June 2012

WORKING GROUP - 8
E9-1-1 Best Practices

Final Report – Part 1

Table of Contents

1 Results in Brief

1.1 Executive Summary[1]

During the aftermath of a severe storm, earthquake, terrorist attack, or other natural or man-made disaster, the rapid restoration of the E9-1-1 infrastructure may make the difference between life and death for the public at large. Public safety personnel and emergency responders need the ability to prioritize their rescue efforts, perform triage to help the most in need first, and to generally be able to assess the impact to life and property.

The risk of damage or significant impairment to the E9-1-1 network following one of these "all hazards" conditions should be considered jointly by Service Providers, Network Operators, and Public Safety through a well-developed and routinely exercised business continuity plan. On the other hand, when impairment does occur despite best efforts, the ability to rapidly restore the infrastructure, and thus connectivity to emergency services, must also be planned well in advance of any impact.

One critical consideration when reacting to a crisis situation is the prioritization of service restoral. Many Service Providers maintain business continuity plans that address the order in which communications are restored that usually include emergency services, government services, internal services, and customer services.

Communications Security, Reliability and Interoperability Council (CSRIC) III Working Group 8 was established to modify and/or develop new Best Practices that will support communication providers in preparing for natural or man-made disasters. These Best Practices will ensure that communication providers are able to plan ahead and restore service quickly in the aftermath of a disaster as well as initiate procedures that could help reduce the effects that a disaster may have on the network. This includes how E9-1-1 traffic might be prioritized in such situations from an infrastructure point of view.

This Final Report - Part 1 is the first part of a larger review of industry Best Practices intended to modernize those that relate specifically to E9-1-1 and more importantly to consider the need for Best Practices for Next Generation E9-1-1 services that may be useful in preparing for natural or man-made disasters.

For Part 1 of the Final Report, the CSRIC III is being asked to accept this document and the recommended Best Practices contained within, and to recommend resolution for any gaps found by this Working Group that were determined to be out of scope during this initiative.

[1] What is an Executive Summary?; Source: http://www.2myprofessor.com/Common/executive_summary.htm

2 Introduction[2]

CSRIC was established as a federal advisory committee designed to provide recommendations to the Commission regarding Best Practices and actions the Commission may take to ensure optimal operability, security, reliability, and resiliency of communications systems, including telecommunications, media, and public safety communications systems.

Due to the large scope of the CSRIC mandate, the committee then divided into a set of Working Groups, each of which was designed to address individual issue areas. In total, 10 different Working Groups were created, including Working Group 8 on E9-1-1 Best Practices.

This Final Report – Part 1 documents the efforts undertaken by CSRIC Working Group 8 – E9-1-1 Best Practices with respect to the long term network requirements to ensure that communication providers are able to restore service quickly in the aftermath of a disaster. The team considered how these Best Practices would apply to originating providers such as legacy wireline, wireless, cable Voice over Internet Protocol (VoIP), internet based VoIP, E9-1-1 and NG9-1-1 network and functional software providers, and database providers.

Working Group 8 officially started its work on November 17, 2011, and was given until June 2012 to produce this Final Report – Part 1 and December 2012 to produce a Final Report – Part 2 on overall Best Practice recommendations. The focus for Working Group 8 is to review the existing set of 1,022 voluntary industry Best Practices developed over the years by the various Network Reliability and Interoperability Council (NRIC) and the previous CSRIC Council.

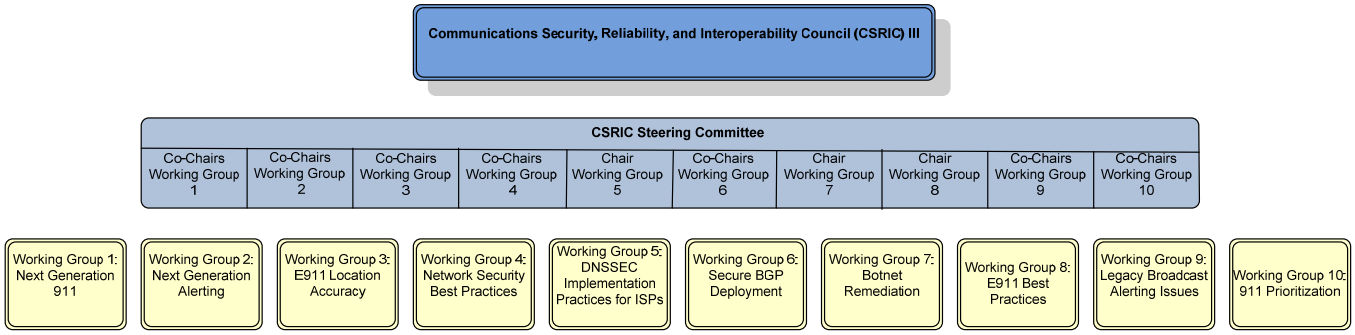
With the introduction of Next Generation E9-1-1 services and the overall changes in technology over the past decade an in-depth review of Best Practices that relate to Cyber security, Physical security, Disaster Recovery and Mutual Aid, Network Reliability and Interoperability, and Public Safety were found to be in scope for this team. This working group is made up of experts from public safety and industry which provided an end to end E9-1-1 network view.

The team began analysis of the entire Best Practice data set and worked to identify those items that would have a direct impact on the Working Group's task of supporting communication providers in preparing for natural or man-made disasters. Once the unrelated Best Practices were removed, those that remained could be further analyzed and applied to the framework that was developed in this report.

The team also addressed gaps that have not been historically addressed through the Best Practice process and that, if implemented by industry, would further protect the E9-1-1 network and improve the resiliency to survive a crisis event or at the least, assist in the rapid restoration in the aftermath.

[2] Writing@CSU; Source: http://writing.colostate.edu/guides/processes/science/pop2a3.cfm

2.1 CSRIC Structure



2.2 Working Group 8 Team Members

Working Group 8 – E9-1-1 Best Practices consists of the members listed below.

Name	Company
Robin Howard – Chair WG 8 & WG8-1	Verizon
Angel Arocho	Comcast
Donna Bethea-Murphy	Iridium
Mary Boyd – Chair WG8-2	Intrado
Lien Dao	AT&T
Thomas Dombrowsky	Wiley Rein LLP
Jeff Hall	T-Mobile
Roger Hixon	National Emergency Number Association
Jeff Hubbard	CenturyLink
Elise Kim	9-1-1 FOR KIDS: Public Education
Cathy Kurnas	Cassidian Communications
Gail Linnell	Applied Communication Sciences
Kathryn Martin	Access Partnership
Jacqueline Randall	Washington State Military Department E911 Program Office
Alisa Simmons	Tarrant County 9-1-1 District
Steve Souder	Fairfax County, VA Department. of 9-1-1 Public Safety Communications
Dorothy Spears-Dean	Virginia Information Technologies Agency
Paul Stoffels – Chair WG8-3	Alliance for Telecommunications Industry Solutions (AT&T)
Jackie Voss	Alliance for Telecommunications Industry Solutions
Steve Zweifach	Sprint

Table 1 - List of Working Group Members

3 Objective, Scope, and Methodology

3.1 Objective

For Final Report - Part 1, the objective was to modify and/or develop new voluntary industry Best Practices that will support communication providers, e.g. originating providers such as legacy wireline, wireless, cable VoIP, internet based VoIP, E9-1-1 and NG9-1-1 network and functional software providers, and database providers, in preparing for natural or man-made disasters.

A framework would be developed that efficiently identifies the Best Practices that are within scope and could be used by any Service Provider, Network Operator, or Public Safety agency to improve reliability and resiliency when developing or enhancing disaster plans or business continuity planning.

The final objective for Working Group 8-1 "*E9-1-1 Disaster Best Practices"* was to focus specifically on the prevention and restoration of the Next Generation E9-1-1 and Legacy E9-1-1 network infrastructures.

3.2 Scope[3]

The scope of the team was to identify current Best Practices that could apply to disaster recovery processes or identify those that could be enhanced with minor modifications. Given this scope, the group found it essential to place an initial focus on the 1,022 Best Practices developed over the years by previous NRIC Focus Groups and CSRIC Working Groups. The Working Group is also tasked with the modification of the Best Practices potentially associated with E9-1-1 infrastructure and will continue its work following submission of this Final Report - Part 1. The Final Report - Part 2, due in December 2012, will address these remaining modifications[4].

The full Best Practice data set does not apply to disaster recovery processes; therefore it was in scope for this team to review and reject those Best Practices that would not directly relate to the prevention and restoration of the E9-1-1 network infrastructure and facilities. Within scope was also the identification of Best Practices, and to identify gaps, that will assist in prioritizing E9-1-1 service restoration in the aftermath of an all hazards event.

It should be noted that industry Best Practices are voluntary in nature and may not apply to all Service Providers due to scope, cost, feasibility, or resource limitations. Best Practices should be used by experts who have the overall experience to interpret the Best Practice in the manner in which it was intended.

[3] Elements of a Research Proposal and Report; Source: http://www.statpac.com/research-papers/research-proposal.htm

[4] It should be noted that Best Practices identified in this Final Report - Part 1 may be altered by the final Working Group 8 team in December of 2012, however, the identified current Best Practices are in force at the time of this report and are appropriate for use by industry to implement these recommendations.

3.3 Methodology[5]

Due to the scope of the work required Working Group 8 was separated into three sub-teams to address specific areas of the Best Practice work. Sub-team 8-1 "*E9-1-1 Disaster Best Practices*" was tasked with modifying and/or developing new Best Practices that will support communication providers in preparing for natural or man-made disasters. This sub-team developed Final Report - Part 1 which focuses on the Best Practices that will ensure that communication providers are able to restore service quickly in the aftermath of a disaster. This includes how E9-1-1 traffic might be prioritized in such situations. This report was due June 2012.

Sub-group 8-2 "*Current E9-1-1 Best Practices*" is tasked with reviewing the existing CSRIC/NRIC E9-1-1 best practices and recommend ways to improve them, accounting for the passage of time, technology changes, operational factors, and any identified gaps. Their deliverable is due December 2012.

Sub-group 8-3 "*PSAP and Consumer Best Practices*" has the challenge of creating two new best practice data sets to address and capture the experiences of Public Safety organizations and to provide consumers a standard set of recommendations on how to properly use 9-1-1 during critical times. Their deliverable is also due December 2012.

3.3.1 Approach to E9-1-1 Disaster Recovery

3.3.1.1 High Level Model – Legacy E9-1-1

The more traditional, or historical, means of transmitting E9-1-1 calls from Service Providers and network operators involves passing voice, Automatic Number Identification (ANI), and Automatic Location Identification (ALI) using the Time Division Multiplexing (TDM) Public Switched Telephone Network (PSTN).

This model includes E9-1-1 call delivery methods involving legacy E9-1-1 networks[6] where call delivery is based on central office and wireless Mobile Switching Center (MSC) dedicated E9-1-1 trunk groups to a selective router(s) and then dedicated trunk groups to the PSAP. Voice over Internet Protocol (VoIP) E9-1-1 calls are transitioned onto the PSTN network through media gateways and, along with wireless E9-1-1 calls, utilize a Pseudo ANI to provide needed information at the PSAP. Traditionally, the Legacy E9-1-1 Network will route calls to a backup location or alternate route in the event the primary PSAP becomes unavailable.

Legacy E9-1-1 infrastructure reliability and resiliency are dependent on factors such as:

- Diversity of facility routes in the originating Service Providers and the legacy E9-1-1 providers interoffice transport systems.
- Mated selective routers and/or tandems to handle failover and excessive call delivery.

[5] Elements of a Research Proposal and Report; Source: http://www.statpac.com/research-papers/research-proposal.htm

[6] Legacy network in this Final Report - Part 1 is a term used to define the telecommunication Time Division Multiplexing (TDM) Public Switched Telephone Network (PSTN) network architecture pre-internet protocol and pre-Next Generation platform.

- Signaling System – 7 architecture for call setup on dedicated trunk groups.
- Robust E9-1-1 call flow over multi-frequency (MF) Centralized Automatic Message Accounting (CAMA) trunks from selective routers to PSAP.
- Sufficient trunk capacity to process E9-1-1 calls at all points in the legacy network.

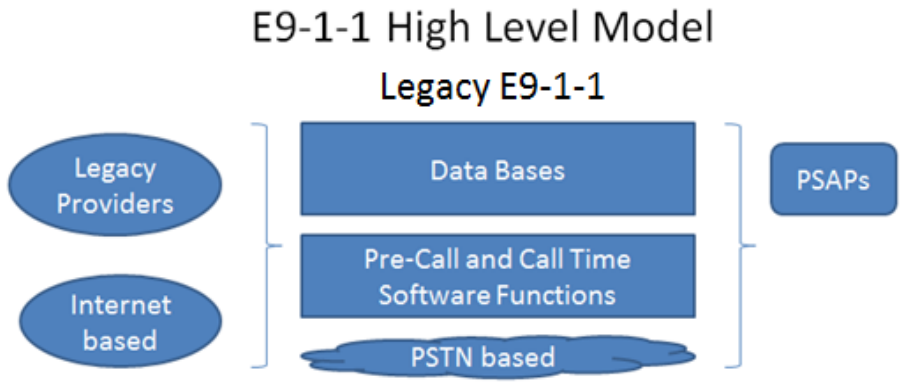


Figure 1: Legacy E9-1-1 Model

3.3.1.2 High Level Model - Multimedia

The Next Generation of transmitting E9-1-1 calls from Service Providers and Network Operators involves passing voice, data, and video simultaneously over internet based facilities. These new platforms are mostly independent of the traditional legacy network and are designed in a mesh arrangement that provides for a robust and resilient network.

