1200 G Street, NW
Suite 500
Washington, DC 20005

P: 202-628-6380
F: 202-393-5453
W: www.atis.org

April 8, 2013

VIA MAIL
Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
P.O. Box 44000
Gaithersburg, MD 20899

Re: Developing a Framework to Improve Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

Attached hereto please find the Alliance for Telecommunications Industry Solutions' (ATIS) *Comments* in response to the National Institute of Standards and Technology's *Request for Information (RFI)* from February 26, 2013.

If there are any questions regarding this matter, please do not hesitate to contact the undersigned.

Sincerely,

Thomas Goode
General Counsel

Alliance for Telecommunications Industry Solutions' (ATIS) Comments to the NIST RFI on Developing a Framework to Improve Critical Infrastructure Cybersecurity

The Alliance for Telecommunications Industry Solutions (ATIS) appreciates the opportunity to provide input in response to the February 26, 2013, Request for Information (RFI) from the National Institute of Standards and Technology (NIST).[1] The RFI seeks input regarding the development of a cybersecurity framework as required by Executive Order 13636 (2013),[2] including in particular what existing cybersecurity standards, guidelines, Best Practices or tools have been developed to support critical infrastructure. As explained more fully below, ATIS has an active work program aimed at the development of security-related standards and technical specifications that is relevant to the NIST framework.

By way of background, ATIS is a technology and solutions development organization that brings together global ICT companies to advance pressing strategic and technical priorities. ATIS' diverse membership includes key stakeholders from the ICT industry – wireless and wireline service providers, equipment manufacturers, broadband providers, software developers, consumer electronics companies, public safety agencies, digital rights management companies, and internet service providers. Nearly 600 industry subject matter experts work collaboratively in ATIS' open industry committees and incubator solutions programs.

To address the need for consistent and comprehensive cybersecurity designs across multiple network technologies, ATIS recently developed end-to-end network topology and security zones to be used as foundation for comprehensively addressing cyber-related design and implementation vulnerabilities in devices, networks and computing infrastructures. This work, developed by the ATIS Technology and Operations (TOPS) Council, may be useful to NIST in its development of a cybersecurity framework. The work identifies the following security zones:

- Untrusted zones, which include terminal equipment border elements such as residential gateways, modems, managed routers, HeNB, etc.;
- Trusted but vulnerable zones, which include network border elements such as base station routers and session border controllers; and
- Trusted zones, which include both carrier network ingress points, such as cell tower receivers, DSLAMs, etc. and carrier network, end office, hub or aggregation facilities.

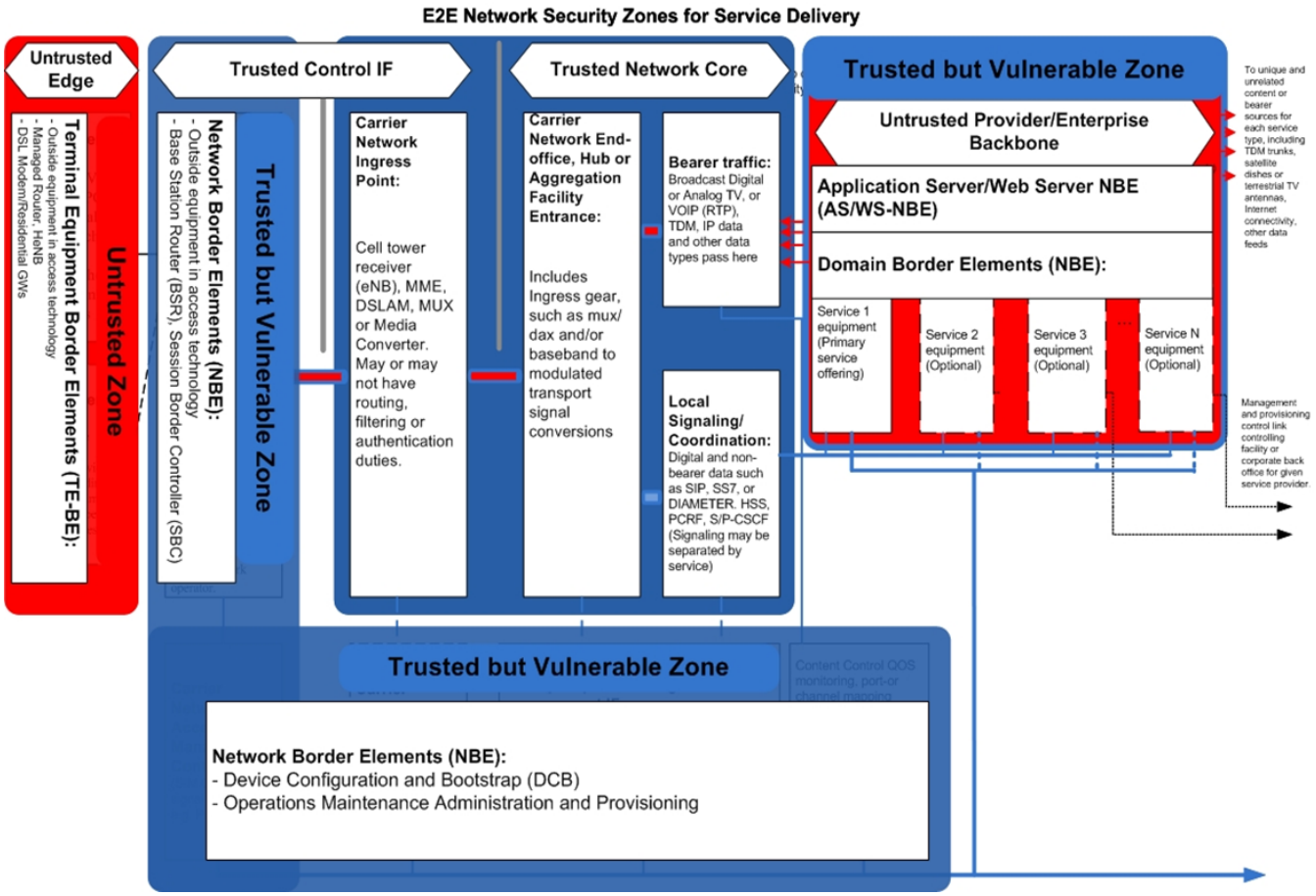
Using this analysis, the work examined four scenarios to identify the appropriate zones of trust for the delivery of service. Below is an example of this analysis as applied to a network facility owned by a single provider with inter-provider/border connections to other facilities. Attached in Appendix 1 are all four scenarios.

The ATIS TOPS Council also developed a matrix of compliance guidelines for each scenario that provides a template approach for equipment suppliers when developing future "cyber-secure"

---

[1] Request for Information (RFI), 78 Fed. Reg. 13024 (Feb. 26, 2013).
[2] Exec. Order No. 13,636, 78 Fed. Reg. 11739-11744 (Feb. 19, 2013).

network elements and devices. This matrix identifies key functions and characterizes each as they relate to confidentiality, integrity, access control, availability and accountability. It is anticipated that this matrix can be further developed for every component of the communications network. This matrix is attached as Appendix 2.



Security zones mapped onto physical/functional view

Future work to develop and further refine the cybersecurity reference architecture will be undertaken by the ATIS' Packet Technologies and Systems Committee (PTSC), which develops and recommends standards and technical reports related to services, architectures, and signaling.

ATIS also notes that there are a number of existing voluntary Best Practices related to cybersecurity. These practices have been developed by the industry through organizations such as the ATIS Network Reliability Steering Committee (NRSC) or via the Federal Communications Commission's Communications Security, Reliability and Interoperability Council (CSRIC) and its predecessors. Of the 1,023 Best Practices, 432 address cybersecurity.[3] Of these, 122 have been

[3] ATIS maintains the industry's list of Best Practices. This list, available at http://www.atis.org/bestpractices/Search.aspx, includes all Best Practices developed by the CSRIC and its

categorized as "critical." These include practices that focus on a variety of security-related issues, including the validation of source addresses, BGP Authentication, SPAM controls, redundancy, the protection of sensitive security information, recovery from specific threats, Botnet detection, etc. A complete list of all 122 critical Best Practices related to cybersecurity is attached as Appendix 3.

ATIS believes that these Best Practices have been effective in enhancing network reliability and security. These industry Best Practices are more than just good ideas – they are practices which address recurring, or potentially recurring, challenges that have been proven through actual implementation, have been developed through rigorous deliberation and expert consensus, and have been confirmed by a broad set of stakeholders. However, it is important to note that Best Practices cannot be assumed to be applicable to all circumstances and therefore must not be mandated. As has been appropriately acknowledged by the FCC's CSRIC, it would be impractical, if not impossible, to mandate compliance with Best Practices because not every Best Practice is appropriate for every sector of the industry, particularly as network and system designs, technologies, and capabilities differ and are evolving.

ATIS notes that the success of Best Practices in enhancing network resilience, reliability and security stems from their development in a voluntary and consensus-based environment that encourages a pooling of vast expertise and considerable resources. The voluntary nature of Best Practices also encourages individual service providers to develop and incorporate internal standards and policies based on the Best Practices elements that are applicable, even when other elements may not be applicable.

Any questions may be directed to Thomas Goode, ATIS General Counsel, at tgoode@atis.org.

