite from Telstar for data and voice transmissions as well as for IP video teleconferences. Eight-to-one (8:1) voice compression is used on a DS-1. A DS-1 separate from that used for voice carries data transmissions. Six MHz of bandwidth is available on the satellite transponder to support analog video broadcasts. Inmarsat service is available for international voice calls, and Globalstar is used for domestic voice calls.

Mr. Whitacre also mentioned that FEMA is investigating the cost of and benefits to be derived from new Ka-band satellite service which offers the potential of increased bandwidth (up to 2 Mbps) on transmission links.<sup>34</sup> Such satellites will use on-board processing and IP switching to provide two-way services to and from small earth stations comparable in size to today's satellite television dish, about 18 inches in diameter. The satellites will employ multiple pencil like spot beams. The fee structure offered will be "bit rate on demand" and a variation, "variable bit rate on demand". Customers will pay for only the time that they use a link.

### **3.1.6 LMR and Two-Way Mobile Radio Products and Services**

The terminology "Land Mobile Radio" as used in this study refers to two-way, simplex, push-to-talk radio services. These radio services can operate in trunked and non-trunked configurations. The bandwidth of these services is low, and, therefore, they are used primarily for low bandwidth, about 3 kilohertz (kHz), voice communications. However,

---

<sup>34</sup> GE Spacenet had been one of the providers of this service, but it has recently been purchased by Gilat.

data transmissions are also available with some products and services at bandwidths up to 9.6 kbps.<sup>35</sup>

LMR Products and Services play very important roles in supporting NS/EP activities. Since base stations can be set up quickly, they can be made operational immediately in locations requiring emergency Telecommunications Services. Federal, state and local public safety organizations use LMR Services as their primary means of communications. LMR Products and Services operate in the very high frequency (VHF), ultra high frequency (UHF), and 800 MHz frequency bands.

### **3.2 Enhanced Priority Treatment**

Enhanced Priority Treatment is a very important Functional Requirement for NS/EP applications since emergency responders and national security implementers often need very rapid access to Telecommunications Services. The following Subsections explain how the Functional Requirement of Enhanced Priority Treatment applies to the Non-Wireline Service categories.

#### **3.2.1 Wireless Services**

Enhanced Priority Treatment for Wireless Services refers to the requirement to prioritize access to the RF connection between the mobile terminal and the Mobile Switching Office (MSO) for both the origination and destination locations of the call. Currently, Enhanced Priority Treatment is unavailable for Wireless Services in most locations within the continental US, but a solution is under development. The FCC has recently granted a temporary waiver to VoiceStream Wireless to begin implementing the Wireless Priority Service (WPS) capability for New York City and Washington, DC.<sup>36</sup>

Ideally, a service similar to that of GETS for Wireline Services should be implemented for Wireless Services. Therefore, the OMNCS is currently conducting an acquisition to incorporate Enhanced Priority Treatment into Wireless Services. This program is in consonance with the WPS Program which has been instituted based on the recommendation of the National Security Telecommunications Advisory Committee (NSTAC). The WPS Program will provide nationwide, uniform, priority access to commercial wireless communications for disaster responders. The WPS Program will address evolving Wireless Service technologies.

Work on Enhanced Priority Treatment for Wireless Services was deemed important by several individuals interviewed for this study. Mr. Bernard Farrell of the NCC indicated

---

<sup>35</sup> The National Telecommunications and Information Administration (NTIA) has required that all very high frequency (VHF) (162-174 MHz) and ultra high frequency (UHF) (406-420 MHz) Federal Government radio systems migrate to narrowband (12.5 kHz) channel operation.

<sup>36</sup> The waiver was granted on March 15, 2002 by the Federal Communications Commission in response to VoiceStream's request for a temporary waiver, with support from the National Communications System. The waiver was required since commercial mobile radio service carriers are otherwise prohibited from providing wireless service priority to subscribers. Without the waiver, all subscribers are to have equal access to the wireless service. The temporary waiver is to expire on or before December 31, 2002.

that the number one telecommunications requirement that they saw at the OMNCS was wireless priority.<sup>37</sup> The need for wireless priority was echoed by Mr. John Jolicoeur of the NRC, Mr. Dave Tyndall of the GSA Federal Protection Service, Mr. Russ Colomo of GSA Region 7, Mr. George Van Tiem of the Los Alamos National Lab, and Mr. Anthony Perales of FEMA.

### **3.2.2 Paging and Short Text Services**

As with Wireless Services, Enhanced Priority Treatment is generally unavailable for Paging and Short Text Services, although some message services can prioritize the messages. However, unlike the congestion experienced with Wireless Services during the September 11 attacks in New York City, these services were able to operate. One reason was that not all paging services relied on the wireless cellular infrastructure that was damaged near the center of the attack. Some paging services, like BlackBerry's, relied on a separate dedicated, terrestrial infrastructure while others were delivered by satellite technology and continued to operate. Many of the Paging and Short Text Services, including advanced messaging and paging, also continued to operate since their transmitters and receivers were still operational.

During an interview, Mr. Farrell, of the NCC, indicated that the BlackBerry service was good for communications at the Pentagon as well as in New York on September 11. Communications could continue while the regular wireless switches were saturated.

### **3.2.3 LMDS and MMDS**

Enhanced Priority Treatment is not available nor required for these services. Since both services are primarily used for point-to-multipoint transmission, congestion is not a problem in this operational mode. For two-way communications using MMDS, current user channel fill is not sufficient to cause congestion and the need for Enhanced Priority Treatment.

### **3.2.4 WLAN and PAN**

Enhanced Priority Treatment is not available nor required for WLAN and PAN services per se. For WLANs, Enhanced Priority Treatment is applicable to the packet protocols as discussed in Section [2.3.1.1](#) on Enhanced Priority Treatment for PSDS and not to the RF protocol stack. Enhanced Priority Treatment has no applicability for PANs due to the different PANs' architectures.

### **3.2.5 Satellite Services**

Enhanced Priority Treatment is not now available for Satellite Services. In fact, the need for Enhanced Priority Treatment for Satellite Services is not clear. Due to the lower number of users for Satellite Services than for Wireless Services, especially those provided by LEO satellite constellations, congestion is less likely to occur than with

---

<sup>37</sup> Executive Order 12472 has assigned the OMNCS the responsibility to identify improved approaches with initiatives underway for Cellular Priority Services, Wireless Data Priority Services, and Enhanced Satellite Capabilities.

terrestrial Wireless Services. Furthermore, if Wireless Services are useable during a domestic NS/EP event, most participants are likely to rely on their Wireless Services first and use satellite communications as a backup or for unique access requirements. Hence, satellite congestion would seem less likely to occur, thereby negating the need for Enhanced Priority Treatment. Of course, the lower probability of congestion on Satellite Services may diminish if the user population significantly increases as these services become widely adopted as a means of backup communications.

Irrespective of the potential for less congestion in Satellite Services, Mr. Farrell, of the NCC, strongly recommends that Enhanced Priority Treatment be made available for all technologies supporting NS/EP activities. This statement is assumed to include Satellite Services.

### **3.2.6 LMR and Two-Way Mobile Radio Products and Services**

Enhanced Priority Treatment is generally not available nor required for Radio Services. However, one commercial radio service, Direct Connect<sup>®</sup> from Nextel<sup>®</sup>, does offer a type of priority calling, but the calls must be placed between subscribers, both of whom subscribe to Direct Connect<sup>®</sup>. Also, due to the architecture for Radio Services, the type of switched network congestion encountered in the PSTN, Wireless Services, or PSDS data networks is generally avoidable. Priority communications among users on radio channels can be controlled through proper call management and discipline because the user community is narrowly defined and controllable. Application of the appropriate calling procedures among users can ensure priority transmissions are completed. As part of proper call management procedures, specific LMR system channels can be reserved for priority treatment and utilized by only designated personnel.

None of the individuals interviewed for this study indicated a need for Enhanced Priority Treatment associated with their Two-Way Mobile Radio Services. Mr. Ben Overbey, Director of Emergency Operations Center at the Department of Veterans Affairs, said that during the September 11 incident cell phones were saturated so Nextel<sup>®</sup> Direct Connect<sup>®</sup> was used.

## **3.3 Secure Networks**

Secure Networks for Non-Wireline Service categories may be implemented in several ways, as described in the following sections.

### **3.3.1 Wireless Services**

Secure Networks are not available for all wireless modulation schemes. One system offering authentication is the Global System for Mobile Communication (GSM), which offers authentication of transmissions via the IS-41 Revision C standard. The Wireless Application Protocol (WAP)<sup>38</sup> employs the Wireless Transport Layer Security (WTLS)

---

<sup>38</sup> WAP is used for wireless connections to the Internet. WAP 2.0 supports protocols such as IP, TCP, and HyperText Transfer Protocol (HTTP). WAP specifications provide an environment that permits wireless devices to utilize existing Internet technologies.

protocol for encryption and a wireless version of the Public Key Infrastructure (PKI) for data transmissions. Encryption of voice transmissions is not available except in particular devices, such as the Motorola 1500 secure phone. Secure wireless communications can be effected with NSA certified Secured Terminal Equipment (STE), including Fortezza cards<sup>39</sup>.

WAP has some security vulnerability. WAP data transactions travel from a wireless device using WTLS to a service provider's WAP gateway and are converted to a Secure Socket Layer (SSL) before being transmitted to the other end user, database, or application. When this conversion to SSL takes place in the gateway, the encrypted information is initially converted to clear text. As the information is presented in clear text, it provides opportunity for those with malicious intent to intercept the information which poses risks to the viability and reliability of the information transmitted.

Evolving 3G Wireless Services will have better encryption and authentication mechanisms than 1G, 2G, or 2.5G systems, but their security risks are not yet fully known. Concerns exist regarding the evolution of GSM networks toward Wideband Code Division Multiple Access (WCDMA)<sup>40</sup> capabilities. Although WCDMA is a more secure option than many current alternatives, WCDMA networks might cause potential problems when an attacker is able to calculate the pattern for changing the WCDMA frequency spreading range, facilitating the ability to eavesdrop on and/or modify transmissions over GSM spectrum.

In addition Qualcomm is developing the "CONDOR" Wireless Secure Telecommunications System, building on top of their commercially available PCS products for the 800 MHz cellular band and the 2 GHz PCS band. The QSEC 800 is CONDOR's CDMA Secure Terminal (CST) with built in encryption. This CST will use Future Narrow Band Digital Technology (FNBDT) signaling to allow interoperability between next generation strategic secure voice products such as the STE, while requiring no changes to the systems' infrastructure. The CST will offer both secure and non-secure private radio and net broadcast modes similar to today's LMR push-to-talk services.

Some computer security experts predict that improvements in wireless network coverage and availability of applications for wireless platforms will increase security risks. Specifically, these wireless improvements may bring a corresponding increased risk of attack by mobile viruses, worms, and malicious hackers. Regardless of security measures instituted by 3G network providers, e.g., encryption keys and mutual authentication capabilities, and other built-in security features offered by hardware developers, the increasing complexity of mobile devices and the growing dependence on interoperability

---

<sup>39</sup> Fortezza cards are the cryptographic tokens to secure the Defense Messaging System. They support data privacy, user ID authentication, data integrity, non-repudiation, and time stamping.

<sup>40</sup> WCDMA is a technique that spreads signals over many frequency slots in a wide spectrum and works by modifying its frequency spreading range in a pseudo-random fashion, making the signal appear to be random noise.

software leaves mobile devices vulnerable to mobile device viruses and hacking attacks. More work is needed in standards bodies to address these vulnerabilities.

Among those individuals interviewed for this study, Mr. John Jolicoeur of the NRC specifically stated a need for secure communications, including Wireless Services, as a top priority.

### **3.3.2 Paging and Short Text Services**

For Paging and Short Text Services, security is achieved only by encryption and decryption of the data message at the sending and receiving points of the communications link rather than by securing the transmission network itself. An example is the secure e-mail messaging product offered by BlackBerry in a handheld device with enterprise software. The BlackBerry encrypts messages using the Triple Data Encryption Standard (DES).

### **3.3.3 LMDS and MMDS**

Secure transmissions incorporating LMDS or MMDS are not available. Security is achieved only by encryption and decryption of the traffic at the sending and receiving points of the communications link rather than by securing the transmission network itself.

### **3.3.4 WLAN and PAN**

Security of WLANs is a serious concern. The NSTAC Network Security/Vulnerability Assessments Task Force Report (NS/VATFR) of March 2002 states, "According to Gartner Group, by the end of 2002, 30 percent of enterprises will suffer serious security exposures because they have deployed WLANs without proper security."<sup>41</sup> WLANs are susceptible to Denial-of-Service (DoS) attacks as well as to client-to-client attacks since clients can interface directly with each other and do not use a wireless access point. Another vulnerability results from the fact that WLANs, when shipped from the factory, are shipped in a low security mode, such as with a set of passwords that hackers know. If the system administrator does not change these passwords, the WLAN is highly vulnerable to hacking.

One means to ensure secure transmission on a WLAN is to employ the Wired Equivalency Privacy (WEP) protocol. The WEP protocol is part of the WLAN IEEE 802.11b standard. WEP uses Ron's Code 4 (RC4) encryption algorithm with a 40-bit key. A 128-bit key is an option. When WEP is enabled, the network administrator assigns each wireless station an encryption key string comprising a set of keys that are passed through the encryption algorithm. The key is used to scramble the data before it is transmitted between a mobile client or server and an access point. The secret key is used to encrypt packets before they are transmitted. At the receiving point, the key is used to perform an integrity check to ensure that a packet has not been altered in transit.

---

<sup>41</sup> *Firewalls Bypassed in Wireless LANs*, <http://biz.yahoo.com/bw/010809/2118.html>, August 9, 2001.

Scrambled packets which are detected as not being encrypted with the appropriate key are not delivered.<sup>42</sup>

Another means to improve WLAN security would be the use of a VPN employing IPSec, as described in Section [2.3.2.6](#). More simple, yet effective, means would be to change default names in WLAN software, move wireless access points to the center of a building, and to switch off a network's broadcast functions.

PANs are "ad hoc" networks with a topology that is not fixed as devices move in and out of devices' transmission range. In the case of Bluetooth, individual devices act as routers relaying messages to one another. Because devices relay messages, DoS attacks are easy. Battery exhaustion attacks could drain the battery's power prematurely; Radio Frequency Interference (RFI) could interrupt the message traffic; and the routing protocol could be disrupted by feeding the network inaccurate information. Authorization, confidentiality, and integrity are also vulnerabilities in ad hoc networks. All security transactions between two or more devices are handled by the link key. The payloads of packets are encrypted using a payload key. Authentication is achieved using a "challenge-response" method in which a 2-move protocol is used to check whether the other device knows the secret key.

Irrespective of the security approaches utilized, Bluetooth security is still quite vulnerable. Bluetooth security may be adequate for a connection between a PDA and mobile phone for non-sensitive data, but its security is not robust enough for handling sensitive information, especially in an ad hoc network setting.<sup>43</sup>

The standards for UWB transmissions are being established as of this writing. UWB has inherently high security features due to the tight control over power limits, which can be adjusted in real-time according to range requirements, as well as the coherent nature of the pulses. Furthermore, the spectral emission of UWB transmissions is so wide that it appears as noise to non-UWB receivers. Hence, UWB transmissions can be hidden amongst other RF signals.

### **3.3.5 Satellite Services**

Iridium and Inmarsat Satellite Services have been used extensively for secure communications in the Afghanistan theater. Special NSA certified STE, including the older Secure Telephone Unit (STU)-IIIs, are being used to encrypt voice and/or data transmission for tactical combat communications. Here again, the method for securing transmissions is to encrypt and decrypt the satellite traffic.

Mr. John Jolicoeur of the NRC, when interviewed for this study, stated a need for secure communications, including Satellite Services, as a top priority. Secure satellite

---

<sup>42</sup> *Newton's Telecom Dictionary, 18<sup>th</sup> edition*, H. Newton, copyright 2002

<sup>43</sup> For a more complete discussion of Bluetooth security see, *Bluetooth Security*, Vainio J. Helsinki University of Technology, (2000-05-25), [Juha.Vainio@iki.fi](mailto:Juha.Vainio@iki.fi)

telecommunications equipment is available to organizations if it is required. For instance, Mr. Ben Overbey of the Department of Veterans Affairs indicated their Emergency Operations Center had access to secure Iridium satellite phones. However, he did not indicate they had been used during the September 11 attacks.

### **3.3.6 LMR and Two-Way Mobile Radio Products and Services**

These services operate via insecure broadcast transmission facilities. Security is achieved only by encryption and decryption of the voice or data call at the sending and receiving points of the communications link rather than by securing the transmission network itself. Secure LMR communications are widely used throughout the public safety community as well as the military for combat command and control. Various products, like Transcrypt's LMR Security Modules, can be used to scramble and encrypt the communications.

## **3.4 Non-Traceability**

The following sections indicate how Non-Traceability may be implemented, if possible.

### **3.4.1 Wireless Services**

Non-Traceability for Wireless Services is unavailable. No plans currently exist to incorporate Non-Traceability into the WPS Program. However, the need for this Functional Requirement is likely to be as important as for Wireline Services. The identity of individuals initiating wireless calls may need to be hidden and, hence, non-traceable.

### **3.4.2 Paging and Short Text Services**

As for Wireless Services, Non-Traceability is generally unavailable for Paging and Short Text Services. An exception is that e-mail messages may have the origination address hidden by passing the e-mail message through a service provider which strips off the originating address and then forwards the message to the intended recipient. This is the same concept as used for e-mail services provided via PSDS.

### **3.4.3 LMDS and MMDS**

Non-Traceability does not apply to implementations of LMDS and MMDS using microwave transmissions. For these implementations, the identity or location of the source of the LMDS or MMDS transmissions could not be easily hidden nor made untraceable due to the spreading of the microwave energy from its transmission source. Receivers not in the direct lobe of the microwave transmitter could receive energy off of the side lobes of the antenna pattern.

However for FSO implementations using infrared laser transmissions in the optical spectrum, offer an opportunity to achieve Non-Traceability. Since the laser beam does not spread like a microwave transmitter's antenna pattern, placing a detector in the beam would be far more difficult, especially if the source and orientation of the laser beam were unknown.

### **3.4.4 WLAN and PAN**

Non-Traceability does not apply to WLANs and PANs. The use of these networks does not require that the identity or location of their users be hidden or untraceable, certainly not in the context that this Functional Requirement was originally intended to apply to the PSTN.

