March 2013

WORKING GROUP - 8
E9-1-1 Best Practices

Final Report – Part 2

Table of Contents

1 Results in Brief

1.1 Executive Summary

The Communications Security, Reliability and Interoperability Council's (CSRIC) mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety.

As defined in the CSRIC Charter for Working Group 8 – *E9-1-1 Best Practices*, 9-1-1 service is a vital part of the nation's emergency response and disaster preparedness system and 9-1-1 service reliability is vital to public safety and consumer wellbeing. As such, during CSRIC II, and before that the Network Reliability & Interoperability Council (NRIC), a substantial body of voluntary Best Practices was developed to promote 9-1-1 reliability. 9-1-1 Best Practices are vital to maintaining a dependable and efficient 9-1-1 infrastructure.

Working Group 8 (WG8) was tasked with the review of existing CSRIC/NRIC 9-1-1 Best Practices and to recommend ways to improve them, accounting for the passage of time, technology changes, operational factors, and any identified gaps. As part of this effort, WG8 was also commissioned to provide recommendations regarding the creation of two new non-industry Best Practice categories: (i) Public Safety Answering Point (PSAP) and (ii) 9-1-1 Consumer which would include recommendations regarding how to better engage PSAPs in the Best Practice process.

In June 2012 WG8 presented its *Final Report – Part 1 E9-1-1 Best Practices* which recommended modifications and new Best Practices that support communication providers in preparing for natural or man-made disasters. These Best Practices will ensure that communication providers are able to restore service quickly in the aftermath of a disaster.

This Final Report – Part 2 is the conclusion of a larger review of industry Best Practices intended to modernize those that relate specifically to E9-1-1 and to provide the initial structure for the newly created non industry Best Practice categories.

For the modernization work, a subteam was established to focus on the analyses and was designated as WG8 Subteam 2 (WG8-2). This team considered the entire set of existing Best Practices and analyzed them from three separate viewpoints as well as gap analysis:

1. Best Practices that have a direct and immediate impact on E9-1-1 reliability and resiliency, the review and update of those deemed out of date or aged.

2. Best Practices that previously were not identified as interrelated with Public Safety that needed modified to include the new "Public Safety" implementer category approved by the CSRIC Council vote in Final Report – Part 1 in June 2012[1].

[1] Working Group 8 Appendix 1 page 19 Non-Best Practice Recommendations *"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*

3. Best Practices that although not directly linked to E9-1-1 nor required the new Public Safety implementer category, if implemented, could have a downstream improvement to the reliability and/or resiliency of the underlying E9-1-1 network.

For the development of the two new categories of Best Practices work, a subteam was established to focus on the outline, structure, and framework and was designated as WG8 Subteam 3 (WG8-3). This team developed the concept and framework needed to provide ongoing guidance and structure for the new categories as well as development of new Best Practices to seed the initial Best Practice development.

For Part 2 of the Final Report, the CSRIC III is being asked to accept this document and the recommended Best Practices contained within, and to take appropriate future steps regarding any gaps found by this Working Group that were determined to be out of scope during this initiative or require future work by a CSRIC Working Group.

---

reliability and resiliency."

2 Introduction

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.

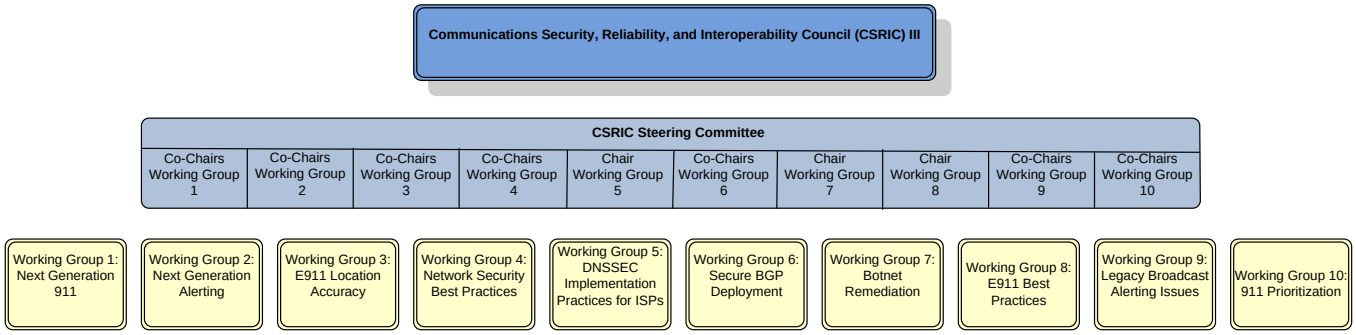
This *Final Report – Part 2 E9-1-1 Best Practices* documents the efforts undertaken by CSRIC WG8 with respect to the review and modernization of existing CSRIC/NRIC 9-1-1 Best Practices and recommendations on the two new categories of Best Practices referenced above. The team considered the ongoing relevance of these Best Practices, the transition to newer technologies for E9-1-1 call delivery, and how existing Best Practices that currently address the areas of Internet Protocol (IP) and Cyber issues could influence the reliability and resiliency of next generation E9-1-1 platforms either directly or indirectly.

