ATTACHMENT 8   NS/EP FUNCTIONAL REQUIREMENTS IMPLEMENTATION PLAN [L.30.2.8, M.2.2(8), G.11.1-G.11.3]

A8.1   INTRODUCTION [G.11]

Approach to Ensure Infrastructure Security

Network security is a cornerstone of MetTel's operating philosophy. By following the security policy and mandate of MetTel's Chief Executive Officer (CEO), Marshall Aronow, as well as applicable regulations and legislation, MetTel protects its own information and resources and customers' information from unauthorized access, disclosure, corruption, or disruption of service. MetTel will notify the government immediately when events arise that may have major consequences to its network. MetTel understands that GSA CO will set priorities and that MetTel will be solely responsible for network operations.

> Agencies are supported by MetTel's continuous oversight and processes in order to support all of the 14 Basic Functional NS/EP Requirements. MetTel provides a secure infrastructure to all of its customers, at both the physical and logical levels.

Our scale and relationships provide MetTel customers with the strongest coverage across multiple products and solutions, leveraging industry leading technologies. MetTel enables Agency mission objectives and increases efficiencies to end users. We work closely with all our partners and providers to design, develop, and install solutions and, ultimately, provide exceptional service to the customer.

MetTel will ensure that services delivered are in compliance with national policy directives that apply to the national telecommunications infrastructure. These include, but are not limited to:

- PL 93-288 (Disaster Preparedness Assistance dated May 22, 1974), PPD-1 (Organization of the National Security Council System dated February 13, 2009)
- PPD-21 (Critical Infrastructure Security and Resilience, dated February 12, 2013)
- NSDD-97, NSDD-145 and its successors
- other applicable laws, regulations, and directives.

Executive Orders (EO) 12472 and 13618 and its successors will also be considered by MetTel in the design and operations of services provided under this contract. MetTel has provided an NS/EP Functional Requirements Implementation Plan with the

proposal as detailed below that addresses the specifications identified in Sections G.11.1-G.11.3, and will update it annually.