This multimedia model includes E9-1-1 call delivery methods involving internet and cloud-based services. Call delivery could also still be based on traditional legacy network up to the point in the network where it is transitioned onto the IP network through media gateways. VoIP and next generation wireless network E9-1-1 calls will route entirely over the IP network maximizing the inherent reliability of the internet to deliver E9-1-1 information. The multimedia model includes routers, gateways, IP protocols, etc. that allow dynamic routing of E9-1-1 calls to PSAPs in either a traditional primary/secondary setup or through a more robust distributed “one to many” application.

Multimedia E9-1-1 infrastructure reliability and resiliency are dependent on factors such as:

- Diversity within Internet based networks in a mesh or distributed fashion.
- Ability to recover from cyber based events.
- Protection from cyber security threats.
- Media gateway availability.
- Robust databases that support E9-1-1 call delivery.

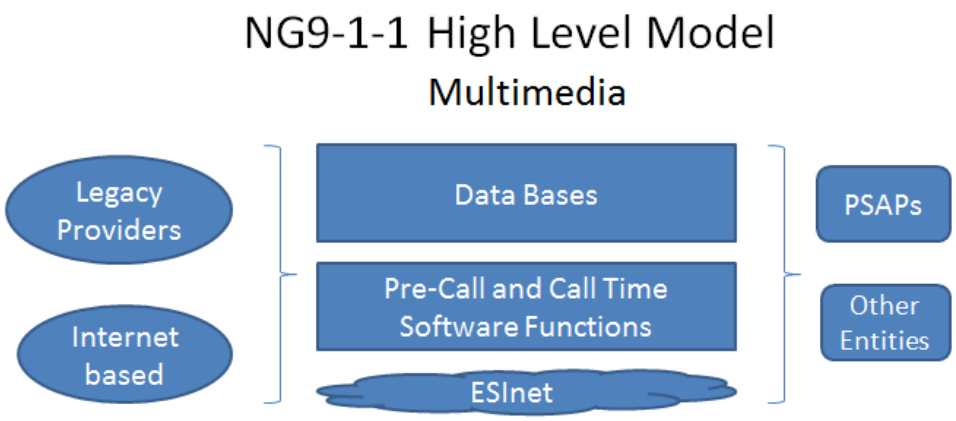


Figure 2: Multimedia Model

3.3.1.3 Elements for Best Practice Study

In both the Legacy E9-1-1 and Multimedia models there are specific elements that the Working Group identified where Best Practices would be applicable for prevention and recovery efforts related to disaster recovery and business continuity planning.

Legacy Providers:

Best Practices for this element include those that address the traditional E9-1-1 network as previously described. This element also addresses the transition points between the legacy TDM network and the IP network when considering VoIP.

Internet Based:

Best Practices for this element include those that address not only the physical assets associated with prevention and restoration but also the cyber issues that have been brought into play by the introduction of the Next Generation platform.

Databases:

Best Practices for this element include those that consider preventative and restoration of critical databases that are needed for proper E9-1-1 call completion. Examples of critical databases include the data used to perform real time routing of an emergency call, and/or to deliver the ALI to the PSAP. These databases are typically provisioned in redundant architecture methods with offsite backup copies of the data created regularly.

Pre-Call and Call Time Software Functions:

Best Practices for this element include those that address the underlying software needs that are critical to the ability of both the Legacy E9-1-1 and multimedia models to properly perform call setup and timing functions. Examples of Pre-call and Call Time software functions include pre-

populating E9-1-1 routing tables when service is installed rather than obtaining customer location information for routing purposes at the time of the call.

Public Switch Telephone Network (PSTN) based:

Best Practices for this element include those that address prevention and restoration of the traditional network elements and facilities that are needed to process voice E9-1-1 based calls through the legacy network. Examples of PSTN related items are E9-1-1 trunk groups, route diversity, and selective routers/tandems and associated diverse network elements, etc.

Emergency Services IP Network (ESInet):

Best Practices for this element include those that address prevention and restoration of the next generation network elements and facilities that are needed to process IP voice, data, and video based calls through the NG9-1-1 network. Examples of ESInet related items are routers, gateways, Border Control Functions (BCFs) and a dedicated, managed IP network infrastructure used to transmit the voice, text, and video. In many cases, Best Practices for ESINets include the use of multiple IP network infrastructures as a collective to increase redundancy and resiliency.

Public Safety Answering Points (PSAPs):

Best Practices for this element include those that apply to the reliable accessibility to the E9-1-1 network by the public and those that address the rapid restoration of the network in the aftermath of a crisis.

Other Entities:

Best Practices for this element include those that apply to third party providers of Next Generation IP or cloud-based services required to process E9-1-1 calls through any Next Generation network. Examples include Network Operators that provide ALI/ANI/PANI lookup services, call routing through non Service Provider networks, etc.

4 Analysis, Findings and Recommendations

4.1 Analysis[7]

Working Group 8-1 analysis encompassed the review of 1,022 current Best Practices whose implementation would enhance the security, reliability, operability and resiliency of infrastructure for communications industry segments.

Prior to beginning work, a preview of the entire Best Practice set was done by the full Working Group to quickly ascertain which Best Practices had a potential E9-1-1 implication with an eye toward Next Generation technology, which of those appeared to related to a disaster recovery or

[7] Elements of a Research Proposal and Report; Source: http://www.statpac.com/research-papers/research-proposal.htm

business continuity issue, and those that could be used with some modification by PSAPs and Public Safety, or to enhance public education on the use of E9-1-1.

Once these individual lists were created, Working Group 8-1 was provided the 548 Best Practices that had the potential to fall in scope of the team's work. The next step was to develop a definition that would provide the team a roadmap for further refining the Best Practice list down to those that would qualify as an E9-1-1 Best Practice used in preparing for natural or man-made disasters. The definition follows:

"*A Best Practice is a suggestion that through its implementation will have a direct impact on preparing for a natural or man-made disaster or through implementation will have a direct impact on the prioritization and restoration of the E9-1-1 infrastructure following an event. A second criterion of a Best Practice is that the suggestion is currently in use by one or more participants in the industry.*"

Next, the team looked for a way to present their findings in a manner that could be quickly applied by the industry or be blended into their existing business continuity plans. The answer to this came from work done previously on a Hurricane Checklist developed by industry experts in disaster recovery and business continuity[8] by the Alliance for Telecommunications Industry Solutions (ATIS) Network Reliability Steering Committee (NRSC). The concept of developing a checklist using the appropriate Best Practices and identifying the elements that they would apply to would give industry a quick guide to use in their internal preparations.

Finally, a gap analysis process needed to be included in the Final Report - Part 1. As the team reviewed each Best Practice they were asked to record any gaps they found that were not addressed from their expert point of view. These gaps and recommendations are included in the Recommendations section of this Final Report - Part 1.

Each of the 548 Best Practices provided to this Working Group 8-1 was compared to the definition discussed above. Through careful analysis, the original list was reduced from 548 to 262 that the team determined would qualify as an E91-1 Best Practice for use in preparing for a natural or man-made disaster.

4.2 Findings

The E9-1-1 Best Practice Disaster Preparedness Checklist provides a list of current Best Practices that apply to the "Legacy E9-1-1" and "Multimedia" models developed by Working Group 8-1. Each Best Practice applies to one or more elements with a check (X) in each of the columns that the team identified as applicable. The figure below illustrates the format the team adopted for the checklist.

[8] ATIS NRSC Hurricane Checklist http: http://www.atis.org/docstore/product.aspx?id=25649

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	Original Best Practice	Category	Status	Legacy Providers	Internet Based	Data Bases	Pre-Call and Call Time Software Functions	ESInet	PSAPs	Other Entities	Legacy Providers	Internet Based	Data Bases	Pre-Call and Call Time Software Functions	PSTN Based	PSAPs

Figure 3: E911 Best Practice Disaster Preparedness Checklist

The team found that many existing Best Practices were equally relevant to the E9-1-1 network due to the commonalities between the technologies. This was most prevalent in the Next Generation E9-1-1 platform, which being based on internet concepts found Best Practices that applied over several categories.

Best Practices identified for the checklist were found in nearly every category of Best Practices available. Included in the checklist is a column that identifies the category the Best Practice applies to and the Status of "All", "Critical", "Highly Important", or "Important" that applies to each Best Practice[9]. The categories are determined by the Best Practice Number assigned by the Federal Communications Commission (FCC) following approval by the Council. Best Practice numbering format is described below:

Description of Best Practice Numbering

For existing NRIC/CSRIC Best Practices[10]: Each Best Practice has a unique number that follows the numbering format: **X - Y - Z # # #**

X = the current, or most recent, NRIC/CSRIC Council (e.g., 8 in 2009-2010)
Y = the Council in which the Best Practice was last edited
Z = 0-4 for Network Reliability and Interoperability
= 1 for Disaster Recovery and Mutual Aid
= 3 for Public Safety
= 5 for Physical Security
= 8 for Cyber Security
= any digits, where every Best Practice has a unique Z # #

Due to the work being done by the larger Working Group 8 in modifying and modernizing E9-1-1 related Best Practices, it was decided that this team would not recommend modifications to the existing Best Practices unless there were only slight modifications needed to clarify the Best Practice for this specific project. Any significant modifications would be done by the Working Group and presented during the Final Report – Part 2 due in December 2012. It should be noted that the 262 Best Practices chosen for this checklist met the definition defined by the team without any modifications necessary.

[9] CSRIC II Working Group 6: Best Practice Implementation Final Report – January 2011.
[10] ATIS NRSC Best Practice Tutorial, November 2011 Presented to Working Group 8 on December 14, 2011.

4.3 Recommendations

Communications organizations should evaluate and implement those Best Practices which they deem appropriate. These organizations should institutionalize the review of Best Practices as part of their planning processes and assess on a periodic basis how implementing selected Best Practices might improve the proficiency and reliability of their operations[11].

During the creation of the E9-1-1 Best Practice Disaster Preparedness Checklist there were a total of 24 gaps documented. Where noted, the team has recommended a new Best Practice be created and approved by Council for use in furthering the teams work. In recommending a new Best Practice, this Working Group complied with the Best Practice Guidelines recommended by the ATIS NRSC tutorial:

Best Practices Guidelines

1. Proven through actual implementation – more than "just a good idea"
2. Address classes of problems (rather than one time issues)
3. A single concept should be captured in each practice (one thought, one practice)
4. Should not endorse specific commercial documents, products or services
5. Developed through rigorous deliberation and expert consensus
6. Confirmed by a broad set of stakeholders
7. Should not be assumed to be applicable in all situations or to all industry types
8. Does not imply mandatory implementation

Gap Analysis:

Listed here are 24 gaps that were identified during the analysis phase. Where possible, following the gap identified WG8-1 has proposed a Best Practice to eliminate the gap.

1. Service providers, network operators, first responders, and other public safety personnel should monitor weather services such as NOAA and/or subscribe to automated storm alerts or RSS feeds on known storm related events such as Hurricanes to stay informed and prepared. This could be the trigger for early communications and coordination efforts.

   Recommended New Best Practice:

   Weather Awareness: Service Providers, Network Operators, Property Managers, and Government should subscribe to weather monitoring services (e.g. NOAA, RSS storm feeds) on known storm related events and used as a decision point for implementing early communications and coordination efforts between entities.

2. A one source official emergency internal and external contact online database that can be accessed by appropriate personnel that is maintained regularly and updated frequently could be addressed and/or adopted by Service Providers, Network Operators to provide a

[11] ATIS Best Practice website, Tutorial Page, http://www.atis.org/bestpractices/Tutorial.aspx

reliable and common database to use for disaster events.

Recommended New Best Practice:

Emergency Contact Database: Service Providers and Network Operators should consider establishing a single database (one source) that is maintained regularly and updated frequently with internal and external contact information that can be accessed by appropriate personnel.

3. No Best Practice could be found addressing a method to mass alert external contacts and critical customers that the Service Provider or Network Operator has entered a disaster recovery posture in preparation for a known event such as hurricane, flooding, fires, etc.

   Recommended New Best Practice:

   Disaster Event Mass Alerting: Service Providers and/or public safety systems should utilize various communications services (i.e. outbound calling services) as necessary to alert specific groups, or the public as a whole based on pre-arranged criteria, or those within a particular geographic area deemed to be susceptible to an event or disaster.

4. As part of business continuity planning, alternate logistics delivery locations should be preplanned and communicated to appropriate personnel.

   Recommended New Best Practice:

   Alternate Logistics Delivery: Service Providers and Network Operators, as part of their business continuity planning should identify alternate logistics delivery locations, document them during pre-planning activities, and communicate to appropriate personnel.

5. Effective communications prior to and following an event should set expectations early, address problem solving, prioritization of services, and timeframes for restoration.

   Recommended New Best Practice:

   Effective Event Communications: Service Providers, Network Operators, Property Managers, and Government should include in their business continuity plans clear guidance for setting and communicating expectations, problem solving, and prioritization of services (e.g. E9-1-1) including timeframes for restoration following a natural or man-made disaster.