WG8 officially began its work on November 17, 2011, and was given until June 2012 to produce Final Report – Part 1 and December 2012 to produce this Final Report – Part 2 on overall Best Practice recommendations. The focus of WG8 was to review the existing set of 1,022 voluntary industry Best Practices developed over the years by the various Network Reliability and Interoperability Councils (NRIC) and the previous CSRIC Council.

With the introduction of Next Generation E9-1-1 services and the overall changes in technology, 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 improving them, accounting for the passage of time, technology changes, operational factors, and any identified gaps. 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.

2.1 CSRIC Structure



2.2 Active 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
Donna Bethea-Murphy	Iridium
Mary Boyd – Chair WG8-2	Intrado
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
Alisa Simmons	Tarrant County 9-1-1 District
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
Ethan Lucarelli	Wiley Rein

Table 1 - List of Working Group Members

3 Objective, Scope, and Methodology

3.1 Objective

Objective 1: Review and enhance current Best Practices
This objective was to review the current set of industry Best Practices and identify a subset of those to be studied for E9-1-1 reliability and resiliency applications. Qualifying Best Practices would be further analyzed to determine any modernization, enhancements, or clarifications that could be made to improve their use by industry and public safety authorities.

A framework would be developed to efficiently identify Best Practices that are within scope of this work effort and could be used by any Service Provider, Network Operator, or Public Safety agency to improve reliability and resiliency of the Time Division Multiplexing (TDM) or Internet Protocol (IP) based E9-1-1 networks.

Objective 2: Create new category of Public Safety Answering Point Best Practices
This objective was to design the framework and structure and make initial recommendations on the development of a new set of Best Practices that can be used by Public Safety Answering Points (PSAPs) to share their successful policies and procedures nationally similar to how Best Practices transcend the communications industry today.

Objective 3: Create new category of Consumer Best Practices
The final objective of WG8 was to also design framework for the development of a second new set of Best Practices that public safety agencies and the general public could use to educate on the proper use of the E9-1-1 and emergency call/notification systems to enhance the safety of the American public at large. The goal was to provide standardization of practice form and to establish a permanent location for these educational tools for ease of future development and use.

3.2 Scope

Working Subteam 8-2:
The scope of WG8-2 subteam for this Final Report was in part to analyze current Best Practices that apply, or could apply, to E9-1-1 Legacy[2] or Next Generation IP networks. Given this scope, the group found it essential to place an initial focus on the full set of 1,022 Best Practices developed over the years by previous NRIC Focus Groups and CSRIC Working Groups.

The full Best Practice data set does not apply to E9-1-1; therefore it was in scope for this team to review and reject those Best Practices that would not directly relate to the reliability and resiliency of the E9-1-1 network infrastructure and facilities. Within the scope of the working group were also the development of new Best Practices, and the identification of any gaps, that will provide additional guidance to industry and public safety authorities.

Working Subteam 8-3:

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

The scope of WG8-3 subteam for this Final Report was to use the existing industry Best Practice concept and design the structure, process, and framework for a new set of non-industry voluntary Best Practices for PSAPs and consumer use of E9-1-1. Also in scope was the development of a new standard format focusing on the flow from conception through publishing online to provide access for PSAPs and the general public.

It is important that Working Group 8 reminds readers that industry Best Practices are voluntary in nature and may not apply to all Service Providers, Network Operators, or Public Safety entities due to scope, cost, feasibility, or resource limitations. Best Practices should be used by experts who have the overall experience to interpret the individual Best Practice in the manner in which it was intended.

3.3 Methodology

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 delivered to the Council and approved in June 2012.