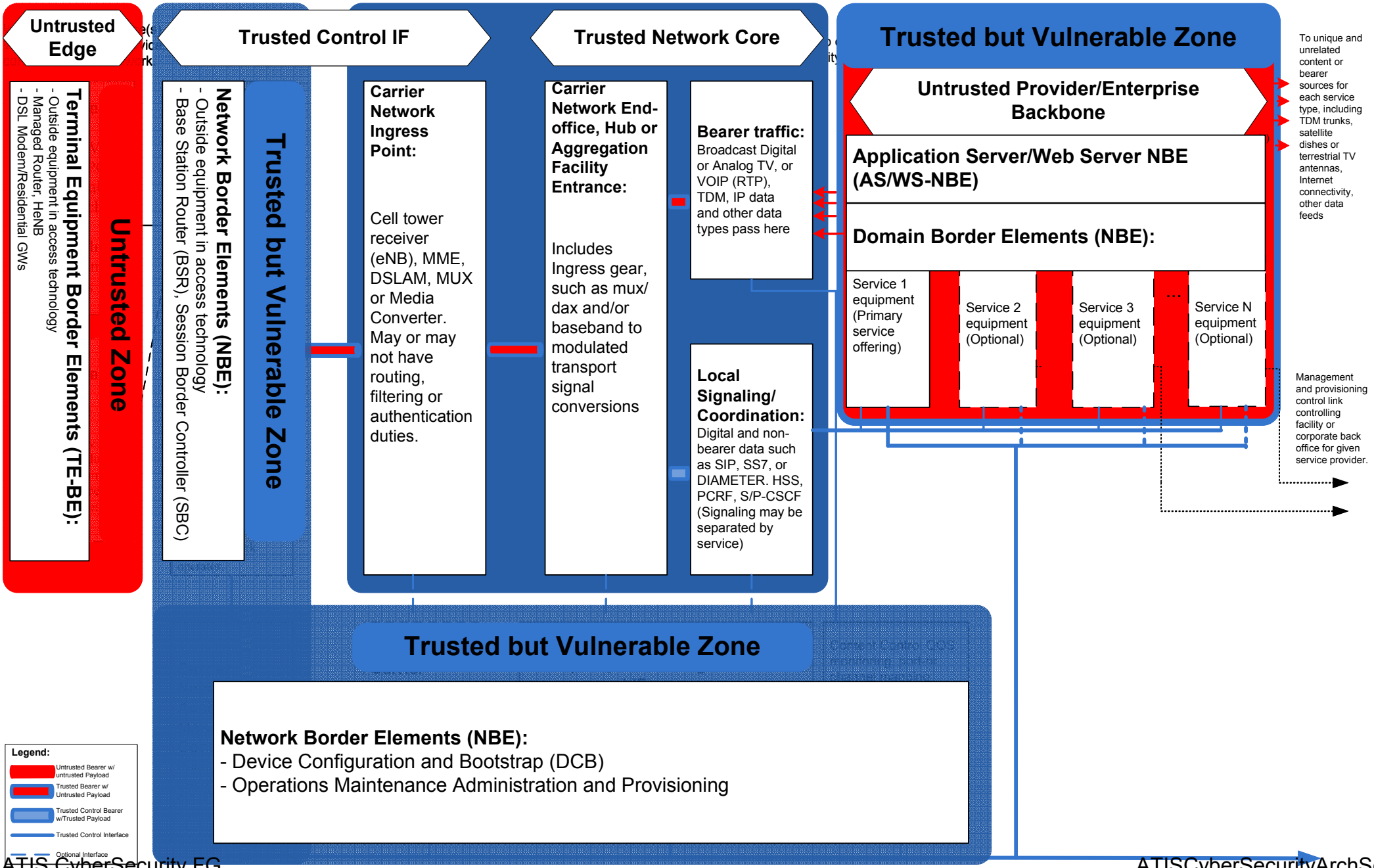
---

predecessors. Each Best Practice has been categorized as "important," highly important," or "critical." The ATIS NRSC reviews and provides guidance to the industry regarding the development of Best Practices and reviews and provides feedback to the FCC regarding new and existing Best Practices.

Appendix 1: Scenarios Used by ATIS to Identify Zones of Trust

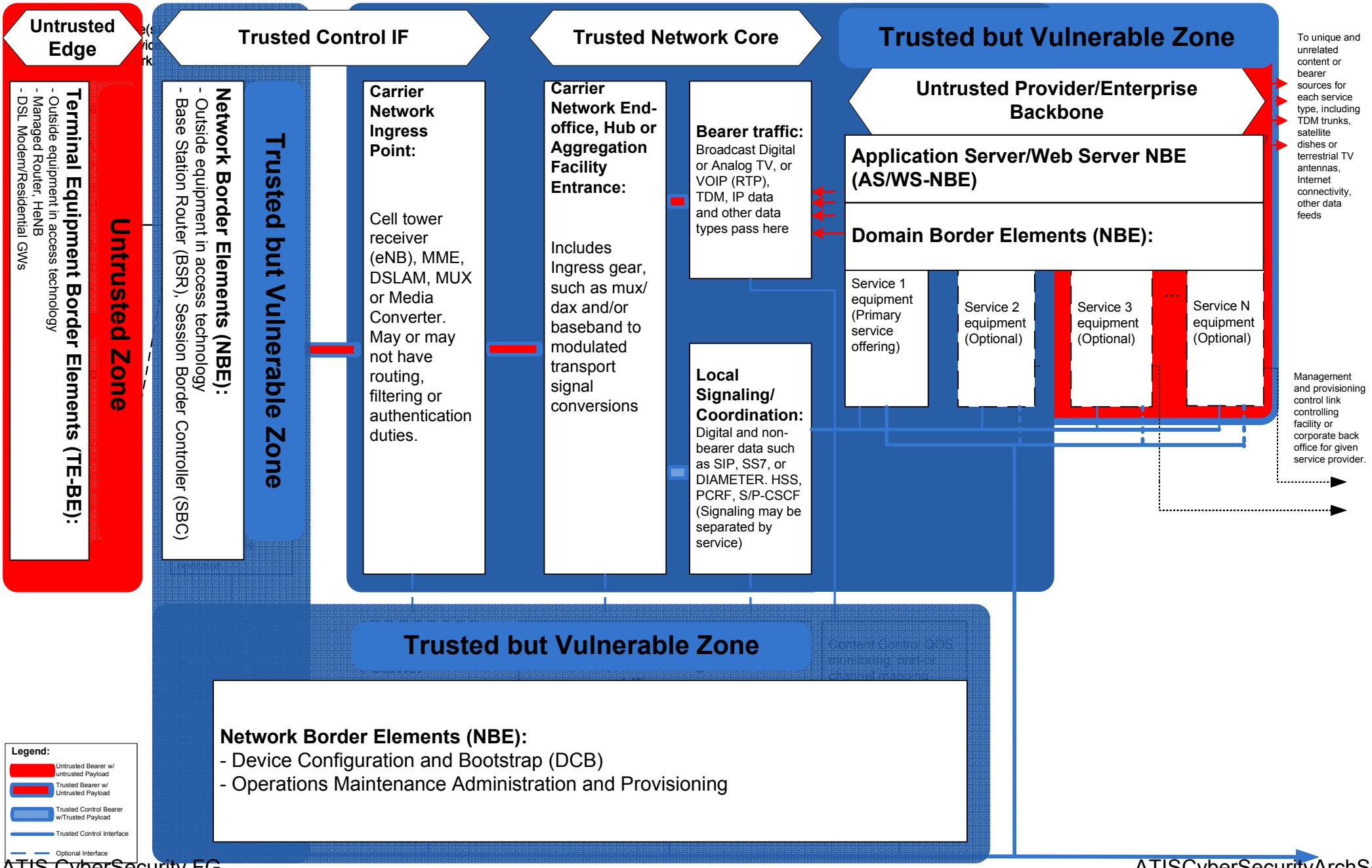
E2E Network Security Zones for Service Delivery- Base Scenario 1

Single provider owned core network facility with inter-provider/border connections to other facilities



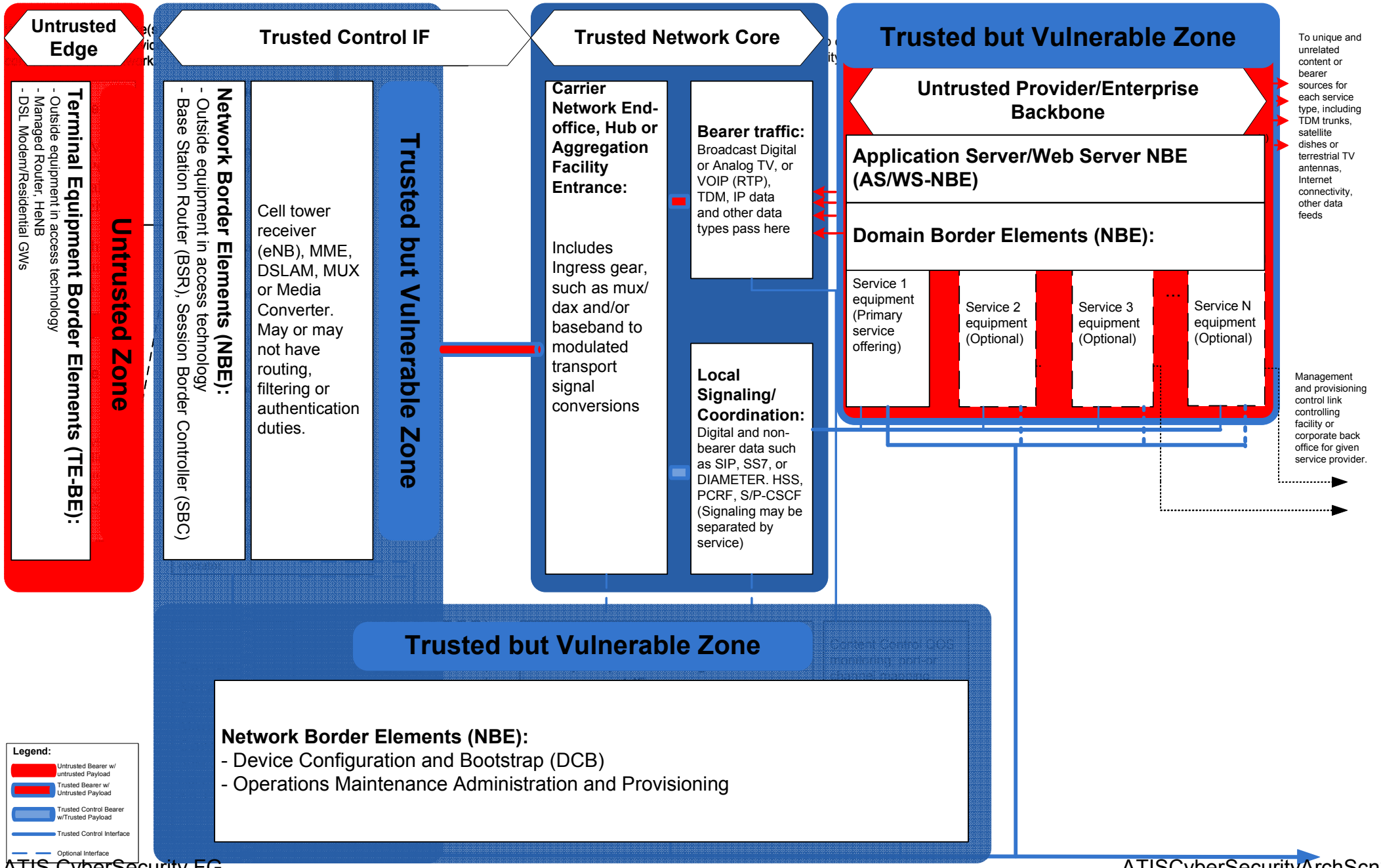
E2E Network Security Zones for Service Delivery- Scenario 2