6. Spare batteries or quick chargers (e.g. power sticks) should be considered for remote devices such as smart phones, blackberries, tablets, etc. Expect battery life to be diminished if low or no cell signal is available.

   Recommended New Best Practice:

   Remote Device Spare Batteries: Service Providers, Network Operators, Property Managers, and Government when planning for a disaster should address spare batteries

or quick chargers (e.g. power sticks) as well as other critical components being available due to the potential of not being able to re-charge the devices in the normal method.

7. Consider cell phones from alternate providers to maximize the potential for accessing the wireless network.

   Recommended New Best Practice:

   Alternate Cell Providers: Service Providers, Network Operators, and Government should consider acquiring cell phones and services from alternate providers to maximize the potential for accessing the wireless network in the aftermath of a significant event.

8. Consider participation in the Alerting and Coordination Network (ACN) and Shared Resources High Frequency Radio Program (SHARES) through the National Coordinating Center (NCC) for Telecommunications.

   Recommended New Best Practice:

   Emergency Communication Plans: Service Providers and Network Operators should consider participating in emergency communications programs offered through the National Coordinating Center (NCC) such as Alerting and Coordination Network (ACN) and Shared Resources High Frequency Radio Program (SHARES).

9. Service Providers and Network operators should quickly establish communications with Public Safety Answering Points (PSAP) and other public safety contacts and pass status on network issues to help mitigate issues related to call processing of E9-1-1 calls.

   Recommended New Best Practice:

   Public Safety Communications: Service Providers and Network Operators should as part of their business continuity planning quickly establish communications with Public Safety Answering Points (PSAP) and other public safety contacts and pass status on network issues following a disaster to help mitigate issues related to call processing of E9-1-1 calls.

10. Service Providers, Network Operators, and Public Safety should develop a switch replacement philosophy in the event of unrecoverable damage to critical infrastructure used to process E9-1-1 calls.

    Recommended New Best Practice:

    Switch Replacement Philosophy: Service Providers and Equipment Suppliers as part of their business continuity planning should develop a switch replacement philosophy in the event of unrecoverable damage to critical infrastructure used to process E9-1-1 calls.

11. Service Providers, Network Operators, and Public Safety should develop a re-entry strategy for the impacted area.

    Recommended New Best Practice:

Re-entry Strategy: Service Providers, Network Operators, and Government should as part of their business continuity planning develop a re-entry strategy for the impacted area following a disaster to reduce restoration timeframes for critical services (e.g. E9-1-1).

12. Consider establishing a joint E9-1-1 strike team dedicated to the assessment and restoration of the E9-1-1 network following an event. The team would consist of members of communication providers, public safety, and first responders.

    Recommendation:

    The team could not determine if any Service Provider or Network Operator has implemented such a system or process. Based on this, we cannot recommend creation of a Best Practice; however, the team does recommend that future consideration be given to this identified gap which would provide dedicated resources to the rapid restoration and prioritization of E9-1-1 services in the aftermath of a natural or man-made disaster.

13. Service Providers and Network Operators should ensure their communications process efficiently advises employees on how to obtain ongoing instructions during the aftermath of an event.

    Recommended New Best Practice:

    Efficient Event Instructions: Service Providers and Network Operators should as part of their business continuity planning processes ensure their communications processes efficiently advises employees on how to obtain ongoing instructions during the aftermath of an disaster.

14. Service Providers, Network Operators, and Public Safety should coordinate with officials (e.g. Police, Military) to provide protection and safety of workers restoring the E9-1-1 infrastructure.

    Recommended New Best Practice:

    Disaster Worker Safety: Service Providers, Network Operators, and Government should coordinate with officials (e.g. Police, Military) to provide protection and safety of workers restoring the E9-1-1 infrastructure in the aftermath of a natural or man-made disaster event.

15. Service Providers, Network Operators and Equipment Vendors should coordinate agreements for the immediate shipping of product following an event.

    Recommended New Best Practice:

    Product Shipping Agreements: Service Providers, Network Operators and Equipment Vendors as part of their business continuity planning should coordinate agreements for the immediate shipping of product following a natural or man-made disaster event.

16. Service Providers and Network Operators should regularly assess the availability of work supplies (e.g. pumps, blowers, chain saws, inside and outside wiring, outside network interfaces, etc.) in preparation of disaster events.

    Recommended New Best Practice:

    Work Supply Availability: Service Providers and Network Operators as part of their business continuity planning processes should regularly assess the availability of work supplies (e.g. pumps, blowers, chain saws, inside and outside wiring, outside network interfaces, etc.) in preparation of disaster events.

17. Service Providers, Network Operators, and Public Safety should validate computer backups are up to date prior to a known event and located in an offsite or cloud storage arrangement. Lack of proven good back up data can delay or make restoration impossible.

    Recommended New Best Practice:

    Up to Date Backups: Service Providers, Network Operators, and Government should validate computer backups are up to date prior to a known event (e.g. hurricane, flooding, and wild fires) and located in an offsite or cloud storage arrangement to prevent delaying or making restoration of computer data impossible.

18. Service Providers and Network Operators should assess transport equipment and their protection facilities to ensure operability to prepare for a known event (e.g. hurricane, flooding, and fire).

    Recommended New Best Practice:

    Protection Facilities Assessment: Service Providers and Network Operators should assess transport equipment and their protection facilities to ensure operability in preparation for a known event (e.g. hurricane, flooding, and wild fires).

19. Service Providers and Network Operators should establish proactive patrolling of critical Inter-Office Facility (IOF) routes to identify damages earlier for faster restoration.

    Recommendation:

    The team could not determine if any Service Provider or Network Operator has implemented such a process. Based on this, we cannot recommend creation of a Best Practice; however, the team does recommend that future consideration be given to this identified gap which would provide dedicated resources to the rapid restoration and prioritization of E9-1-1 services in the aftermath of a natural or man-made disaster.

20. Service Providers and Network Operators should consider establish roaming restoration teams to quickly reduce troubles.

    Recommendation:

The team could not determine if any Service Provider or Network Operator has implemented such a process. Based on this, we cannot recommend creation of a Best Practice and this gap should be addressed by a future CSRIC.

21. Service Providers, Network Operators, and Public Safety should establish preplanning for the redirection or rerouting of critical circuits and communications in affected areas that may impact E9-1-1 call delivery.

    Recommended New Best Practice:

    Redirection and Rerouting of Critical Circuits: Service Providers, Network Operators, and Government should establish preplanning for the redirection or rerouting of critical circuits and communications in affected areas that may impact E9-1-1 call delivery during a natural or man-made disaster event.

22. Service Providers, Network Operators, and Public Safety should document and provide power down and power up procedures for critical equipment. Power down processes can extend service and power up process is critical to reduce start up times.

    Recommended Best Practice:

    Power Up and Down Procedures: Service Providers, Network Operators should document and provide power down and power up procedures for critical equipment to extend service and reduce start up times if critical equipment is powered down.

23. Text to E9-1-1 implementation.

    Recommendation:

    The implementation of "Text to E9-1-1" by some wireless Service Providers is in progress at the time of this Final Report - Part 1. Based on this, we cannot recommend creation of a Best Practice and this gap should be addressed by a future CSRIC.

24. Best Practices do not have a "Public Safety" option.

    Recommendation:

    During review and creation of recommended Best Practices that relate to the E9-1-1 network the team found that no category existed for the use of "Public Safety" in the verbiage of the Best Practices. Traditionally, the available options have been "Service Provider, Network Operator, Equipment Supplier, Property Manager, and Government". The importance of Best Practices as related to E9-1-1 apparently omits one of the key contributors to the success of any implementation process. This omission resulted in our recommendations using "Government" as an implication of "Public Safety". Working Group 8 recommends that an implementer category be recognized for future Best Practice development of "Public Safety" to appropriately recognize the importance of this key contributor to E9-1-1 reliability and resiliency.

5 Conclusions

Working Group 8 – E9-1-1 Best Practices concludes that providing a set of voluntary industry Best Practices that, if implemented, will strengthen the up-front planning processes for Service Providers, Network Operators, Property Managers, and Government entities. These Best Practices when used in preparing for disaster events that may interrupt E9-1-1 services during and in the aftermath of a natural or man-made disaster can minimize and/or mitigate their effect on the E9-1-1 network infrastructure.

6 Appendix 1 – CSRIC III Council Considerations

The following items are recommended for a CSRIC III Council vote:

Non-Best Practice Recommendations	CSRIC WG 8 Recommendation
Working Group 8 recommends that an implementer category be recognized for future Best Practice development of "Public Safety" to appropriately recognize the importance of this key contributor to E9-1-1 reliability and resiliency.	Approve
Adoption of Working Group 8 - E911 Best Practice Disaster Preparedness Checklist	Approve

Best Practice Recommendations	CSRIC WG 8 Recommendation
Weather Awareness: Service Providers, Network Operators, Property Managers, and Government should subscribe to weather monitoring services (e.g. NOAA, RSS storm feeds) on known storm related events and used as a decision point for implementing early communications and coordination efforts between entities.	Approve
Emergency Contact Database: Service Providers and Network Operators should consider establishing a single database (one source) that is maintained regularly and updated frequently with internal and external contact information that can be accessed by appropriate personnel.	Approve
Disaster Event Mass Alerting: Service Providers and/or public safety systems should utilize various communications services (i.e. outbound calling services) as necessary to alert specific groups, or the public as a whole based on pre-arranged criteria, or those within a particular geographic area deemed to be susceptible to an event or disaster.	Approve
Alternate Logistics Delivery: Service Providers and Network Operators, as part of their business continuity planning should identify alternate logistics delivery locations, document them during pre-planning activities, and communicate to appropriate personnel.	Approve

Effective Event Communications: Service Providers, Network Operators, Property Managers, and Government should include in their business continuity plans clear guidance for setting and communicating expectations, problem solving, and prioritization of services (e.g. E9-1-1) including timeframes for restoration following a natural or man-made disaster.	Approve
Remote Device Spare Batteries: Service Providers, Network Operators, Property Managers, and Government when planning for a disaster should address spare batteries or quick chargers (e.g. power sticks) as well as other critical components being available due to the potential of not being able to re-charge the devices in the normal method.	Approve
Alternate Cell Providers: Service Providers, Network Operators, and Government should consider acquiring cell phones and services from alternate providers to maximize the potential for accessing the wireless network in the aftermath of a significant event.	Approve
Emergency Communication Plans: Service Providers and Network Operators should consider participating in emergency communications programs offered through the National Coordinating Center (NCC) such as Alerting and Coordination Network (ACN) and Shared Resources High Frequency Radio Program (SHARES).	Approve
Public Safety Communications: Service Providers and Network Operators should as part of their business continuity planning quickly establish communications with Public Safety Answering Points (PSAP) and other public safety contacts and pass status on network issues following a disaster to help mitigate issues related to call processing of E9-1-1 calls.	Approve
Switch Replacement Philosophy: Service Providers and Equipment Suppliers as part of their business continuity planning should develop a switch replacement philosophy in the event of unrecoverable damage to critical infrastructure used to process E9-1-1 calls.	Approve
Re-entry Strategy: Service Providers, Network Operators, and Government should as part of their business continuity planning develop a re-entry strategy for the impacted area following a disaster to reduce restoration timeframes for critical services (e.g. E9-1-1).	Approve
Efficient Event Instructions: Service Providers and Network Operators should as part of their business continuity planning processes ensure their communications processes efficiently advises employees on how to obtain ongoing instructions during the aftermath of an disaster.	Approve
Disaster Worker Safety: Service Providers, Network Operators, and Government should coordinate with officials (e.g. Police, Military) to provide protection and safety of workers restoring the E9-1-1 infrastructure in the aftermath of a natural or man-made disaster event.	Approve
Product Shipping Agreements: Service Providers, Network Operators and Equipment Vendors as part of their business continuity planning should coordinate agreements for the immediate shipping of product following a natural or man-made disaster event.	Approve

Work Supply Availability: Service Providers and Network Operators as part of their business continuity planning processes should regularly assess the availability of work supplies (e.g. pumps, blowers, chain saws, inside and outside wiring, outside network interfaces, etc.) in preparation of disaster events.	Approve
Up to Date Backups: Service Providers, Network Operators, and Government should validate computer backups are up to date prior to a known event (e.g. hurricane, flooding, and wild fires) and located in an offsite or cloud storage arrangement to prevent delaying or making restoration of computer data impossible.	Approve
Protection Facilities Assessment: Service Providers and Network Operators should assess transport equipment and their protection facilities to ensure operability in preparation for a known event (e.g. hurricane, flooding, and wild fires).	Approve
Redirection and Rerouting of Critical Circuits: Service Providers, Network Operators, and Government should establish preplanning for the redirection or rerouting of critical circuits and communications in affected areas that may impact E9-1-1 call delivery during a natural or man-made disaster event.	Approve
Power Up and Down Procedures: Service Providers, Network Operators should document and provide power down and power up procedures for critical equipment to extend service and reduce start up times if critical equipment is powered down.	Approve