### **3.4.5 Satellite Services**

Current implementations of commercial Satellite Services do not offer the feature of Non-Traceability. Therefore, implementation of this requirement within commercial services is unlikely since the demand for it is minimal. Possibly, military or intelligence gathering operations require this capability and have it installed in selected satellite systems. However, such implementations are unknown. Even if such capabilities exist, those individuals in the NS/EP user community who would be authorized to use or have access to these capabilities are unknown.

### **3.4.6 LMR and Two-Way Mobile Radio Products and Services**

Depending upon the radio system's design, an identifier for the mobile or base station units may, or may not, be assigned. If no such identifier is assigned, then the user of the mobile or base units could be anonymous because no identifier would be transmitted in the radio signal. On the other hand, if the mobile or base units do have unique identifiers that would be transmitted as part of the signal, such as would occur in a trunked radio system, then the unit's user may also be identified by association with the unit's identification code.

If the Functional Requirement of Non-Traceability is applied to hiding the location of mobile or base transmitting units, then the Requirement would be difficult, if not impossible, to meet. Since antennas associated with radio services usually emit radiation in multiple directions, the location of the transmitting location could be determined through triangulation techniques.

## **3.5 Restorability**

Various methods could be applied to Non-Wireline Services to achieve Restorability. The following sections describe these methods.

### **3.5.1 Wireless Services**

Just as with Wireline Services, TSP could be applied to Wireless Services too. The wireline circuit connections between wireless MSOs and the terrestrial wireline network may be covered by existing TSP procedures.<sup>44</sup>

Restoration priority for any hardware or software and for the RF portion of the wireless communications link would have to be accomplished by the individual service providers. Arrangements for priority restoration would have to be negotiated on a bilateral basis

---

<sup>44</sup> A legal interpretation of TSP may be necessary to ensure these connections are covered.

between each of the individual Wireless Service providers and the NS/EP users of the service. Although not a panacea for enlisting rapid restoration, Service Level Agreements (SLAs) in service contracts, with strong incentives and/or penalties to minimize restoration times, could be negotiated with service providers to contractual bind them to quickly restore services.

Restoration of Wireless Services could be accomplished via backup equipment which could be brought into operation at a location where the wireless infrastructure had been damaged or destroyed. An example in which Restorability was achieved during the WTC disaster was the replacement of destroyed cellular sites by Cellsites On Wheels (COWs) provided by Verizon.<sup>45</sup> The COWs were able to quickly replace some of the cellular capacity lost in that part of New York City. In this case, the provision of the COWs was equivalent to providing TSP to the RF, or cell site, component of the Wireless Service.

Two individuals interviewed for this study indicated a need for TSP. Mr. Bernard Farrell of the NCC said that all NS/EP technologies should have TSP included in their requirements. Furthermore, Mr. John Jolicoeur of the NRC said that priority wireless restoration is a critical requirement.

### **3.5.2 Paging and Short Text Services**

Paging and Short Text Services may be restored in a manner similar to that for Wireless Services by using backup equipment to replace damaged or destroyed terrestrial infrastructure. Paging services using Satellite Services would have to be restored within the satellite or the ground control station(s). Incorporation of SLAs, with strong incentives for minimizing restoration times, could be used to facilitate rapid restoral of Paging and Short Text Services.

### **3.5.3 LMDS and MMDS**

Temporary implementation of LMDS and MMDS systems could make possible rapid restoration of wired telecommunications facilities destroyed or damaged by an NS/EP event. For instance, LMDS was used in New York City after the September 11 attack to replace destroyed wireline and fiber optic infrastructure.

Restoration of LMDS and MMDS facilities themselves would have to be done in a manner similar to that for Wireless Services. Arrangements for priority restoration would have to be negotiated on a bilateral basis with individual service providers. SLAs to minimize restoration times would have to be part of the service contracts. The use of backup equipment to replace damaged or destroyed terrestrial infrastructure would be another option if the LMDS or MMDS equipment was owned by the user.

---

<sup>45</sup> *Wireless Emergency Response Team (WERT) Final Report for the September 11, 2001 New York City World Trade Center Terrorist Attack*, October 2001.

#### **3.5.4 WLAN and Pan**

Restorability of WLANs and PANs would be based on equipment replacement or SLAs, as with the other services. SLAs to minimize restoration times would have to be part of the any service contracts under which the WLAN and PAN services were procured. The use of backup equipment to replace damaged or destroyed infrastructure would be another option if the WLAN and PAN equipment was owned by the user.

#### **3.5.5 Satellite Services**

TSP could be applied to Satellite Services as it would be applied to Wireless and Wireline Services. The wireline circuit connections between satellite earth stations and the terrestrial wireline network with which they connect may be covered by existing TSP procedures. However, a legal interpretation may have to be made on this point.

Furthermore, restorability of Satellite Services could be based on equipment replacement or SLAs. An action that could be taken to deal with priority restoration of Satellite Services would be negotiations with individual Satellite Service providers for restoration SLAs. These SLAs should be written to minimize restoration times and would have to be part of the service contracts. The use of backup equipment to replace damaged or destroyed terrestrial infrastructure would be another option if the equipment was owned by the user.

#### **3.5.6 LMR and Two-Way Mobile Radio Products and Services**

As with Wireless and Satellite Services, arrangements for priority restoration would have to be negotiated on a bilateral basis between each of the individual Radio Service providers and the NS/EP users of the services. In the context of Radio Services, Restorability would then apply to repair and/or replacement of mobile and base station radio equipment as well as dispatch and control equipment. SLAs for rapid restoration of service would have to be negotiated with any service providers. The use of backup equipment to replace damaged or destroyed infrastructure would be another option if the equipment was owned by the user. Of course, for non-repeater operation, radio handsets could communicate directly with each other even if the base station infrastructure were unavailable.

### **3.6 International Connectivity and Interoperability**

In this section, the Functional Requirement of International Connectivity is combined with the Functional Requirement of Interoperability because of the similarity in the issues associated with them for Non-Wireline Services.

#### **3.6.1 Wireless Services**

Wireless Services provide International Connectivity via commercial wireline voice and packet service providers. Wireless international connections would be accomplished in the same manner as if the wireless call or wireless data session were originated from a wireline source and, consequently, would be prone to the same failure mechanisms as international connections initiated from a wireline source.

As with International Connectivity, Interoperability of Wireless Services is often accomplished via wireline interconnections, either within the PSTN or packet networks. Indeed, a vexing problem within the United States is the lack of Interoperability among Wireless Service providers at the RF interface. The lack of Interoperability at this interface is a consequence of the several incompatible modulation schemes being employed, i.e., analog AMPS and the digital modulation schemes of Time Division Multiple Access (TDMA), CDMA, and GSM, as well as a consequence of the different frequency bands in which the different services operate.

However, a solution to this lack of Interoperability at the RF interface exists even without wireline interconnections. Interoperability can be achieved with the choice of the appropriate carrier and the appropriate technology in wireless handsets. For example, one interoperable solution would be to use a tri-mode/multi-frequency wireless phone employing GSM and another modulation scheme, such as AMPS. Since the GSM protocol is the same in the US and much of the world, wireless phones operating on GSM in the US could operate on GSM in other countries, if the phone was capable of operating on the correct frequencies in the various geographic regions. A Subscriber Identification Module (SIM) card can be utilized to allow a phone to be used with the same telephone number. With the phone capable of operating on the correct frequencies in the various geographic regions, International Connectivity and Interoperability via GSM could be obtained. If the third mode in the phone were AMPS, then additional coverage could be obtained in the US where GSM coverage is unavailable since AMPS is still a pervasive technology in most geographic areas of the US.

Another solution to Interoperability is offered by the GSM ANSI Interworking Team (GAIT).<sup>46</sup> With the recent adoption of GSM technology by the major domestic TDMA service providers, i.e., AT&T and VoiceStream, the prevalence of dual mode GSM/TDMA-capable mobiles will increase dramatically. GAIT mobile phones would allow users to roam between TDMA and GSM networks using the same phone. Nokia and Siemens have launched GAIT mobile phones.

Wireless devices incorporating Software Defined Radio (SDR) technology could also provide Interoperability among disparate Wireless Services. These SDR phones could be programmed to work on different frequencies with different modulation schemes to interoperate with the current domestic and international set of Wireless Service providers. Hence, Interoperability could be achieved at the RF interface. The use of multi-mode handsets and SDR phones would allow NS/EP personnel to move to new locations, take their existing equipment, and interoperate in the new wireless environment at the new location even if the wireless technologies employed were different than those in their home territories. This reuse of equipment would save time and money.

---

<sup>46</sup> GAIT is a combined effort of the North American GSM operators and the Universal Wireless Communications Consortium to establish dual-mode Interoperability for GSM and TDMA wireless handsets.

### **3.6.2 Paging and Short Text Services**

For messaging traffic, an interoperable solution employing wireline connections would be the use of SMS, which is used to send short alphanumeric messages over the SS7 signaling channel in the PSTN. The company InphoMatch provides a bridging service for SMS between carriers using different wireless modulation schemes. The InphoMatch SMS messages originated on one carrier's wireless network are sent via a terrestrial network and interpreted to be understood on another carrier's network using a different wireless modulation scheme. Use of SMS with such a bridging service has the potential to provide wireless messaging Interoperability for situations in which wireless voice Interoperability does not exist.

### **3.6.3 LMDS and MMDS**

LMDS and MMDS are short range services and are designed to interoperate with equipment of like vendors. They are not designed to operate cross international boundaries, such as the PSTN does, nor to interoperate with equipment from different vendors. Therefore, the Functional Requirements of International Connectivity and Interoperability do not apply to them.

### **3.6.4 WLAN and PAN**

WLAN and PAN Services are short range services and are not designed to cross international boundaries. WLAN and PAN equipment is designed to interoperate with equipment of like vendors. Therefore, the Functional Requirements of International Connectivity and Interoperability do not apply to them.

### **3.6.5 Satellite Services**

Some Satellite Services inherently offer International Connectivity. For instance, geosynchronous systems, like Glocall SP (which is using the Eutelsat with a coverage footprint in Europe, the Atlantic ocean, North Africa, and the Middle East) would achieve International Connectivity (i.e., international coverage) directly through the satellite. A LEO system, like Iridium, can also provide International Connectivity. Iridium has earth stations in Arizona, Hawaii, and a backup in Italy. For Iridium, International Connectivity could be accomplished via RF interconnections directly between satellites without having to rely upon traditional wireline interconnections from the terrestrial hubs. Calls placed in one country to a satellite in the constellation would be handed off to another satellite for ultimate delivery to an earth station in the United States. From there, the call would be delivered using the terrestrial wireline network. The result would be an international space-based interconnection.

Although Satellite Services offer International Connectivity, they are not interoperable with each other. Dissimilar modulation schemes and operational frequencies preclude interoperation at the RF interface. Again, Interoperability must occur at the wireline interconnection points within the PSTN, or packet networks, through the earth stations and terrestrial hubs.

### **3.6.6 LMR and Two-Way Mobile Radio Products and Services**

Interoperability of different radio services is a major concern in many municipalities and across different organizations. The different technologies employed in radio services often are incompatible. Differences occur in operational frequencies and modulation schemes, such as analog versus digital. Operational control of radio services also differ. In this sense, the situation with radio services is similar to that with Wireless and Satellite Services.

The most promising solution to these Interoperability issues would be incorporation of SDR technology. SDR technology provides software control of various modulation techniques, wide-band or narrow-band operation, and control of waveform requirements. The SDR technology would overcome the differences in operational frequencies and modulation schemes so that Interoperability could be achieved at the RF interface. Control of the SDRs would also have to be adaptable to the control mechanisms employed by various Radio Services. A program is underway within the Department of Defense in the Joint Tactical Radio System Joint Program Office to define the architecture for an SDR that meets all military requirements. The use of SDR radios would allow NS/EP personnel to move to new locations, take their existing equipment, and interoperate in the new radio environment at the new location even if the radio and control technologies employed were different than those in their home territories. This reuse of equipment would save time and money.

The issue of Interoperability among disparate radio systems is well known in the NS/EP community. For instance, Mr. William Belote, Emergency Planning Coordinator for the National Telecommunications and Information Administration (NTIA), thinks some standardization of radio frequencies is needed in order to foster Interoperability. Mr. Bernard Farrell, of the NCC, mentioned widespread radio interference in New York City during the September 11 incident. Mr. George Van Tiem, Group Leader for Emergency Management and Response at the Los Alamos National Lab indicated that, during the forest fires in and near Los Alamos, 1000 portable radios really saved the day. These radios were part of a GE/Ericsson VHF trunked broadband radio system with 15 frequencies. However, because of incompatibilities among radio frequencies, the Lab loaned some of their radios to promote local communications.

In order to satisfy concerns such as those raised by these individuals, and others, a report issued by the Federal Law Enforcement Wireless Users Group (FLEWUG) on the need for interoperable radio communications capabilities for the public safety community led to the formation of the Public Safety Wireless Network (PSWN) Program. The program is jointly sponsored by the Departments of Justice and Treasury, with guidance from the FLEWUG and an Executive Committee that includes prominent state and local public safety officials.

The PSWN Program includes:

- Identifying both technical approaches and policy-oriented solutions to promote and enhance interoperability and more efficient use and sharing of resources
- Initiating state government interoperability campaigns
- Developing a roadmap, known as the Public Safety Wireless Interoperability National Strategy (WINS)
- Coordinating partnerships and pilots, along with funding, spectrum, standards, technology and security issues.

An initiative underway is a voice communications interoperability gateway that is being tested and evaluated by Washington DC area Public Safety organizations. This “AGILE” project is sponsored by the Department of Justice’s National Institute of Justice and provides direct connectivity between disparate radio systems. Each agency uses radio repeater sites to provide communications coverage on each agency’s frequencies for its areas of responsibility. The gateway allows radio channels of these agencies to be linked together over-the-air through their existing radios. The gateway also provides a capability for the radio to connect to the PSTN and includes interfaces (radio and telephone) for conference/group calls to support multi-jurisdictional and/or mutual aid responses.

Another effort underway to ensure LMR Interoperability is one taken by the Office of Management and Budget (OMB). OMB is planning to reassign various federal government wireless efforts to one e-government initiative under FEMA, an agency which is planned to be incorporated into the Department of Homeland Security. The plan is for FEMA to organize the federal government’s communications capabilities under Project SafeCom to ensure that emergency workers and first responders have available Interoperable radio equipment. FEMA plans to establish equipment standards by the end of CY 2002.<sup>47</sup>

The Functional Requirement for International Connectivity for LMR and Two-Way Mobile Radio Products and Services has the same limitations regarding radio equipment compatibility as mentioned above regarding Interoperability. Consequently, the potential solutions are similar except that they must be developed by international authorities.

### **3.7 Mobility**

In general, Non-Wireline Services provide the mobility needed to support NS/EP events.

#### **3.7.1 Wireless Services**

Wireless Services inherently provide Mobility and have proven to be key telecommunications mechanisms during NS/EP events for the obvious reason that communications is possible in locations where a wireline infrastructure is unavailable and

---

<sup>47</sup> *FEMA Taking Charge of Wireless*, Federal Computer Week, June 21,2002, by Megan Lisagor

the Functional Requirement of Mobility is necessary. Indeed, Wireless Services are necessary to support the Mobility Functional Requirement.

### **3.7.2 Paging and Short Text Services**

To the extent that they are provided by Non-Wireline Services, Paging and Short Text Services are inherently mobile and meet this Functional Requirement.

### **3.7.3 LMDS and MMDS**

LMDS and MMDS are usually considered fixed services. However, transportable systems are available. Since they are not operational when in motion, they are not considered truly “mobile”.

### **3.7.4 WLAN and PAN**

WLAN and PAN Services fulfill this Functional Requirement.

In the past, WLANs have operated in only a fixed environment. Although they could be considered to be mobile since they could operate in a large moving vehicle, such as the Mobile Air Transportable System (MATS) vehicle employed by FEMA, their design for a fixed environment means that they are “transportable” as opposed to “mobile”. However, the technology of WLANs has evolved to the point in which WLANs are now used by military aircraft to communicate with each other while in flight, a truly “mobile” implementation. These WLANs are termed “Flying Local Area Networks (FLANs).

PANs are designed to be mobile. The equipment employing PAN technology can be mobile in the sense that the equipment is not tethered to each other, and one device can be moved relative to the other. One evolving application is the use of PANs to connect items comprising wearable computers. Hence, PANs could be used in a stationary environment or in a moving environment.

### **3.7.5 Satellite Services**

Satellite Services are key to providing mobile communications. LEO systems, like Iridium and Globalstar, provide voice and data telecommunications via handheld or transportable terminals. Satellite Services are a principal means to support the Mobility Functional Requirement.

### **3.7.6 LMR and Two-Way Mobile Radio Products and Services**

Radio Services are specifically designed to support this Functional Requirement during NS/EP events. Modern designs have made mobile units even more portable due to reduced size with increased operational capabilities.

Use of radio equipment is standard within the NS/EP user community. Radio usage was specifically mentioned by several of the individuals interviewed, i.e., Mr. Ben Overbey of Veterans Affairs, Mr. Pao Lin Hatch of GSA’s National Capital Region (NCR), Mr. Rex

Whittaker of FEMA, Mr. Warren Schwart of the United States Postal Service (USPS), and Mr. George Van Tiem of the Los Alamos National Lab.

### **3.8 Ubiquitous Coverage**

Some Non-Wireline Services can provide Ubiquitous Coverage or “nearly” Ubiquitous Coverage as discussed in the following sections. Other Non-Wireline Services do not meet this Functional Requirement.

#### **3.8.1 Wireless Services**

Wireless Services are not ubiquitous in and of themselves. Coverage is limited to locations where the infrastructure has been installed and sufficient capacity exists. Even roaming agreements among service providers can not ensure Ubiquitous Coverage since the modulation schemes and frequencies used in the roaming wireless devices must be compatible with the wireless infrastructure in the roaming location.

Multi-mode phones help increase the coverage areas of wireless operations while not necessarily affording Ubiquitous Coverage. One use of multi-mode wireless devices would be to employ two or three wireless technologies, such as analog AMPS and one of the digital technologies, such as TDMA, CDMA, or GSM. The ability for the device to operate in any one of three modes would provide flexibility to effect connectivity in a variety of locations in which coverage provided by one or two of the technologies may not be available but the third is. This approach would be useful in the US and in other countries, such as using GSM in Europe operating on the European frequencies, as one of the modes. For example, VoiceStream offers roaming throughout the world using tri-mode/multi-frequency phones. (See Section [3.6.1](#) for a more complete discussion.)