Exhibit A8-1 provides an overview of the MetTel network architecture. ▮▮▮▮

▮▮
▮▮
▮▮
▮▮
▮▮▮▮▮
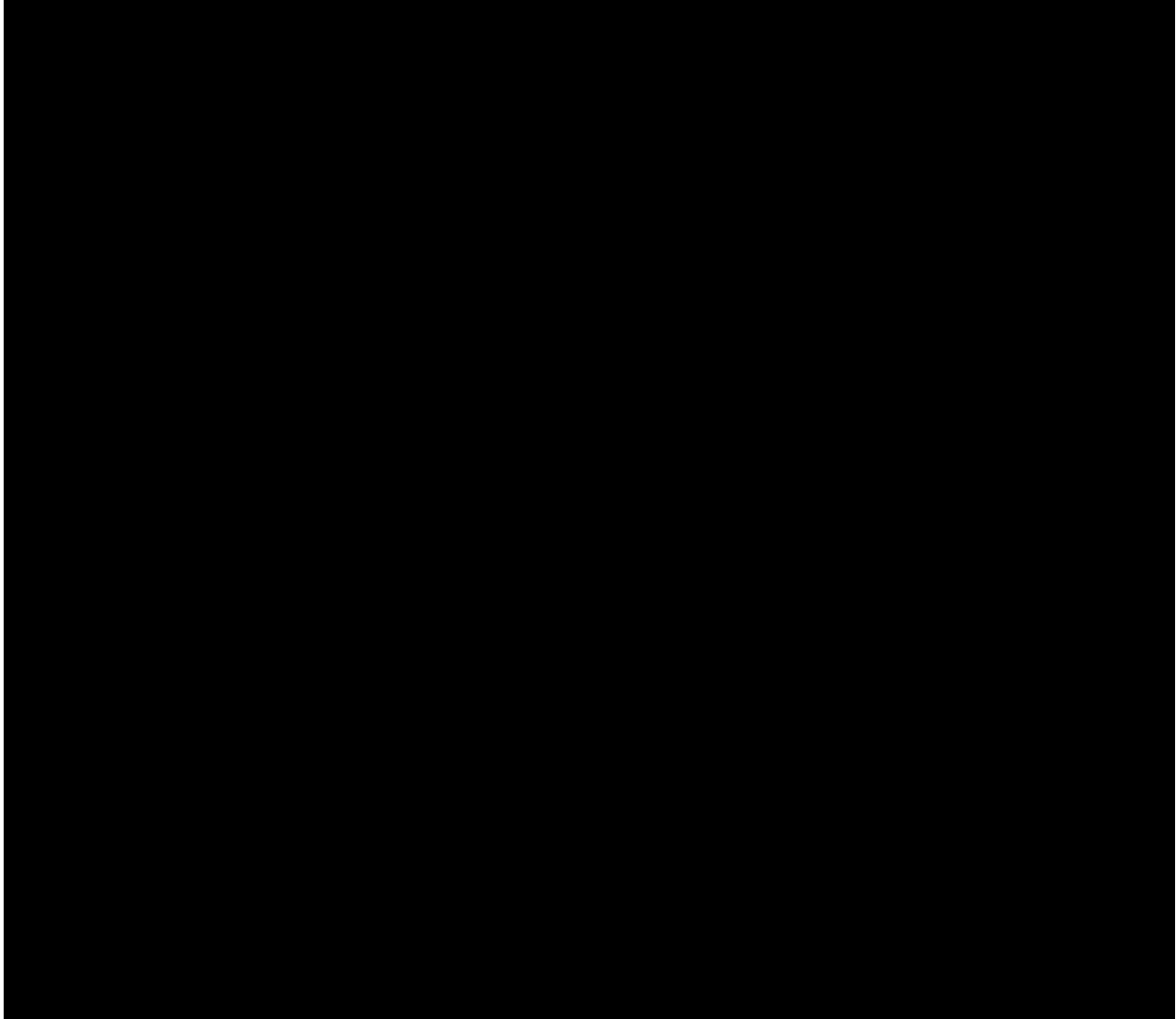
Exhibit A8-1. MetTel Network Architecture