7 Appendix 2 – E911 Best Practice Disaster Preparedness Checklist

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-8-8133	Consistent Security Controls for DR Configurations: A Service Provider's or Network Operator's disaster recovery or business continuity solutions should adhere to the same Information Security best practices as the solutions used under normal operating conditions.	Cyber Security	All	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
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.	Cyber Security	All	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
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.	Cyber Security	Critical	X	X	X	X	X	X	X	X	X	X	X	X	X
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.	Cyber Security	Critical	X	X	X	X	X	X	X	X	X				
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.	Cyber Security	Critical	X	X				X	X	X	X				

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
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.	Cyber Security	Critical	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**			**X**	**X**
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.	Cyber Security	Critical	**X**	**X**				**X**	**X**	**X**	**X**				**X**	**X**

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
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.	Cyber Security	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**				
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.	Cyber Security	Critical	**X**	**X**			**X**			**X**	**X**				
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 0 positives.	Cyber Security	Critical	**X**	**X**			**X**			**X**	**X**				

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
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.	Cyber Security	Critical	**X**	**X**			**X**	**X**	**X**	**X**	**X**				
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.	Cyber Security	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**				

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
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.	Cyber Security	Critical	**X**	**X**						**X**	**X**				
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.	Cyber Security	Critical	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**				

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
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.	Cyber Security	Critical	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**				
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.	Cyber Security	Critical	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**				
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,	Cyber Security	Critical	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**				

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
	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.															
8-8-8523	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.	Cyber Security	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**				
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.	Cyber Security	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**				

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
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.	Cyber Security	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**				
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.	Cyber Security	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**				

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
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.	Cyber Security	Critical	X	X	X	X	X	X	X	X	X				
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.	Cyber Security	Critical	X	X			X		X	X	X			X	
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.	Cyber Security	Critical	X	X			X		X	X	X			X	

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
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.	Cyber Security	Critical	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
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.	Cyber Security	Critical	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
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.	Cyber Security	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**				
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	Cyber Security	Critical	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
	· Develop corporate message(s) for all significant events – disseminate as appropriate If not already established, create contact and escalation procedures for all significant events."															
8-8-8559	Recovery from Lack of IDS/IPS Maintenance: In the event of a security threat, Service Providers and Network Operators should upload current IDS/IPS signatures from vendors and re-verify stored data with the updated signatures. Evaluate platform's ability to deliver service in the face of evolving threats and consider upgrade/replacement as appropriate. Review Incident Response Post-Mortem Checklist (NRIC BP 8564).	Cyber Security	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**				

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
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.	Cyber Security	Critical	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
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.	Cyber Security	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**		**X**				**X**

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
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.	Cyber Security	Critical	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
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	Cyber Security	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**				

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
	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.															
8-6-1017	Network Operators and Service Providers should have documented plans or processes to assess damage to network elements, outside plant, facility infrastructure, etc. for implementation immediately following a disaster.	Disaster Recovery and Mutual Aid	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-6-1022	Network Operators, Service Providers and Equipment Suppliers should consider the development of a vital records program to protect vital records that may be critical to restoration efforts.	Disaster Recovery and Mutual Aid	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-1001	Network Operators, Service Providers, Equipment Suppliers and Property Managers should formally document their business continuity processes in a business continuity plan covering critical business functions and business partnerships. Key areas for consideration include: Plan Scope, Responsibility, Risk Assessment, Business Impact Analysis, Plan Testing, Training and Plan Maintenance.	Disaster Recovery and Mutual Aid	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-7-1005	Network Operators, Service Providers and Equipment Suppliers should perform a Business Impact Analysis (BIA) to assess the impact of the loss of critical operations, support systems and applications.	Disaster Recovery and Mutual Aid	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-7-1010	Network Operators, Service Providers and Equipment Suppliers should designate personnel responsible for maintaining Business Continuity and Disaster Recovery Plans.	Disaster Recovery and Mutual Aid	Critical	**X**	**X**				**X**	**X**	**X**	**X**				**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-1011	Network Operators, Service Providers, Equipment Suppliers and Public Safety Authorities should establish alternative methods of communication for critical personnel.	Disaster Recovery and Mutual Aid	Critical	**X**	**X**				**X**	**X**	**X**	**X**				**X**
8-7-1023	Network Operators, Service Providers and Equipment Suppliers should identify essential staff within their organizations that are critical to disaster recovery efforts. Planning should address the availability of these individuals and provide for backup staff.	Disaster Recovery and Mutual Aid	Critical	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**	**X**		**X**	**X**
8-7-1028	Network Operators, Service Providers and Property Managers should engage in preventative maintenance programs for network site support systems including emergency power generators, UPS, DC plant (including batteries), HVAC units, and fire suppression systems.	Disaster Recovery and Mutual Aid	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-1033	Network Operators should develop a strategy for deployment of emergency mobile assets such as Cell on Wheels (COWs), cellular repeaters, Switch on Wheels (SOWs), transportable satellite terminals, microwave equipment, power generators, HVAC units, etc. for emergency use or service augmentation for planned events (e.g., National Special Security Event (NSSE)).	Disaster Recovery and Mutual Aid	Critical	**X**	**X**						**X**	**X**				
8-7-1034	Network Operators should ensure that the emergency mobile assets are maintained at a hardware and software level compatible with the existing network infrastructure so that the emergency mobile assets will be immediately available for deployment.	Disaster Recovery and Mutual Aid	Critical	**X**	**X**				**X**		**X**	**X**				**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-1063	Network Operators and Service Providers should set Initial Address Messages (IAMs) to congestion priority in accordance with applicable ANSI standards. This will ensure government emergency calls (e.g., 911, GETS) receive proper priority during national emergency situations. Implementation in all networks should be in accordance with ANSI T1.111.	Disaster Recovery and Mutual Aid	Critical	**X**	**X**						**X**	**X**				
8-7-0401	Network Surveillance: Network Operators and Service Providers should monitor their network to enable quick response to network issues.	Network Reliability and Interoperability	Critical	**X**	**X**	**X**		**X**			**X**	**X**	**X**		**X**	

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
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).	Network Reliability and Interoperability	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-7-0417	Capacity Management: Network Operators should design and implement procedures to evaluate failure and emergency conditions affecting network capacity.	Network Reliability and Interoperability	Critical	**X**	**X**						**X**	**X**				
8-7-0456	Network Operators should maintain records of pertinent information related to a cell site for its prioritization in disaster recovery and key coverage areas (e.g., emergency services, government agencies, proximity to hospitals).	Network Reliability and Interoperability	Critical	**X**							**X**					

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0476	Network Operators and Property Managers should consider conducting physical site audits after a major event (e.g., weather, earthquake, auto wreck) to ensure the physical integrity and orientation of hardware has not been compromised.	Network Reliability and Interoperability	Critical	X	X	X	X	X	X	X	X	X	X	X	X	X
8-7-0491	Network Operators, Service Providers and Equipment Suppliers should, where programs exist, coordinate with local, state and/or federal emergency management and law enforcement agencies for pre-credentialing to help facilitate access by technicians to restricted areas during an event.	Network Reliability and Interoperability	Critical	X	X			X	X	X	X	X			X	
8-7-0492	Network Operators should provide back-up power (e.g., some combination of batteries, generator, fuel cells) at cell sites and remote equipment locations, consistent with the site specific constraints, criticality of the site, the expected load and reliability of primary power.	Network Reliability and Interoperability	Critical	X	X						X	X			X	

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0493	Network Operators and Property Managers should consider placing fixed power generators at cell sites, where feasible.	Network Reliability and Interoperability	Critical	**X**							**X**					
8-7-0495	Network Operators and Property Managers should consider pre-arranging contact information and access to restoral information with local power companies.	Network Reliability and Interoperability	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-7-0499	Network Operators and Service Providers should consider ensuring that the back-haul facility equipment located at the cell site is provided with backup power duration is equal to that provided for the other equipment at the cell site.	Network Reliability and Interoperability	Critical	**X**							**X**					

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0510	Network Operators, Service Providers and Equipment Suppliers should, by design and practice, manage critical Network Elements (e.g., Domain Name Servers, Signaling Servers) that are essential for network connectivity and subscriber service as critical systems (e.g., secure, redundant, alternative routing).	Network Reliability and Interoperability	Critical	**X**	**X**			**X**	**X**		**X**	**X**				
8-7-0543	Service Providers should establish agreements with Property Managers for both regular and emergency power.	Network Reliability and Interoperability	Critical	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
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).	Network Reliability and Interoperability	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0566	Network Operators and Service Providers should consider placing and maintaining 911 circuits over diverse interoffice transport facilities (e.g., geographically diverse facility routes, automatically invoked standby routing, diverse digital cross-connect system services, self-healing fiber ring topologies, or any combination thereof).	Network Reliability and Interoperability	Critical	X	X	X	X	X	X	X	X	X	X	X	X	X
8-7-0568	Network Operators and PSAPs should establish a routing plan so that in the case of a lost connection from the selective router to the PSAP, 911 calls are routed to an alternate answering point (e.g., alternate PSAP, appropriate telephone line).	Network Reliability and Interoperability	Critical	X	X			X	X	X	X	X			X	X
8-7-0571	Network Operators should consider deploying dual active 911 selective router architectures to enable circuits from the caller's serving end office to be split between two selective routers in order to eliminate single points of failure (SPOF). Diversity should also be considered on interoffice transport facilities connecting each 911 selective router to the PSAP serving end office.	Network Reliability and Interoperability	Critical	X	X			X	X	X	X	X			X	X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0577	Network Operators, Service Providers and Public Safety Agencies responsible for PSAP operations should jointly and periodically test and verify that critical components (e.g., automatic re-routes, PSAP Make Busy keys) included in contingency plans work as designed.	Network Reliability and Interoperability	Critical	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-7-0579	Network Operators, Service Providers, and 911 administrators, and public safety agencies should routinely team to develop, implement, periodically test, evaluate and update as needed plans for 911 disruption contingencies (e.g., share information about network and system security and reliability where appropriate).	Network Reliability and Interoperability	Critical	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-7-0651	Network Operators, Service Providers and Property Managers should consider providing diversity within power supply and distribution systems so that single point failures (SPOF) are not catastrophic. For large battery plants in critical offices, consider providing dual AC feeds (odd/even power service cabinets for rectifiers). Transfer switches should be listed to a UL standard for Transfer Switch Equipment. When transfer breaker systems are used, they must be mechanically and electrically interlocked.	Network Reliability and Interoperability	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0655	Network Operators, Service Providers and Property Managers should coordinate hurricane and other disaster restoration work with electrical and other utilities as appropriate.	Network Reliability and Interoperability	Critical	X	X			X	X	X	X	X			X	X
8-7-0658	Network Operators, Service Providers and Property Managers should maintain adequate fuel on-site and have a well-defined re-supply plan. Generator life support systems (e.g., radiator fan, oil cooler fan, water transfer pumps, fuel pumps, engine start battery chargers) should be on the essential AC bus of the generator they serve.	Network Reliability and Interoperability	Critical	X	X			X	X	X	X	X			X	X
8-7-0672	Network Operators and Service Providers should provide a minimum of 3 hours battery reserve for central offices equipped with fully automatic standby systems.	Network Reliability and Interoperability	Critical	X	X	X	X	X	X	X	X	X	X	X	X	X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0758	Network Operators and Service Providers should, upon restoration of service in the case of an outage where 911 call completion is affected, make multiple test calls to the affected PSAP(s) to ensure proper completion.	Network Reliability and Interoperability	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-7-0780	Network Operators and Service Providers should consider including coordination information of Public Safety Authorities when developing disaster restoration and prioritization plans.	Network Reliability and Interoperability	Critical	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-8-0574	Network operators and service providers (of any technology type) should remotely monitor and manage the 9-1-1 network components using network management controls, where available, to quickly restore 9-1-1 service and provide priority repair during network failure events. When multiple interconnecting providers and vendors are involved, they will need to cooperate to provide end-to-end analysis of complex call-handling problems. In NG9-1-1, the mechanism used to handle call congestion and outages is diversion of calls to alternate PSAPs that have	Network Reliability and Interoperability	Critical	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
	the capability to effectively answer and provide assistance. PSAPs should create relationships with other PSAPs that have the capabilities to serve as a backup so that their calls can be answered even under extreme overload or network failure scenarios. ESInets must be designed with redundant interconnect to OSPs and PSAPs to maintain connectivity in the face of extensive disaster damage. The characteristics of IP routing are of great assistance in ensuring 9-1-1 calls will reach a PSAP if there is any path possible.															
8-8-0575	Network operators and service providers (of any technology type) should deploy location identification systems used by Public Safety in a redundant, geographically diverse manner (i.e., two identical ALI/Mobile Positioning Center (MPC) Gateway Mobile Location Center (GMLC)/VPC/LIS database systems with mirrored data located in geographically diverse locations). These include, but are not limited to, ALI, MPC/GMLC, VPC systems, and LIS.	Network Reliability and Interoperability	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
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).	Network Reliability and Interoperability	Critical	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-6-5055	Network Operators, Service Providers and Equipment Suppliers should establish and maintain (or contract for) a 24/7 emergency call center for internal communications. Ensure staff at this center has access to all documentation pertinent to emergency response and up to date call lists to notify appropriate personnel. The number to this call center should be appropriately published so personnel know where to report information.	Physical Security	Critical	X	X			X	X	X	X	X			X	X
8-6-5143	Network Operators and Service Providers (e.g., Satellite Operators) should maintain access to a back-up or secondary 'uplink site' to provide tracking, telemetry and control (T.T.&C.) support for all operational communications spacecraft. The back-up or secondary site must be geographically diverse from the primary uplink facility, active and tested on some regular schedule to insure readiness and timely response.	Physical Security	Critical	X							X					
8-7-5107	Network Operators, Service Providers and Equipment Suppliers should evaluate and manage risks (e.g., alternate routing, rapid response to emergencies) associated with a concentration of infrastructure components.	Physical Security	Critical	X	X	X	X	X	X	X	X	X	X	X	X	X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-5112	Network Operators, Service Providers and Equipment Suppliers should, at the time of the event, coordinate with the appropriate local, state, or federal agencies to facilitate timely access by their personnel to establish, restore or maintain communications, through any governmental security perimeters (e.g., civil disorder, crime scene, disaster area).	Physical Security	Critical	X	X			X	X	X	X	X			X	X
8-7-5126	Network Operators, Service Providers and Equipment Suppliers should plan for contingency staffing to perform critical functions in response to crisis situations (e.g., natural disasters, labor strike, terrorist attack).	Physical Security	Critical	X	X			X	X	X	X	X			X	X
8-7-5127	Network Operators, Service Providers, Equipment Suppliers and Public Safety Authorities should provide a Government Emergency Telecommunications Service (GETS) card to essential staff critical to disaster recovery efforts and should consider utilizing Wireless Priority Service (WPS) for essential staff. Appropriate training and testing in the use of GETS & WPS should occur on a regular basis (i.e. in conjunction with testing of the corporate disaster recovery plan).	Physical Security	Critical	X	X			X	X	X	X	X			X	X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-5128	Network Operators, Service Providers, Equipment Suppliers and Public Safety Authorities should maintain accurate records for Government Emergency Telecommunications Service (GETS) cards and Wireless Priority Service (WPS) phone assignments as staff changes occur.	Physical Security	Critical	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-7-5203	Network Operators, Service Providers, and Property Managers should develop, maintain and administer a comprehensive program to sustain a reliable power infrastructure.	Physical Security	Critical	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**	**X**		**X**	**X**
8-7-5204	Service Providers, Network Operators and Property Managers should ensure availability of emergency/backup power (e.g., batteries, generators, fuel cells) to maintain critical communications services during times of commercial power failures, including natural and manmade occurrences (e.g., earthquakes, floods, fires, power brown/black outs, terrorism). The emergency/backup power generators should be located onsite, when appropriate.	Physical Security	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-5206	Network Operators, Service Providers and Property Managers should maintain sufficient fuel supplies for emergency/backup power generators running at full load to allow for contracted refueling.	Physical Security	Critical	**X**	**X**				**X**	**X**	**X**	**X**				**X**
8-7-5207	Network Operators, Service Providers and Property Managers should take appropriate precautions to ensure that fuel supplies and alternate sources of power are available for critical installations in the event of major disruptions in a geographic area (e.g., hurricane, earthquake, pipeline disruption). Consider contingency contracts in advance with clear terms and conditions (e.g., Delivery time commitments, T&Cs).	Physical Security	Critical	**X**	**X**				**X**	**X**	**X**	**X**				**X**
8-7-5232	Network Operators, Service Providers, and Property Managers should test fuel reserves used for standby or backup power for contamination at least once a year or after any event (e.g., earth tremor, flood) that could compromise the integrity of the tank housing, fill pipe or supply pipe.	Physical Security	Critical	**X**	**X**				**X**	**X**	**X**	**X**				**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-5275	Network Operators, Service Providers and Equipment Suppliers should consider backup power capabilities for Command and Control (Crisis Teams) so that communications and access to critical systems can be maintained in the event of a significant disruption to commercial power.	Physical Security	Critical	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-7-8062	IR (Incident Response) Team: Network Operators and Service Providers should identify and train a Computer Security Incident Response (CSIRT) Team. This team should have access to the CSO (or functional equivalent) and should be empowered by senior management. The team should include security, networking, and system administration specialists but have the ability to augment itself with expertise from any division of the organization. Organizations that establish part-time CSIRTs should ensure representatives are detailed to the team for a suitable period of time bearing in mind both the costs and benefits of rotating staff through a specialized team.	Cyber Security	Highly Important	**X**	**X**				**X**	**X**	**X**	**X**				
8-8-8063	Intrusion Detection/Prevention Tools (IDS/IPS): Service Providers and Network Operators should install and actively monitor IDS/IPS tools. Sensor placement should focus on resources critical to the delivery of service.	Cyber Security	Highly Important	**X**	**X**			**X**			**X**	**X**				