Another approach would be to incorporate wireless and satellite technologies into a single device. A combination of the two technology types may, together, approach meeting the Ubiquitous Coverage requirement. Some tri-mode phones combine a satellite technology as one mode with the other two modes being two of the wireless modulation schemes. For instance, Globalstar combines GSM service with its satellite service in a single dual-mode handheld device.

None of the individuals interviewed for this study, nor any of the other information received, have indicated the use of tri-mode phones in past NS/EP events. In fact, GSA Regional Emergency Communications Planners have suggested to the OMNCS that tri-mode devices are needed by GSA’s Regional Managers to function while deployed on Federally Declared Disasters.

#### **3.8.2 Paging and Short Text Services**

Paging and short text messaging wireless services are available throughout most of the world, but coverage cannot be considered to be Ubiquitous. Coverage typically depends on the use of server gateways for message routing as well as terrestrial telecommunications facilities. For example, a message sent via ORBCOMM, a data

service based on LEO satellites, is initially routed to one of the ORBCOMM satellites which relays the message to a gateway earth station that then sends it to a network control center. The network control center e-mails the message to the end-user. Although theoretically available world-wide, the ORBCOMM service is not available in a number of countries due to regulatory prohibition.

NovelSoft provides SMS in which a user sends a short text message via a global access number to a NovelSoft server. The server processes the message and relays it to the appropriate mobile phone recipient. The NovelSoft service is currently available in over 100 countries, but its operation is contingent on arrangements with Wireless Service providers in the countries served.

Skytel offers paging and SMS over a network using satellite transmissions of data to earth stations. Skytel coverage is primarily for North America, although limited international coverage is available.

### **3.8.3 LMDS and MMDS**

LMDS and MMDS have not been designed for Ubiquitous Coverage and do not fulfill this Functional Requirement. These services are provided on only a localized basis.

### **3.8.4 WLAN and PAN**

The Functional Requirement of Ubiquitous Coverage does not apply to WLAN and PAN Services.

### **3.8.5 Satellite Services**

Satellite coverage is generally available in most locations, but it does have limitations. For instance, coverage may not be available in some locations within urban areas or at other locations, such as in mountainous terrain, where the user's line of sight to a geosynchronous satellite or to a constellation of LEO satellites may be blocked.

As discussed in Section [3.8.1](#), Wireless Services. Satellite coverage can be augmented by Wireless Services to provide coverage for areas in which direct LOS to the satellite is unavailable. Therefore, Satellite Services may be considered to have "nearly" Ubiquitous Coverage.

### **3.8.6 LMR and Two-Way Mobile Radio Products and Services**

Because the equipment supporting radio services is portable and mobile, radio systems can be relocated to geographical areas in which they are needed on a case-by-case basis. In this sense, Two-Way Mobile Radio Services provide Ubiquitous Coverage.

## **3.9 Survivability/Endurability**

A common vulnerability among all Non-Wireline Services is that of jamming at the RF interface. Jamming would require a sufficiently strong signal source that could overwhelm the desired signal at the Non-Wireline device's receiver. The necessary signal

strength for jamming at the receiver's location would be dependent upon the specific Non-Wireline Service. Alternatives and mitigation strategies should be developed and implemented based on each type of Radio Service. These specifics are discussed, along with other Survivability/Endurability issues, in the following Subsections.

### **3.9.1 Wireless Services**

The Survivability and Endurability of terrestrial Wireless Services is inherently at risk from any natural or man-made disaster events since their transmitter/receiver/switching infrastructure is fixed and locations are easily known. Wireless systems are also vulnerable because of their dependence on terrestrial wireline connections, whether with the PSTN, packet networks, or their own networks. These wireline connections could be attacked and disrupted. Disruptions could arise from DoS congestion on packet networks or physical attack on the cable plant, other equipment within the network infrastructures, or attacks on system software. Wireless vulnerability also exists to the Home Location Register (HLR)<sup>48</sup>. Since the HLR is absolutely necessary for wireless calls to be established and completed, its destruction would prevent Wireless Services from being offered anywhere by the disrupted carrier. The loss of the HLR would constitute a catastrophic failure of a carrier's wireless network.

Several solutions exist to support this Functional Requirement. One solution would be implementing robust designs and physical protection of buildings, cable plants, and equipment. Nuclear hardening would be an example. Another solution would be in the form of back-up and replacement systems, which could be quickly activated to replace those systems lost. In a sense, rapid Restorability is a solution for this vulnerability of Wireless Services. Access to the wireless systems' software should be limited and protected.

In terms of RFI due to jamming, the sensitivity of wireless receivers is somewhat dependent upon the modulation scheme employed. Analog systems may be more susceptible to RFI than digital systems due to the characteristics of the two modulation schemes. For instance, in the case of CDMA with a broad spread spectrum-type receiving bandwidth, low level, narrow band RFI may appear only as an increase in the RF noise floor. The modulated CDMA signal could still be detected and demodulated in the presence of this low level RFI. Therefore, to impair performance, the attacker using the RFI technique would have to ensure a sufficiently high RFI signal level in the presence of the target wireless receiver to increase the digital bit error rate (BER) beyond the allowable system limits.

### **3.9.2 Paging and Short Text Services**

Paging and Short Text Services are prone to the same system hardware and software failure mechanisms as Wireless Services, discussed in Section [3.9.1](#) above. The

---

<sup>48</sup> The HLR uses the SS7 network to access data about a wireless subscriber in order to acknowledge the user's privileges on the carrier's wireless network, whether for operation in the home or in a roaming coverage area.

transmitter and switching infrastructure supporting these services is at risk from physical destruction, and the system software could be vulnerable to corruption. Paging and Short Text Services supported by Wireless Services would be prone to failure of the HLR too.

Similar solutions exist to support this Functional Requirement as those for Wireless Services. Hardening of the physical infrastructure is necessary as well as immediate accessibility to back-up and replacement systems, which could be quickly activated. Access to the paging and text systems' software should be limited and protected.

As with Wireless Services, Paging and Short Text Services are vulnerable to RFI. However, because these systems use digital modulation schemes, they inherently have some protection against RFI. The RFI signal would have to be high enough to exceed the signal detection threshold resulting in an unacceptable BER .

### **3.9.3 LMDS and MMDS**

LMDS and MMDS systems are also at risk to physical damage of the transmitting and receiving equipment as well as to software needed to operate this equipment. Hardening of the physical infrastructure and accessibility to back-up and replacement systems are means to improve Survivability and Endurability of LMDS and MMDS systems.

Successful jamming via RFI of LMDS or MMDS systems may be more difficult than with other Non-Wireline Services because a jamming source, to be effective, would have to be directed at the receiving antenna and antenna pattern lobes instead of being transmitted in an omni-directional fashion. The reason being that the antennas used with LMDS and MMDS are directional and would be somewhat insensitive to an RFI signal not falling within the receiving antenna's lobes. Therefore, deliberate jamming of the LMDS or MMDS signal would be more difficult and entail knowledge of the receiving antenna's location and its beam's orientation.

### **3.9.4 WLAN and PAN**

Systems supporting WLANs and PANs may be more Survivable and Endurable than other Non-Wireline systems because they are portable and mobile. They could be removed from harm's way.

Hardening of the facilities and readily available spare equipment would be options to improve Survivability and Endurability. However, in some cases the equipment may not be contained in a structure specifically designed for it. Instead, the equipment may be dispersed throughout a work environment. In a field setting, this work environment could be a tent or in the open. Readily available spare or replacement equipment would also help to improve Survivability and Endurability.

Intentional RFI jamming of WLANs and PANs probably would not be difficult. For instance, a microwave oven could introduce interference into a WLAN using the Institute of Electrical and Electronics Engineers (IEEE) 802.11b technology, which operates in the

2.4 GHz band. Another potential source of RFI would be the operation of a WLAN and PAN using the same frequencies and operating in close proximity to each other. An example would be an 802.11b WLAN operating near a Bluetooth PAN, both of which use the unlicensed 2.4 GHz band.

### **3.9.5 Satellite Services**

Satellite systems are prone to risks of physical attacks similar to those of Section [3.9.1](#), Wireless Services. Earth stations could be attacked and destroyed. Connections to the terrestrial wireline circuit-switched and packet networks could be disrupted or destroyed just as those supporting Wireless Services. The satellite's equivalent to the wireless HLR would also be vulnerable. Furthermore, even the satellite transponders themselves are vulnerable from a nuclear electromagnetic pulse (EMP) or a conventional explosive device in space.

As for Wireless Services, hardening of equipment sites can be done to mitigate the risks of physical attack. Another solution would be the availability of back-up and replacement systems, which could be quickly activated to replace those systems lost. Software should be protected from unauthorized access.

RFI for Satellite Systems could result in two forms. The first would be to jam the receiving devices. This approach would require a sufficiently strong RFI generator in the vicinity of the receiver. This approach would be a difficult undertaking if the receivers were mobile since the jammer would have to move with the receivers in order to remain in their vicinity. Also satellite receivers have some directionality in their antenna patterns. Hence, the jamming RFI would have to be directed towards these antenna pattern's lobes in order to be most effective. This jamming technique would be a situation similar to that encountered with LMDS and MMDS systems.

A final form of RFI could result from a ground-based jammer interfering with the receiver of the satellite's transponder. Jamming could be accomplished by a moderately powered ground transmitting unit operating on the transponder's "up" channel. A strong enough signal at the satellite's receiver from the jammer could block legitimate signals from other earth stations. This approach would be applicable for Satellite Services employing low lower mobile ground transmitting units, like those from Iridium or Globalstar.

### **3.9.6 LMR and Two-Way Mobile Radio Products and Services**

The Survivability and Endurability of certain fixed portions of the Radio Services infrastructure is inherently at risk from any natural or man-made disaster events since their transmitter/receiver infrastructure is fixed and locations easily known. Radio Services, in some instances, are also vulnerable because of their dependence on terrestrial wireline connections between control sites and transmitter/receiver facilities. These wireline connections could also be physically attacked and disrupted.

The same techniques used for other Non-Wireline Services can be employed to mitigate the risk of damage to LMR and Two-Way Mobile Radio systems. Equipment sites and control system infrastructures should be hardened and protected against physical assaults. Back-up or replacement systems should be ready for immediate deployment and operation. Control software should be protected from unauthorized access too.

RFI could impair Survivability and Endurability. For those radio systems using mobile receiving devices, the RFI generator probably would need to move to remain in the vicinity of the receivers, a situation which might prove difficult for the attacker to implement. Use of digital receiving technology probably would help improve a radio system's Survivability and Endurability since the requirements for successful jamming would be more difficult to achieve with a digital modulation scheme than with an analog scheme. Of course for fixed receivers, jamming could be done more easily since the receiving antennas' locations probably would be known, and RFI could be aimed directly towards the antennas.

### **3.10 Voice Band Service**

Non-Wireline Services support Voice Band Service. The following Subsections explain how.

#### **3.10.1 Wireless Services**

Wireless Services were originally designed to provide Voice Band Service, as they still do. As such, Voice Band Service continues to be the predominant service used during NS/EP events. Wireless Voice Band Service was especially useful in coordinating disaster recovery efforts at the WTC and Pentagon sites on September 11. For example, Mr. Ashley Cohen of GSA in Region 2 found wireless telephones to be a "godsend" as they continued to be the only means of communication for a month in their facility at 26 Federal Plaza in New York City. The importance of Wireless Voice Band Service was evident when the lack of it, due to network congestion in New York City and Washington, sorely taxed relief efforts in those locations. Because of its utility and ubiquity, wireless Voice Band Service is anticipated to remain an important component of NS/EP telecommunications.

#### **3.10.2 Paging and Short Text Services**

Short Text Services are not designed to support Voice Band Services.

However, some Paging Services offer the option of recording a digitized voice message for relay to the message's recipient. In this sense, these Paging Services provide Voice Band Services, as well as text messages.

#### **3.10.3 LMDS and MMDS**

LMDS and MMDS systems are designed to deliver data bandwidths far exceeding those required for Voice Band Service alone. Within these large data bandwidths, many individual channels supporting Voice Band Service can be accommodated.

#### **3.10.4 WLAN and PAN**

WLANs and PANs are not designed for carrying Voice Band Service per sé since their primary purpose is for data transmission. Nevertheless, they can support Voice Band Service under certain conditions. For example, if the data network WLAN is used for VoIP service, then the WLAN would be supporting Voice Band Service. PANs can also handle Voice Band Service in certain situations. For instance, the PAN used between a wireless phone and a headset is supporting voice whereas a PAN that used to connect a printer to a computer is not handling voice.

#### **3.10.5 Satellite Services**

Voice Band Service is available from most Satellite Service providers. Examples of such providers are Iridium, Globalstar, Inmarsat, and ORBCOMM.

Satellite Voice Band Service also has proven to be very valuable in NS/EP events. In locations where line of sight exists to a geosynchronous satellite or to a constellation of LEO satellites, satellite Voice Band Service has been used as backup to terrestrial-based Wireless and Wireline Voice Band Services. For example, during the rollover to the year 2000, the Iridium satellite service was employed by numerous federal government agencies as a backup to a potential failure of the PSTN. Geosynchronous satellites are generally not favored for full duplex voice communications because of the inherent perceptible transmission delay caused by communicating through the satellite transponder almost 24,000 miles away.

#### **3.10.6 LMR and Two-Way Mobile Radio Products and Services**

LMR and Two-Way Mobile Radio Products and Services inherently provide Voice Band Service. Although messaging is also available from some radio services, Voice Band Service continues to be the predominant service used during NS/EP events. All members of the NS/EP user community with access to radios will employ them in Voice Band Service, if necessary. Radios sometimes are the last resort for communications if other means fail.

Mr. Ben Overbey of Veterans Affairs has high frequency (HF) radios as one of his communications alternatives. He used them when cellular phones were saturated during the September 11 incident. GSA Regional Emergency Coordinators also have access to HF radios. Mr. Rex Whittaker of FEMA has phones supporting radio groups. The radio portion of these phones uses an unlicensed band so if the phone becomes inoperable, he can use the radio feature. East, west, and overall radio groups have been identified within FEMA.

### **3.11 Broadband Service and Scaleable Bandwidth**

Many Non-Wireline Services support Broadband Service and, as a consequence, also support Scaleable Bandwidth. LMR and Two-Way Mobile Radio and Paging and Short Text Services do not support either Broadband Service or Scaleable Bandwidth.

### **3.11.1 Wireless Services**

Broadband Service is not yet a reality with current 2G Wireless Services, although 2.5G Wireless Services using General Packet Radio Service (GPRS) are expected to provide data speeds between about 65 kbps and 115 kbps. 3G and 4G wireless technologies are expected to increase the bandwidth even more, perhaps as high as 2 Mbps for 3G and up to 100+ Mbps for 4G. These higher data rates will be designed to support mobile intranet/extranet access, multimedia messaging, and high quality mobile video phone services.

### **3.11.2 Paging and Short Text Services**

These services are not designed for Broadband Service and do not support Scaleable Bandwidth.

### **3.11.3 LMDS and MMDS**

LMDS and MMDS are designed to provide Broadband Service. LMDS free space optics technology can support data rates from between 10 Mbps and 1.25 Gbps. Microwave versions of LMDS can support data rates up to OC-3. MMDS supports data rates up to 10 Mbps.

### **3.11.4 WLAN and PAN**

WLANs and PANs offer Broadband Service. The IEEE 802.11b version of WLAN technology supports data rates up to 11 Mbps. Future WLAN technologies, like IEEE 802.11a and 802.11g promise even higher data rates, i.e., up to 54 Mbps.

The Bluetooth technology for PANs offers data rates of 432 kbps. PAN UWB technology promises data rates up to 100 Mbps.

### **3.11.5 Satellite Services**

Satellite Services support Broadband Services. The Glocall SP system operates at data rates from 128 kbps to 2 Mbps. Two-way Direct Broadcast Satellite services are now available that support 600 kbps downlinks and 100 kbps uplinks utilizing TCP/IP. The Starband and DirecPC geopositioned satellite systems support two-way broadband communications at 40 - 70 kbps uplink speeds and 400 - 700 kbps downlinks. Teledesic is a LEO satellite system that is under development with service expected by 2005. It plans to offer data speeds up to 64 Mbps for Internet and intranet access. SkyBridge is another future system similar to Teledesic.

### **3.11.6 LMR and Two-Way Mobile Radio Products and Services**

LMR and Two-Way Mobile Radio Products and Services are not designed for Broadband Service nor Scaleable Bandwidth. Radio Services offer limited channel bandwidth for voice and low speed data services only. Channel bandwidths are too small to accommodate any Broadband Services.

### **3.12 Affordability**

In general, Non-Wireline Services are considered affordable since they are based primarily on COTS products and services. For those services, such as Wireless Services and LMR and Two-Way Mobile Radio Products and Services, developments are continuing in new technology. Hence the prices for products and services based on these new technologies may remain higher than for COTS-based products.

#### **3.12.1 Wireless Services**

Wireless Services employed today for use during NS/EP events are generally COTS service offerings, using the existing infrastructure and being provided by commercial carriers. As a consequence, the government will not be procuring unique services and should not be expected to be paying higher prices when using commercially available services and features.<sup>49</sup> Hence, these COTS service offerings are expected to be relatively affordable.

However, the future implementation of Wireless Services in unique devices (a tri-mode device or SDR, as examples) may incur higher equipment and service charges relative to current charges for commercial Wireless Services and equipment simply because the user base is likely to be smaller. Under these conditions, the NS/EP user community may have to bear the additional costs. Nevertheless, additional costs for such equipment and services are likely to be minimized as long as commercial use could be made of the products and the NS/EP community does not have to bear the full burden of design, production, and operation.

#### **3.12.2 Paging and Short Text Services**

Paging and Short Text Services are COTS-based services and should be considered affordable.

#### **3.12.3 LMDS and MMDS**

LMDS and MMDS are COTS-based services and should be considered affordable.

#### **3.12.4 WLAN and PAN**

WLAN and PAN equipment will be COTS-based and should be considered affordable. UWB technology is still under development so its initial costs may be somewhat higher than other WLAN and PAN products. However, UWB products are expected to be priced competitively with devices using alternative PAN technologies in order to establish UWB products in the marketplace.

#### **3.12.5 Satellite Services**

Many Satellite Services are COTS-based services and should be considered affordable. Even with new satellite technologies, such as Teledesic and SkyBridge plan to offer,

---

<sup>49</sup> The federal government will be charged for wireless priority service as it becomes available since this feature will be unique to the federal government.

pricing for these Satellite Services should be in line with existing COTS services since the new service providers will need to be price competitive with the COTS services.