Single provider owned core network facility with other providers co-located in the same facility, on dedicated hardware, with direct physical inter-connections into primary provider core



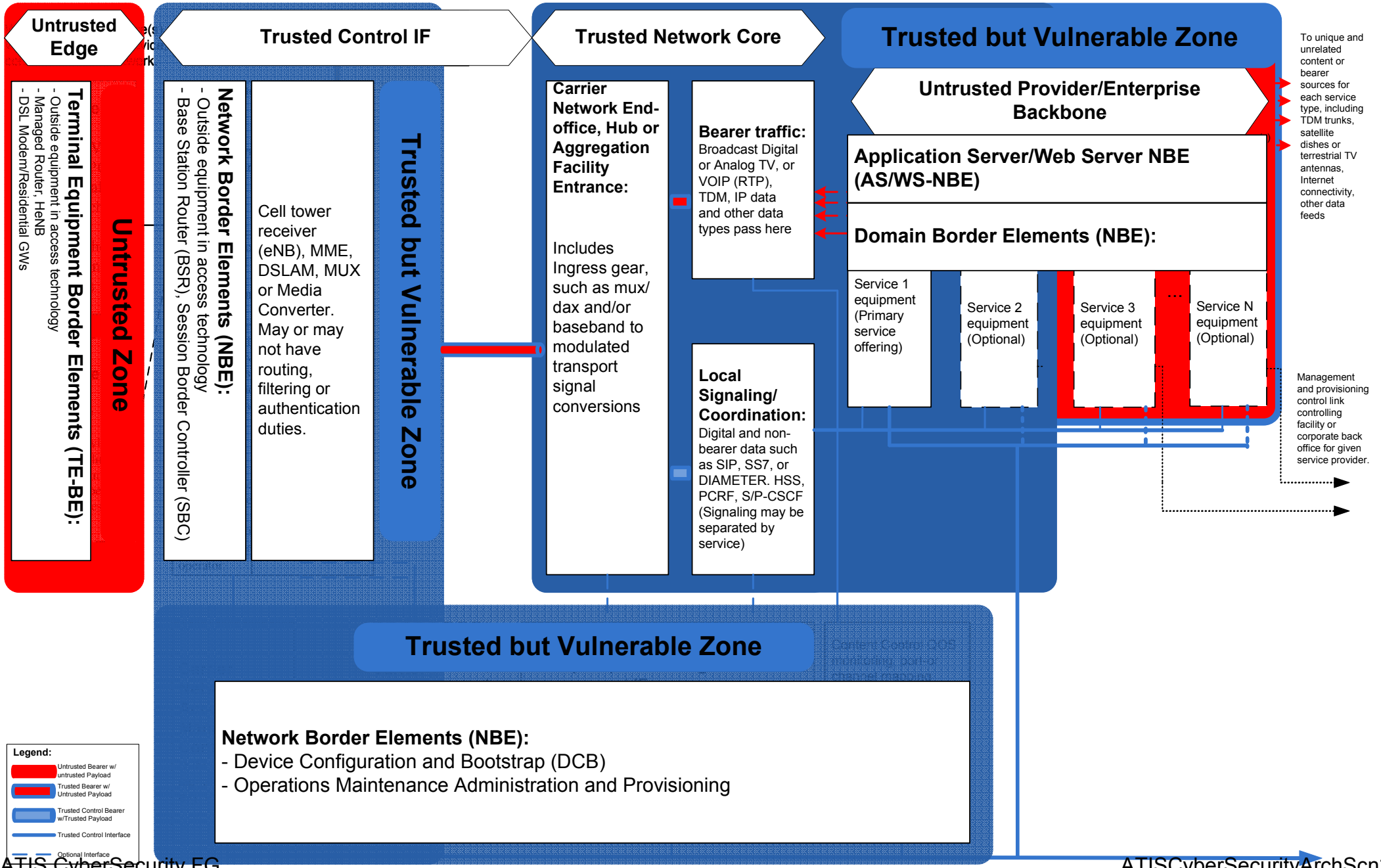
E2E Network Security Zones for Service Delivery- Scenario 3A

Single provider owned core network facility with de-centralized core elements and a centralized policy control. De-centralized elements are located closer to the customer edge and remain physically independent.



E2E Network Security Zones for Service Delivery- Scenario 3B

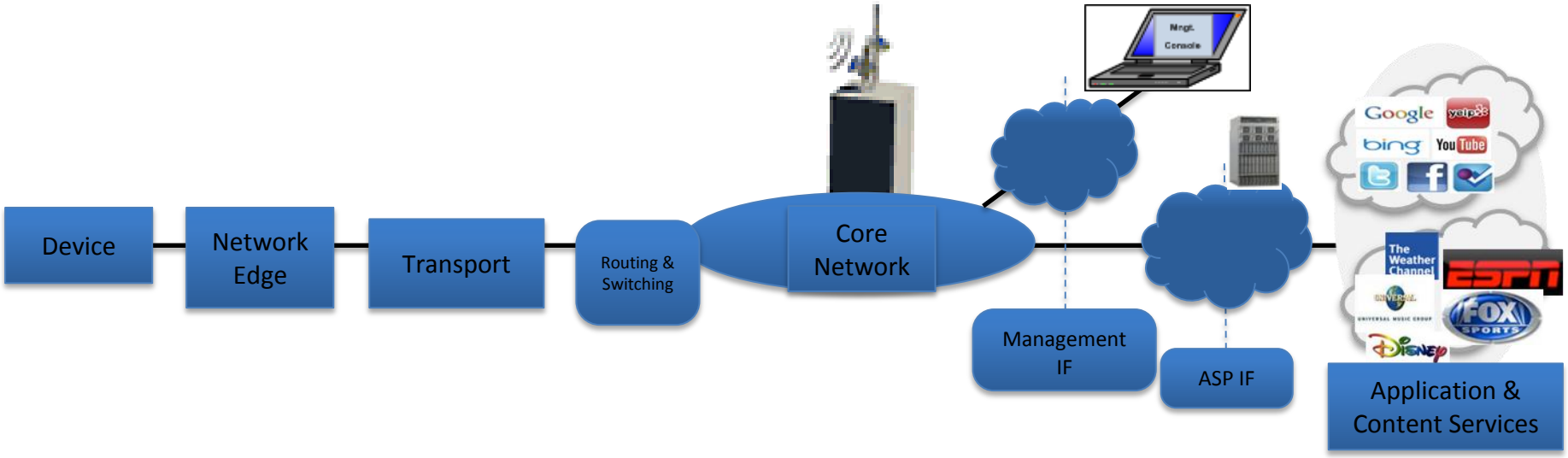
Single provider owned core network facility with de-centralized core elements and a centralized policy control. De-centralized elements are located closer to the customer edge and remain physically independent. **Other providers co-located in the core network facility i.e. shift of core network to right.**



Appendix 2: Cybersecurity Requirements Characterization Scenarios

Scenario 1: Classical Central Office Core Network with single provider ownership Usage

Description: Single Provider owned core network facility with elements physically installed at a centralized location and owned by the provider



Scenario 1: Classical Central Office Core Network with Single Provider Ownership Usage

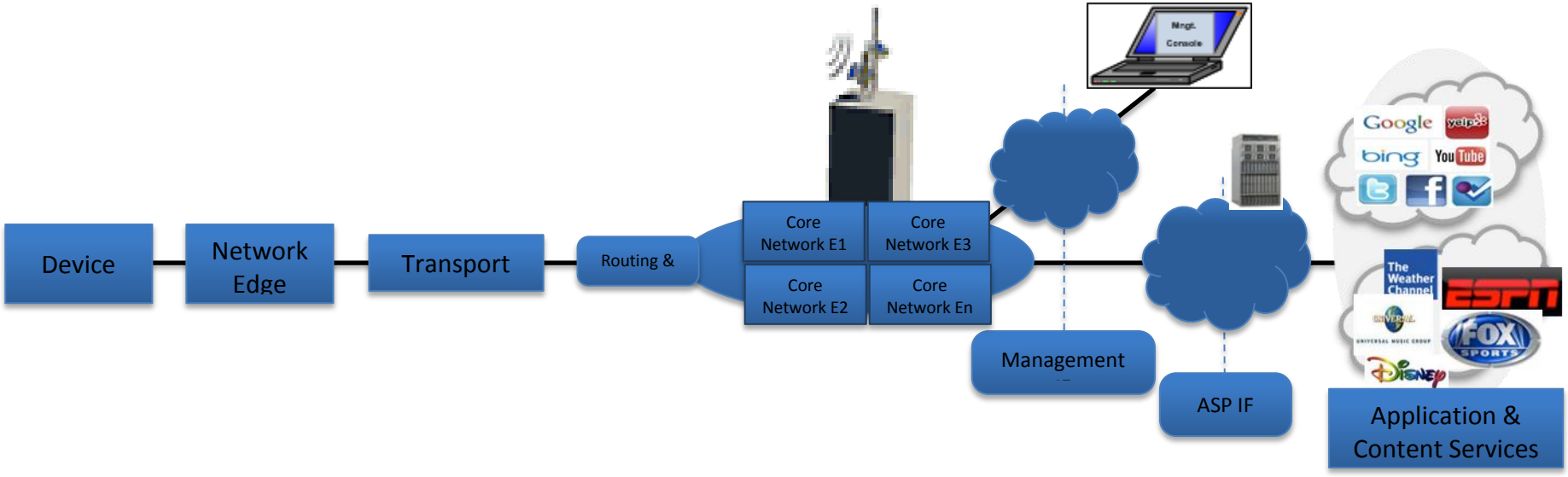
		Security Characterization Vectors				
Element	**Scenario 1 Classical Functions**	**Confidentiality**	**Integrity**	**Access Control**	**Availability**	**Accountability**
MME	The MME shall support protocol encryption for confidentiality	y				
	The MME shall implement Role-Based Access Control (RBAC) for management and administrative users			y		
	The MME shall be hardened (for example, in compliance with CIS benchmarks)			y		
	The MME shall implement password controls covering complexity, reuse, aging etc.			y		
	The MME shall implement secure logging and integrity checking of security logs					y
	The MME shall implement controls against denial of service (DoS/DDoS) attacks				y	
	The MME shall support key management for NAS signalling (in accordance with 3GPP)	y	y	y		
	The MME shall use DIAMETER for retrieval of security data from HSS for UE NAS security (in accordance with 3GPP)			y		
	The MME shall implement NAS ciphering and integrity protection (in accordance with 3GPP)	y	y			
	The MME shall set up security context with eNodeB for RRC and user plane ciphering (in accordance with 3GPP)	y				