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-8-8090	Restrict Use of Dynamic Port Allocation Protocols: Service Providers, Network Operators, and Equipment Suppliers should restrict dynamic port allocation protocols such as Remote Procedure Calls (RPC) and some classes of Voice-over-IP protocols (among others) from usage, especially on mission critical assets, to prevent host vulnerabilities to code execution. Dynamic port allocation protocols should not be exposed to the internet. If used, such protocols should be protected via a dynamic port knowledgeable filtering firewall or other similar network protection methodology.	Cyber Security	Highly Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**		
8-8-8096	Users Should Employ Protective Measures: Service Providers and Network Operators should educate service customers on the importance of, and the methods for, installing and using a suite of protective measures (e.g., strong passwords, anti-virus software, firewalls, IDS, encryption) and update as available.	Cyber Security	Highly Important	**X**	**X**				**X**	**X**	**X**	**X**			**X**	**X**
8-8-8130	Staff Trained on Incident Reporting: Service Providers, Network Operators, and Equipment Suppliers should provide procedures and training to staff on the reporting of security incidents, weaknesses, and suspicious events.	Cyber Security	Highly Important	**X**	**X**				**X**	**X**	**X**	**X**			**X**	**X**

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-8-8505	Roll-out of Secure Service Configuration, or Vulnerability Recovery Configurations: When new default settings introduce vulnerabilities or the default configuration is found to be vulnerable, Service Providers and Network Operators should work with the Equipment Supplier to resolve the inadequacies of the solution, using a pre-deployment, staging area, where hardened configurations can be tested.	Cyber Security	Highly Important	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**				
8-8-8506	Document Single Points of Failure During Recovery: Following a compromise and reestablishment of lost service, Service Providers and Network Operators should re-evaluate the architecture for single points of failure. Review the process of evaluating and documenting single points of failure and provide spares for redundancy in the architecture to ensure adequacy of the security architecture.	Cyber Security	Highly Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**				
8-6-1006	Network Operators, Service Providers and Equipment Suppliers should consider establishing a designated Emergency Operations Center. This center should contain tools for coordination of service restoral including UPS, alternate means of communications, maps, and documented procedures to manage business interruptions and/or disasters.	Disaster Recovery and Mutual Aid	Highly Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-6-1007	Network Operators, Service Providers and Equipment Suppliers should consider establishing a geographically diverse back-up Emergency Operations Center.	Disaster Recovery and Mutual Aid	Highly Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-6-1038	Network Operators, Service Providers and Equipment Suppliers should consider during times of disaster, communicating the disaster response status frequently and consistently to all appropriate employees - so that they all understand what processes have been put in place to support customers and what priorities have been established in the response.	Disaster Recovery and Mutual Aid	Highly Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-6-1041	Equipment Suppliers should consider providing a "Disaster Information Checklist" to all of the Service Providers they support. The checklist should provide a set of questions which the Service Provider would address immediately after a disaster and then promptly inform the Equipment Supplier to facilitate equipment delivery.	Disaster Recovery and Mutual Aid	Highly Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-1004	Network Operators, Service Providers, Equipment Suppliers and Property Managers should review their Business Continuity Plan(s) on an annual basis to ensure that plans are up-to-date, relevant to current objectives of the business and can be executed as written.	Disaster Recovery and Mutual Aid	Highly Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-7-1009	Network Operators, Service Providers and Equipment Suppliers should regularly conduct exercises that test their Disaster Recovery Plans. Exercise scenarios should include natural and man-made disasters (e.g., hurricane, flood, nuclear, biological, and chemical).	Disaster Recovery and Mutual Aid	Highly Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-7-1018	Network Operators, Service Providers and Equipment Suppliers should emphasize employee and public safety during a disaster and all phases of disaster recovery.	Disaster Recovery and Mutual Aid	Highly Important	X	X	X		X	X	X	X	X	X		X	X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-1020	Network Operators, Service Providers and Equipment Suppliers should assess the need for Chemical, Biological, Radiological and Nuclear (CBRN) response program to safely restore or maintain service in the aftermath of fuel/chemical contamination or a Weapons of Mass Destruction (WMD) attack.	Disaster Recovery and Mutual Aid	Highly Important	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**	**X**		**X**	**X**
8-7-1025	Network Operators and Service Providers should consider using a team to quickly determine appropriate actions both pro-active or re-active to address potential or real threats.	Disaster Recovery and Mutual Aid	Highly Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-7-1031	Network Operators and Service Providers should consider entering into Mutual Aid agreements with partners best able to assist them in a disaster situation using the templates provided on the NRIC and NCS websites. These efforts could include provisions to share spectrum, fiber facilities, switching, and/or technician resources.	Disaster Recovery and Mutual Aid	Highly Important	**X**	**X**			**X**			**X**	**X**			**X**	
8-7-1032	Network Operators and Service Providers should document their critical equipment suppliers, vendors, contractors and business partners in their Business Continuity Plans along with an assessment of the services, support, and capabilities available in the event of a disaster.	Disaster Recovery and Mutual Aid	Highly Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-1037	Network Operators, Service Providers, Equipment Suppliers and Public Safety Authorities should use a disaster recovery support model that provides a clear escalation path to executive levels, both internally and to business partners.	Disaster Recovery and Mutual Aid	Highly Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-7-1039	Equipment Suppliers should develop support processes that include interfaces with those internal organizations (e.g., sales, logistics, manufacturing) that have a potential role in assisting Network Operators and Service Providers in disaster response efforts.	Disaster Recovery and Mutual Aid	Highly Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-7-1048	Network Operators and Service Providers should consider supplementing media backup storage with full system restoral media and documented restoration procedures that can be utilized at an alternate "hot site", in case of total failure of the primary service site.	Disaster Recovery and Mutual Aid	Highly Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-1052	Network Operators and Service Providers should periodically assess the functionality of business critical systems during a disaster exercise.	Disaster Recovery and Mutual Aid	Highly Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-7-1058	Network Operators, Service Providers and Equipment Suppliers should work collectively with local, state, and federal governments to develop relationships fostering efficient communications, coordination and support for emergency response and restoration.	Disaster Recovery and Mutual Aid	Highly Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-7-1067	Network Operators, Service Providers and Property Managers should consider, in preparation for predicted natural events, placing standby generators on line and verifying proper operation of all subsystems (e.g., ice, snow, flood, hurricanes).	Disaster Recovery and Mutual Aid	Highly Important	X		X			X		X		X			X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-5-0524	Network Operators and Service Providers should operate a route database. That database should provide the routing advertisement source from the Network Operator's perspective. The database should be accessible by peers, customers and other users. The access can be via a web interface similar to the looking glass server's or just telnet access. The database is informational only and can not be used to effect or impact the actual routing table. The need to provide security and isolation to such a database is high.	Network Reliability and Interoperability	Highly Important		**X**	**X**		**X**								
8-5-0536	As appropriate, Network Operators and Service Providers should deploy security and reliability related software updates (e.g., patches, maintenance releases, dot releases) when available between major software releases. Prior to deployment, appropriate testing should be conducted to ensure that such software updates are ready for deployment in live networks. Equipment Suppliers should include such software updates in the next generic release and relevant previous generic releases.	Network Reliability and Interoperability	Highly Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-6-0762	Network Operators should engineer networks supporting VoIP applications to provide redundant and highly available application layer services. Examples of such services include DNS and other directory services, SIP, H.323, and other application-level gateways. To ensure interoperability, all implementations of such IP-based application protocols should conform to the applicable IETF standards for those protocols.	Network Reliability and Interoperability	Highly Important		**X**			**X**								
8-6-0767	Service Providers implementing a SIP-signaled VoIP network should consider using media gateway controllers according to IETF RFC 3372 BCP 63, "Session Initiation Protocol for Telephones (SIP-T): Context and Architectures," in order to achieve interoperability with SS7/ISUP-signaled TDM voice networks.	Network Reliability and Interoperability	Highly Important		**X**											
8-7-0405	Network Performance: Network Operators and Service Providers should periodically examine and review their networks to ensure that it meets the current design specifications.	Network Reliability and Interoperability	Highly Important	**X**	**X**						**X**	**X**				

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0407	NOC Communications: Network Operators and Service Providers should establish processes for NOC-to-NOC (Network Operations Center) peer communications for critical network activities (e.g., scheduled maintenance, upgrades and outages).	Network Reliability and Interoperability	Highly Important	**X**	**X**						**X**	**X**				
8-7-0415	Data Back-up Verification: Network Operators and Service Providers should test the restoral process associated with critical data back-up, as appropriate. The goal is to demonstrate that data restoration is complete and works as expected.	Network Reliability and Interoperability	Highly Important			**X**							**X**			
8-7-0421	Fast Failover of Redundancies: Equipment Suppliers should design network elements intended for critical hardware and software recovery mechanisms to minimize restoration times.	Network Reliability and Interoperability	Highly Important	**X**	**X**	**X**		**X**	**X**		**X**	**X**	**X**		**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0425	Software Management: Network Operators and Service Providers should maintain software version deployment records, as appropriate.	Network Reliability and Interoperability	Highly Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-7-0428	Software & Hardware Vulnerability Tracking: Service Providers should monitor software and hardware vulnerability reports and take the recommended action(s) to address problems, where appropriate. These reports and recommendations are typically provided by equipment suppliers and CERTs (Computer Emergency Response Teams).	Network Reliability and Interoperability	Highly Important		X	X	X	X				X	X	X		
8-7-0430	Software Configurations: Equipment Suppliers should be able to recreate supported software from source and, where feasible, software obtained from third parties.	Network Reliability and Interoperability	Highly Important				X							X		