### **3.12.6 LMR and Two-Way Mobile Radio Products and Services**

Much COTS LMR and Two-Way Mobile Radio equipment exists. Prices have stabilized and are considered affordable. This equipment could be considered to be commodities. Even SDR equipment is not expected to have a significantly higher production cost. However, the development costs associated with SDR technology could increase the price of this equipment. Currently, the SDR development is being undertaken by the military with a concomitant set of higher requirements than would be needed for the civilian market. Consequently, higher development costs ensue. Development of SDR equipment for the civilian community does not seem likely now since major radio manufacturers have little incentive to develop mass produce SDR radios due to their current inventories of legacy equipment or market share position.

### **3.13 Reliability and Availability**

The Functional Requirement of Reliability and Availability is closely related to the Requirements of Restorability and Survivability/Endurability. In addition, good equipment and system designs, along with implementation techniques, will help to ensure adequate Reliability and Availability.

#### **3.13.1 Wireless Services**

The Reliability and Availability of Wireless Services is generally good. These services can become unavailable due to system and network failures, congestion, and loss of infrastructure. Unavailability due to network failures should be dealt with through improved component reliability and necessary component redundancy. Unavailability as a consequence of congestion at the RF interface should be addressed through the WPS Program as discussed in Section [3.2.1](#) about Enhanced Priority Treatment for Wireless Services. Unavailability at the wireline level should be handled as with Wireline Services discussed in Section [2.1.1.10](#). Unavailability due to infrastructure destruction should be addressed through transportable backup equipment, such as COWs. In this sense, Reliability and Availability issues are closely linked with those of Restorability, as discussed in Section [3.5.1](#) regarding Wireless Services Restorability.

Nevertheless, the Reliability and Availability of Wireless Services, when compared to the PSTN, is less. One reason being that the wireless networks have not been designed to the same reliability and availability specifications to which the PSTN has been designed, i.e., 99.999% availability. Another reason for lower service availability is that of transmission impairments as a consequence of poor RF signal reception, impairments with which the Wireline Service providers do not have to deal.

Another non-technical consideration regarding the Reliability and Availability of Wireless Services is the viability of the Wireless Service provider from a business standpoint. Wireless Services providers' businesses have undergone many changes

during the past several years. Mergers and acquisitions have been commonplace. Some service providers have simply gone out of business while others have been absorbed into larger organizations. In some cases, service in a particular area may have been lost or the type of service provided changed to accommodate the business practices of the new owner. In any case, a wireless user may have some concern as to the stability of a particular service and feature set being employed in a particular location(s).

### **3.13.2 Paging and Short Text Services**

The factors affecting Reliability and Availability of Paging and Short Text Services are similar to those for Wireless Services, discussed in the previous section. Similar solutions are available for Paging and Short Text Services delivered via Wireless Services. Issues affecting service restoration apply as discussed in Section [3.5.2](#).

### **3.13.3 LMDS and MMDS**

Reliability and Availability issues associated with LMDS and MMDS systems involve system failures and loss of infrastructure. Reliability and Availability performance for the system would be dependent upon the Reliability and Availability performance of individual system components and the implementation of redundancy for certain components with low availability in order to achieve the desired performance levels of the system. Unavailability due to infrastructure destruction should be addressed through transportable backup equipment. Availability issues are closely linked with those of Restorability, as discussed in Section [3.5.3](#) regarding LMDS and MMDS Restorability.

### **3.13.4 WLAN and PAN**

The Reliability and Availability of WLANs and PANs is dependent upon the quality of the equipment and its installation. Users of these networks should investigate the quality of the products they procure to implement the networks, or the service providers from which they purchase services, to help determine the predicted reliability of the WLANs and PANs implemented. Furthermore, reliable service is due in part to the RFI experienced by these networks. If RFI is too severe, frequency management should be used to avoid overlapping operational frequencies among collocated equipment. Selection of different WLAN or PAN technology may be needed to avoid RFI.<sup>50</sup> Although the WLAN or PAN infrastructure is less likely to be damaged than the infrastructure of a Wireless Service, it is still prone to damage. Rapid replacement of damaged equipment can improve overall system Reliability and Availability.

As with Wireless and Satellite Services, some uncertainty exists as to the longevity of certain equipment or service providers. Since the WLAN and PAN technologies are evolving rapidly, uncertainty remains regarding the viability of a specific technology in light of its competition. Therefore, choices of technologies employed should be carefully made to ensure that technical support and replacement equipment is available in the future to support system operation. Similarly, the financial health of a particular company

---

<sup>50</sup> For instance, using UWB instead of Bluetooth for a PAN to avoid interference with an IEEE 802.11b WLAN implementation.

supplying equipment or services should be examined in order to determine the company's viability for long term existence.

### **3.13.5 Satellite Services**

Technical Reliability and Availability issues associated with Satellite Services are similar to other services regarding system failures and loss of infrastructure. Solutions are similar to those for the services previously mentioned.

In addition to the technical issues affecting service Availability, the user of Satellite Services should also be cognizant of the business conditions affecting the Satellite Services providers, such as bankruptcies. For instance, Iridium and Globalstar recently underwent financial reorganizations that left their users uncertain about the continuation of their service offerings.<sup>51</sup> Of course, other Satellite Service providers have had more stable financial situations and are not as prone to business failure. Nevertheless, the shakeout in service providers is expected to continue for the next year or two. This uncertainty as to the viability of providers must be considered when determining what services to procure to support NS/EP activities.

### **3.13.6 LMR and Two-Way Mobile Radio Products and Services**

Reliability and Availability of LMR and Two-Way Mobile Radio systems are based on the same issues affecting the other Non-Wireline Services. Quality equipment with good Reliability and Availability numbers are needed along with robust system designs and implementations to help preclude system failures. Sufficient and readily accessible backup equipment will help improve system availability in light of infrastructure failures.

As with new technologies for other Non-Wireline Services, NS/EP users of LMR and Two-Way Mobile Radio systems must be aware of the longevity of the technologies used in the equipment they implement or the radio services they procure. Therefore, choices of technologies used should be carefully made to ensure that technical support and replacement equipment is available in the future to support system operation. Likewise, the financial health of a particular company supplying equipment or services should be examined in order to determine the company's viability for long term existence.

---

<sup>51</sup> Iridium, under its reorganized structure, is now being cited in a positive light.

## 4 IT SYSTEMS and SERVICES

Frequently making a distinction between a Telecommunications System and an IT System is difficult. The reason being that IT Systems are integral parts of Telecommunications Systems. For example, the Advanced Intelligent Network (AIN) architecture of the PSTN relies on a telecommunications network device called a Service Control Point (SCP), which acts like an information repository or database. The SCP could be considered an IT System embedded in a Telecommunications System. In fact, the internal architecture of a modern digital telephone network switch is really a computer, which too could be considered an IT System.

Therefore, this study will make the following distinction between a Telecommunications System and an IT System. IT Systems in this study will not include those IT Systems which are an integral part of a Telecommunications System. Furthermore, the term “IT Systems and Services”, as used in this study, refers to services and systems which process information in a digital form. “Process” means that the information is, in some way, acquired, stored, processed, displayed, and/or interchanged. A Telecommunications System is considered a system which primarily transports information between various locations and between IT Systems. Telecommunications Systems, though, do process data for routing purposes.

As an example, the demarcation between a PC and a LAN occurs at the interface of the PC, which processes data, and the LAN, which transports data. The physical and electrical interface would be the cable connector that connects the PC to the LAN on the back of the PC. For this study, the LAN would be considered a telecommunications network. The equipment which would connect the LAN to a metropolitan area network (MAN) or a wide area network (WAN) would also be considered part of the Telecommunications System. The IT System would be contained in only the PC.

Another example would be that of a distributed web hosting environment, which processes information existing in different locations and is connected via a LAN, MAN, and/or WAN. The IT component of this distributed system would be only the processing systems. Only in a distributed computing environment in which the computing systems are directly connected to each other, that is the cable(s) from one device connect directly to another device(s), would no Telecommunications System be involved.

Even with the direction to outsource more IT functions to managed service providers, a significant portion of IT Systems and Services continue to be under the direct control and management of government entities. Multiple standards, some at times differing, have evolved resulting in added complexities to interoperability and sharing of information. The National Institute of Standards and Technology (NIST) has produced Federal Information Processing Standards. A major initiative has been underway to “standardize” Enterprise Architectures across government. The Federal Chief Information Officer (CIO) Council has produced *A Practical Guide to Federal Enterprise Architecture* as a

model for agencies to follow in developing their respective customized enterprise architectures. Enterprise architectures are blueprints for systematically and completely defining an agency's current or desired environment.

Within the Technology Service Group "IT Systems and Services", three major categories of IT Systems and Services have been identified and are examined in this study. They are:

1. Information Repository Systems, e.g., databases,
2. Monitoring and Control Systems, and
3. E-Commerce Systems.

These three categories have been identified based on their relative uniqueness. One exception may be the identification of an "Information Repository" as a separate category. Although Monitoring and Control Systems, as well as systems supporting E-Commerce, contain such repositories, this category is listed separately because it is an underlying basic component within each of the other two categories. Furthermore, it can function as a separate category without inclusion in the other two categories.

The remainder of this section describes each of the IT Systems and Services categories and explores how each of these categories are related to the 14 Functional Requirements. Since the Functional Requirements originally were identified for Telecommunications Services, some of the Requirements may not relate to one or more of the IT Services categories. In addition, the definition for some of the Requirements, as given in Table A-1 of Appendix A, may not be interpreted exactly the same for IT Systems and Services as they are for Telecommunications Services. In order to accommodate the application of some Functional Requirements to IT Services, the Functional Requirement itself may be slightly redefined. In this case, the modified Requirement name and its definition will be identified. Finally, some of the Functional Requirements have been grouped together because of their commonality.

## **4.1 Description of IT Systems and Service Categories**

### **4.1.1 Information Repository Systems**

An "Information Repository" is a collection of data that is structured and organized in a disciplined manner so that the information of interest may be quickly accessed.

Information Repositories may support NS/EP applications in several ways. First, they can be storage areas of equipment inventories and personnel information, which would be needed during a national security or emergency event. Second, they could contain information related to security, such as certificates, PINs, authorization codes, etc., which would be utilized when sending and receiving secure transmissions. Third, they could contain financial information, such as pay records, income, debits, prices, etc., which could be used to pay individuals and purchase equipment.

#### **4.1.2 Monitor and Control Systems**

A Monitor and Control System is specifically designed to acquire raw information from digital and analog sensors, process the information, and then control an output from the system. Analog sensors are devices that respond to a physical stimulus like thermal, optical, magnetic, and other electromagnetic energy. They are also sensitive to acoustic energy, mechanical deformation, and motion. Sensors are embedded in a variety of physical objects, like roads, pipes, and vehicles as well as being connected to measure electrical power, flow rates, and pressures. Digital sensors can be implemented in various devices to alert Monitoring and Control Systems of an “abnormal” situation in some IT and/or Telecommunications System, including excessive error recovery that may signal a requirement to replace certain components.

A particular type of Monitor and Control System is the Supervisory Control and Data Acquisition (SCADA) system. SCADA systems are used extensively by power, water, gas, and other utility companies to monitor and manage distribution systems. Such systems are also used for remote metering and load shedding. Since SCADA systems monitor and control crucial infrastructure distribution systems, they are key in supporting NS/EP activities. Processing and control decision-making processes within these systems are IT functions. Data input and output to these systems is accomplished via Telecommunications Systems.

Monitor and Control Systems rely on Telecommunications Systems to connect agents, i.e., devices that measure and collect data as well as responding with an action to a control command, and managers, i.e., devices that process the input data to generate output reports and control information for the agents. Even though the agents and managers of a Monitor and Control System are considered to be the IT System components, the Telecommunications System is essential for interconnecting them. Therefore, relating the NS/EP Functional Requirements to a Monitor and Control System will, by necessity, include consideration of the Telecommunications System between the agents and managers. In order for a Monitor and Control System to support NS/EP missions, its associated Telecommunications System must also adhere to the NS/EP Functional Requirements.

#### **4.1.3 E-Commerce Systems**

An E-Commerce System is an “on-line”<sup>52</sup> system for the electronic interchange of products, services, and information, which are made accessible via a portal or web browser interface. Often the data network is the Internet, but enterprise intranets and extranets may also be employed. On-line connections could be completed over LANs, MANs, and/or WANs. E-Commerce Systems can include e-mail systems and real-time tools, such as instant messaging, white boarding, and video/audio conferencing. E-Commerce can be conducted from among any combination of governments, government constituents, businesses, and consumers.

---

<sup>52</sup> “On-line” means the connection between the information supplier and information consumer is accomplished via a data network.

E-Commerce Systems support NS/EP missions by permitting personnel or organizations involved in NS/EP activities to conduct various types of transactions on-line to exchange and disseminate information. The ability to conduct these transactions during an NS/EP event may be imperative to get needed personnel and materiel to locations affected by a national security or emergency event. E-Commerce Systems also support preparatory activities for NS/EP events.

## **4.2 Enhanced Priority Treatment**

For NS/EP applications, Enhanced Priority Treatment for IT Systems and Services is as important a consideration as it is for Telecommunications Services. In the context of IT Systems and Services, Enhanced Priority Treatment refers to the priority given to processing of, or manipulating, data in a central processing unit (CPU) and the priority given to data input to and output from the IT device.

### **4.2.1 Information Repository Systems**

For an Information Repository, as an example, Enhanced Priority Treatment could be related to the priority given users to access information in the repository. During NS/EP events, the query load on the repository may increase dramatically since many users may be seeking information at the same time. As a consequence, the user queue may have to be prioritized so that those individuals needing immediate access to the repository's information can be placed at higher levels in the queue.

Higher priority can be accomplished in a number of ways. The transactions utilizing the data could be given priority. The critical information/data (or their indices) could be retrieved and stored in cache memory to shorten the access time. Another method would be to simply deny system access to any user not directly involved in the NS/EP event. This capability could be easily defined by a system administrator and invoked as needed during an event. It could be combined with a robust ad hoc query capability to ensure that personnel involved in the NS/EP event have access to required data.

### **4.2.2 Monitor and Control Systems**

In the context of a Monitor and Control System, Enhanced Priority Treatment relates to assigning priority to the functions of acquisition and processing of input signals along with the generation and distribution of control signals. For instance, in a SCADA system, some of the inputs may be related to distribution systems mandatory to supporting NS/EP activities while other signals are not so related. Priority treatment could be assigned to the handling of those input and output signals associated with the NS/EP activities.

In addition to assigning priority to the handling of the IT functions, priority could also be placed on the transmission of this input and output data by the Telecommunications System(s) transporting it. Otherwise, the Priority Treatment expended within the IT System may go for naught. Enhanced Priority Treatment for the Telecommunications

Systems connecting the Monitor and Control System's agents and managers would be accomplished as described in Section 2 of this study.

#### **4.2.3 E-Commerce Systems**

For E-Commerce Systems, Enhanced Priority Treatment relates to the rapidity with which a transaction is conducted. The speed of the transaction is dependent upon the priority given to processing data in a CPU and the priority given to data input to and output from the IT device. During an NS/EP event, Enhanced Priority Treatment should be applied to those transactions associated with the event relative to transactions not associated with the event. Those critical government information processing and telecommunications functions required during NS/EP events should be identified and appropriate measures, such as SLAs, implemented.

### **4.3 Security**

For IT Systems and Services, the Functional Requirement of "Secure Networks" should be restated as "Security". Within each of the three IT Systems and Services categories, Security issues must be addressed. The following discussion pertains to all three IT Systems and Services categories.

Securing the infrastructures and services that support critical government functions is paramount throughout all the processes associated with IT Services. Security policies, procedures, and practices must be in place and must cover systems end-to-end and between systems. Policies, procedures, and practices include physical and personnel security as well as security for IT and Telecommunications Systems. Stringent SLAs may need to be implemented and adhered to by IT and telecommunications service providers. A comprehensive, overarching Security Management Program must be implemented that covers all communities of interest. Since perfect security is not possible, the right mix of people, processes, and technologies must be brought together to address the appropriate levels of risks.

Security must be applied to allow only authorized individuals or systems to interact with the Information Repository, Monitor and Control, or E-Commerce Systems. Systems, processes, and/or procedures are required to permit only authorized access. Attempts at unauthorized access should be denied and recorded.

Access should be limited using various means. Access could be limited to only authorized individuals by using multi-level authentication and biometrics (including iris scan, hand geometry, fingerprints, voice prints, etc.), smart cards, PINs, and digital signatures. For some of these techniques, PKI would be required to handle keys for encryption and certificates associated with digital signatures. Access could be limited to authorized systems through the use of secure telecommunications connections and secure authorization codes. Classified communications could use the NSA approved STU-III, or next generation follow-on STE that will take advantage of digital communications, like ISDN and ATM. Access could be restricted to the system itself or to the information

contained within the system. Enterprise Directory Services could be used to manage and provide authorization to systems down to the database level. Relational Database Management Systems could also be employed to provide added security for limiting access and/or update authority on specific data elements to only authorized individuals.

Attempts to disable the computing systems and networks that are part of the critical infrastructures can take a number of forms. Viruses and worms, such as NIMDA, Code Red, and Melissa, can cause wide spread system and network problems. Trojan horses can remain in systems for later activation. Regular reviews, installation of virus/worm prevention patches, and virus scanning are critical to maintaining system integrity. In order to counter this threat, OMB recommends that continuous monitoring and testing be built into and funded as part of agency IT investments.

Corrupted information in any of the three IT Systems and Services categories could result in an inability to process the information or result in incorrectly processed information as an output. Three types of service denial attacks are possible.

The first is a DoS attack, which could occur if information is corrupted during its input or output process or while in the system itself. DoS could occur due to requests for inputs and outputs in such great quantities that the processing of the requests overloads the system, and it can not function. DoS could also result from denial of access to the system. The end result would be a DoS situation for the information's user.

Two other types of service denials are Distributed Denial of Service (DDoS)<sup>53</sup> and Distributed Reflection Denial of Service (DRDoS)<sup>54</sup> attacks. DDoS attacks can be originated from multiple distributed systems to concentrate attacks on certain systems or network elements. DRDoS is a more advanced DDoS malicious attack in which "innocent" servers, thinking they are doing their jobs, are reflecting floods of packets to a targeted server.