Scenario 1: Classical Central Office Core Network with Single Provider Ownership Usage

		Security Characterization Vectors				
Element	**Scenario 1 Classical Functions**	**Confidentiality**	**Integrity**	**Access Control**	**Availability**	**Accountability**
	The MME shall support IPsec for S1-MME interface (in accordance with 3GPP)	y	y	y		
	The MME shall support mutual authentication with other LTE network elements (in accordance with 3GPP)			y		
SGW	The SGW shall support protocol encryption for confidentiality	y				
	The SGW shall implement Role-Based Access Control (RBAC) for management and administrative users			y		
	The SGW shall be hardened (for example, in compliance with CIS benchmarks)			y		
	The SGW shall implement password controls covering complexity, reuse, aging etc.			y		
	The SGW shall implement secure logging and integrity checking of security logs					y
	The SGW shall implement controls against denial of service (DoS/DDoS) attacks				y	
	The SGW shall support IPsec for S1-U interface (in accordance with 3GPP)	y	y	y		
	The SGW shall support mutual authentication with other LTE network elements (in accordance with 3GPP)			y		

Scenario 2: Classical Central Office Core Network with multi-tenant vendor usage

Description: Single Provider owned core network facility with elements physically installed at a centralized location and owned by multiple tenant vendors. - Remote access management interfaces to individual vendors or tenant delegates

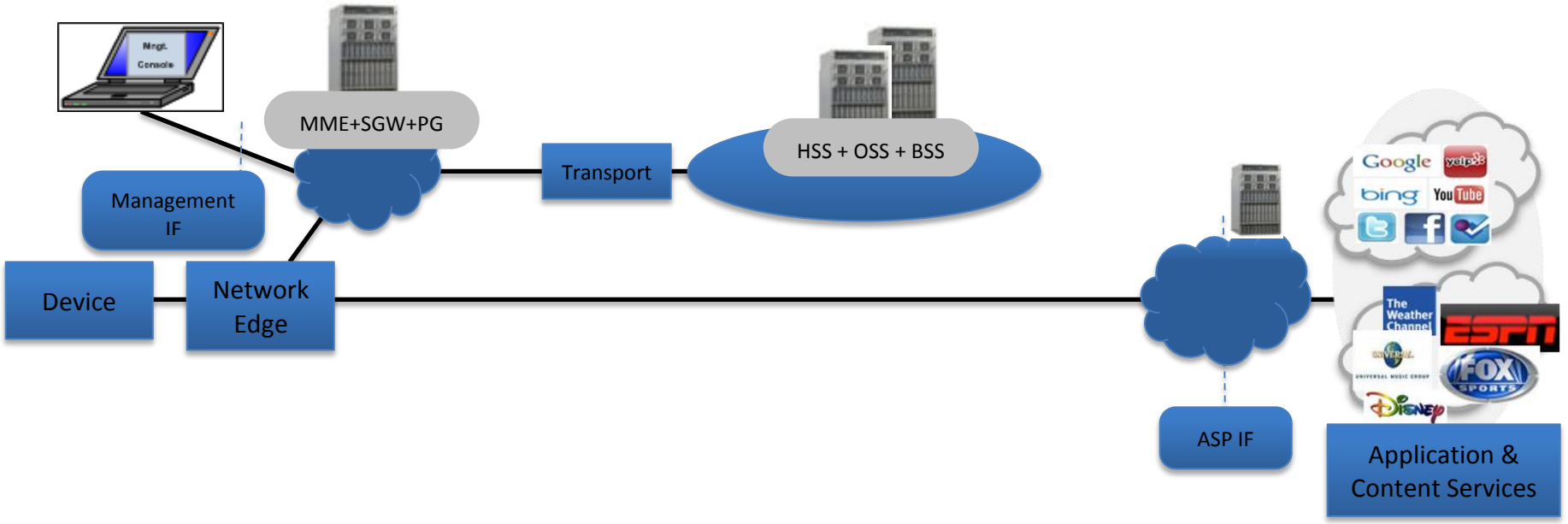


Scenario 2: Classical Central Office Core Network with Multi-Tenant Vendor Usage

		Security Characterization Vectors				
Element	**Scenario 2 Specific Functions**	**Confidentiality**	**Integrity**	**Access Control**	**Availability**	**Accountability**
Scenario 2 Specific Functions						
MME	The MME supports functions for addition/removal into a trusted tenant vendor base of the centralized facility	Y	Y	Y		Y
SGW	The SGW supports functions for addition/removal into a trusted tenant vendor base of the centralized facility	Y	Y	Y		Y

Scenario 3: Distributed Virtualized Core Network with single provider ownership Usage

Description: Single Provider owned core network with virtualized elements distributed as software instances at the edge and a centralized database at the carrier backbone enforcing SLAs. - Remote access management interfaces to **authorized delegates**



Scenario 3: Distributed Virtualized Core Network with Single Provider Ownership Usage

		Security Characterization Vectors				
Element	**Scenario 3 Specific Functions**	**Confidentiality**	**Integrity**	**Access Control**	**Availability**	**Accountability**
MME	The MME is able to be run as a virtualized software instance in a hosted cloud infrastructure without any dilution of physical security requirements of CIS/3GPP		Y			
	The MME supports functions for addition/removal as a trusted delegate in a commonly hosted cloud infrastructure	Y		Y		Y
	The MME supports functions for remote authorization of trusted management delegates	Y		Y	Y	Y
SGW	The SGW is able to be run as a virtualized software instance in a hosted cloud infrastructure without any dilution of physical security requirements of CIS/3GPP		Y			
	The SGW supports functions for addition/removal as a trusted delegate in a commonly hosted cloud infrastructure	Y		Y		Y
	The SGW supports functions for remote authorization of trusted management delegates	Y		Y	Y	Y

Appendix 3: Critical Industry Best Practices on Cybersecurity

Critical Industry Best Practices on Cybersecurity

Number	Description
8-6-5162	Network Operators, Service Providers and Equipment Suppliers should ensure adequate physical protection for facilities/areas that are used to house certificates and/or encryption key management systems, information or operations.
8-6-5170	Network Operators, Service Providers and Equipment Suppliers should control or disable all administrative access ports (e.g., manufacturer) into R&D or production systems (e.g., remap access ports, require callback verification, add second level access gateway).
8-6-8023	Scanning Operations, Administration, Management and Provisioning (OAM&P) Infrastructure: Network Operators and Service Providers should regularly scan infrastructure for vulnerabilities/exploitable conditions. Operators should understand the operating systems and applications deployed on their network and keep abreast of vulnerabilities, exploits, and patches.
8-6-8028	Distribution of Encryption Keys: When Network Operators, Service Providers and Equipment Suppliers use an encryption technology in the securing of network equipment and transmission facilities, cryptographic keys must be distributed using a secure protocol that: a) Ensures the authenticity of the recipient, b) Does not depend upon secure transmission facilities, and c) Cannot be emulated by a non-trusted source.
8-6-8093	Validate Source Addresses: Service Providers should validate the source address of all traffic sent from the customer for which they provide Internet access service and block any traffic that does not comply with expected source addresses. Service Providers typically assign customers addresses from their own address space, or if the customer has their own address space, the service provider can ask for these address ranges at provisioning. (Network Operators may not be able to comply with this practice on links to upstream/downstream providers or peering links, since the valid source address space is not known).
8-7-0401	Network Surveillance: Network Operators and Service Providers should monitor their network to enable quick response to network issues.
8-7-0402	Single Point of Failure: Network Operators and Service Providers should, where appropriate, design networks to minimize the impact of a single point of failure (SPOF).
8-7-0439	BGP Authentication: Network Operators and Service Providers should authenticate BGP sessions (e.g., using TCP MD5) with their own customers and other providers.
8-7-0449	Network Operators and Service Providers should, where feasible, deploy SPAM controls in relevant nodes (e.g., message centers, email gateways) in order to protect critical network elements and services.
8-7-0546	Network Operators and Service Providers should minimize single points of failure (SPOF) in paths linking network elements deemed critical to the operations of a

	network (with this design, two or more simultaneous failures or errors need to occur at the same time to cause a service interruption).
8-7-8029	Network Access to Critical Information: Network Operators and Service Providers and Equipment Suppliers should carefully control and monitor the networked availability of sensitive security information for critical infrastructure by: Periodic review public and internal website, file storage sites HTTP and FTP sites contents for strategic network information including but not limited to critical site locations, access codes. Documenting sanitizing processes and procedures required before uploading onto public internet or FTP site. Ensuring that all information pertaining to critical infrastructure is restricted to need-to-know and that all transmission of that information is encrypted. Screening, limiting and tracking remote access to internal information resources about critical infrastructure.
8-7-8065	Sharing Information with Law Enforcement: Network Operators, Service Providers and Equipment Suppliers should establish a process for releasing information to members of the law enforcement and intelligence communities and identify a single Point of Contact (POC) for coordination/referral activities.
8-7-8086	Define User Access Requirements and Levels: Based on the principles of least–privilege (the minimum access needed to perform the job) and separation of duties (certain users perform certain tasks), Network Operators and Service Providers should develop processes to determine which users require access to a specific device or application. Equipment Suppliers should provide capability to support access levels.
8-7-8089	Conduct Risk Assessments to Determine Appropriate Security Controls: Network Operators, Service Providers and Equipment Suppliers should perform a risk assessment of all systems and classify them by the value they have to the company, and the impact to the company if they are compromised or lost. Based on the risk assessment, develop a security policy which recommends and assigns the appropriate controls to protect the system.
8-7-8109	Automated Patch Distribution Systems: Network Operators, Service Providers and Equipment Suppliers should ensure that patching distribution hosts properly sign all patches. Critical systems must only use OSs and applications which employ automated patching mechanisms, rejecting unsigned patches.
8-8-0785	Network Operation Center (NOC) Communications Remote Access: Network Operators and Service Providers should consider secured remote access to critical network management systems for network management personnel working from distributed locations (e.g., back-up facility, home) in the event of a situation where the NOC cannot be staffed (e.g., pandemic).
8-8-0806	Service Policies: Service Providers should establish policies and develop internal controls to ensure that the infrastructure supporting high speed broadband is protected from external threats, insider threats and threats from customers. These policies should cover protocol and port filtering as well as general security best practices.