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0452	Network Operators, Service Providers and Property Managers should post emergency contact number(s) and unique site identification in an externally visible location at unmanned communication facilities (e.g., towers, cell sites, Controlled Environment Vault (CEV), satellite earth stations). This signage should not reveal additional information about the facility, except when necessary.	Network Reliability and Interoperability	Highly Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-7-0454	Network Operators and Service Providers should consider establishing technical and managerial escalation policies and procedures based on the service impact, restoration progress and duration of the issue.	Network Reliability and Interoperability	Highly Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-7-0459	Equipment Suppliers should design outdoor equipment (e.g., base station) to operate in expected environmental conditions (e.g., weather, earthquakes).	Network Reliability and Interoperability	Highly Important	**X**							**X**				**X**	

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0461	Equipment Suppliers should provide the capability to test failover routines of redundant network elements.	Network Reliability and Interoperability	Highly Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-7-0496	Network Operators and Property Managers should consider storing their portable generators at critical sites that are not otherwise equipped with stationary generators.	Network Reliability and Interoperability	Highly Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-7-0497	Network Operators and Property Managers should consider connecting the power load to portable generators where they are stored, and configuring them for auto-engage in the event of a failover.	Network Reliability and Interoperability	Highly Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0498	Network Operators and Property Managers should consider alternative measures for cooling network equipment facilities (e.g., powering HVAC on generator, deploying mobile HVAC units) in the event of a power outage.	Network Reliability and Interoperability	Highly Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-7-0504	Network Operators and Service Providers, in order to facilitate asset management and increase the likelihood of having usable spares in emergency restorations, should consider maintaining "hot spares" (circuit packs electronically plugged in and interfacing with any element management system, as opposed to being stored in a cabinet) for mission critical elements.	Network Reliability and Interoperability	Highly Important	X	X	X		X	X	X	X	X	X		X	X
8-7-0513	Network Operators and Service Providers should maintain a "24 hours by 7 days" contact list of other providers and operators for service restoration of inter-connected networks. Where appropriate, this information should be shared with Public Safety Service and Support providers.	Network Reliability and Interoperability	Highly Important	X	X			X	X	X	X	X			X	X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0530	Network Operators, Service Providers and Equipment Suppliers should participate in interoperability testing (including services), as appropriate, to maintain reliability across connected networks.	Network Reliability and Interoperability	Highly Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-7-0532	Diversity Audit: Network Operators should periodically audit the physical and logical diversity called for by network design and take appropriate measures as needed.	Network Reliability and Interoperability	Highly Important	X	X	X		X		X	X	X	X		X	
8-7-0541	Network Operators, Service Providers and Equipment Suppliers should store multiple software versions for critical network elements and be able to fallback to an earlier version.	Network Reliability and Interoperability	Highly Important	X	X	X	X	X	X	X	X	X	X	X	X	X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0547	Network Operators and Service Providers should place critical network databases (e.g., directory server, feature server, Service Control Point (SCP)) in a secure environment across distributed locations to provide service assurance (e.g., maintainability, connectivity, security, reliability) consistent with other critical network elements.	Network Reliability and Interoperability	Highly Important	X	X	X					X	X	X		X	
8-7-0576	Network Operators and Service Providers should move network access for pre-planned high volume call events away from the 911 selective router.	Network Reliability and Interoperability	Highly Important	X	X			X	X	X	X	X			X	X
8-7-0619	Network Operators, Service Providers, Property Managers and Public Safety Providers should coordinate with fire agencies in emergency response preplanning efforts for communications equipment locations.	Network Reliability and Interoperability	Highly Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-7-0653	Network Operators, Service Providers and Property Managers should retain complete authority about when to transfer from the electric utility and operate standby generators.	Network Reliability and Interoperability	Highly Important	X	X			X	X	X	X	X			X	X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0660	Network Operators, Service Providers and Property Managers should have a plan that is periodically verified for providing portable generators to offices with and without stationary engines.	Network Reliability and Interoperability	Highly Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-7-0669	Network Operators, Service Providers, and Property Managers should develop and/or provide appropriate emergency procedures for AC transfer.	Network Reliability and Interoperability	Highly Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-7-0679	Network Operators, Service Providers and Equipment Suppliers should provide diverse power feeds for all redundant links (e.g., SS7, BITS clocks) and any components identified as "critical" single points of failure (SPOF) in transport and operations of the network.	Network Reliability and Interoperability	Highly Important	**X**							**X**	**X**			**X**	

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0695	Network Operators, Service Providers and Property Managers should develop and test plans to address situations where normal power backup does not work (e.g., commercial AC power fails, the standby generator fails to start, automatic transfer switch fails).	Network Reliability and Interoperability	Highly Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-7-0699	Network Operators, Service Providers, Equipment Suppliers and Property Managers should design standby systems (e.g., power) to withstand harsh environmental conditions.	Network Reliability and Interoperability	Highly Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-7-0776	Network Operators, Service Providers and Equipment Suppliers should conduct and periodically re-validate physical security assessments on critical network facilities.	Network Reliability and Interoperability	Highly Important	X	X			X	X	X	X	X			X	X

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-8-0599	Crisis event simulation: Network Operators and Service Providers should conduct exercises periodically to test a network's operational readiness for various types of events (e.g., hurricane, flood, nuclear, biological, and chemical), through planned, simulated exercises. The exercise should be as authentic as practical. Scripts should be prepared in advance and team members should play their roles as realistically as possible.	Network Reliability and Interoperability	Highly Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-6-5073	Network Operators, Service Providers and Equipment Suppliers should perform risk assessment on significant network changes (e.g., technology upgrades).	Physical Security	Highly Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-6-5131	Network Operators should provide appropriate security for emergency mobile trailers (both pre- and post-deployment) in order to protect against a coordinated terrorist attack on emergency communications capabilities.	Physical Security	Highly Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-6-5133	Network Operators should protect the identity of locations where emergency mobile trailers and equipment are stored.	Physical Security	Highly Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-6-5146	Network Operators and Service Providers should develop and manage recovery plans to ensure the timely restoration of services in the event of transponder loss, satellite payload failure, and satellite failure.	Physical Security	Highly Important	**X**							**X**					
8-6-5194	Equipment Suppliers should design electronic hardware to minimize susceptibility to electrostatic discharge.	Physical Security	Highly Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-6-5231	Network Operators, Service Providers, Equipment Suppliers and Property Managers should develop documentation for the restoration of power for areas of critical infrastructure including such things as contact information, escalation procedures, restoration steps and alternate means of communication. This documentation should be maintained both on-site and at centralized control centers.	Physical Security	Highly Important	X	X	X		X	X	X	X	X	X		X	X
8-6-5248	Network Operators, Service Providers and Equipment Suppliers should perform risk assessment on significant network changes, both temporary and permanent, resulting from restoration efforts.	Physical Security	Highly Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-6-5249	Network Operators should consider geographic separation of network redundancy during restoration, and address losses of redundancy and geographic separation following restoration.	Physical Security	Highly Important	X	X	X	X	X	X	X	X	X	X	X	X	X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-6-5250	Network Operators should consider intra-office diversity of all critical resources during restoration, and address losses of diversity following restoration.	Physical Security	Highly Important	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**	**X**		**X**	**X**
8-6-5253	Network Operators, Service Providers and Equipment Suppliers should use lessons learned from restoration efforts to update recovery plans for transponder loss, satellite payload failure and satellite failure.	Physical Security	Highly Important	**X**							**X**					
8-6-5264	Satellite Operators should maintain an alternate recovery facility that would duplicate operations and Tracking, Telemetry, Control and Monitoring (TTC&M). The alternate recovery facility should be geographically diverse from the primary facility, maintained and tested on a regular schedule to ensure readiness and timely response.	Physical Security	Highly Important	**X**							**X**					

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-5123	Network Operators should maintain and control access to accurate location information of critical network facilities in order to identify physical locations hosting critical infrastructure assets.	Physical Security	Highly Important	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**	**X**		**X**	**X**
8-7-5138	Network Operators should plan for the possibility that impacted network nodes cannot be accessed by company personnel for an extended period of time and define the corporate response for restoration of service.	Physical Security	Highly Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-7-5139	Network Operators, Service Providers and Equipment Suppliers should consider establishing procedures for managing personnel who perform functions at disaster area sites.	Physical Security	Highly Important	**X**	**X**				**X**	**X**	**X**	**X**				**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-5160	Network Operators, Service Providers, Equipment Suppliers and Property Managers should account for the possible absence of critical personnel in their business continuity plan.	Physical Security	Highly Important	X	X				X	X	X	X				X
8-7-5212	Network Operators, Service Providers and Property Managers should consider placing generator sets and fuel supplies for critical sites within a secured area to prevent unauthorized access, reduce the likelihood of damage and/or theft, and to provide protection from explosions and weather.	Physical Security	Highly Important	X	X				X	X	X	X				X
8-7-5214	Network Operators, Service Providers and Property Managers should consider placing all power and network equipment in a location to increase reliability in case of disaster (e.g., floods, broken water mains, fuel spillage). In storm surge areas, consider placing all power related equipment above the highest predicted or recorded storm surge levels.	Physical Security	Highly Important	X	X				X	X	X	X				X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-5222	Network Operators, Service Providers and Equipment Suppliers should consider providing trouble call centers with a physically diverse back-up capability that can quickly be configured to receive the incoming traffic and take appropriate action.	Physical Security	Highly Important	**X**	**X**				**X**	**X**	**X**	**X**				**X**
8-7-5223	Network Operators, Service Providers and Equipment Suppliers should establish a plan for providing technical support that prevents the loss of one facility or location from disabling their ability to provide support.	Physical Security	Highly Important	**X**	**X**				**X**	**X**	**X**	**X**				**X**
8-7-5226	Network Operators, Service Providers and Property Managers should maintain liaison with local law enforcement, fire department, other utilities and other security and emergency agencies to ensure effective coordination for emergency response and restoration.	Physical Security	Highly Important	**X**	**X**				**X**	**X**	**X**	**X**				**X**
8-7-5229	Network Operators, Service Providers and Property Managers should have controlled access to comprehensive facility cabling documentation (e.g., equipment installation plans, network connections, power, grounding and bonding) and keep a backup copy of this documentation at a secured off-site location.	Physical Security	Highly Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-5237	Network Operators, Service Providers and Equipment Suppliers should verify the integrity of system spares and replenish utilized spares, as appropriate, as part of a disaster response at a facility.	Physical Security	Highly Important	X	X	X		X	X	X	X	X	X		X	X
8-7-5242	Network Operators, Service Providers and Equipment Suppliers should reassess the criticality of associated facilities following a catastrophic incident (i.e. loss of one facility may make others more critical).	Physical Security	Highly Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-7-5252	Network Operators should evaluate the priority on re-establishing diversity of facility entry points (e.g., copper or fiber conduit, network interfaces for entrance facilities) during the restoration process.	Physical Security	Highly Important	X	X				X	X	X	X				X
8-7-5259	Network Operators, Service Providers, Equipment Suppliers and Property Managers should establish and enforce access control and identification procedures for all individuals (including temporary contractors, and mutual aid workers) at restoration sites for which they have responsibility. Provide for issuing and proper displaying of ID badges, and the sign-in and escorting procedures, where appropriate.	Physical Security	Highly Important	X	X	X	X	X	X	X	X	X	X	X	X	X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-5261	Network Operators, Service Providers and Property Managers should identify carrier interconnection points and coordinate restoral plans, as appropriate.	Physical Security	Highly Important	**X**				**X**	**X**	**X**	**X**			**X**	**X**	**X**
8-7-5267	Network Operators, Service Providers, Equipment Suppliers and Property Managers should ensure that operating procedures are clearly defined, and followed by personnel during emergency situations in order to avoid degradation of cyber and physical security due to a diversion.	Physical Security	Highly Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-7-5270	Network Operators, Service Providers, Equipment Suppliers and Property Managers personnel should be aware that terrorists or malicious groups may use 0 information to cause heightened public or employee awareness to divert attention and resources to other areas away from their intended physical or cyber target. Where feasible, information (e.g., news sources, e-mail) should be authenticated and cross-verified to ensure accuracy of information.	Physical Security	Highly Important	**X**	**X**			**X**	**X**	**X**	**X**				**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-5272	Network Operators, Service Providers and Equipment Suppliers should include security considerations in disaster recovery plans for critical infrastructure sites.	Physical Security	Highly Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-7-5279	Network Operators, Service Providers and Equipment Suppliers should consider site specific (e.g., location, region, country) threat information during security program development.	Physical Security	Highly Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-7-5281	Network Operators, Service Providers and Property Managers with buildings serviced by more than one emergency generator, should design, install and maintain each generator as a stand alone unit that is not dependent on the operation of another generator for proper functioning, including fuel supply path.	Physical Security	Highly Important	X				X	X	X	X				X	X
8-8-0569	In E9-1-1, the PSTN may be used as a backup to dedicated trunks. Two implementation options exist: Option 1: PSTN as a Backup for Normal 9-1-1	Physical Security	Highly Important	X	X			X	X		X				X	X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
	Connectivity—An alternative for handling E9-1-1 calls during periods of failure in the connectivity between an originating network and the emergency services network is to use the PSTN as a backup (i.e., fallback) connection mechanism between the caller's originating network and the PSAP. Such connectivity may route calls to the appropriate PSAP without the associated information that would normally be present. If the primary path to the emergency services network is interrupted by a ""failure"" (not when all trunks are simply busy), the call may be forwarded over the PSTN to a number specified by the PSAP that is answered at the PSAP on a 24/7 basis. It is desirable for that specified number to be a type that can provide the original CallerID/Automatic Number Identification (ANI). This best practice does not propose that any 9-1-1 call delivery stakeholder bypass acceptable congestion control techniques commonly applied within the industry for 9-1-1 calls. Option 2: Wireless Public or Private Networks as Backup for 9-1-1 Dedicated Trunks—Similar to Option 1 above (PSTN backup) for completing 9-1-1 calls when the primary transport facility is interrupted by a ""failure"" (not when all trunks are simply busy), wireless public or private networks, or satellite-based services may be used to provide an additional alternate path to the PSTN, providing IP multimedia connectivity for															