Point of Presence (POP) Architecture

▮▮
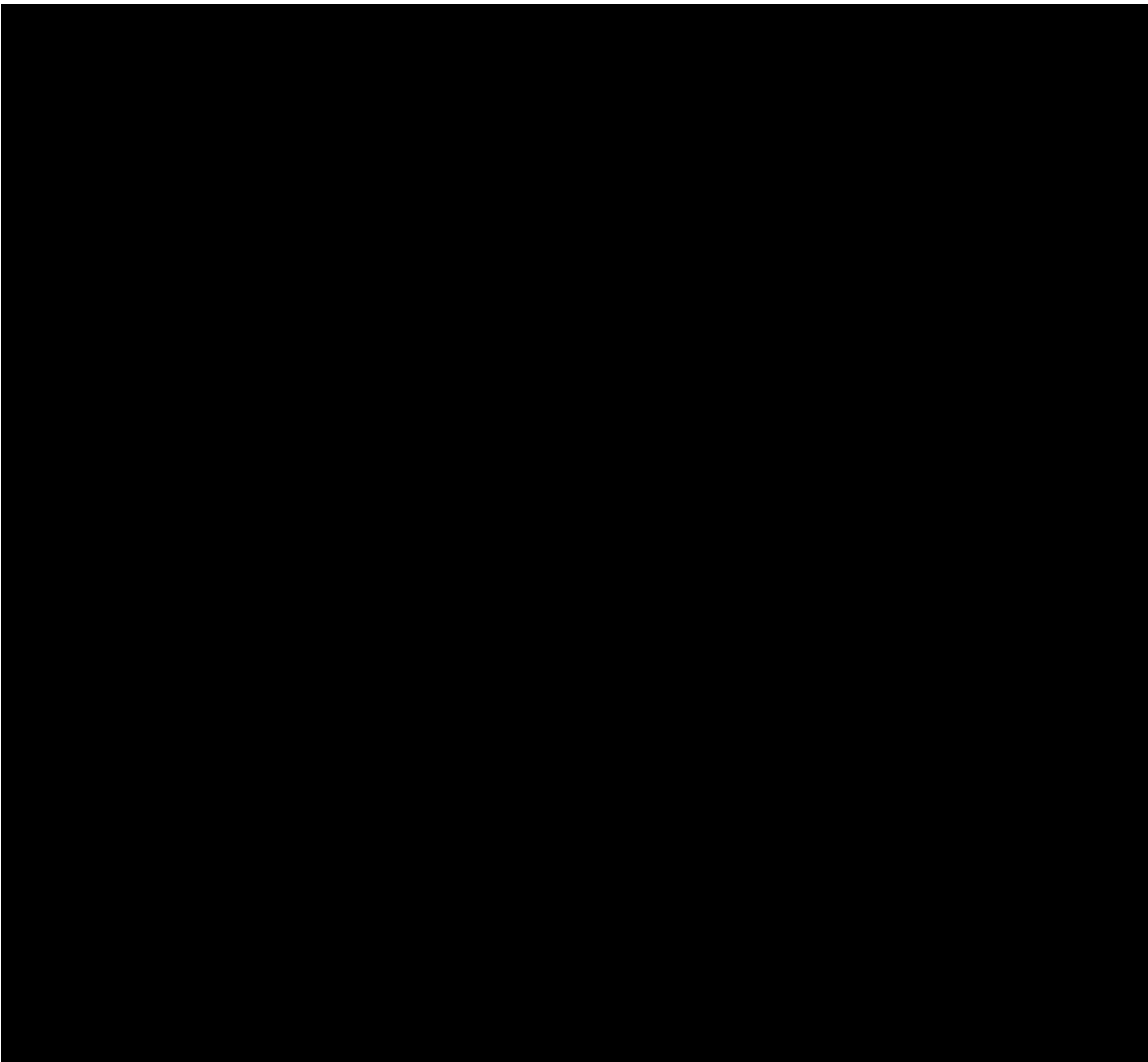
Exhibit A8-2. MetTel POP Architecture

Protecting Our Network

███

██

███

███

██

███

███

██

███

████████

██

███

███

██

██

██

███████████

██

███

██

██

███

██

██████████████████████████████████████

Exhibit A8-3 Basic Functional Requirements for NS/EP details how MetTel
addresses each of the basic requirements.

Exhibit A8-3. Basic Functional Requirements for NS/EP

#	Description of Requirement	████████████████████████
1.	Enhanced Priority Treatment. Voice and data services	████████████████████████████████

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

#	Description of Requirement	██████████████████
	supporting NS/EP missions will be provided preferential treatment over other traffic.	████████████████████████ ██████████████████████████████ ██████████████████████████████ ██████████████████████ ██████████████████████████████ ██████████████████████████████ ██████████████████████████████ ███████████████
2.	Secure Networks. Networks will have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.	████████████████████████ ████████████████████ ██████████████████████████████ ██████████████████ █████
3.	Non-Traceability. Selected users will be able to use NS/EP services without risk of usage being traced (i.e., without risk of user or location being identified).	██████████████████████████ ████████████████
4.	Restorability. Should a service disruption occur, voice and data services will be capable of being re-provisioned, repaired, or restored to required service levels on a priority basis.	██████████████████████████ ██████████████████████████████ ██████████████████████████████ ████████████████████ ███
5.	International Connectivity. Voice and data services will provide access to and egress from international carriers.	██████████████████████████ ██████████████████████████████ ███████████████████
6.	Interoperability. Voice and data services will interconnect and interoperate with other government or private facilities, systems, and networks which will be identified after contract award.	██████████████████████████ ██████████████████████████████ ██████████████████████████████ ██████████████████████████ ████
7.	Mobility. The ability of voice and data infrastructure to support transportable, re-deployable, or fully mobile voice and data communications.	██████████████████████████ ██████████████████████████████ ██████████████████████ ███████████████████
8.	Nationwide Coverage. Voice and data services will be readily available to support the national security leadership and inter- and intra- agency emergency operations, wherever they are located.	██████████████████████████ ████████████████████████ ██████████████████████████████ █████████████
9.	Survivability/Endurability. Voice and data services will be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or manmade disaster up to and including nuclear war.	██████████████████████████ ██████████████████████████████ ██████████████████████████████ ██████████████████████████████ ██████████████████████████████ █████████████