8-8-0807	Service Policies: Service Providers should establish policies and develop internal controls to ensure that individual users have availability, integrity, and confidentiality and are protected from external threats, insider threats and threats from other customers. These policies should cover protocol and port filtering as well as general security best practices.
8-8-0813	Service Awareness: Service Providers should encourage users to take steps to maintain the availability, integrity and confidentiality of their systems and to protect their systems from unauthorized access. Service Providers should enable customers to get the tools and expertise to secure their systems.
8-8-8008	Network Architecture Isolation/Partitioning: Network Operators and Service Providers should implement architectures that partition or segment networks and applications using means such as firewalls, demilitarized zones (DMZ), or virtual private networks (VPN) so that contamination or damage to one asset does not disrupt or destroy other assets. In particular, where feasible, it is suggested the user traffic networks, network management infrastructure networks, customer transaction system networks, and enterprise communication/business operations networks be separated and partitioned from one another.
8-8-8015	Segmenting Management Domains: For OAM&P activities and operations centers, Service Providers and Network Operators should segment administrative domains with devices such as firewalls that have restrictive rules for traffic in both directions and that require authentication for traversal. In particular, segment OAM&P networks from the Network Operator's or Service Provider's intranet and the Internet. Treat each domain as hostile to all other domains. Follow industry recommended firewall policies for protecting critical internal assets.
8-8-8018	Hardening OAM&P User Access Control: Service Providers, Network Operators, and Equipment Suppliers should, for OAM&P applications and interfaces, harden the access control capabilities of each network element or system before deployment to the extent possible (typical steps are to remove default accounts, change default passwords, turn on checks for password complexity, turn on password aging, turn on limits on failed password attempts, turn on session inactivity timers, etc.). A preferred approach is to connect each element or system's access control mechanisms to a robust AAA server (e.g., a RADIUS or TACAS server) with properly hardened access control configuration settings.
8-8-8019	Hardening OSs for OAM&P: Service Providers, Network Operators, and Equipment Suppliers with devices equipped with operating systems used for OAM&P should have operating system hardening procedures applied. Harding procedures include (a) all unnecessary services are disabled; (b) all unnecessary communications pathways are disabled; (c) all critical security patches have been evaluated for installations on said systems/applications; and d) review and implement published hardening guidelines, as appropriate. Where critical security patches cannot be applied, compensating controls should be implemented.

8-8-8020	Expedited Security Patching: Service Providers, Network Operators, and Equipment Suppliers should have special processes and tools in place to quickly patch critical infrastructure systems when important security patches are made available. Such processes should include determination of when expedited patching is appropriate and identifying the organizational authority to proceed with expedited patching. This should include expedited lab testing of the patches and their affect on network and component devices.
8-8-8022	Remote Operations, Administration, Management and Provisioning (OAM&P) Access: Service Providers and Network Operators should have a process by which there is a risk assessment and formal approval for all external connections. All such connections should be individually identified and restricted by controls such as strong authentication, firewalls, limited methods of connection, and fine-grained access controls (e.g., granting access to only specified parts of an application). The remote party's access should be governed by contractual controls that ensure the provider's right to monitor access, defines appropriate use of the access, and calls for adherence to best practices by the remote party.
8-8-8025	"Protection from SCADA Networks: Telecom/Datacomm OAM&P networks for Service Providers and Network Operators should be isolated from other OAM&P networks, e.g., SCADA networks, such as for power, water, industrial plants, pipelines, etc. · Isolate the SCADA network from the OAM&P network (segmentation) · Put a highly restrictive device, such as a firewall, as a front-end interface on the SCADA network for management access. · Use an encrypted or a trusted path for the OAM&P network to communicate with the SCADA ""front-end.""""
8-8-8026	Distribution of Encryption Keys: When Service Providers, Network Operators, and Equipment Suppliers use an encryption technology in the securing of network equipment and transmission facilities, cryptographic keys must be distributed using a secure protocol that: a) Ensures the authenticity of the sender and recipient, b) Does not depend upon secure transmission facilities, and c) Cannot be emulated by a non-trusted source.
8-8-8031	LAES Interfaces and Processes: Service Providers, Network Operators, and Equipment Providers should develop and communicate Lawfully Authorized Electronic Surveillance (LAES) policy. They should: · Limit the distribution of information about LAES interfaces · Periodically conduct risk assessments of LAES procedures · Audit LAES events for policy compliance · Limit access to those who are authorized for LAES administrative functions or for captured or intercepted LAES content · Promote awareness of all LAES policies among authorized individuals
8-8-8036	Exceptions to Patching: Service Provider and Network Operator systems that are not compliant with the patching policy should be noted and these particular elements should be monitored on a regular basis. These exceptions should factor heavily into the organization's monitoring strategy. Vulnerability mitigation plans should be developed and implemented in lieu of the patches. If no acceptable mitigation exists, the risks should be communicated to management.

8-8-8039	Patch/Fix Verification: Service Providers and Network Operators should perform a verification process to ensure that patches/fixes are actually applied as directed throughout the organization. Exceptions should be reviewed and the proper patches/fixes actually applied.
8-8-8042	BGP (Border Gateway Protocol) Validation: Service Providers and Network Operators should validate routing information to protect against global routing table disruptions. Avoid BGP peer spoofing or session hijacking by applying techniques such as: 1) eBGP hop-count (TTL) limit to end of physical peering link, 2) MD5 session signature to mitigate route update spoofing threats (keys should be changed periodically where feasible).
8-8-8043	Prevent BGP (Border Gateway Protocol) Poisoning: Service Providers and Network Operators should use existing BGP filters to avoid propagating incorrect data. Options include: 1) Avoid route flapping DoS by implementing RIPE-229 to minimize the dampening risk to critical resources, 2) Stop malicious routing table growth due to de-aggregation by implementing Max-Prefix Limit on peering connections, 3) Employ ISP filters to permit customers to only advertise IP address blocks assigned to them, 4) Avoid disruption to networks that use documented special use addresses by ingress and egress filtering for "Martian" routes, 5) Avoid DoS caused by unauthorized route injection (particularly from compromised customers) by egress filtering (to peers) and ingress filtering (from customers) prefixes set to other ISPs, 6) Stop DoS from un-allocated route injection (via BGP table expansion or latent backscatter) by filtering "bogons" (packets with unauthorized routes), not running default route or creating sink holes to advertise "bogons", and 7) Employ "Murphy filter" (guarded trust and mutual suspicion) to reinforce filtering your peer should have done.
8-8-8045	Protect Interior Routing Tables: Service Providers and Network Operators should protect their interior routing tables with techniques such as 1) Not allowing outsider access to internal routing protocol and filter routes imported into the interior tables 2) Implementing MD5 between IGP neighbors.
8-8-8046	Protect DNS (Domain Name System) Servers Against Compromise: Service Providers and Network Operators should protect against DNS server compromise by implementing protection such as physical security, removing all unnecessary platform services, monitoring industry alert channels for vulnerability exposures, scanning DNS platforms for known vulnerabilities and security breaches, implementing intrusion detection on DNS home segments, not running the name server as root user/minimizing privileges where possible, and blocking the file system from being compromised by protecting the named directory.
8-8-8050	MPLS (Multi-Protocol Label Switching) Configuration Security: Service Providers and Network Operators should protect the MPLS router configuration by 1) Securing machines that control login, monitoring, authentication and logging to/from routing and monitoring devices, 2) Monitoring the integrity of customer specific router configuration provisioning, 3) Implementing (e)BGP filtering to protect against labeled-path poisoning from customers/peers.

8-8-8061	IR (Incident Response) Procedures: Service Providers and Network Operators should establish a set of standards and procedures for dealing with computer security events. These procedures can and should be part of the overall business continuity/disaster recovery plan. Where possible, the procedures should be exercised periodically and revised as needed. Procedures should cover likely threats to those elements of the infrastructure which are critical to service delivery/business continuity. See appendix X and Y.
8-8-8064	Security-Related Data Collection: Service Providers and Network Operators should generate and collect security-related event data for critical systems (i.e., syslogs, firewall logs, IDS alerts, remote access logs, etc.). Where practical, this data should be transmitted to secure collectors for storage and should be retained in accordance with a data retention policy. A mechanism should be enabled on these systems to ensure accurate timestamps of this data (e.g., Network Time Protocol).
8-8-8068	Incident Response Communications Plan: Service Providers, Network Operators, and Equipment Suppliers should develop and practice a communications plan as part of the broader Incident response plan. The communications plan should identify key players and include as many of the following items as appropriate for your organization: contact names, business telephone numbers, home tel. numbers, pager numbers, fax numbers, cell phone numbers, home addresses, internet addresses, permanent bridge numbers, etc. Notification plans should be developed prior to an event/incident happening where necessary. The plan should also include alternate communications channels such as alpha pagers, internet, satellite phones, VOIP, private lines, blackberries, etc. The value of any alternate communications method needs to be balanced against the security and information loss risks introduced.
8-8-8071	Threat Awareness: Service providers and Network Operators should subscribe to vendor patch/security notifications and services to remain current with new vulnerabilities, viruses, and other security flaws relevant to systems deployed on the network.
8-8-8072	Intrusion Detection/Prevention Tools (IDS/IPS) Maintenance: Service Provider and Network Operator should maintain and update IDS/IPS tools regularly to detect current threats, exploits, and vulnerabilities.
8-8-8073	Intrusion Detection/Prevention (IDS/IPS) Tools Deployment: Service Providers and Network Operators should deploy Intrusion Detection/Prevention Tools with an initial policy that reflects the universe of devices and services known to exist on the monitored network. Due to the ever evolving nature of threats, IDS/IPS tools should be tested regularly and tuned to deliver optimum performance and reduce false positives.