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
	next generation networks or used solely as an alternate call delivery path for the voice component of 9-1-1 calls.															
8-6-3204	Service Providers should work with Public Safety Service and Support providers to educate the public on the proper use of N11 Access codes (211, 311 and 511 services) such that it enables the 911 network and personnel to be exclusively focused on emergencies. Proper use of all N11 codes, including 911, prevents exhaustion of resources of emergency personnel on non-emergency situations. (Reference NRIC BP 0578)	Public Safety	Highly Important	**X**	**X**			**X**	**X**		**X**	**X**			**X**	**X**
8-7-3201	Service Providers and Public Safety organizations should jointly develop a response plan to notify the public, through the broadcast media, of alternate means of contacting emergency services during a 911 outage.	Public Safety	Highly Important	**X**	**X**			**X**	**X**		**X**	**X**			**X**	**X**
8-7-3211	Network Operators and Service Providers should develop and maintain operations plans that address network reliability issues. Network Operators and Service Providers should proactively include Public Safety authorities when developing network reliability plans in support of 911 services.	Public Safety	Highly Important	**X**	**X**			**X**	**X**		**X**	**X**			**X**	**X**

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-3217	E9-1-1 Service Provider Contact Information: Network Operators and Service Providers should provide and maintain current 24/7/365 contact information accessible to Public Safety Answering Points (PSAPs) so that PSAPs may obtain additional subscriber information as appropriate.	Public Safety	Highly Important	**X**	**X**				**X**	**X**	**X**	**X**				**X**
8-8-0901	VSPs should conduct extensive 9-1-1 call-through testing for environments that have a high user capacity (e.g., university campuses, large commercial enterprise campuses, and densely populated multi-tenant buildings/complexes). This testing immediately reduces the risk of misrouting a block of callers at a particular facility and in turn reduces the liability for those same entities. Because the "originating end user" customers are also stakeholders in the success of a 9-1-1 call, they should also participate in testing with the VSP. This best practice is also applicable to legacy private branch exchange (PBX) environments; the PBX service provider should perform the extensive call-through testing steps.	Network Reliability and Interoperability	Highly Important	**X**	**X**				**X**		**X**	**X**				**X**

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-8-0902	When service providers or carriers reconfigure their network, for example, make changes to VPC/MPC/GMLC/Emergency Services Gateway (ESGW) providers, they must assess the impact on the routing of 9-1-1 calls. Service providers and/or carriers should coordinate and perform necessary testing of all new call paths between their network and the emergency services network (e.g., SRs, or the ESInet). This testing should include a test call using all routing elements (e.g., pANI, Emergency Route Tuple [ERT], and Emergency Services Gateway Route Identifier [ESGWRI]).	Network Reliability and Interoperability	Highly Important	**X**	**X**				**X**	**X**	**X**	**X**				**X**
8-6-8037	System Inventory Maintenance: Network Operators and Service Providers should maintain a complete inventory of elements to ensure that patches/fixes can be properly applied across the organization. This inventory should be updated each time a patch/fix is identified and action is taken.	Cyber Security	Important	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**	**X**			
8-7-8548	Incident Response (IR) Procedures: When a service outage or security incident occurs, Network Operators and Service Providers should follow processes similar to Appendix X.	Cyber Security	Important													

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-8-8056	Operational Voice over IP (VoIP) Server Hardening: Network Operators should ensure that network servers have authentication, integrity, and authorization controls in place in order to prevent inappropriate use of the servers. Enable logging to detect inappropriate use.	Cyber Security	Important	**X**	**X**				**X**	**X**	**X**	**X**				
8-8-8060	Protect Against Cellular Network Denial of Service: Service Providers & Network Operators should ensure strong separation of data traffic from management/signaling/control traffic, via firewalls. Network operators should ensure strong cellular network backbone security by employing operator authentication, encrypted network management traffic and logging of security events. Network operators should also ensure operating system hardening and up-to-date security patches are applied for all network elements, element management system and management systems.	Cyber Security	Important	**X**							**X**					
8-8-8066	Sharing Information with Industry & Government: Service Providers, Network Operators, and Equipment Suppliers should participate in regional and national information sharing groups such as the National Coordinating Center for Telecommunications (NCC), Telecom-ISAC, and the ISP-ISAC (when chartered). Formal membership and participation will enhance the receipt of timely threat information and will provide a forum for response and coordination. Membership will also afford access to	Cyber Security	Important	**X**	**X**				**X**	**X**	**X**	**X**			**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
	proprietary threat and vulnerability information (under NDA) that may precede public release of similar data.															
8-8-8075	Identity Administration: Network Operators and Service Providers should have procedures for verifying identity of users to IT department and IT personnel to users (secret PINs, callback procedures, etc.).	Cyber Security	Important	**X**	**X**				**X**	**X**	**X**	**X**			**X**	**X**
8-8-8100	Training for Security Staff: Service Providers, Network Operators, and Equipment Suppliers should establish security training programs and requirements for ensuring security staff knowledge and compliance. This training could include professional certifications in cyber security.	Cyber Security	Important	**X**	**X**				**X**	**X**	**X**	**X**				
8-8-8101	Document and Verify All Security Operational Procedures: Service Providers and Network Operators should ensure that all security operational procedures, system processes, and security controls are documented, and that documentation is up to date and accessible by appropriate staff. Perform gap analysis/audit of security operational procedures as often as security policy requires relative to the asset being protected. Using results of analysis or audit, determine which procedures, processes, or controls need to be updated and documented.	Cyber Security	Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**			

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-8-8117	DNS Servers Disaster Recovery Plan: Service Providers and Network Operators should prepare a disaster recovery plan to implement upon DNS server compromise.	Cyber Security	Important	X	X						X	X				
8-8-8124	Conduct Organization Wide Security Awareness Training: Service Providers, Network Operators, and Equipment Suppliers should ensure staff is given awareness training on security policies, standards, procedures, and general best practices. Awareness training should also cover the threats to the confidentiality, integrity, and availability of data including social engineering. Training as part of new employee orientation should be supplemented with regular "refreshers" to all staff.	Cyber Security	Important	X	X				X	X	X	X			X	X
8-8-8132	Leverage Business Impact Analysis for Incident Response Planning: Service Providers and Network Operators should leverage the BCP/DR Business Impact Assessment (BIA) efforts as input to prioritizing and planning Information Security Incident Response efforts.	Cyber Security	Important	X	X				X	X	X	X			X	X

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-8-8134	Security of Devices Beyond Scope of Control: Service Providers should carefully consider possible impacts on their networks from changes in the configuration or authentication information on devices beyond the service demarcation point, and thus beyond their physical or logical scope of control. Service Providers should consider network filters or network authentication to protect against malicious traffic or theft of service caused by such insecure devices.	Cyber Security	Important	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-8-8136	Protect Network/Management Infrastructure from Unexpected File System Changes: Service Providers and Network Operators should deploy tools to detect unexpected changes to file systems on Network Elements and Management Infrastructure systems where feasible and establish procedures for reacting to changes. Use techniques such as cryptographic hashes.	Cyber Security	Important	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**	**X**		**X**	**X**
8-8-8508	Post-Mortem Review of Security Architecture after Recovery: Immediately following incident recovery, Service Providers and Network Operators should re-evaluate the adequacy of existing security architecture and implement revisions as needed. Ensure any changes are adequately documented to reflect the current configuration. Review existing processes for establishing and maintaining security architectures update as necessary to maintain currency.	Cyber Security	Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**				

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-8-8534	Recover from Anonymous SS7 Use: If logs or alarms determine an SS7 table has been modified without proper authorization, Service Provider and Network Operators should remove invalid records, or in the event of a modification, rollback to last valid version of record. Investigate the attack to identify required security changes.	Cyber Security	Important	**X**	**X**			**X**		**X**	**X**	**X**			**X**	
8-8-8694	Threat Management: Network Operators, Service Providers and Equipment Suppliers should keep their programs flexible. What is considered a security best practice today might be obsolete tomorrow. Changing factors include new technologies, changing business models, emerging threats and growth of the network and the user base.	Cyber Security	Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-8-8711	Media Gateway Availability: Network Operators and Service Providers should engineer networks to provide redundant and highly available application layer services. (e.g., DNS and other directory services, SIP, H.323).	Cyber Security	Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**				

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-8-8712	Media Gateway Interoperability: Network Operators and Service Providers should implement applicable industry standards governing protocol (e.g., IP Protocols from the IETF) and established policies and procedures to maintain currency within these publications to ensure interoperability.	Cyber Security	Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**				
8-8-8713	Media Gateway Interoperability With Legacy Networks: Network Operators and Service Providers implementing a signaling gateway should consider using media gateway controllers that map gateway responses to SS7 in an anticipated and predictable fashion (e.g., RFC 3398 for SIP-to-SS7 mapping).	Cyber Security	Important	**X**	**X**			**X**			**X**	**X**				
8-8-8727	Maintaining Physical Link Diversity: Network Operators and Service Providers should implement industry guidelines for validating physical diversity, and consider performing signaling link diversification validation on a scheduled basis (e.g., twice a year). Processes and procedures should exist for tracking discrepancies and maintaining a historical record.	Cyber Security	Important	**X**	**X**			**X**			**X**	**X**				

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-8-8728	Maintaining Logical Link Diversity: Network Operators who deploy next generation signaling networks should consider industry guidelines for logical diversity (e.g. multi-homing), and perform network diversification validation on a scheduled basis (e.g., twice a year). Processes and procedures should exist for tracking discrepancies and maintaining a historical record.	Cyber Security	Important	X	X	X	X	X	X	X						
8-8-8746	Public Key Infrastructure (PKI): For environments where traditional PKI infrastructures are problematic, service providers should use an alternate approach such as a "web of trust" for public key validation / authenticaton.	Cyber Security	Important	X	X			X	X	X						
8-8-8749	Risk Assessment Process: Service providers and network operators should have documented processes in place for reviewing new vulnerabilities as they are announced.	Cyber Security	Important	X	X	X	X	X	X	X	X	X				X

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-8-8757	Incident Response Preventative Measures: Service providers and network operations should set policy within each corporation or agency to provide guidance when there is a security breach.	Cyber Security	Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**			**X**
8-8-8758	Post DoS Practice: Network Operators and Service Providers should establish policies, and procedures to support early recognition and isolation of potential bad actors to minimize impact to the network.	Cyber Security	Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**		**X**				**X**
8-8-8771	Media Gateways Signaling: Service Providers and Network Operators implementing a control-signaled (i.e. SIP) network should consider using media gateway controllers according to appropriate industry standards (i.e. Internet Engineering Task Force (IETF)) in order to achieve interoperability between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks.	Cyber Security	Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**						

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-6-1043	Equipment Suppliers should consider, during their response to major disasters, editing the support "hotline" calling tree by adding a specific entry for disaster events.	Disaster Recovery and Mutual Aid	Important	X	X	X	X	X		X	X	X	X	X	X	
8-6-1044	Equipment Suppliers should consider providing a "Disaster Recovery Services Checklist" to all of the Service Providers they support. The checklist would provide a listing of the Equipment Supplier's professional services which the Service Provider may require during an event.	Disaster Recovery and Mutual Aid	Important	X	X	X	X	X		X	X	X	X	X	X	
8-6-1051	Network Operators and Service Providers should work with Equipment Suppliers and Government entities to identify criteria and procedures for handling network elements affected by nuclear attack or nuclear accidents (e.g., shock wave, Electro-magnetic Pulse (EMP), Thermal, Fallout, fiber darkening of phosphorous based fiber cable).	Disaster Recovery and Mutual Aid	Important	X	X	X	X	X	X	X	X	X	X	X	X	X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-1008	Network Operators, Service Providers, and Equipment Suppliers should use the Incident Command System Standard for incident coordination and control in the emergency operations center and at the incident site.	Disaster Recovery and Mutual Aid	Important	X	X				X	X	X	X				X
8-7-1015	Network Operators and Service Providers should make available to the disaster recovery team "as-built" drawings of network sites.	Disaster Recovery and Mutual Aid	Important	X	X			X	X	X	X	X			X	X
8-7-1024	Network Operators, Service Providers and Equipment Suppliers should plan for the possibility of a disaster occurring during a work stoppage.	Disaster Recovery and Mutual Aid	Important	X	X	X		X	X	X	X	X	X		X	X
8-7-1026	Network Operators and Service Providers should consider creating a corporate policy statement that defines a remote system access strategy, which may include a special process for disaster recovery.	Disaster Recovery and Mutual Aid	Important	X	X	X	X	X	X	X	X	X	X	X	X	X