#	Description of Requirement	████████████████
10.	Voice Band Service. The service will provide voice band service in support of presidential communications.	███████████████████████ ████████████████
11.	Broadband Service. The service will provide broadband service in support of NS/EP missions (e.g., video, imaging, Web access, multimedia).	███████████████████████ ███████████████████ █████████████
12.	Scalable Bandwidth. NS/EP users will be able to manage the capacity of the communications services to support variable bandwidth requirements.	████████████████████████ ███████████████████
13.	Affordability. The service will leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf (COTS) technologies, and services).	████████████████ ██████████████████████████ █████████████████ ███████████████████████ ████████████████████ ██████
14.	Reliability/Availability. Services will perform consistently and precisely according to their design requirements and specifications, and will be usable with high confidence.	████████████████ ███████████████████████████ █████████████████████ ███████████████████ ██████

MetTel's security policy is applicable to all of MetTel's network elements, systems, applications, and workstations owned or managed by MetTel. Execution of this policy is led by the MetTel security organization at the corporate and worldwide operational units. Security has ultimate responsibility for all aspects of network security. Specifically, security's role is to perform the following tasks:

- Own and manage security standards and guidelines

- Protect managed assets

- Supply security guidance and strategic direction to the business, worldwide security, and operational groups

- Provide consistent compliance, globally to the network security program

- Implement and practice security standards

- Provide accountability of senior executives for security compliance in their business or region

- Coordinate a security review program to measure the degree of security compliance and implement and execute a remediation plan derived from the review.

- Maintain awareness of security industry changes and trends and be especially mindful of information security vulnerabilities, which have been exposed in IT systems, and patch the software or firmware just as soon as the fix is available

- Develop and manage the corporation's global security education program

- Deliver security alerts and advisories to the corporate and worldwide service organizations

- Provide security specialist support to the operations and security teams

- Monitor and facilitate compliance with legal and regulatory security requirements

In addition, security standards, operating procedures, tools, and other protective measures are reviewed regularly to verify that high standards of security are observed throughout the company. As the Information Technology (IT) environment and IT security concerns change, MetTel is helping to mold the next iteration of standards. MetTel is an active member/leader/founder of several standards committees and consortia at the state, national, and international levels.

MetTel's own security assets are complemented by, and supplemented by, the participation of its security teammate, Raytheon. █████████████████████████
███
███
███
██████████████████████████████████

A8.2 SATISFACTION OF BASIC FUNCTIONAL REQUIREMENTS [G.11.1]

MetTel will support the 14 basic functional requirements for NS/EP telecommunications and IT services as outlined in **Exhibit A8-3. Basic Functional Requirements for NS/EP** above. We understand they have been identified by the Department of Homeland Security (DHS) Office of Emergency Communications (OEC) (formerly NCS) and the Office of Science and Technology Policy for NS/EP telecommunications services and are now being endorsed by ANSI T1 and ITU-TSS standard bodies and widely supported by contractor communities.

MetTel has Network-to-Network Interfaces (NNIs) with all of the major IXC's and thereby has vast interconnectivity. █████████████████████████████████

[REDACTED]

A8.3 PROTECTION OF CLASSIFIED AND SENSITIVE INFORMATION [G.11.2]

MetTel understands that NS/EP related information includes, but is not limited to, databases for classified information; critical users' locations, identifications, authorization codes, and call records; and customer profiles. Additionally, MetTel understands that:

- We are being provided with access to certain classified and sensitive materials required for the planning, management, and operations for NS/EP

- That information is in various forms, including hardcopy and electronic media

- Information will be identified as to its classification and shall be protected by MetTel in accordance with applicable industrial security regulations (National Industrial Security Program Operating Manual [NISPOM] and NSA-approved standards as applicable for Safeguarding Classified Information). [REDACTED]