8-8-8074	Denial of Service (DoS) Attack - Target: Where possible, Service Provider and Network Operator networks and Equipment Supplier equipment should be designed to survive significant increases in both packet count and bandwidth utilization. Infrastructure supporting mission critical services should be designed for significant increases in traffic volume and must include network devices capable of filtering and/or rate limiting traffic. Network engineers must understand the capabilities of the devices and how to employ them to maximum effect. Wherever practical, mission critical systems should be deployed in clustered configuration allowing for load balancing of excess traffic and protected by a purpose built DoS/DDoS protection device. Operators of critical infrastructure should deploy DoS survivable hardware and software whenever possible.
8-8-8098	Create Policy on Removal of Access Privileges: Service Providers, Network Operators, and Equipment Suppliers should have policies on changes to and removal of access privileges upon staff members status changes such as terminations, exits, transfers, and those related to discipline or marginal performance.
8-8-8103	Protect Network/Management Infrastructure from Malware: Service Providers and Network Operators should deploy malware protection tools where feasible, establish processes to keep signatures current, and establish procedures for reacting to an infection.
8-8-8105	Protection of Cellular User Voice Traffic: Service Providers and Network Operators should incorporate cellular voice encryption services and ensure that such encryption services are enabled for end users. (Voice encryption services depend on the wireless technology used, and are standards based).
8-8-8106	Protect Wireless Networks from Cyber Security Vulnerabilities: Service Providers, Network Operator, and Equipment Suppliers should employ operating system hardening and up-to-date security patches for all accessible wireless servers and wireless clients. Employ strong end user authentication for wireless IP connections. Employ logging of all wireless IP connections to ensure traceability back to end user. Employ up-to-date encryption capabilities available with the devices. In particular, vulnerable network and personal data in cellular clients must be protected if the handset is stolen.
8-8-8108	Authentication System Failure: In the event of an authentication system failure, Service Providers and Network Operators should determine how the system requiring support of the authentication system responds (i.e., determine what specific effect(s) the failure caused). The system can either be set to open or closed in the event of a failure. This will depend on the needs of the organization. For instance, an authentication system supporting physical access may be required to fail OPEN in the event of a failure so people will not be trapped in the event of an emergency. However, an authentication system that supports electronic access to core routers may be required to fail CLOSED to prevent general access to the routers in the event of authentication system failure. In addition, it is important to have a means of alternate authenticated access to a system in the event of a failure. In the case of core routers failing CLOSED, there should be a secondary means of authentication (e.g., use of a one-time password) reserved for use only in such an

	event; this password should be protected and only accessible to a small key-contingent of personnel.
8-8-8115	Mitigate Control Plane Protocol Vulnerabilities in Suppliers Equipment: Equipment Suppliers should provide controls to protect network elements and their control plane interfaces against compromise and corruption. Vendors should make such controls and filters easy to manage and minimal performance impacting
8-8-8118	Protect Against DNS (Domain Name System) Distributed Denial of Service: Service Providers and Network Operators should provide DNS DDoS protection by implementing protection techniques such as: 1) Rate limiting DNS network connections 2) Provide robust DNS capacity in excess of maximum network connection traffic 3) Have traffic anomaly detection and response capability 4) Provide secondary DNS for back-up 5) Deploy Intrusion Prevention System in front of DNS.
8-8-8119	Security-Related Data Correlation: Service Providers and Network Operators should correlate data from various sources, including non-security related sources, (i.e., syslogs, firewall logs, IDS alerts, remote access logs, asset management databases, human resources information, physical access logs, etc.) to identify security risks and issues across the enterprise.
8-8-8120	Revocation of Digital Certificates: Service Providers, Network Operators, and Equipment Suppliers should use equipment and products that support a central revocation list and revoke certificates that are suspected of having been compromised.
8-8-8125	Policy Acknowledgement: Service Providers, Network Operators, and Equipment Suppliers should ensure that employees formally acknowledge their obligation to comply with their corporate Information Security policies.
8-8-8129	Staff Training on Technical Products and Their Controls: To remain current with the various security controls employed by different technologies, Service Providers, Network Operators, and Equipment Suppliers should ensure that technical staff participate in ongoing training and remain up-to-date on their certifications for those technologies.
8-8-8500	Recovery from Digital Certificate Key Compromise: In the event the key in a digital certificate becomes compromised, Service Providers, Network Operators, and Equipment Suppliers should immediately revoke the certificate, and issue a new one to the users and/or devices requiring it. Perform Forensics and Post-mortem, as prescribed in NRIC BP 8061, to review for additional compromise as soon as business processes allow.
8-8-8501	Recovery from Root Key Compromise: In the event the root key in a digital certificate becomes compromised, Service Providers, Network Operators, and Equipment Providers should secure a new root key, and rebuild the PKI (Public Key Infrastructure) trust model. Perform Forensics and Post-mortem, as prescribed in NRIC BP 8061, to review for additional compromise as soon as business processes allow.

8-8-8502	Recovery from Vulnerable or Unnecessary Services: When a compromise occurs, or new exploits are discovered, Service Providers and Network Operators should perform an audit of available network services to reassess any vulnerability to attack and re-evaluate the business need to provide that service, or explore alternate means of providing the same capability.
8-8-8503	Recovery from Encryption Key Compromise or Algorithm Failure. When improper use of keys or encryption algorithms is discovered, or a breach has occurred, Service Providers and Network Operators should conduct a forensic analysis to assess the possibility of having potentially compromised data and identify what may have been compromised and for how long it has been in a compromised state; implement new key (and revoke old key if applicable), or encryption algorithm, and ensure they are standards-based and implemented in accordance with prescribed procedures of that standard, where possible. When using wireless systems, ensure vulnerabilities are mitigated with proper and current security measures.
8-8-8513	Recovery from Not Having and Enforcing an Acceptable Use Policy: In the event that an Acceptable Use Policy is not in place, or an event occurs that is not documented within the AUP, Service Providers and Network Operators should consult with legal counsel. Consulting with legal counsel, develop and adapt a policy based on lessons learned in the security incident and redistribute the policy when there are changes.
8-8-8514	Recovery from Network Misuse via Invalid Source Addresses: Upon discovering the misuse or unauthorized use of the network, Service Providers should shut down the port in accordance with AUP (Acceptable Use Policy) and clearance from legal counsel. Review ACL (Access Control List) and temporarily remove offending address pending legal review and reactivate the port after the threat has been mitigated.
8-8-8515	Recovery from Misuse or Undue Consumption of System Resources: If a misuse or unauthorized use of a system is detected, Service Providers and Network Operators should perform forensic analysis on the system, conduct a post-mortem analysis and enforce system resource quotas.
8-8-8517	Recovery from Unauthorized Information Dissemination: If information has been leaked or the release policy has not been followed, Service Providers, Network Operators, and Equipment Suppliers should review audit trails; Change passwords, review permissions, and perform forensics as needed; Inform others at potential risk for similar exposure; and include security responsibilities in performance improvement programs that may include security awareness refresher training.
8-8-8523	Recovery from Network Element Resource Saturation Attack: If the control plane is under attack, Service Providers and Network Operators should: 1) Turn on logging where appropriate to analyze the logs, 2) Implement the appropriate filter and access list to discard the attack traffic 3) Utilize DoS/DDoS tracking methods to identify the source of attack.
8-8-8525	Recovery from BGP (Border Gateway Protocol) Poisoning: If the routing table is under attack from malicious BGP updates, Service Providers and Network Operators

	should apply the same filtering methods used in NRIC BP 8043 more aggressively to stop the attack. When under attack, the attack vector is usually known and the performance impacts of the filter are less of an issue than when preventing an attack. The malicious routes will expire from the table, be replaced by legitimate updates, or in emergencies, can be manually deleted from the tables. Contact peering partner to coordinate response to attack.
8-8-8527	Recover from Compromised DNS (Domain Name System) Servers or Name Record Corruption: If the DNS (Domain Name System) server has been compromised or the name records corrupted, Service Providers and Network Operators should first flush the DNS cache and, failing that, implement the pre-defined disaster recovery plan. Elements may include but are not limited to: 1) bring-on additional hot or cold spare capacity, 2) bring up a known good DNS server from scratch on different hardware, 3) Reload and reboot machine to a know good DNS server software (from bootable CD or spare hard drive), 4) Reload name resolution records from a trusted back-up. After the DNS is again working, conduct a post-mortem of the attack/response.
8-8-8528	Recover from DNS (Domain Name Server) Denial of Service Attack: If the DNS server is under attack, Service Providers and Network Operators should consider one or more of the following steps 1) Implement reactive filtering to discard identified attack traffic, if possible, 2) Rate-limiting traffic to the DNS server complex, 3) Deploy suitable Intrusion Prevention System in front of DNS servers, 4) Deploy additional DNS server capacity in a round-robin architecture, 5) Utilize DoS/DDoS tracking methods to identify the source(s) of the attack, or 6) Move name resolution service to a 3rd party provider.
8-8-8530	Recover from DHCP-based DoS Attack: If a DHCP ((Dynamic Host Configuration Protocol) attack is underway, Service Provider and Network Operators should isolate the source to contain the attack. Plan to force all DHCP clients to renew leases in a controlled fashion at planned increments. Re-evaluate architecture to mitigate similar future incidents.
8-8-8531	Recover from MPLS (Multi-Protocol Label Switching) Misconfiguration: If a customer MPLS-enabled trusted VPN (Virtual Private Network) has been compromised by mis-configuration of the router configuration, Service Provider and Network Operators should 1) restore customer specific routing configuration from a trusted copy, 2) notify customer of potential security breach, 3) Conduct an investigation and forensic analysis to understand the source, impact and possible preventative measures for the security breach.
8-8-8532	Recover from SCP Compromise: No prescribed standard procedures exist for Service Providers and Network Operators to follow after the compromise of an SCP (Signaling Control Point). It will depend on the situation and the compromise mechanism. However, in a severe case, it may be necessary to disconnect it to force a traffic reroute, then revert to known good, back-up tape/disk and cold boot.
8-8-8533	Recover from SS7 DoS Attack: If an SS7 Denial of Service (DoS) attack is detected, Service Provider and Network Operators should more aggressively apply the same thresholding and filtering mechanism used to prevent an attack (NRIC BP 8053).