A particular set of security vulnerabilities have been identified for the Simple Network Management Protocol (SNMP) version 1. These vulnerabilities exist within network devices as well as for data being transmitted in an unsecured manner. The vulnerabilities could be exploited in a DoS attack, resulting in a service interruption, or by a malicious user looking to gain access to certain systems. The vulnerabilities are bi-directional in

---

<sup>53</sup>A DDoS attack exploits the vulnerabilities of one computing system, making it the DDoS "master". The master system then identifies and communicates with other systems that can be compromised. These systems are set up to launch an attack simultaneously on some specified target(s) by inundating it (them) with packets from multiple systems.

<sup>54</sup> DRDoS utilizes publicly accessible Internet servers and "spoofs" them with SYN packets that have an attack target address to which the "return", or the "ACK", message is sent. The receiving server sends these ACK packets on to the target server thinking it is responding to the originator of the SYN. The targeted server then can be overwhelmed by the "ACK" messages. ("SYN" is a transmission control character used to "synchronize" transmissions, and "ACK" is a transmission control character used to "acknowledge" receipt of a transmission.)

that messages from network agents to a manager and from a manager to an agent in a Monitor and Control System could be affected. Individual network device manufacturers have published work-arounds to avoid the risks associated with these vulnerabilities in SNMP version 1 until permanent fixes can be developed and implemented, i.e., most likely with a version 3 of the SNMP code.

Encrypting the data is also critical to maintaining security and privacy. Data can be encrypted in the data store. The Advanced Encryption Standard (AES)<sup>55</sup> is now in place since the former DES is too easy to “crack”. Use of the AES is compulsory and binding on federal agencies for the protection of sensitive, unclassified information. The NIST Federal Information Processing Standard (FIPS) PUB 197 should be followed for unclassified data.

Encryptors to secure payload data as it traverses telecommunications links can be utilized. For classified data, NSA-certified encryptors, including the TACLANE–E-100 and TACLANE (KG-175), can be used for handling Type 1<sup>56</sup> security requirements. These encryptors were developed by the NSA to provide network communications security on the IP and ATM networks for the individual user or for enclaves of users at the same security level. KG-175s can be used to overlay Secure Virtual Networks (SVNs) on top of existing public and/or private network infrastructures, including the public Internet.

#### **4.4 Audit Trails and Non-Traceability**

For most IT Services, the Functional Requirement of “Non-Traceability” is inapplicable and should be replaced with the requirement for “Audit Trails”. Audit Trails are necessary for IT Systems since users and operators usually need to know the derivation of data and actions occurring in the IT System itself. For this study, the discussion of Audit Trails applies to all three IT Systems and Services.

IT Systems can maintain logs and Audit Trails. An Audit Trail is a series of records of computer events about an application, such as an Information Repository, a user, or an operating system. Audit Trails have a number of uses in computer security. An individual’s activities can be tracked allowing for personal accountability. Audit Trails can be used to reconstruct events after a problem has occurred. They may also be used as on-line tools to monitor problems in real-time as they occur. Real-time problems can range from network failure to various types of DoS attacks. Audit trails can also be used to help identify attempts to penetrate a system and gain unauthorized access. For example, all E-Commerce transactions can be logged for later analysis and review, in

---

<sup>55</sup> The effective date for using the AES was May 26, 2002. AES is defined in Federal Information Processing Standard Pub 197.

<sup>56</sup> The Endorsed Cryptographic Products List (ECPL) - Contains a variety of items ranging from components to finished products with embedded cryptography. Items are divided into two categories: Type 1 which are used to secure classified information and Type 2 which are used to protect only sensitive Government Information.

part, to collect trend data. Monitor and Control System events can be logged and reviewed on a real-time basis to determine unusual activities, such as persistent unauthorized attempts to penetrate the systems and/patterns to disable the systems.

In the case of Monitor and Control systems, the Functional Requirement of “Non-Traceability” is applicable under certain circumstances. For instance, data transmitted between devices in a monitor and control system may have a requirement to be untraceable. A possible reason would be that the system manager or the agents being controlled are so sensitive that their location, or even existence, must remain unknown to unauthorized parties. To effect Non-Traceability in this instance, the transmitted sensory/control data would have to have its origination and destination addresses encrypted, removed, or otherwise hidden to unauthorized parties

#### **4.5 Interconnectivity and Interoperability**

The Functional Requirement of “International Connectivity” is not truly applicable to IT Systems and Services since it was originally developed for domestic Telecommunications Systems, which must be able to connect internationally with other Telecommunications Systems to support NS/EP activities in foreign countries. A more appropriate requirement for IT Systems is “Interconnectivity”. Furthermore, the Functional Requirement of “Interoperability” is closely aligned with Interconnectivity and does have applicability to IT Systems as well as to Telecommunications Systems. Therefore, the two requirements have been grouped together for this discussion.

For this study, the “Interconnectivity and Interoperability” requirement applies to the ability to share information among IT Systems as well as to permit Interoperability between IT Systems. During an NS/EP event, Interconnectivity and Interoperability would be very important when different organizations need to share data, each of which may be using different systems and/or data formats. The ability to harmoniously interchange information during NS/EP events would significantly increase efficiency in dealing with the situations.

##### **4.5.1 Information Repository Systems**

Interoperability problems among IT Systems using different data formats and data exchange protocols can be alleviated by employing standards governing information exchange. Interconnectivity and Interoperability among Information Repository Systems is accomplished by common standardized data formats and languages, such as the Structured Query Language (SQL) for databases, and protocols for interoperation of systems.

Some of these protocols, which may be used for the interchange of data between IT Systems, are SNMP, the X.400 protocol for e-mail, the X.500 protocol for directories, and the Utility Communications Architecture (UCA) for communications by utilities.<sup>57</sup>

---

<sup>57</sup> See Appendix E for additional information about these protocols.

Higher level applications protocols use the TCP/IP for Internet access. These higher level applications protocols include the World Wide Web's Hypertext Transfer Protocol (HTTP), the FTP, Telnet (which allows a user to logon to remote computers), and the Simple Mail Transfer Protocol (SMTP). These, and other protocols, are often packaged together with TCP/IP as a "suite". In those instances in which non-common formats, languages, or protocols are used in Information Repository Systems, software data conversion programs would be needed to effect information interchange between the non-standard IT Systems.

#### **4.5.2 Monitor and Control Systems**

Interconnectivity and Interoperability for Monitor and Control Systems need to be accomplished at the protocol level. Recognized sensory/control protocols, like SNMP, are needed to correctly interpret data transferred among different Monitor and Control Systems as well as data transferred between agents and managers.

As a particular example, the utilities industry has created the UCA, which is a standards-based approach to utilities communications and is designed to apply across all of the functional areas within the electric, gas, and water utilities. It is an architecture rather than a simple protocol and incorporates a family of communications protocols designed to meet the requirements of a wide variety of utility environments. The profiles in UCA version 2 include connection-oriented or connectionless communications running over a wide variety of media including those specific to utilities, such as radio.<sup>58</sup>

Furthermore, if a Monitor and Control System employs multiple Telecommunications Systems between the agents and managers, these Telecommunications Systems must support Interconnectivity and Interoperability among each other. An example of this scenario would be that of a power grid that relies on multiple Telecommunications Systems to connect a power measurement agent with its manager. In order to transport the data between the agent and manager, the Telecommunications Systems must be interconnected and interoperable.

#### **4.5.3 E-Commerce Systems**

E-Commerce Systems require Interconnectivity among many different IT databases, processors, and servers in order to access, process, and deliver information. E-Commerce Systems rely on a diverse set of components, such as standard PCs, mobile laptops, or handheld devices, like PDAs, cell phones, or radios, which must be able to interconnect.

Interoperability also includes the interface to the human users and operators of the E-Commerce System. These interfaces can be in the form of a Graphical User Interface (GUI), which is designed for a specific E-Commerce application, or a web browser interface. In either case, the interface must be intuitive and serve as the mechanism that pulls together specific information that a particular user's needs. Hundreds of portal

---

<sup>58</sup> See Appendix E for additional information about UCA.

software providers exist with products that vary from being platform specific to ones which are more open and flexible. Two of the more widely used portals are from Vignette and Plumtree. Two common web browser applications are the Netscape Communicator and Microsoft Internet Explorer.

Supporting end-users are web server programs, which serve the files that form web pages. Two leading COTS web servers are Apache, the most widely-installed web server, and Microsoft's Internet Information Server (IIS). Other servers include IBM's Lotus Domino, which is primarily for IBM's mainframe server customers. Web servers often are part of a larger package of Internet-related programs for serving e-mail, downloading files via FTP, as well as building and publishing web pages. These web servers could be part of an outsourced or in-house web hosting environment with multiple servers of various brands and technologies<sup>59</sup>, all of which must interoperate.

The next level above the web servers would be the application and/or data servers, which support the E-Commerce applications with the business rules and the data repositories. The application and data servers could be separate or the same mid-tier or mainframes systems.

A number of software products are on the market that facilitate the communications and exchange of data among different E-Commerce System components. For example, the Extensible Markup Language (XML) is a flexible way to create common information formats and share both the format and the data. XML requires strict adherence to coding standards, but it also enables a rich form of data interchange. By describing data using XML, data is made more useful for access via internets, intranets, and extranets.

Also supporting the Interconnection and Interoperability of E-Commerce Systems are various "middleware" products that "glue together" or mediate between two separate systems or applications. Middleware forms a transition layer that allows for Interoperability between components of the E-Commerce infrastructure. When two or more hardware devices or software applications need to work together, middleware is the interpreter that enables communications over similar or different platforms. As an example, IBM provides a software platform called WebSphere with a middleware solution called MQSeries that facilitates the connection of a web server to a legacy mainframe or to other platforms. As another example, Sun has an E-Commerce platform called Sun ONE, or its core component iPlanet, that includes integration and messaging servers.

Interconnectivity and Interoperability among E-Commerce Systems is not only a technical issue, but it is also a management issue. A variety of permutations and combinations of ownership and operational responsibilities comprise the E-Commerce environment. Interrelationships must be established among E-Commerce System

---

<sup>59</sup> The most common platforms are Intel-based systems running Windows NT/2000/XP operating systems or UNIX mid-tier systems, such as Sun or IBM RISC S/6000.

components which are outsourced and those which are owned in-house by the operating organization. Hence, activities associated with the different E-Commerce System components must be coordinated in an organized and logical manner.

#### **4.6 Mobility**

Mobility for IT Systems is imperative to support NS/EP events. Often fixed IT Systems may be damaged or destroyed during an NS/EP event, and mobile systems would be required to replace the original systems. Furthermore, as NS/EP responders move to a location to deal with the emergency or national security event, they would need to have mobile IT Systems to bring with them.

For this discussion, a slight distinction is made between a “Transportable” IT System and a “Mobile” IT System. The former type of system is designed to be easily moved and to not, necessarily, be operative during the move. The latter designation, i.e., “Mobile”, implies that the IT System could be operative while in motion and could be interconnected via a Non-Wireline technology with the remainder of the IT infrastructure.

##### **4.6.1 Information Repository Systems**

Mobile and Transportable Information Repository Systems are necessary to support NS/EP events. They can reside on mobile PCs, like laptops, and larger systems, like mini-computers.

A Mobile Information Repository System could reside on a large vehicle, such as the FEMA MATS. While the vehicle was in motion, the Information Repository System could be operational. When the vehicle was stationary, the Information Repository System could be interconnected with Wireline and Non-Wireline data networks.

A Transportable Information Repository System could be part of a transportable temporary DFO that would be temporarily established until a permanent DFO could be put in place. The Transportable Repository System using a mini-computer, for instance, could be driven or flown into a site and deployed in a short time for use until a permanent system could be established or was no longer temporarily needed. Then the Information Repository System could be interconnected with Wireline and Non-Wireline data networks.

##### **4.6.2 Monitor and Control Systems**

Depending upon the implementation of Monitor and Control Systems supporting NS/EP missions, Mobility may be a requirement. For instance, if a Monitor and Control System is monitoring the deployment of personnel or material, a monitoring agent may be attached to a mobile vehicle, or even a person. This agent may be measuring the position of the vehicle or person and reporting this information back to a central dispatch point. GPS could be used in this situation to track various types of resources. For example, if emergency vehicles were deployed during an event, a GPS receiver could collect vehicle

data, such as speed, vehicle location, and activation of specific events associated with the vehicle.

If mobile monitoring is required, the communications link from the mobile agent to the agent's manager could be accomplished in whole or in part via radio, satellite, or cellular links. Private or public wireline Telecommunications Systems may be used to complete the link between the agent and the manager if the RF link is insufficient to complete the link.

#### **4.6.3 E-Commerce Systems**

E-Commerce Systems are unlikely to be used in a Mobile fashion to support NS/EP events. Generally, these systems consist of relatively large and fixed equipment housed in data centers. Because the electronic transactions such systems involve include a number of back-office functions, such as billing and electronic payments, they are not generally deployed in a Mobile fashion, in that they would not be in operation while in motion.

However, E-Commerce Systems could be made Transportable. For example, they could be deployed to temporary DFOs during the NS/EP event and connected with users via wireline and non-wireline Telecommunications Services.

### **4.7 Restorability**

All three IT Systems and Services categories rely upon rapid Restorability in order to be effective supporting NS/EP activities. Each category has unique requirements for Restorability. However, one general requirement is the availability and use of a comprehensive disaster recovery plan which lays out procedures for the processes used to restore the particular IT System or Service of interest. IT Systems may employ a number of operational precautionary procedures to aid in restoration.

#### **4.7.1 Information Repository Systems**

In order to be effective in supporting NS/EP missions, Information Repository Systems must have architectures that allow the information that the systems contain to be quickly and easily accessed following a system failure. System failures may be due to such diverse causes as natural disasters, system software failures, destructive viruses, or sabotage. The ability to restore essential and full service following a disruption is one of the four key characteristics of a survivable system (see Section [4.8](#)).

For Information Repository Systems, processes for restoration resulting from localized failures, e.g., disk storage failures, must be implemented. For instance, backup copies of standard or customized software with write protection features should be maintained in a physically separate, but accessible, site away from the IT System. Complete system backups should be performed on a regular basis with incremental backups occurring more frequently, also on a scheduled basis. The number of backup generations to be maintained should be determined upon implementation of the Information Repository System. Database management systems and associated transactions should be logged to

assist in restoration. The feasibility of reconstruction of the system using existing backup copies of the system data should be established. Periodic checks on the quality of the backup medium should be made.

Additionally, evolving technology is producing new techniques designed to prevent system disruption in case of system component failure. An example of this is in data “mirroring”. Data is collected and stored redundantly on two or more co-located disks. This is a parallel rather than sequential process so no performance penalty ensues. The mirrored data could alternately be transmitted to a remote location via a high-speed telecommunications network connection to achieve greater resiliency, but this technique does incur a performance penalty.

Another technique using mirroring for rapid restoration after a system-wide catastrophe, as opposed to a limited local equipment failure, is to employ a “hot” backup site. At this site, the entire operation of an Information Repository is maintained, i.e., “mirrored”, in real-time in an identical hardware and software backup repository in another physical location. The “hot” backup site, must be configured such that the backup repository can be made the active repository immediately upon failure of the primary repository. The switch to the backup repository system would require that the Telecommunications Systems connected to the backup system also be quickly activated. Based on a risk versus affordability analysis, a “cold” backup scheme may be selected that provides for near-term availability of additional equipment at a secondary site allowing resumption of operations in a reasonable period of time. A variation of these two techniques would be a hot standby scoped only to support “essential” as opposed to “full” services. Redundancy in the telecommunications network and a connection(s) to the alternate site are important components of this technique.

#### **4.7.2 Monitor and Control Systems**

The same restoration techniques used for Information Repository Systems apply to Monitor and Control Systems. Restoration for Monitor and Control Systems could be accomplished via rapid automatic switchovers to redundant network agent and manager equipment. In addition to redundant equipment, automatic restoration could entail redundant or alternate telecommunications paths between an agent and manager. Monitor and Control System software would have to support whatever restoration scenario is implemented.

#### **4.7.3 E-Commerce Systems**

Techniques similar to those used for Information Repository Systems and Monitor and Control Systems should be employed for E-Commerce Systems. Mirroring could also support E-Commerce in that the multiple copies of the data could be intended for purposes other than system recovery, e.g., accounting and marketing usage. Rapid automatic switch over to a database system or other Information Repository would be needed as well as activation of the Telecommunications System connected to the backup facilities, as outlined in Section [4.7.1](#).

#### 4.8 Survivability/Endurability

Many considerations regarding Survivability and Endurability affect all three major IT Systems and Services categories. For this reason, a general discussion of Survivability and Endurability follows. However, additional considerations apply to Monitor and Control Systems and are discussed in Section [4.8.1](#). Furthermore, conditions affecting the Survivability and Endurability for the operation of any IT System are dependent, in part, upon the Restorability and the Reliability/Availability of the system. Restorability issues are described in Section [4.7](#), and Reliability/Availability issues are discussed in Section [4.9](#).

Survivability may be defined as the capability of a system to fulfill its mission or organizational objectives in a timely manner, even in the presence of attacks, accidents, or failures. Virtually all organizations in defense, business, and government are dependent on large-scale, networked information systems. The Computer Emergency Response Team (CERT)/ Software Engineering Institute (SEI) has developed a methodology called Survivable Network Analysis (SNA) that is designed to provide a means to assess and improve system Survivability. Survivable systems have been characterized in this methodology as having four primary properties<sup>60</sup>:

1. Resistance to attacks,
2. Recognition of attacks and damage,
3. Restoration (or recovery) of essential and full services after the attack, and
4. Adaptation and evolution to reduce the effectiveness of future attacks.

A number of techniques may be used to resist attacks. In terms of resisting physical attack, access to the facility housing the system should be restricted. In some cases, the physical site may be hardened, depending upon the criticality of the system's mission. A number of techniques are applicable to the system itself. User authentication can limit access to a group of authorized users. Access controls can range from simple passwords to biometric recognition and can control access ranging from the system level down to individual data items. Encryption can protect data, either within a system or in transit between systems. Encryption can also be used for authentication and other assurance purposes. Message filtering at the system boundary can be used to selectively block messages, such as those associated with known attacks. Message filters could also be applied at the operations system interface level. These filters could be used at this level for purposes such as operand checking or to impose a restrictive access control policy on a given application. Functional isolation, when achievable, will reduce or eliminate dependencies among services so that an attack on one service will not compromise other services. Survivability places stringent requirements on system development and testing practices. Software errors can produce the equivalent of an attack due to malfunction and can also provide opportunities for intruder exploitation.