- The level of classification will be up to and including Top Secret / SCI (Sensitive Compartmented Information), and identified by the government. [REDACTED]

A8.4 DEPARTMENT OF HOMELAND SECURITY OFFICE OF EMERGENCY COMMUNICATIONS PRIORITY TELECOMMUNICATIONS SERVICES [G.11.3]

MetTel will fully comply and interoperate with all Department of Homeland Security (DHS) Office of Emergency Communications (OEC) Priority Telecommunications Services including TSP, Government Emergency Telecommunications Service (GETS), and Wireless Priority Service (WPS) and, when released, Next Generation Network

Priority Services (NGN-PS). MetTel understands that the OEC's Communications Portfolio Management (CPM) Branch collaborates with the public and private sectors to ensure the NS/EP communications community has access to priority telecommunications and restoration services to communicate under all circumstances. Our MetTel EIS portal will safeguard and house critical information on NS/EP and allow access to authorized users only.

A8.4.1   Government Emergency Telecommunications Service [G.11.3.1]

MetTel understands that the Government Emergency Telecommunications Service (GETS) is a White House-directed emergency telephone service provided by the DHS OEC and:

- During emergencies, the public telephone network can experience congestion due to increased call volumes and/or damage to network facilities, hindering the ability of NS/EP personnel to complete calls. MetTel fully supports GETS. We have the ability to issue GETS cards to our critical infrastructure clients,

- GETS provides NS/EP personnel priority access and prioritized processing in the local and long distance segments of the landline networks, greatly increasing the probability of call completion.

- GETS is an easy-to-use calling card program; no special phones are required and MetTel fully participates and supports GETS. We have arrangements with DHS to do so and have provided critical infrastructure clients with GETS cards and training on how to use them.

- There is no cost to enroll in GETS, though usage fees may apply. GETS calls will receive priority over normal calls; however, GETS calls do not preempt calls in progress or deny the general public's use of the telephone network.

- GETS is in a constant state of readiness.

- It also provides priority calling to most cell phones on major carrier networks.

- MetTel will fully comply and interoperate with the GETS service, has in the past, and will continue to do so.

Exhibit A8-4. GETS Screen Shot

A8.4.2   Wireless Priority Service [G.11.3.2]

G.11.3.2 Wireless Priority Service

MetTel's wireless service is fully compliant with the WPS feature requirements shown in Section C.2.6.2. This feature is invoked by dialing *272 prior to the destination number on wireless devices that have subscribed to WPS ██████████████████████

██

████████████████████████████████████

A8.4.3   Telecommunication Service Priority [G.11.3.3]

MetTel understands that the Telecommunication Service Priority (TSP) System (FCC 88-341):

- Provides a framework for telecommunications services contractors to initiate, restore, or otherwise act on a priority basis to ensure effective NS/EP telecommunication services.

██

██

████████████████████████████████████

██

██

████████████████████████████████

- Applies to common carriers, to government, and to private systems that interconnect with commercially provided services or facilities.

- Is intended to apply to all aspects of end-to-end NS/EP telecommunication services. Allows five (5) levels of priorities for restoration (5, 4, 3, 2, or 1) and provisioning (5, 4, 3, 2, 1, or E).

MetTel will fully comply and interoperate with the TSP system for priority provisioning (i.e., installation of new circuits), restoration of previously provisioned circuits, and priority level for design change of circuits, including coordination between local access providers and the transport segment. MetTel will fully comply and interoperate with any future TSP replacement system. ██████████████████ ██

Should MetTel's network experience significant degradation or failure, MetTel will provide priority restoration of affected services in accordance with the TSP system five levels of priorities. In addition, MetTel will ensure that the restored circuits retain the property of the original circuits (i.e., TSP levels).

███ ███ ███ ███████████████████████████████

MetTel understands that TSP Authorization Codes are active for three (3) years, at which point the service user will need to revalidate them and that service users must request TSP restoration priority before a service outage occurs. We have an ongoing program with many of our customers who have been designated critical infrastructure by DHS, providing the systems, methods and practices to work appropriately with TSP priorities.