	The alert/alarm will specify the target of the attack. Isolate, contain and, if possible, physically disconnect the attacker. If necessary, isolate the targeted network element and disconnect to force a traffic reroute.
8-8-8535	Recover from Voice over IP (VoIP) Device Masquerades or Voice over IP (VoIP) Server Compromise: If a Voice over IP (VoIP) server has been compromised, Service Provider and Network Operators should disconnect the server; the machine can be rebooted and reinitialized. Redundant servers can take over the network load and additional servers can be brought on-line if necessary. In the case of VoIP device masquerading, if the attack is causing limited harm, logging can be turned on and used for tracking down the offending device. Law enforcement can then be involved as appropriate. If VoIP device masquerading is causing significant harm, the portion of the network where the attack is originating can be isolated. Logging can then be used for tracking the offending device.
8-8-8537	Recover from Cellular Service Anonymous Use or Theft of Service: If anonymous use or theft of service is discovered, Service Providers and Network Operators should 1) disable service for attacker, 2) Involve law enforcement as appropriate, since anonymous use is often a platform for crime. If possible, triangulate client to identify and disable. If the wireless client was cloned, remove the ESN (Electronic Serial Number) to disable user thus forcing support contact with service provider.
8-8-8539	Recover from Cellular Network Denial of Service Attack: If the attack is IP based, Service Provider and Network Operators should reconfigure the Gateway General Packet Radio Service Support Node (GGSN) to temporarily drop all connection requests from the source. Another approach is to enforce priority tagging. Triangulate the source(s) to identify and disable. (It is easier to recover from a cellular network denial of service attack if the network is engineered with redundancy and spare capacity).
8-8-8540	Recover from Unauthorized Remote OAM&P Access: When an unauthorized remote access to an OAM&P system occurs, Service Providers and Network Operators should consider terminating all current remote access, limiting access to the system console, or other tightened security access methods. Continue recovery by re-establishing new passwords, reloading software, running change detection software, or other methods, continuing quarantine until recovery is validated, as practical.
8-8-8549	Lack of Business Recovery Plan: When a Business Recovery Plan (BRP) does not exist, Service Providers and Network Operators should bring together an ad-hoc team to address the current incident. The team should have technical, operations, legal, and public relations representation. Team should be sponsored by senior management and have a direct communication path back to management sponsor. If situation exceeds internal capabilities consider contracting response/recovery options to 3rd party security provider.
8-8-8551	Responding to New or Unrecognized Event: When responding to a new or unrecognized event, Service Providers and Network Operators should follow processes similar to Appendix Y of the NRIC VII, Focus Group 2B Report

	Appendices.
8-8-8553	Sharing Information with Industry & Government during Recovery: During a security event, Service Providers, Network Operators, and Equipment Suppliers should release to the National Communications Service National Coordination Center (ncs@ncs.gov) or USCERT (cert@cert.org) information which may be of value in analyzing and responding to the issue, following review, edit and approval commensurate with corporate policy. Information is released to these forums with an understanding redistribution is not permitted. Information which has been approved for public release and could benefit the broader affected community should be disseminated in the more popular security and networking forums such as NANOG and the SecurityFocus Mailing Lists.
8-8-8554	Evidence Collection Procedures during Recovery: Insomuch as is possible without disrupting operational recovery, Service Providers and Network Operators should handle and collect information as part of a computer security investigation in accordance with a set of generally accepted evidence-handling procedures. Example evidence handling processes are provided in Appendix X, Section 2f of the NRIC VII, Focus Group 2B Report Appendices.
8-8-8555	"Recovery from Lack of an Incident Communications Plan: If an incident occurs and a communications plan is not in place, Service Providers, Network Operators, and Equipment Suppliers should, depending on availability of resources and severity of the incident, assemble a team as appropriate: · In person · Conference Bridge · Other (Email, telephonic notification lists) Involve appropriate organizational divisions (business and technical) · Notify Legal and PR for all but the most basic of events · PR should be involved in all significant events · Develop corporate message(s) for all significant events – disseminate as appropriate If not already established, create contact and escalation procedures for all significant events."
8-8-8557	Recovery from Lack of Security Reporting Contacts: If an abuse incident occurs without reporting contacts in place, Service Providers and Network Operators should: 1) Ensure that the public-facing support staff is knowledgeable of how both to report incidents internally and to respond to outside inquiries. 2) Ensure public facing support staff (i.e, call/response center staff) understands the security referral and escalation procedures. 3) Disseminate security contacts to industry groups/coordination bodies where appropriate. 4) Create e-mail IDs per rfc2142 and disseminate.
8-8-8561	Recovery from Denial of Service Attack - Target: If a network element or server is under DoS attack, Service Providers and Network Operators should evaluate the network and ensure issue is not related to a configuration/hardware issue. Determine direction of traffic and work with distant end to stop inbound traffic. Consider adding more local capacity (bandwidth or servers) to the attacked service. Where available, deploy DoS/DDoS specific mitigation devices and/or use anti-DoS capabilities in local hardware. Coordinate with HW vendors for guidance on optimal device configuration. Where possible, capture hostile code and make available to organizations such as US-CERT and NCS/NCC for review.

8-8-8562	Recovery from Denial of Service Attack - Unwitting Agent: If an infected (zombie) device is detected, Service Providers and Network Operators should isolate the box and check integrity of infrastructure and agent. Adjust firewall settings, patch all systems and restart equipment. Consider making system or hostile code available for analysis to 3rd party such as US-CERT, NCC, or upstream provider's security team if hostile code does not appear to be known to the security community. Review Incident Response Post-Mortem Checklist (NRIC BP 8548).
8-8-8563	Recovery from Denial of Service Attack – Equipment Vulnerability: When a denial of service vulnerability or exploit is discovered, Equipment Suppliers should work with clients to ensure devices are optimally configured. Where possible, analyze hostile traffic for product improvement or mitigation/response options, disseminate results of analysis.
8-8-8564	Recovery Incident Response (IR) Post Mortem Checklist: After responding to a security incident or service outage, Service Providers and Network Operators should follow processes similar to those outlined in Appendix X to capture lessons learned and prevent future events.
8-8-8600	Ad-hoc Wifi Policies: Service Providers and Network Operators should implement policies and practices that prohibit ad-hoc wireless networks. An ad-hoc wireless network is a peer-to-peer style network connecting multiple computers with no core infrastructure. They are not considered secure and are commonly associated with malicious activity.
8-8-8601	Wifi Policies: Service Providers and Network Operators should establish policies to ensure only authorized wireless devices approved by the network managing body or network security are allowed on the network. Unauthorized devices should be strictly forbidden.
8-8-8602	Wifi Standards: Service Providers and Network Operators, should implement applicable industry standards for wireless authentication, authorization, and encryption (e.g. WPA2 should be considered a minimum over WEP which is no longer considered secure).
8-8-8603	Wifi Standards: Service Providers and Network Operators should implement applicable industry standards to ensure all devices on the Wireless LAN (WLAN) network enforce network security policy requirements.
8-8-8689	Network Access Control for Signaling: Network Operators should ensure that signaling interface points that connect to IP Private and Corporate networks interfaces are well hardened and protected with firewalls that enforce strong authentication policies.
8-8-8729	Signaling Services Requested Changes: Network Operators should establish policies and processes for adding and configuring network elements, that include approval for additions and changes to configuration tables (e.g., screening tables, call tables, trusted hosts, and calling card tables). Verification rules should minimize the possibility of receiving inappropriate messages.

8-8-8736	Identity Information Access Control: Service Providers should ensure that identity information is only be accessible to authorized entities subject to applicable regulation and policy. Specifically, (a) an entity (e.g., relying party or requesting party) requesting identity data should be authenticated, and its authorization to obtain the requested information verified before access to the information is provided or the requesting identity data is exchanged, (b) policy and rules for requesting and exchanging identity data among multiple parties involved (e.g., users, relying party and identity provider) should be clearly defined and enforced.
8-8-8740	Protect Sensitive Data in Transit for Externally Accessible Applications: Service Providers and Network Operators should encrypt sensitive data from web servers, and other externally accessible applications, while it is in transit over any networks they do not physically control.
8-8-8745	Key Management: In cases where the cloud provider must perform key management, service providers should define processes for key management lifecycle: how keys are generated, used, stored, backed up, recovered, rotated, and deleted. Further, understand whether the same key is used for every customer or if each customer has its own key set.
8-8-8748	Security Testing on New Devices and Infrastructure: Service providers, network operators, and equipment vendors should test new devices to identify unnecessary services, outdated software versions, missing patches, and misconfigurations, and validate compliance with or deviations from an organization’s security policy prior to being placed on a network.
8-8-8752	Vulnerability Assessment Policies: Service providers, network operators, and equipment vendors should use custom policies created by OS, device, or by industry standard (SANS Top 20, Windows Top 10 Vulnerabilities, OWASP Top 10) and specific to your environment. Organizations should identify what scanning methods and operating procedures are best for their company, and document how they would proceed in a standard operating procedure.
8-8-8754	Vulnerability Reporting and Remediation: Service providers, network operators, and equipment vendors should focus on the highest risk vulnerabilities by ranking them by the vulnerability risk rating.
8-8-8756	General Patching: Service providers and network operators should establish and implement procedures to ensure that all security patches and updates relevant to the device or installed applications are promptly applied. The patching process should be automated whenever possible. The system should be rebooted immediately after patching if required for the patch to take effect.
8-8-8760	Recover from Voice over IP (VoIP) Compromise: If a Voice over IP (VoIP) server has been compromised, Service Provider and Network Operators should remove the device from the network until remediated.