---

<sup>60</sup> *Survivable Network Analysis Method*, CMU/SEI-2000-TR-013

Recognition of an attack can be critical to system survival. Intrusion detection is one means of attack detection. It can be accomplished through recognition of deviations from established baseline behavior or through recognition of known attack patterns. Both techniques can be applied to platform or application specific data as well as to network traffic. System audits and logging provide sources of information for integrity checking at the application level. Corruption of data can be detected by computing a baseline checksum or cryptographic signature to be used for periodic comparison to the current data contents.

Methods for restoration or recovery, the third component of survivability, are discussed in Section [4.7](#).

The fourth area of Survivability is system adaptation and evolution. Systems will evolve in response to user requirements for new functions and intruders' increasing knowledge of system structure and behavior. Survivability requires that a system evolve faster than intruder knowledge. Adaptation and evolution prevent the accumulation of information about invariant system structures and behaviors needed for successful system penetration and exploitation. Evolution also involves creating defenses for never-before-seen attacks or intrusions and is an area of current research.

#### **4.8.1 Monitor and Control Systems**

In addition to all the fundamentals for a Survivable and Endurable system described in the introduction of Section [4.8](#), Monitor and Control Systems have additional requirements for protection of agents and the telecommunications links between the agents and manager.

Since agents probably will be distributed in a field environment, they may not have as much physical protection against man-made or natural disasters as a centralized site. They may also be more susceptible to compromise by individuals with malicious intentions due to their accessibility and the remoteness of their locations. Consequently agent redundancy requirements and operational scenarios assuming some loss of agents should be a part of survivability planning.

The Survivability and Endurability of Monitor and Control Systems is also very dependent upon the Survivability and Endurability of the Telecommunications System(s) connecting the agents to the manager. Without a robust Telecommunications System, the agents will lose connectivity with their manager, and the Monitor and Control System probably will fail. For critical applications, two separate, diversely routed and redundant telecommunications networks may be required for data transport.

#### **4.9 Reliability and Availability**

High Reliability and Availability are necessary conditions for obtaining a Survivable and Endurable IT System. Means for achieving the required conditions are dependent upon the system's design, implementation, maintenance, and operation. An IT System's

Reliability and Availability are only as good as the system's most vulnerable component or link. The ability to quickly restore the system after a failure goes directly to computing the Mean Time Between Failure (MTBF) and, hence, the system's Reliability and Availability.

A system design architecture, including redundancy of critical components coupled with high Reliability and Availability of the individual components, will add to the overall system's Reliability and Availability. Regular system backups and alternate storage sites for databases along with periodic drills on the recovery procedures can improve system Availability. Recovery from hardware crashes should be an integral part of the Disaster Recovery/Business Continuity procedures employed by the IT System's operator.

To ensure Reliable and Available systems, thorough regression and integration testing of changes and updates must be done prior to deployment. Any subsequent changes or updates to the systems must be reviewed and authorized by the Configuration/Change Control Board (CCB) at the enterprise level after thorough regression and integration testing before "promoting" the changes or updates to the production environment.<sup>61</sup> This review includes all fixes and/or patches that may be subsequently provided for the IT System components.

For any portions of the IT System that are under the management of a Managed Service Provider (MSP), SLAs with specific metrics for Reliability and Availability should be negotiated and included in the contracts. Overall coordination and management of the end-to-end system must be implemented with specific policies, practices, procedures, and delineated responsibilities. An encompassing concept of operations should be developed. Since commercial product vendors, integration contractors, and MSPs are so important in the ultimate Reliability and Availability of the total IT System, they must be treated as partners and appropriately managed with incentives based on outcomes using the concepts of Performance Based Contracting.

"Best Practices" for software acquisition and development should follow standards or models like those from the Carnegie Mellon SEI. Numerous tools and "best practice" guidelines are available and can be found at the SEI web site <http://www.sei.cmu.edu/>. The SEI has a number of best practices and/or initiatives including their COTS-Based Systems (CBS) Initiative that is focused on improving the technologies and practices used for assembling previously existing components (COTS and other non-developmental items) into large software systems and migrating existing systems toward CBS approaches.<sup>62</sup>

---

<sup>61</sup> A technical organization, like an Engineering Review Board, typically reviews all changes and updates before they go for final review by the CCB.

<sup>62</sup> This CBS approach changes the focus of software engineering from one of traditional systems specification and construction to one requiring simultaneous consideration of the system characteristics such as requirements, cost, schedule, operating, and support environment capabilities of products in the marketplace, and viable architectures and designs.

Complementary to the CBS is the Software Acquisition Capability Maturity Model (SA-CMM), which provides practices and processes for acquisition of software systems and products. It is a model that describes the key elements of managing and improving the acquisition process in an organization. The SA-CMM outlines a managed path for improving the process for acquiring software from an ad hoc approach to a mature, disciplined approach in which all aspects of the acquisition and oversight process are managed to enhance the organization's overall performance of the work.

However, the development of COTS-based systems continues to involve significant technical risks, and higher Reliability and Availability are often a challenge to fulfill. In addition, government agencies have traditionally adopted more stable and mature IT solutions, allowing private industry to pioneer the technologies and work out the bugs. Terrorist threats have prompted federal officials to look to more advanced, leading edge technologies and attempt to accelerate their implementation and deployment. This acceleration has the potential to decrease the IT System's Reliability and Availability.

Therefore, another SEI best practice, the Software Risk Evaluation (SRE) Service can provide a disciplined approach to proactive program management for software development. SRE can provide diagnostic and decision-making tools that enable the identification, analysis, tracking, mitigation, and communication of risks in software intensive programs. An SRE can be used to identify and categorize specific program risks emanating from COTS products, integration requirements, process, management, resources, and constraints.

#### **4.9.1 Information Repository Systems**

Information Repository System contamination may require specialized recovery procedures. Since all transactions should be logged and the data backed-up, the databases can be re-created. Partitioning of the databases will allow certain portions to remain operational while other portions are being recovered. Appropriate security mechanisms are available to minimize the likelihood and exposure to contamination. For example, only authorized individuals and associated transactions should be allowed to update specific data fields. Passwords and other multi-level security authentication techniques, including biometrics, could be utilized.

#### **4.9.2 Monitor and Control Systems**

In addition to the general considerations for achieving high Reliability and Availability and the more specific considerations described for Information Repository Systems, Monitor and Control Systems have the additional requirement to consider the Reliability and Availability of the telecommunications links between agents and their managers. To this end, approaches described in Sections 2 and 3 regarding achieving high Reliability and Availability for Telecommunications Services should be followed.

To enhance the Reliability and Availability of the network elements being monitored, “out-of-band” management can be utilized to determine the state of the network element, i.e., agent and manager, and attempt to restore its normal state. If returning to the normal state is not possible, then the “out-of-band” management can be used to determine the nature of the failure and take appropriate actions, including manual initiation of a backup capability. Alerts generated by the agents can be monitored and actions taken. Logging of the events can provide analysis for trends and potential failures or attempts to disable the system.

### **4.9.3 E-Commerce Systems**

The Reliability and Availability considerations for the Information Repository and Monitor and Control Systems also apply to E-Commerce Systems. Since the E-Commerce Systems have multiple IT and telecommunications components that include COTS, as well as customized and user developed system and application software, the SEI best practices and procedures should be followed. In addition, since E-Commerce transactions could go over the public Internet, specialized implementations may be required to “isolate” and duplicate major E-Commerce System components. This isolation may include reserving and duplicating servers, network components, conduits/cable, fiber, and/or fiber optic wavelengths for critical government functions. If an ISP is used, a second ISP should be available as an alternative. If certain components of the E-Commerce environment are outsourced, e.g., web hosting, then an alternative source should be available for the outsourced components.

## **4.10 Voice Band Service**

The Functional Requirement of Voice Band Service was originally created to describe a type of Telecommunications Service necessary to support NS/EP activities, that is the voice service available from the PSTN. However, the Functional Requirement of Voice Band Service has some limited applicability to IT Systems and Services, if only in the context of Telecommunications Services closely associated with the IT Systems and Services.

### **4.10.1 Information Repository Systems**

In general, Information Repositories, in this discussion, have focused on large databases as repositories. Voice Band Service is not typically applicable to the operation of such large Information Repository Systems. However, voice band circuits can connect to these systems. These circuits do, however, operate at low data rates, such that transmission of large data volumes may not be practical. Small volumes of data or system control information could be transmitted, as is regularly done by individuals using PSTN dial-up connections, to the repository. In addition, voice messages can be recorded and the message files entered into and retrieved from these repositories.

### **4.10.2 Monitor and Control Systems**

Voice Band Service circuits may be an alternative to effect control of agents by their manager in the event of a failure of the primary telecommunications sensory/control

network connecting the agents and managers. As a backup, e.g., as a dial or radio backup, voice band communications may be used by personnel on site at an agent's location to forward sensory information from the agent to personnel at the manager's location. Similarly, control information from the manager could be directed to personnel at the agent. Voice Band Service could be provided by wireless, satellite, or radio services if Wireline Services were not available. This out-of-band control may have to have added security to ensure unauthorized parties do not tamper with the information transmitted.

Similarly Voice Band Service circuits could also be the permanent low data bandwidth telecommunications links between agents and their manager. Some analog voice channels operating over radio links, for example, could support low data bandwidths too.

#### **4.10.3 E-Commerce Systems**

In general, Voice Band Service is not applicable to the operation of E-Commerce Systems. However, as with Information Repository Systems, Telecommunications Services connected to E-Commerce Systems and providing digital or analog voice band services may provide adequate accessibility to the E-Commerce Systems.

#### **4.11 Broadband Service**

As with Voice Band Service, the Functional Requirement of Broadband Service was originally created to characterize the of Telecommunications Services to support higher data bandwidths. Again, this Functional Requirement has some limited applicability to IT Systems and Services, if only in the context of Telecommunications Services closely associated with the IT Systems and Services.

##### **4.11.1 Information Repository Systems**

In general, Broadband Service is not applicable to the operation of Information Repositories. However, the data bandwidth required of the telecommunications network connected to the repositories for data transmission purposes may require Broadband Service. The determination of the need for Broadband Service is dependent upon the applications using the repositories and the required data transmission rate to and from the repositories.

##### **4.11.2 Monitor and Control Systems**

A Monitor and Control System may require Broadband Services, depending upon the system's telecommunications network architecture and traffic load. For instance, if the agents are connected to the manager via a "bus topology"<sup>63</sup>, then all of the data to and from the manager is carried by a single communications link. Depending upon the maximum data rate the link must carry, a Broadband Service may be needed to support the traffic load on the bus. Wireline, wireless, and satellite services could be employed for Broadband Service.

---

<sup>63</sup> In a "bus topology" the agents are connected to a single communications link, i.e., "bus", which connects the agents to the manager. Data is transmitted by the manager to all of the agents. Each agent receives only that information designated for it. Similarly, each agent transmits its data to the manager on the bus.

Furthermore, a Monitor and Control System may also require a broadband telecommunications link between the managers in the system and an operational control center. The need for this link is dependent upon the design of the Monitor and Control System.

#### **4.11.3 E-Commerce Systems**

As with Information Repositories, Broadband Service is not applicable, per sé, to the operation of E-Commerce Systems. However, the data bandwidth required of the telecommunications network connected to the E-Commerce System may require Broadband Service. Since many transactions may occur simultaneously with an E-Commerce System, the connection of the system's servers to the telecommunications network may be accomplished via broadband services, like IP, FR, or ATM.

#### **4.12 Scalable Bandwidth**

As with Voice Band Service and Broadband Service, the Functional Requirement of Scalable Bandwidth was originally created to characterize the Telecommunications Services to accommodate varying data bandwidths. This Functional Requirement has some limited applicability to IT Systems and Services, if only in the context of Telecommunications Services closely associated with the IT Systems and Services.

##### **4.12.1 Information Repository Systems**

As with the Functional Requirement for Broadband Service, Scalable Bandwidth is not a requirement for an Information Repository System's operation itself. However, the telecommunications network connected to the Information Repository may require Scalable Bandwidth depending upon traffic load into and out of the system.

##### **4.12.2 Monitor and Control Systems**

As with the Functional Requirement for Broadband Service, a Monitor and Control System may require Scalable Bandwidth. The system's communication network architecture and traffic load requirements between the agents and managers will determine the bandwidth(s) needed.

##### **4.12.3 E-Commerce Systems**

As with Information Repositories, Scalable Bandwidth is not an applicable requirement to the operation of E-Commerce Systems themselves. However, the data bandwidth required of the telecommunications network connected to a system may require the bandwidth to be scalable depending upon the number of simultaneous attempts to transact business with the E-Commerce System. The processing capabilities of the E-Commerce System will help determine the varying telecommunications traffic loads expected.

### 4.13 Affordability

This section addresses Affordability on a total system basis, which includes hardware, software, and any associated supporting telecommunications along with design, implementation, and operational costs for IT Systems. Issues concerning Affordability are equally applicable to Information Repository Systems, Monitor and Control Systems, and E-Commerce Systems.

Affordability is relative, particularly with reference to IT Systems and Services. Typically, an organization looks at the Total Cost of Ownership (TCO), which includes the hardware and software costs along with costs for development, testing, integration, security certification/accreditation, on-going maintenance, operations, depreciation, as well as facilities and personnel (for management, development, administration, and operations). Costs will also accrue for any component of the IT System which is outsourced.

In the past, hardware costs have generally followed Moore's law<sup>64</sup> in that processing power has significantly increased over the years while chip prices have decreased. Hardware technology has progressed such that many hardware components within IT Systems are COTS with accompanying commodity prices.

However, high-end hardware, e.g., mainframe servers and software systems, may be customized and include significant application development and/or COTS product customization in order to support critical government functions. The requirements for security, reliability, availability, survivability, and recoverability could double the TCO because of the redundancies that need to be built in to systems. Finally, large scale software projects require significant testing and integration. All these factors could negate the Affordability available with COTS products.

One way to control, and possibly reduce, government-wide costs for IT Systems and Services is to minimize the duplicate stovepipes that exist within organizations. For example, in the federal government, OMB is promoting the use of a components-based enterprise architecture that allows one agency to use technology that has proven successful at another agency. In addition, adhering to the enterprise architecture and following best practices, like those from the SEI, permits an organization to increase the possibilities of the system development activities coming in on-time and on-budget.

In some cases, outsourcing certain IT functions can reduce the overall cost of providing an IT Service. The benefits of outsourcing need to be investigated on a case-by-case basis. Within the federal government, outsourcing could also provide much needed IT skills that are not being replaced in government agencies as key personnel retire. Finally, the outsourcer may be in a better position to provide more immediate scalable resources

---

<sup>64</sup> George Moore, the Intel executive, forecasted that the chip density would double every 18 to 24 months and price-performance ratio would decrease proportionally.

to address immediate needs. Overall, the outsourcing approach may be the most affordable alternative for providing IT Services.

Affordability should always be considered as a “relative” term. IT System Affordability must be compared against possible alternatives and the expenses associated with them. Because of the criticality of IT Systems used to support NS/EP activities, one must consider the cost of the IT System in terms of the cost of not accomplishing the NS/EP activities. In a case in which national security could be compromised through IT System failure, the importance of securing the system environment could justify expenditures far exceeding the cost of the basic system itself.

The relative Affordability of a system can be determined by an analysis of potential risk events to the system, the consequences if those risk events occur, and the costs associated with the risk events occurring. OMB (as a part of Circular A-130, Appendix III, *Security of Federal Automated Information Resources*) requires federal agencies to consider risk when deciding what security controls to implement. The Circular states that a risk-based approach is required to determine adequate security. A risk assessment program will identify mission-critical systems, assess the importance and sensitivity of the system information, and assess the likelihood of system corruption or penetration. Based on the results of the risk analysis, security measures may be defined.

Some of the other issues impinging on determining relative system Affordability are also discussed in Section [4.3](#) “Security”, Section [4.7](#) “Restorability”, and Section [4.8](#) “Survivability/Endurability”.

#### **4.14 Ubiquitous Coverage**

Ubiquitous Coverage is not considered to be applicable to IT Systems and Services since this Functional Requirement was originally created to apply to the coverage of Telecommunications Services.

**Appendix A**

**Table A-1 – NS/EP Telecommunication Services Functional Requirements**

NS/EP Telecommunication Services Functional Requirements	Description
Enhanced Priority Treatment	Services supporting NS/EP missions must be provided priority treatment over other traffic.
Secure Networks	Networks must have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.
Non-Traceability	Selected users must be able to use NS/EP services without risk of usage being traced (i.e., without risk of user or location being identified).
Restorability	Should a disruption occur, services must be capable of being reprovisioned, repaired, or restored to required service levels on a priority basis.
International Connectivity	Services must provide access to and egress from international carriers.
Interoperability	Services must interconnect and interoperate with other selected government or private facilities, systems, and networks.
Mobility	The communications infrastructure must support transportable, redeployable, or fully mobile communications (e.g., personal communications service, cellular, satellite, high frequency radio).
Ubiquitous Coverage	Services must be readily accessible to support the national security leadership and inter- and intra-agency emergency operations, wherever they are located.
Survivability/Endurability	Services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or man-made disaster up to and including nuclear war.
Voice Band Service	The service must provide voice band service in support of presidential and other communications.
Broadband Service	The service must provide broadband service in support of NS/EP missions (e.g., video, imaging, web access, multimedia).
Scaleable Bandwidth	NS/EP users must be able to manage the capacity of the communications services to support variable bandwidth requirements.
Affordability	Services must leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf technologies, services).
Reliability/Availability	Services must perform consistently and precisely according to their design requirements and specifications, and must be usable with high confidence.