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-1029	Network Operators and Service Providers should periodically review their portable power generator needs to address changes to the business.	Disaster Recovery and Mutual Aid	Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-7-1035	Network Operators and Service Providers should include trial deployment of emergency mobile assets in disaster response exercises to evaluate level of personnel readiness.	Disaster Recovery and Mutual Aid	Important	**X**	**X**				**X**		**X**	**X**				**X**
8-7-1036	Network Operators should determine in advance if they will use line of sight systems (microwave radio, free space optics, and satellite communications systems) to re-establish communications. If these technologies are to be deployed it is recommended that path designs be developed for each critical area in advance with personnel trained to install and optimize the systems.	Disaster Recovery and Mutual Aid	Important	**X**	**X**				**X**		**X**	**X**				**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-1040	Network Operators, Service Providers and Equipment Suppliers should consider using lab, demonstration or training equipment if replacement equipment is unavailable in disaster situations.	Disaster Recovery and Mutual Aid	Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-5-0540	Equipment Suppliers should share countermeasures resulting from analysis of an outage with Network Operators using the same equipment.	Network Reliability and Interoperability	Important	**X**	**X**						**X**	**X**				
8-5-0570	Intraoffice 911 Termination to Mobile PSAP - Commonly, the transport facility between the PSAP and the serving end office may not have facility route diversity. To accommodate instances where these facilities are interrupted or it becomes necessary to evacuate the PSAP location, some PSAPs have established mobile PSAP systems that may be connected to phone jacks at the serving end office. The phone jacks, although usually installed inside the end office for security purposes, are typically installed in an accessible location for ease in locating them during an emergency. Some PSAPs have prearranged with the serving LEC to permit a jurisdictional employee having an emergency vehicle (e.g., police car) equipped with radio capability to retain a key to	Network Reliability and Interoperability	Important	**X**					**X**		**X**				**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
	the LECs' end office and to connect to an RJ-11 jack for 911 call interception. Another type of receptacle may be pre-installed in the end office for connection to a mobile PSAP.															
8-6-0803	Network Operators, Service Providers and Equipment Suppliers are encouraged to continue to participate in the development and expansion of industry standards for traffic management that promote interoperability and assist in meeting end user quality of service needs.	Network Reliability and Interoperability	Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	
8-7-0488	Network Operators and Service Providers should ensure that critical wireless circuits (e.g., high priority cells, SS7 circuits, 911 circuits) are registered with Telecom Service Priority (TSP).	Network Reliability and Interoperability	Important	**X**							**X**				**X**	

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0489	Network Operators, Service Providers and Equipment Suppliers should consider provisions in labor contracts to provide for cooperation between union and non-union personnel during disaster recovery situations.	Network Reliability and Interoperability	Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-7-0490	Network Operators and Service Providers should consult National Fire Prevention Association Standards (e.g., NFPA 75 and 76) for guidance in the design of fire suppression systems. When zoning regulations require sprinkler systems, an exemption should be sought for the use of non-destructive systems.	Network Reliability and Interoperability	Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-7-0587	Government, Network Operators and Service Providers of critical services to National Security and Emergency Preparedness (NS/EP) users should avail themselves of the Telecommunications Service Priority (TSP) program and support / promote as applicable.	Network Reliability and Interoperability	Important		**X**			**X**	**X**	**X**		**X**				**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-0702	Network Operators and Service Providers should minimize dependence on equipment requiring AC power feeds in favor of DC-powered components.	Network Reliability and Interoperability	Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-7-0779	Network Operators, Service Providers and Equipment Suppliers should establish a means to allow for coordination between cyber and physical security teams supporting preparedness, response, investigation and analysis.	Network Reliability and Interoperability	Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
8-8-0787	Back-Up Power Fuel Supply: Network Operators, Service Providers, and Property Managers should consider the use of fixed alternate fuel generators (e.g., natural gas) connected to public utility supplies to reduce the strain on refueling.	Network Reliability and Interoperability	Important	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

				Multimedia NG9-1-1							**Legacy E9-1-1**					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-8-0795	Virtual Collaboration: Network Operators, Service Providers, and Equipment Suppliers should plan for elevated utilization of virtual collaboration and remote meetings during pandemics or other crisis situations.	Network Reliability and Interoperability	Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-8-0796	Deferral of Operations Activities: Network Operators, Service Providers, and Equipment Suppliers should consider developing guidelines for the deferral of specific maintenance or provisioning activities during certain situations (e.g., pandemic, holiday, National Special Security Event).	Network Reliability and Interoperability	Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-8-0797	Workforce Augmentation: Network Operators, Service Providers, and Equipment Suppliers should consider creating a workforce augmentation plan prior to a pandemic or other crisis situation.	Network Reliability and Interoperability	Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-6-0761	Network Operators and Service Providers should conduct periodic verification of the office synchronization plan and the diversity of timing links, power feeds and alarms.	Network Reliability and Interoperability	Important	X	X			X	X	X	X	X			X	X
8-6-5054	When guard services are utilized by Network Operators, Service Providers, Equipment Suppliers or Property Managers, a process should be developed to quickly disseminate information to all guard posts. This process should be documented and should clearly establish specific roles and responsibilities.	Physical Security	Important	X	X			X	X	X	X	X			X	X
8-6-5098	Network Operators, Service Providers and Equipment Suppliers should ensure that all network infrastructure equipment meets the minimum requirements of ANSI T1.319 (fire resistance).	Physical Security	Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-6-5106	Equipment Suppliers should consider participating in and complying with an industry organization that develops standards in their security, logistics and transportation practices.	Physical Security	Important	X	X			X		X	X	X			X	

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-6-5132	Network Operators should identify primary and alternate transportation (e.g., air, rail, highway, boat) for emergency mobile trailers and other equipment and personnel.	Physical Security	Important	X	X			X	X	X	X	X			X	X
8-6-5210	Network Operators, Service Providers and Property Managers should discourage use of Emergency Power Off (EPO) switches between the primary battery supplies and the main power distribution board. EPO switches are not recommended for use in traditional -48V DC battery plants.	Physical Security	Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-6-5228	Network Operators, Service Providers and Equipment Suppliers should consider including cross-subsidiary resource sharing and communications in business continuity plans to support emergency response and restoration.	Physical Security	Important	X	X	X		X	X	X	X	X	X		X	X
8-6-5239	Property Managers for multi-tenant facility should maintain a crisis management plan for restoration following an incident.	Physical Security	Important	X	X			X	X	X	X	X			X	X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-6-5243	Network Operators, Service Providers and Equipment Suppliers should restrict visits and tours at the affected areas during the restoration period following a major incident.	Physical Security	Important	X	X	X		X	X	X	X	X	X		X	X
8-6-5244	Network Operators, Service Providers and Equipment Suppliers should make all employees, contractors, and others with access to critical infrastructure during restoration aware of changes to security posture resulting from the incident, and increased vigilance should be encouraged.	Physical Security	Important	X	X			X	X	X	X	X			X	X
8-6-5254	During restoration efforts, Network Operators and Service Providers should not permit unsecured wireless access points for the distribution of critical data or operating system upgrades.	Physical Security	Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-6-5255	Network Operators, Service Providers and Equipment Suppliers should ensure that temporary wireless networks (e.g., terrestrial microwave, free-space optical, satellite, point-to-point, multi-point, mesh) used during an incident are subsequently disabled or secured.	Physical Security	Important	X	X			X	X	X	X	X			X	X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-5151	Network Operators, Service Providers and Property Managers located in the same facility should coordinate security matters and include all tenants in the overall security and safety notification procedures, as appropriate.	Physical Security	Important	**X**	**X**				**X**	**X**	**X**	**X**				**X**
8-7-5191	Network Operators, Service Providers that are tenants within telecom hotels should plan accordingly to protect their own facilities from potential risks within the building complex (e.g., fire suppression system, plumbing, hazardous materials).	Physical Security	Important	**X**	**X**					**X**	**X**	**X**				
8-7-5192	Network Operators and Service Providers tenants of a telecom hotel should provide a current list of all persons authorized for access to the Property Manager, provide periodic updates to this list, and provide instructions for exceptions (e.g., emergency restoration personnel).	Physical Security	Important	**X**	**X**					**X**	**X**	**X**				

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-5216	Network Operators, Service Providers and Property Managers should consider providing secure pre-constructed exterior wall pathways for mobile generator connections or tap box connections.	Physical Security	Important	**X**	**X**				**X**	**X**	**X**	**X**				**X**
8-7-5225	Network Operators, Service Providers, Equipment Suppliers and Property Managers should ensure that Business Continuity Plan(s) are restricted to those with a need-to-know.	Physical Security	Important	**X**	**X**				**X**	**X**	**X**	**X**				**X**
8-7-5234	Network Operators, Service Providers and Property Managers should provide or arrange for security to protect temporary equipment placements and staging areas for critical infrastructure equipment in a disaster area.	Physical Security	Important	**X**	**X**				**X**	**X**	**X**	**X**				**X**
8-7-5238	Network Operators, Service Providers who are tenants in multi-tenant facilities (e.g., telecom hotels) should coordinate security and restoration efforts with the Property Manager.	Physical Security	Important	**X**	**X**				**X**	**X**	**X**	**X**				**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-5245	Network Operators, Service Providers and Equipment Suppliers should document the use of non-standard equipment during restoration to review and/or replace those devices as appropriate.	Physical Security	Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-7-5256	Network Operators, Service Providers and Equipment Suppliers should monitor temporary connections of network test equipment that are established for restoration to prevent access by unauthorized personnel.	Physical Security	Important	X	X	X	X	X	X	X	X	X	X	X	X	X
8-7-5258	Network Operators, Service Providers and Equipment Suppliers should define and assign responsibility for retrieval of all corporate assets (e.g., access cards, equipment) and ensure temporary physical and logical access is removed after completion of a restoration effort for all temporary personnel associated with the restoration.	Physical Security	Important	X	X			X	X	X	X	X			X	X
8-7-5260	Network Operators, Service Providers, Equipment Suppliers and Property Managers should brief affected personnel involved in a restoration on any significant changes to access control procedures.	Physical Security	Important	X	X	X	X	X	X	X	X	X	X	X	X	X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-5269	Network Operators, Service Providers, Equipment Suppliers and Property Managers should incorporate various types of diversionary tactics into exercises to assess the security response.	Physical Security	Important	X	X	X		X	X	X	X	X	X		X	X
8-7-5271	Network Operators and Service Providers should consider physical and cyber security issues in Mutual Aid Agreements (e.g., authorization, access control, badging).	Physical Security	Important	X	X			X	X	X	X	X			X	X
8-7-5280	Network Operators, Service Providers and Equipment Suppliers should instruct security personnel to confirm the authenticity of directions to supersede existing security processes or procedures.	Physical Security	Important	X	X			X	X		X	X	X	X	X	X
8-6-3203	Service Providers should consider developing options that allow for call delivery from Emergency Notification Services to subscribers with call blocking/screening services in order to assist in the effectiveness of Emergency Notification Systems (Public Safety Mass Calling) and return calls from PSAPs.	Public Safety	Important	X	X			X	X		X	X			X	X

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-3202	The Service Provider and the Public Safety Agency or its agent that utilize Public Safety mass calling systems for emergency notification should have a pre-established procedure to notify all impacted network operators, prior to launching an alert event.	Public Safety	Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-7-3205	Network Operators, Service Providers and Public Safety organizations should consider participating in standards bodies and other forums contributing to Emergency Telecommunications Services (ETS).	Public Safety	Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-7-3209	CATV Service Providers, shall where practical, receive signals from local broadcasters via fiber as the primary source with automatic fail over to the off-air signal as the secondary source, to support public notification in disasters or emergencies.	Public Safety	Important	**X**	**X**			**X**	**X**	**X**	**X**	**X**			**X**	**X**
8-7-3210	Emergency Operations Centers and PSAPs should consider obtaining connections to provide video (for viewing local weather and news information and monitoring distribution of information over EAS), and utilize that connection to provide diverse access to the Internet and telecommunications.	Public Safety	Important						**X**							**X**

				Multimedia NG9-1-1							Legacy E9-1-1					
Best Practice Number	**Original Best Practice**	**Category**	**Status**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**ESInet**	**PSAPs**	**Other Entities**	**Legacy Providers**	**Internet Based**	**Data Bases**	**Pre-Call and Call Time Software Functions**	**PSTN Based**	**PSAPs**
8-7-3212	Network Operators and Service Providers should consider including notification of Public Safety Authorities, as appropriate, in their trouble notification plans.	Public Safety	Important	**X**	**X**			**X**	**X**		**X**	**X**			**X**	**X**