8-8-8761	Recover from Voice over IP (VoIP) Device Masquerades or Voice over IP (VoIP) Server Compromise: If a VoIP masquerading event is occurring the service provider or network operator should attempt to collect data via log files or other means to aid law enforcement investigations If VoIP device masquerading is causing significant harm, the portion of the network where the attack is originating can be isolated.
8-8-8762	Recover from DoS Attack: Network Operators and Service Providers should work together to identify, filter, and isolate the originating points of Denial of Service (DoS) attacks when detected, and reroute legitimate traffic in order to restore normal service.
8-8-8763	Recovery from Password Management System Compromise: When a password management system or other source of passwords has been compromised, the Network Operator should act swiftly to mitigate the weaknesses that allowed the compromise, restore the compromised system to a secure state, and require all users to change their passwords immediately. Procedures should be in place to notify all affected users that their passwords have been reset or need to be changed immediately.
8-8-8765	Identity Enrollment and Issuance: Service Providers should only issue the identity information (e.g., identifiers, credentials and attributes) associated with an identity after successful identity proofing of the entity. An entity requesting enrollment should be verified and validated according to the requirements of the context (i.e., in which the identity will be used) before enrolling or issuing any associated identifiers, credentials or attributes. The proofing process and policies should be based on the value of the resources (e.g., services, transactions, information and privileges) allowed by the identity and the risks associated with an unauthorized entity obtaining and using the identity. Specifically, measures to ensure the following is recommended: (a) An entity (e.g., person, organization or legal entity) with the claimed attributes exists, and those attributes are suitable to distinguish the entity sufficiently according to the needs of the context. (b) An applicant whose identity is recorded is in fact the entity to which the identity is bound; (c) It is difficult for an entity which has used the recorded identity and credentials to later repudiate the registration/enrolment and dispute an authentication.
8-8-8766	Identity Maintenance and Updates: Service Providers should ensure secure management and maintenance of the identity data and the status of data (e.g., identifiers, credentials, attributes) by logging updates or changes to an identity, provide notifications about the updates or changes to an identity(s) or any of the data associated with the identity(s) to the systems and network elements that needs to be aware of the updates or changes, and by periodically validating the status of an identity.
8-8-8767	Identity Revocation: Service Providers should have applicable policies and enforcement for revoking an identity. Specifically, (a) Enforce policies and terminate or destroy the credentials associated (e.g., digital certificates or tokens) with an identity when it is no longer valid or has a security breach. (b) Provide notifications about the revocation or termination of an identity(s) or any of the data associated with the identity to the entity and to the systems and network elements

	that needs to be aware (i.e., All systems and processes with which the identity can be used for access have to be notified that the identity is no longer valid).
8-8-8772	Sharing Information with Law Enforcement: Service Providers, Network Operators, and Equipment Suppliers should establish a process for releasing information to members of the law enforcement and intelligence communities and identify a single Point of Contact (POC) for coordination/referral activities.
8-8-8902	Prevention 3 - ISP Provision of Anti-Virus/Security Software: ISPs should make available anti-virus/security software and/or services for its end-users. If the ISP does not provide the software/service directly, it should provide links to other software/services through its safe computing educational resources.
8-8-8903	Protect DNS Servers: ISPs should protect their DNS servers from DNS spoofing attacks and take steps to ensure that compromised customer systems cannot emit spoofed traffic (and thereby participate in DNS amplification attacks). Defensive measures include: (a) managing DNS traffic consistent with industry accepted procedures; (b) where feasible, limiting access to recursive DNS resolvers to authorized users; (c) blocking spoofed DNS query traffic at the border of their networks, and (d) routinely validating the technical configuration of DNS servers by, for example, utilizing available testing tools that verify proper DNS server technical configuration.
8-8-8904	Utilize DNSSEC: ISPs should use Domain Name System (DNS) Security Extensions (DNSSEC) to protect the DNS. ISPs should consider, at a minimum, the following: sign and regularly test the validity of their own DNS zones, routinely validate the DNSSEC signatures of other zones; employ automated methods to routinely test DNSSEC-signed zones for DNSSEC signature validity.
8-8-8905	Encourage Use of Authenticated SMTP/Restrict Outbound Connections to Port 25: ISPs should encourage users to submit email via authenticated SMTP on port 587, requiring Transport Layer Security (TLS) or other appropriate methods to protect the username and password. In addition, ISPs should restrict or otherwise control inbound and outbound connections from the network to port 25 (SMTP) of any other network, either uniformly or on a case by case basis, e.g., to authorized email servers.
8-8-8906	Authentication of Email: ISPs should authenticate all outbound email using DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF). Authentication should be checked on inbound emails; DKIM signatures should be validated and SPF policies verified.
8-8-8907	Immediately Reject Undeliverable Email: ISPs should configure their gateway mail servers to immediately reject undeliverable email, rather than accepting it and generating non-delivery notices (NDNs) later, in order to avoid sending NDNs to forged addresses.
8-8-8908	Share Dynamic Address Space Information: ISPs should share lists of their dynamic IP addresses with operators of DNS Block Lists (DNSBLs) and other similar tools. Further, such lists should be made generally available, such as via a public website.

8-8-8909	Share Dynamic Address Space Information: ISPs should share lists of their dynamic IP addresses with operators of DNS Block Lists (DNSBLs) and other similar tools. Further, such lists should be made generally available, such as via a public website.
8-8-8910	Make Dynamic IPv4 Space Easily Identifiable by Reverse DNS Pattern: ISPs should make IPv4 dynamic address space under their control easily identifiable by reverse DNS pattern, preferably by a right-anchor string with a suffix pattern chosen so that one may say that all reverse DNS records ending in *.some.text.example.com are those that identify dynamic space.
8-8-8911	Make Dynamic Address Space Easily Identifiable by WHOIS: ISPs should make all dynamic address space under their control easily identifiable by WHOIS or RWHOIS lookup.
8-8-8913	Maintain Methods to Detect Bot/Malware Infection: ISPs should maintain methods to detect likely malware infection of customer equipment. Detection methods will vary widely due to a range of factors. Detection methods, tools, and processes may include but are not limited to: external feedback, observation of network conditions and traffic such as bandwidth and/or traffic pattern analysis, signatures, behavior techniques, and forensic monitoring of customers on a more detailed level.
8-8-8915	Do Not Block Legitimate Traffic: ISPs should ensure that detection methods do not block legitimate traffic in the course of conducting botnet detection, and should instead employ detection methods which seek to be non-disruptive and transparent to their customers and their customers' applications.
8-8-8916	Bot Detection and the Corresponding Notification Should Be Timely: ISPs should ensure that bot detection and the corresponding notification to end users be timely, since such security problems are time-sensitive. If complex analysis is required and multiple confirmations are needed to confirm a bot is indeed present, then it is possible that the malware may cause some damage, to either the infected host or remotely targeted system (beyond the damage of the initial infection) before it can be stopped. Thus, an ISP must balance a desire to definitively confirm a malware infection, which may take an extended period of time, with the ability to predict the strong likelihood of a malware infection in a very short period of time. This 'definitive-vs.-likely' challenge is difficult and, when in doubt, ISPs should err on the side of caution by communicating a likely malware infection while taking reasonable steps to avoid false notifications.

8-8-8917	Notification to End Users: ISPs should develop and maintain critical notification methods to communicate with their customers that their computer and/or network has likely been infected with malware. This should include a range of options in order to accommodate a diverse group of customers and network technologies. Once an ISP has detected a likely end user security problem, steps should be undertaken to inform the Internet user that they may have a security problem. An ISP should decide the most appropriate method or methods for providing notification to their customers or internet users, and should use additional methods if the chosen method is not effective. The range of notification options may vary by the severity and/or criticality of the problem. Examples of different notification methods may include but are not limited to: email, telephone call, postal mail, instant messaging (IM), short messaging service (SMS), and web browser notification.
8-8-8919	Mitigation 1 - Industry Cooperation During Significant Cyber Incidents: ISPs should maintain an awareness of cyber security threat levels and, when feasible, cooperate with other organizations during significant cyber incidents, helping to gather and analyze information to characterize the attack, offer mitigation techniques, and take action to deter or defend against cyber attacks as authorized by applicable law and policy.
8-8-8920	Temporarily Quarantine Bot Infected Devices: ISPs may temporarily quarantine a subscriber account or device if a compromised device is detected on the subscribers' network and the network device is actively transmitting malicious traffic. Such quarantining should normally occur only after multiple attempts to notify the customer of the problem (using varied methods) have not yielded resolution. In the event of a severe attack or where an infected host poses a significant present danger to the healthy operation of the network, then immediate quarantine may be appropriate. In any quarantine situation and depending on the severity of the attack or danger, the ISP should seek to be responsive to the needs of the customer to regain access to the network. Where feasible, the ISP may quarantine the attack or malicious traffic and leave the rest unaffected.
8-8-8922	Privacy Considerations in Botnet Detection, Notification, and Remediation: Because technical measures to (a) detect compromised end-user devices, (b) notify end-users of the security issue, and (c) assist in addressing the security issue, may result in the collection of customer information (including possibly "personally identifiable information" and other sensitive information, as well as the content of customer communications), ISPs should ensure that all such technical measures address customers' privacy, and comply and be consistent with all applicable laws and corporate privacy policies.

8-8-8923	Measures to Protect Privacy in Botnet Response: In designing technical measures for identification, notification, or other response to compromised end-user devices ("technical measures"), ISPs should pursue a multi-prong strategy to protect the privacy of customers' information, including but not limited to the following: a) ISPs should design technical measures to minimize the collection of customer information; b) In the event that customer information is determined to not be needed for the purpose of responding to security issues, the information should promptly be discarded; c) Any access to customer information collected as a result of technical measures should at all times be limited to those persons reasonably necessary to implement the botnet-response security program of the ISP, and such individuals' access should only be permitted as needed to implement the security program; d) In the event that temporary retention of customer information is necessary to identify the source of a malware infection, to demonstrate to the user that malicious packets are originating from their broadband connection, or for other purposes directly related to the botnet-response security program, such information should not be retained longer than reasonably necessary to implement the security program (except to the extent that law enforcement investigating or prosecuting a security situation, using appropriate procedures, has requested that the information be retained); and e) The ISP's privacy compliance officer, or another person not involved in the execution of the security program, should verify compliance by the security program with appropriate privacy practices.