**Appendix B**

**Table B-1 Relationship of Functional Requirements to Wireline Services**

Legend:

1. Enhanced Priority Treatment
2. Secure Networks
3. Non-Traceability
4. Restorability
5. International Connectivity
6. Interoperability
7. Mobility
8. Ubiquitous Coverage
9. Survivability/Endurability
10. Voice Band Service
11. Broadband Service
12. Scaleable Bandwidth
13. Affordability
14. Reliability/Availability

Wireline Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13	14
<b>CSVS</b>	<a href="#">2.1.1</a>	X		X	X	X	X		X	X	X			X	X
Priority Dial Tone	<a href="#">2.1.2.1</a>	X													
Priority Call Setup Message	<a href="#">2.1.2.2</a>	X													
Exemption From Restrictive Network Controls	<a href="#">2.1.2.3</a>	X								X					
Attendant Override	<a href="#">2.1.2.4</a>	X													
User Verification	<a href="#">2.1.2.5</a>	X	X												
Authorization Codes	<a href="#">2.1.2.6</a>	X	X												
Automated Verification of Authorization Codes	<a href="#">2.1.2.7</a>	X	X												

National Security/Emergency Preparedness Telecommunications Applications  
 Study for the Office of Information Assurance and Critical Infrastructure Protection

**Appendix B**

**Table B-1 Relationship of Functional Requirements to Wireline Services (Continued)**

Wireline Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Call Pickup	<a href="#">2.1.2.8</a>			X											
Suppression of Calling Number Delivery	<a href="#">2.1.2.9</a>			X											
Route or Path Avoidance	<a href="#">2.1.2.10</a>		X							X					X
Route or Path Diversity	<a href="#">2.1.2.11</a>				X					X					X
Dedicated Transmission	<a href="#">2.1.2.12</a>		X							X					X
Call Forwarding	<a href="#">2.1.2.13</a>	X													
Make Busy Arrangement	<a href="#">2.1.2.14</a>												X		
Call Screening	<a href="#">2.1.2.15</a>	X													
Class of Service and Restrictions	<a href="#">2.1.2.15.1</a>	X													
Traveling Classmark	<a href="#">2.1.2.15.2</a>	X													
Code Block	<a href="#">2.1.2.15.3</a>		X										X		
Security Procedures	<a href="#">2.1.2.16</a>		X												
Toll Free Calling	<a href="#">2.1.2.17</a>													X	
Routing Control for Toll Free Numbers	<a href="#">2.1.2.17.1</a>									X				X	X
Time of Day Routing for Toll Free Calling	<a href="#">2.1.2.17.2</a>												X	X	
Day of Week Routing for Toll Free Calling	<a href="#">2.1.2.17.3</a>												X	X	
Percentage Routing for Toll Free Calling	<a href="#">2.1.2.17.4</a>												X	X	
NPA/NXX Routing for Toll Free Calling	<a href="#">2.1.2.17.5</a>									X				X	X
ANI-Based Routing for Toll Free Calling	<a href="#">2.1.2.17.6</a>									X				X	X
Command Routing for Toll Free Calling	<a href="#">2.1.2.17.7</a>				X					X			X	X	X

National Security/Emergency Preparedness Telecommunications Applications  
 Study for the Office of Information Assurance and Critical Infrastructure Protection

**Appendix B**

**Table B-1 Relationship of Functional Requirements to Wireline Services (Continued)**

Wireline Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Cascade Routing for Toll Free Calling	<a href="#">2.1.2.17.8</a>				X					X			X	X	X
Network Call Distributor Routing for Toll Free Calling	<a href="#">2.1.2.17.9</a>				X					X			X	X	X
Network Queuing for Toll Free Calling	<a href="#">2.1.2.17.10</a>	X												X	
Agency Based Routing Database for Toll Free Calling	<a href="#">2.1.2.17.11</a>				X					X			X	X	X
Call Redirection for Toll Free Calling	<a href="#">2.1.2.17.12</a>			X										X	
Dialed Number Identification for Toll Free Calling	<a href="#">2.1.2.17.13</a>		X											X	
Call Prompter Routing for Toll Free Calling	<a href="#">2.1.2.17.14</a>			X										X	
Call Prompter Routing - Electronic Access for Toll Free Calling	<a href="#">2.1.2.17.15</a>								X					X	
Call Status Report for Toll Free Calling	<a href="#">2.1.2.17.16</a>		X												X
Caller Profile Report for Toll Free Calling	<a href="#">2.1.2.17.17</a>		X												X
Caller Information Report for Toll Free Calling	<a href="#">2.1.2.17.18</a>		X										X		X
Caller Response Report for Toll Free Calling	<a href="#">2.1.2.17.19</a>		X												
Real-Time Call Status for Toll Free Calling	<a href="#">2.1.2.17.20</a>		X												X
Operator Connect Bridging for Toll Free Calling	<a href="#">2.1.2.17.21</a>			X											
Basic ATB Rerouting for Toll Free Calling	<a href="#">2.1.2.17.22</a>				X					X			X	X	X

National Security/Emergency Preparedness Telecommunications Applications  
 Study for the Office of Information Assurance and Critical Infrastructure Protection

**Appendix B**

**Table B-1 Relationship of Functional Requirements to Wireline Services (Continued)**

Wireline Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Service Assurance Rerouting for Toll Free Calling	<a href="#">2.1.2.17.23</a>									X					X
Service Level Agreements	<a href="#">2.1.2.18</a>				X					X					X
<b>CSDS</b>	<a href="#">2.2.1</a>				X	X	X		X	X	X	X	X	X	X
Priority Dial Tone	<a href="#">2.2.2.1</a>	X													
Priority Call Setup Message	<a href="#">2.2.2.2</a>	X													
Exemption From Restrictive Network Controls	<a href="#">2.2.2.3</a>	X								X					
User Verification	<a href="#">2.2.2.4</a>	X	X												
Authorization Codes	<a href="#">2.2.2.5</a>	X	X												
Automated Verification of Authorization Codes	<a href="#">2.2.2.6</a>	X	X												
Suppression of Calling Number Delivery	<a href="#">2.2.2.7</a>			X											
Route or Path Avoidance	<a href="#">2.2.2.8</a>		X							X					X
Route or Path Diversity	<a href="#">2.2.2.9</a>				X					X					X
Dedicated Transmission	<a href="#">2.2.2.10</a>		X							X					X
Call Screening	<a href="#">2.2.2.11</a>	X													
Class of Service and Restrictions	<a href="#">2.2.2.12</a>	X													
Traveling Classmark	<a href="#">2.2.2.12.1</a>	X													
Code Block	<a href="#">2.2.2.12.2</a>		X									X			
Security Procedures	<a href="#">2.2.2.13</a>		X												
Toll Free Calling	<a href="#">2.2.2.14</a>													X	
Routing Control for Toll Free Numbers	<a href="#">2.2.2.14.1</a>									X				X	X
NPA/NXX Routing for Toll Free Calling	<a href="#">2.2.2.14.2</a>									X				X	X
ANI-Based Routing for Toll Free Calling	<a href="#">2.2.2.14.3</a>									X				X	X

**Appendix B**

**Table B-1 Relationship of Functional Requirements to Wireline Services (Concluded)**

Wireline Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Command Routing for Toll Free Calling	<a href="#">2.2.2.14.4</a>				X					X			X	X	X
Cascade Routing for Toll Free Calling	<a href="#">2.2.2.14.5</a>				X					X			X	X	X
Network Queuing for Toll Free Calling	<a href="#">2.2.2.14.6</a>	X												X	
Agency Based Routing Database for Toll Free Calling	<a href="#">2.2.2.14.7</a>				X					X			X	X	X
Dialed Number Identification for Toll Free Calling	<a href="#">2.2.2.14.8</a>		X											X	
Call Status Report for Toll Free Calling	<a href="#">2.2.2.14.9</a>		X												X
Caller Profile Report for Toll Free Calling	<a href="#">2.2.2.14.10</a>		X												X
Caller Information Report for Toll Free Calling	<a href="#">2.2.2.14.11</a>		X										X		X
Real-Time Call Status for Toll Free Calling	<a href="#">2.2.2.14.12</a>		X												X
Basic ATB Rerouting for Toll Free Calling	<a href="#">2.2.2.14.13</a>				X					X			X	X	X
Service Assurance Rerouting for Toll Free Calling	<a href="#">2.2.2.14.14</a>									X					X
Service Level Agreements	<a href="#">2.2.2.15</a>				X					X					X
<b>PSDS</b>	<a href="#">2.3.1</a>	X		X	X	X	X		X	X	X	X	X	X	X
Dedicated Transmission	<a href="#">2.3.2.1</a>		X							X					X
Route or Path Avoidance	<a href="#">2.3.2.2</a>		X							X					X
Route or Path Diversity	<a href="#">2.3.2.3</a>				X					X					X
Security Procedures	<a href="#">2.3.2.4</a>		X												
Service Level Agreements	<a href="#">2.3.2.5</a>				X					X					X
Security Features	<a href="#">2.3.2.6</a>		X												

**Appendix C**

**Table C-1 Relationship of Functional Requirements to Non-Wireline Services**

Legend:

1. Enhanced Priority Treatment
2. Secure Networks
3. Non-Traceability
4. Restorability
5. International Connectivity and Interoperability
6. Mobility
7. Ubiquitous Coverage
8. Survivability/Endurability
9. Voice Band Service
10. Broadband Service and Scaleable Bandwidth
11. Affordability
12. Reliability/Availability

Non-Wireline Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12
<b>Wireless Services</b>	<a href="#">3.1.1</a>												
Wireless Priority Service (WPS) available NYC and Wash. DC; underdevelopment nationwide	<a href="#">3.2.1</a>	X											
Qualcomm's CONDOR™ Wireless Secure telecommunications System and GSM with authentication offer some security features; otherwise encrypt transmitted signal	<a href="#">3.3.1</a>		X										
Non-Traceability Unavailable	<a href="#">3.4.1</a>												
Use of TSP for wireline interconnections to MSOs; SLAs with service providers; backup equipment	<a href="#">3.5.1</a>				X								

**Appendix C**

**Table C-1 Relationship of Functional Requirements to Non-Wireline Services (Continued)**

<b>Non-Wireline Services and Functions/Features</b>	<b>Section</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>	<b>10</b>	<b>11</b>	<b>12</b>
Via commercial wireline voice and packet service providers; use of GSM under certain conditions; multimode handsets; use of SDR technology	<a href="#">3.6.1</a>					X							
Inherently mobile	<a href="#">3.7.1</a>						X						
"Nearly" Ubiquitous Coverage dependent upon the wireless equipment and system implementation	<a href="#">3.8.1</a>							X					
Robust designs and physical protection; back-up and replacement systems; radio frequency interference (RFI) prevention	<a href="#">3.9.1</a>								X				
Inherently	<a href="#">3.10.1</a>									X			
Available with 2.5G (using General Packet Radio Service), 3G, and potentially 4G	<a href="#">3.11.1</a>										X		
Rely on COTS services	<a href="#">3.12.1</a>											X	
Dependent upon equipment quality and system designs; adequate and uncorrupted radio frequency (RF) signals; WPS Program should help; rapid restoration a key element; need financially viable service providers	<a href="#">3.13.1</a>												X
<b>Paging and Short Text Services</b>	<a href="#">3.1.2</a>												
Enhanced Priority Treatment Unavailable	<a href="#">3.2.2</a>												
BlackBerry offers secure e-mail; otherwise encrypt and decrypt the data message itself	<a href="#">3.3.2</a>		X										
Generally unavailable except for e-mail sent with originating address removed	<a href="#">3.4.2</a>			X									
SLAs with service providers; backup equipment	<a href="#">3.5.2</a>				X								
Use of SMS for Interoperability	<a href="#">3.6.2</a>					X							
Inherently mobile	<a href="#">3.7.2</a>						X						
Nearly worldwide paging services available	<a href="#">3.8.2</a>							X					

**Table C-1 Relationship of Functional Requirements to Non-Wireline Services (Continued)**

<b>Non-Wireline Services and Functions/Features</b>	<b>Section</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>	<b>10</b>	<b>11</b>	<b>12</b>
Robust designs and physical protection; back-up and replacement systems; RFI prevention	<a href="#">3.9.2</a>								X				
Available only as a voice message	<a href="#">3.10.2</a>									X			
Broadband Service and Scaleable Bandwidth Unavailable	<a href="#">3.11.2</a>												
Rely on COTS services	<a href="#">3.12.2</a>											X	
Dependent upon equipment quality and system designs; adequate and uncorrupted RF signals; rapid restoration a key element; need financially viable service providers	<a href="#">3.13.2</a>												X
<b>LMDS and MMDS</b>	<a href="#">3.1.3</a>												
Enhanced Priority Treatment Unavailable	<a href="#">3.2.3</a>												
Encryption and decryption of the traffic only	<a href="#">3.3.3</a>		X										
Non-Traceability Not Applicable	<a href="#">3.4.3</a>												
SLAs with service providers; backup equipment	<a href="#">3.5.3</a>				X								
International Connectivity and Interoperability Not Applicable	<a href="#">3.6.3</a>												
May be considered "transportable"	<a href="#">3.7.3</a>						X						
Ubiquitous Coverage Not Applicable	<a href="#">3.8.3</a>												
Robust designs and physical protection; back-up and replacement systems; RFI prevention	<a href="#">3.9.3</a>								X				
Inherently	<a href="#">3.10.3</a>									X			
Available with free space optics and microwave implementations	<a href="#">3.11.3</a>										X		
Rely on COTS services	<a href="#">3.12.3</a>											X	
Dependent upon equipment quality and system designs; rapid restoration a key element	<a href="#">3.13.3</a>												X
<b>WLAN and PAN</b>	<a href="#">3.1.4</a>												
Enhanced Priority Treatment Unavailable	<a href="#">3.2.4</a>												

**Table C-1 Relationship of Functional Requirements to Non-Wireline Services (Continued)**

<b>Non-Wireline Services and Functions/Features</b>	<b>Section</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>	<b>10</b>	<b>11</b>	<b>12</b>
Use WEP protocol (part of WLAN IEEE 802.11b standard) or VPN on WLAN; PAN Bluetooth security not sufficient; UWB under development, and has some inherent security	<a href="#">3.3.4</a>		X										
Non-Traceability Unavailable	<a href="#">3.4.4</a>												
SLAs with service providers; backup equipment	<a href="#">3.5.4</a>				X								
International Connectivity and Interoperability Not Applicable	<a href="#">3.6.4</a>												
PANs are inherently mobile; certain applications of WLANs can be mobile	<a href="#">3.7.4</a>						X						
Ubiquitous Coverage Not Applicable	<a href="#">3.8.4</a>												
Care in physical location and physical protection; back-up and replacement systems; RFI prevention	<a href="#">3.9.4</a>								X				
Dependent on the WLAN and PAN usage	<a href="#">3.10.4</a>									X			
WLANs via IEEE 802.11b, a, and g standards; PANs via Bluetooth and UWB	<a href="#">3.11.4</a>										X		
Most WLAN and PAN implementations currently rely on COTS services; UWB under development but expected to be competitively priced	<a href="#">3.12.4</a>											X	
Dependent upon equipment quality and system designs; rapid restoration a key element; selection of viable service provider and long-lived technology	<a href="#">3.13.4</a>												X
<b>Satellite Services</b>	<a href="#">3.1.5</a>												
Enhanced Priority Treatment Unavailable	<a href="#">3.2.5</a>												
Encryption and decryption of the traffic	<a href="#">3.3.5</a>		X										
Non-Traceability Unavailable	<a href="#">3.4.5</a>												

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table C-1 Relationship of Functional Requirements to Non-Wireline Services (Continued)**

Non-Wireline Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12
Use of TSP for wireline interconnections between satellite earth stations and the terrestrial wireline network; SLAs with service providers; backup equipment	<a href="#">3.5.5</a>				X								
Interoperability via commercial wireline voice and packet service providers; International Connectivity by use of certain Satellite Services, such as Glocall SP or Iridium	<a href="#">3.6.5</a>					X							
Inherently mobile	<a href="#">3.7.5</a>						X						
“Nearly” Ubiquitous Coverage dependent upon the system	<a href="#">3.8.5</a>							X					
Robust designs and physical protection; back-up and replacement systems; RFI prevention	<a href="#">3.9.5</a>								X				
Inherently	<a href="#">3.10.5</a>									X			
Via services like Glocall SP, Two-way Direct Broadcast Satellite services, Starband, and DirecPC; Teledesic and SkyBridge in the future	<a href="#">3.11.5</a>										X		
Rely on COTS services	<a href="#">3.12.5</a>											X	
Dependent upon equipment quality and system designs; rapid restoration a key element; selection of viable service provider	<a href="#">3.13.5</a>												X
<b>Land Mobile Radio and Two-Way Mobile Radio Services</b>	<a href="#">3.1.6</a>												
For some LMR systems, channels can be reserved for priority treatment	<a href="#">3.2.6</a>	X											
Encryption and decryption of the voice and traffic	<a href="#">3.3.6</a>		X										
Only if no identification is ascribed to particular transmissions	<a href="#">3.4.6</a>			X									

**Appendix C**

**Table C-1 Relationship of Functional Requirements to Non-Wireline Services (Concluded)**

<b>Non-Wireline Services and Functions/Features</b>	<b>Section</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>	<b>10</b>	<b>11</b>	<b>12</b>
SLAs with service providers; backup equipment	<a href="#">3.5.6</a>				X								
Interoperability via SDR technology; through projects like AGILE and Project SafeCom	<a href="#">3.6.6</a>					X							
Inherently mobile	<a href="#">3.7.6</a>						X						
Relocation of mobile equipment can provide Ubiquitous Coverage	<a href="#">3.8.6</a>							X					
Robust designs and physical protection; back-up and replacement systems; RFI prevention	<a href="#">3.9.6</a>								X				
Inherently Unavailable	<a href="#">3.10.6</a>									X			
Unavailable	<a href="#">3.11.6</a>												
Many implementations rely on COTS products; systems employing SDR may be more expensive unless user base grows	<a href="#">3.12.6</a>											X	
Dependent upon equipment quality and system designs; rapid restoration a key element; selection of viable service provider and long-lived technology	<a href="#">3.13.6</a>												X

**Appendix D**

**Table D-1 Relationship of Functional Requirements to IT Services**

Legend:

1. Enhanced Priority Treatment
2. Security
3. Audit Trails and Non-Traceability
4. Interconnectivity and Interoperability
5. Mobility
6. Restorability
7. Survivability/Endurability
8. Reliability/Availability
9. Voice Band Service
10. Broadband Service
11. Scaleable Bandwidth
12. Affordability
13. Ubiquitous Coverage

IT Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13
<b>Information Repository Systems</b>	<a href="#">4.1.1</a>													
Prioritize data access and transactions; place critical information/data in cache memory; deny system access to non-critical users	<a href="#">4.2.1</a>	X												
Implement Security policies, procedures, and practices via a Security Management Program; permit system interaction by only authorized personnel; limit system access; continuously update security patches; conduct frequent virus scanning; take measures for prevention of DoS, DDoS, and DRDoS attacks; employ encryption	<a href="#">4.3</a>		X											

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table D-1 Relationship of Functional Requirements to IT Services (Continued)**

IT Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13
Use Audit Trails to track personal accountability; monitor problems in real-time; reconstruct events; identify attempts to penetrate a system; log events; determine trends	<a href="#">4.4</a>			X										
Use common standardized data formats and languages, such as SQL, SNMP, X.400, X.500, UCA, HTTP, FTP, SMTP, and TCP/IP;	<a href="#">4.5.1</a>				X									
Maintain operations while in motion using large vehicle like FEMA's MATS ; also consider "transportable" systems	<a href="#">4.6.1</a>					X								
Availability and use of a comprehensive disaster recovery plan; maintain backup copies of standard or customized software with periodic checks of medium's quality; perform regular frequent system backups; log database management systems and associated transactions; consider implementing "mirroring"; maintain a "hot" or "cold" backup site	<a href="#">4.7.1</a>						X							

**Table D-1 Relationship of Functional Requirements to IT Services (Continued)**

IT Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13
Provide resistance to attacks by: 1) restricting physical access, hardening the physical site, employing user authentication, using access controls, data encryption, message filtering at system boundary, functional isolation among systems, maintaining stringent requirements on system development and testing practices and quality control of software; 2) intrusion detection, performing system audits, using baseline checksum or cryptographic signatures for periodic comparison to the current data contents; 3) implement mechanisms for rapid system restoration; 4) developing systems capable of evolving in response to user requirements for new functions and intruders' increasing knowledge of system structure and behavior	<a href="#">4.8</a>							X						

**Table D-1 Relationship of Functional Requirements to IT Services (Continued)**

IT Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13
In general, employ system design architecture with redundant critical components and high Reliability and Availability of the individual components; perform regular system backups; maintain alternate storage sites for databases; conduct periodic drills on the recovery procedures; maintain continuity of operations, concept of operation, and disaster recovery plans; perform regression and integration testing of changes and updates; employ a Configuration/Change Control Board to review and approve system changes or updates; employ SLAs and Performance Based Contracting for outsourced functions; follow "best practices" for software development such as those published by the SEI, the SA-CMM and the SRE Service; specifically for Information Repository Systems, log all transactions; create backup databases; limit which data fields may be updated and the personnel authorized to do so; employ multi-level security authentication techniques	<a href="#">4.9</a> and <a href="#">4.9.1</a>								X					
Telecommunications facilities capable of Voice Band Service would be able to handle transfers of small amounts of data via permanent low data rate or dial-up connections to the Information Repository; voice messages can be recorded and the message files entered into and retrieved from these repositories	<a href="#">4.10.1</a>									X				
Telecommunications facilities capable of Broadband Service would handle data transfers to and from the repositories	<a href="#">4.11.1</a>										X			

**Table D-1 Relationship of Functional Requirements to IT Services (Continued)**

<b>IT Services and Functions/Features</b>	<b>Section</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>	<b>10</b>	<b>11</b>	<b>12</b>	<b>13</b>
Telecommunications facilities capable of Scalable Bandwidth may be required to connect to the repository depending upon traffic load into and out of the system	<a href="#">4.12.1</a>											X		
Ways to manage Affordability are: consider the Total Cost of Ownership and any necessary modifications to COTS hardware and software; minimize the duplicate IT System stovepipes that exist within organizations by promoting use of a components-based enterprise architecture; following best practices, like those from the SEI; possibly outsource certain IT functions; compare results of a risk analysis against cost to implement system functions	<a href="#">4.13</a>												X	
Ubiquitous Coverage Not Applicable	<a href="#">4.14</a>													
<b>Monitor and Control Systems</b>	<a href="#">4.1.2</a>													
Prioritize acquisition and processing of signal input and output (I/O); prioritize data handling by Telecommunications Systems between agents and managers	<a href="#">4.2.2</a>	X												
Same as for Information Repository Systems	<a href="#">4.3</a>		X											
Audit trails same as for Information Repository Systems; Use Non-Traceability to hide origination or destination of sensory/control data for Monitor and Control Systems	<a href="#">4.4</a>			X										
Use common standardized data formats and languages, such as UCA and SNMP between a manger and its agents. For Telecommunications Systems, refer to Interoperability in Section 2 for Wireline Services	<a href="#">4.5.2</a>				X									

**Table D-1 Relationship of Functional Requirements to IT Services (Continued)**

IT Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13
Agents may be mobile; use GPS to track agents monitoring various types of resources; connect agents to manager via Non-Wireline technology	<a href="#">4.6.2</a>					X								
Use same approaches as for Information Repository Systems; in addition, use rapid automatic switchovers to redundant network agent and manager equipment; use redundant or alternate telecommunications paths between an agent and manager	<a href="#">4.7.2</a>						X							
Same as for Information Repository Systems; additionally planning for agent redundancy and continued operation assuming some loss of some agents; maintaining robust Telecommunications System(s) between agents and manager by employing diverse routing or redundant telecommunication facilities	<a href="#">4.8</a> and <a href="#">4.8.1</a>							X						
Same techniques as for Information Repository Systems plus maintaining the Reliability and Availability of the Telecommunications System between the agents and managers; employ "out of band" management to determine the state of the network element, determine the nature of the failure, and attempt restoration to the normal state; log events	<a href="#">4.9</a> and <a href="#">4.9.2</a>								X					

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Assurance and Critical Infrastructure Protection

**Table D-1 Relationship of Functional Requirements to IT Services (Continued)**

IT Services and Functions/Features	Section	1	2	3	4	5	6	7	8	9	10	11	12	13
Telecommunications facilities capable of Voice Band Service would be used as a permanent low bandwidth data connection between agents and managers or as an alternative link in the event of a failure of the primary telecommunications facilities; voice communication may be used by individuals to verbally communicate information between agents and their managers	<a href="#">4.10.2</a>									X				
Telecommunications facilities capable of Broadband Service to handle communications between agents and their manager and between managers and the control center	<a href="#">4.11.2</a>										X			
Telecommunications facilities capable of Scaleable Bandwidth may be needed depending upon traffic load requirements between the agents and managers	<a href="#">4.12.2</a>											X		
Same as for Information Repository Systems	<a href="#">4.13</a>												X	
Ubiquitous Coverage Not Applicable	<a href="#">4.14</a>													
<b>E-Commerce Systems</b>	<a href="#">4.1.3</a>													
Prioritize NS/EP-related transactions in CPU; implement strong SLAs	<a href="#">4.2.3</a>	X												
Same as for Information Repository Systems	<a href="#">4.3</a>		X											
Audit Trails same as for Information Repository Systems;	<a href="#">4.4</a>			X										
Use common standardized data formats and languages, such as XML; use GUIs for human interface; use COTS software and servers; establish interrelationships among E-Commerce components	<a href="#">4.5.3</a>				X									

National Security/Emergency Preparedness Telecommunications Applications  
Study for the Office of Information Security

**Appendix D**

**Table D-1 Relationship of Functional Requirements to IT Services (Concluded)**

<b>IT Services and Functions/Features</b>	<b>Section</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>	<b>10</b>	<b>11</b>	<b>12</b>	<b>13</b>
E-commerce systems are likely to be Mobile; they could be made Transportable	<a href="#">4.6.3</a>					X								
Use same approaches as for Information Repository Systems	<a href="#">4.7.3</a>						X							
Same as for Information Repository Systems	<a href="#">4.8</a>							X						
Same techniques as for Information Repository Systems plus SEI best practices; employing specialized implementations to “isolate” and duplicate major E-Commerce System components; providing redundant or backup components and telecommunications facilities	<a href="#">4.9</a> and <a href="#">4.9.3</a>								X					
Voice Band Telecommunications Services connected to E-Commerce Systems may be adequate to provide the necessary connectivity to the systems	<a href="#">4.10.3</a>									X				
Broadband Telecommunications Services connected to E-Commerce Systems may be needed to provide the necessary connectivity to the systems	<a href="#">4.11.3</a>										X			
Scaleable Bandwidth may be needed to connect to the E-Commerce System depending on the varying telecommunications traffic loads	<a href="#">4.12.3</a>											X		
Same as for Information Repository Systems	<a href="#">4.13</a>												X	
Ubiquitous Coverage Not Applicable	<a href="#">4.14</a>													

## Appendix E

TCP/IP is the basic communication language of the Internet. It can also be used as a protocol in private networks. TCP/IP is a two-layer protocol stack. TCP at Layer 4<sup>65</sup> manages the assembling of a message or file into packets that are transmitted over the network and then received by a TCP layer at the destination which reassembles the packets into the original transmission. IP at Layer 3<sup>66</sup> handles the address portion of each packet to ensure that the packet gets to the correct destination. TCP/IP communication is primarily point-to-point, meaning communication is from one host on the network to another.

SNMP is the protocol suite governing network management and the monitoring of network devices and their functions. It has become the de facto standard for inter-network management and is used in, but not necessarily limited to, TCP/IP networks. SNMP is based on the manager/agent model. It is referred to as “simple” because the agent requires minimal software. SNMP includes a limited set of management commands and responses. The management system can retrieve data from the agent or establish the value of a variable. The managed agent sends a response message completing the request for data or acknowledges the establishment of the variable value. The agent can also send an event notification to the manager to identify the occurrence of a condition, such as a threshold that exceeds a predetermined value. The agents store data about themselves in Management Information Bases (MIBs).

A MIB may be thought of as a description of network objects that can be managed using SNMP. The basic format of the MIB is defined as a part of SNMP. All other MIBs are extensions of this basic information base. MIBs, or MIB extensions, exist for each set of network entities that can be managed. Companies that have created MIB extensions for their product include IBM, Cisco, Novell, and Fore.

Open Systems Interconnection (OSI) is an International Standards Organization (ISO) standard for communication between two end users in a network. It defines a networking framework for implementing protocols in seven layers. At one time vendors agreed to support OSI in some form or another, but this support did not happen due largely to entrenched proprietary standards and relatively loosely defined ISO standards. Exceptions to this lack of industry support are the OSI standards for e-mail (X.400) and directories (X.500) that are currently in use. The chief contribution of the OSI model to current networking standards is to serve as a reference model for all other protocols.

The need for communications standards tailored for the utilities infrastructure was recognized by the Electric Power Research Institute (EPRI). EPRI developed the Utility Communications Architecture (UCA), which is a standards-based approach to utilities communications and is designed to apply across all of the functional areas within the electric, gas, and water utilities. It serves as a guideline for use by utilities and equipment

---

<sup>65</sup> TCP is at the “Transport” Layer, i.e., Layer 4 of the Open Systems Interconnection (OSI) model.

<sup>66</sup> Layer 3 is at the “Network” Layer of the OSI model.

manufacturers in developing interoperable information systems used for business and operations applications. It is an architecture rather than a simple protocol and incorporates a family of communications protocols designed to meet the requirements of a wide variety of utility environments. These protocols are organized according to the OSI reference model mentioned above. The UCA Version 2 includes profiles employing both TCP/IP and other OSI protocols. The profiles include connection oriented or connectionless communications running over a wide variety of media including those specific to utilities, such as radio. The common protocol definition of UCA is especially timely in consideration of the communications requirements brought about by deregulation. The architecture supports the two major classes of applications in the utilities industry. The first is access to data in real-time databases such as Emergency Management Systems (EMS) and SCADA. The second application is access to real-time end devices such as meters and remote terminal units. *IEEE-SA TR 1550 on Utility Communications Architecture* contains a detailed description of the architecture.

**LIST OF ACRONYMS**

ABR	Available Bit Rate	CS	Circuit-Switched
AES	Advanced Encryption Standard	CSDS	Circuit-Switched Data Services
AIN	Advanced Intelligent Network	CST	CDMA Secure Terminal
AMPS	Advance Mobile Phone System	CSVS	Circuit-Switched Voice Services
ANI	Automatic Number Identification	DDoS	Distributed Denial of Service
ANSI	American National Standards Institute	DES	Data Encryption Standard
ASCII	American Standard Code for Information Interchange	DFO	Disaster Field Office
ATB	All Trunks Busy	DoS	Denial of Service
ATIS	Alliance for Telecommunications Industry Solutions	DRDoS	Distributed Reflection Denial of Service
ATM	Asynchronous Transfer Mode	DSL	Digital Subscriber Line
		DTMF	Dual Tone Multi-Frequency
		DXC	Digital Cross Connect
		E911	Enhanced 911
BER	Bit Error Rate	ECPL	Endorsed Cryptographic Products List
BOD	Bandwidth-On-Demand	EMP	Electromagnetic Pulse
CBR	Constant Bit Rate	EMS	Emergency Management Systems
CBS	COTS-Based Systems	EPRI	Electric Power Research Institute
CCB	Configuration/Change Control Board		
CDMA	Code Division Multiple Access	FEMA	Federal Emergency Management Agency
CERT	Computer Emergency Response Team	FCC	Federal Communications Commission
CIO	Chief Information Officer	FIPS	Federal Information Processing Standard
CIR	Committed Information Rate	FLEWUG	Federal Law Enforcement Wireless Users Group
CLEC	Competitive Local Exchange Carrier	FLAN	Flying Local Area Network
COTS	Commercial-Off-The-Shelf	FNBDT	Future Narrow Band Digital Technology
COS	Class Of Service		
COW	Cellsite On Wheels	FR	Frame Relay
CPE	Customer Premises Equipment	FSO	Free-Space Optics
CPU	Central Processing Unit	FTP	File Transfer Protocol

**LIST OF ACRONYMS (Continued)**

		IXC	Interexchange Carrier
1G	First Generation	ITU	International Telecommunications Union
2G	Second Generation		
2.5G	Extension of 2G		
3G	Third Generation	kbps	kilobits per second
GAIT	GSM ANSI Interworking Team	kHz	Kilohertz
Gbps	Gigabits Per Second	LAN	Local Area Network
GETS	Government Emergency Telecommunication Service	LEO	Low Earth Orbiting
GHz	Gigahertz	LOS	Line Of Sight
GPRS	General Packet Radio Service	LMDS	Local Multipoint Distribution System
GPS	Global Positioning System	LMR	Land Mobile Radio
GSA	General Services Administration	LSP	Label Switched Path
GSM	Global System for Mobile Communications	LSR	Label Switch Router
GUI	Graphical User Interface	MAE	Metropolitan Area Exchange
HF	High Frequency	MAN	Metropolitan Area Network
HLR	Home Location Register	MATS	Mobile Air Transportable System
HPC	High Priority Call	Mbps	Megabits per second
HTTP	HyperText Transfer Protocol	MHz	Megahertz
IIS	Internet Information Server	MIB	Management Information Base
IEEE	Institute of Electrical and Electronics Engineers	MMDS	Multipoint Multichannel Distribution System
IETF	Internet Engineering Task Force	MPEG	Motion Picture Experts Group
IIS	Internet Information Server	MPLS	Multi-Protocol Label Switching
ILEC	Incumbent Local Exchange Carrier	MSO	Mobile Switching Office
I/O	Input and Output	MSP	Managed Service Provider
IP	Internet Protocol	MTBF	Mean Time Between Failure
IPSec	IP Security	mW	Milliwatt
IrDA	InfraRed Data Association	NAP	Network Access Point
ISDN	Integrated Services Digital Network	NCC	National Coordinating Center
ISO	International Standards Organization	NCR	National Capital Region
ISP	Internet Service Provider	NGN	Next Generation Network
IT	Information Technology	NIST	National Institute of Standards and Technology

**LIST OF ACRONYMS (Continued)**

NMC	Network Management Control	PSTN	Public Switched Telephone Network
NOC	Network Operations Center	PSWN	Public Safety Wireless Network
NPA	Numbering Plan Area		
NPCS	Narrowband Personal Communications Services	PVC	Permanent Virtual Circuit
NRC	Nuclear Regulatory Commission	QoS	Quality of Service
NSA	National Security Agency	RC4	Ron's Code 4
NS/EP	National Security/Emergency Preparedness	RF	Radio Frequency
		RFI	Radio Frequency Interference
NSTAC	National Security Telecommunications Advisory Committee	RSVP	Resource Reservation Protocol
NS/VATFR	Network Security/Vulnerability Assessments Task Force Report	SA-CMM	Software Acquisition Capability Maturity Model
		SCADA	Supervisory Control and Data Acquisition
NTIA	National Telecommunications and Information Administration	SCP	Service Control Point
		SCR	Sustainable Cell Rate
		SDR	Software Defined Radio
		SEI	Software Engineering Institute
OMB	Office of Management and Budget	SIM	Subscriber Identification Module
OC	Optical Carrier	SIP	Session Initiation Protocol
OC-3	Optical Carrier Level 3	SLA	Service Level Agreement
OMNCS	Office of the Manager National Communications System	SMS	Short Message Service
		SMTP	Simple Mail Transfer Protocol
OSI	Open Systems Interconnection	SNA	Survivable Network Analysis
PAN	Personal Area Network	SNMP	Simple Network Management Protocol
PBX	Private Branch Exchange		
PC	Personal Computer	SONET	Synchronous Optical Network
PCS	Personal Communications Service	SS7	Signaling System 7
PDA	Personal Digital Assistant	SRAS	Special Routing Arrangement Service
PKI	Public Key Infrastructure		
PIN	Personal Identification Number	SRE	Software Risk Evaluation
		SQL	Structured Query Language
PSDS	Packet-Switched Data Services	SSL	Secure Socket Layer

**LIST OF ACRONYMS (Concluded)**

STE	Secure Terminal Equipment	WINS	Wireless Interoperability National Strategy
STU	Secure Telephone Unit	WPS	Wireless Priority Service
SVN	Secure Virtual Network	WTC	World Trade Center
		WTLS	Wireless Transport Layer Security
TCO	Total Cost of Ownership		
TCOS	Traveling Classmark		
TCP/IP	Transmission Control Protocol/Internet Protocol	XML	Extensible Markup Language
TDD	Terminal Device for the Deaf		
TDM	Time Division Multiplex		
TDMA	Time Division Multiple Access		
TSP	Telecommunications Service Priority		
TTY	TeleTYpewriter		
UBR	Unspecified (or Undefined) Bit Rate		
UCA	Utility Communications Architecture		
UHF	Ultra High Frequency		
USPS	United States Postal Service		
UWB	Ultra-Wideband		
VC	Virtual Circuit		
VBR	Variable Bit Rate		
VHF	Very High Frequency		
VoIP	Voice over IP		
VPN	Virtual Private Network		
VTC	Video Teleconference		
WAN	Wide Area Network		
WCDMA	Wideband Code Division Multiple Access		
WERT	Wireless Emergency Response Team		
WLAN	Wireless LAN		
WAP	Wireless Application Protocol		
WEP	Wired Equivalency Privacy		