Sub-group 8-2 "*Current E9-1-1 Best Practices*" established methodologies for the review of Best Practices that were developed by previous NRIC and CSRIC councils. These assisted the team in identifying the subset of data that would be further examined and modified according to the charter. Generally the sub-team agreed that:

1. Best Practices that, in their expert opinion, had a direct or indirect impact on E9-1-1 reliability or resiliency would qualify for enhancement, modernization, or deletion.
2. A Best Practice could be recommended for deletion, even if not 9-1-1 related, as a general housekeeping responsibility if that Best Practice was determined to be no longer relevant to industry.
3. When enhancing or modifying a Best Practice, the structure outlined in the ATIS Network Reliability Steering Committee (NRSC) Best Practice Tutorial[3] would be used whenever possible.
4. Best Practices determined to be out of scope by the majority of the team would be discounted from the final data set and from any further consideration.
5. Qualifying Best Practices that contained multiple concepts or thoughts would be restructured into multiple Best Practices.
6. If a gap was identified and if possible a recommended Best Practice would be drafted, otherwise the gap would be documented for future CSRIC Council action in the Final Report.

[3] ATIS NRSC Best Practice Tutorial, November 2011 Presented to Working Group 8 on December 14, 2011 found at http://www.atis.org/bestpractices/Tutorial.aspx

Sub-group 8-3 "*PSAP and Consumer Best Practices*" established methodologies for the creation of two new categories of Best Practices. These assisted the team in developing processes to establish an ongoing framework for development, availability, and future review needed for these new categories. Generally the sub-team agreed that:

1. Initial set of Best Practices to "seed" both new categories would be developed from existing government sources, freely available sources, or from sub-team expertise.
2. The structure of a Best Practice as outlined in the ATIS NRSC Best Practice Tutorial would be used as the model for the new categories.
3. Best Practices would be written with a voluntary nature in mind so as not to imply a mandatory environment.
4. It would be assumed that new Best Practices would eventually be placed online in a similar fashion as industry Best Practices.
5. Best Practices in these two new categories would not be integrated with existing industry Best Practices.

3.3.1 Approach to E9-1-1 Best Practices

3.3.1.1 Current Best Practices

A three step evaluation process was utilized to review the current set of Best Practices as outlined in Figure 1 below. It was necessary to review the data set in a multi-step manner to first quickly eliminate a bulk of Best Practices that were out of scope for the team or identify those obviously out of date that could be recommended for deletion. Secondly, split the data set into two parts, one part that would be enhanced only through addition of a note to the Remarks/Comments section of the Best Practice, and the second part constituting Best Practices that needed modifications or restructuring. The third and final evaluation step was to complete the bulk of the modifications and complete the gap identification process.

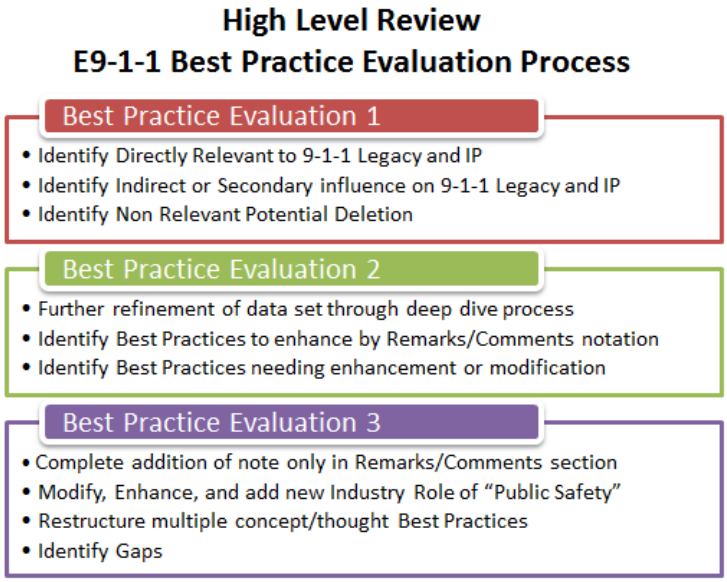


Figure 1 – Evaluation Process

3.3.1.2 PSAP and Consumer Best Practices

The creation of two new categories of Best Practices required the development of the entire framework that would be necessary to establish an initial set of Best Practices to "seed" an ongoing process. The structure of the new categories although similar to the current industry Best Practices would also need unique Industry Roles, Keywords, Categories, and Status definitions. Recommendations would also need to be developed on how to maintain the new Best Practices, where and how they would be stored, and what entity(s) should provide web hosting services. Another important consideration for these two new categories was to create the framework for legitimizing the Best Practices through a body such as CSRIC to establish them as a recognized and certified source of information for public safety agencies and the general public. The approach for this framework is demonstrated in Figure 2.

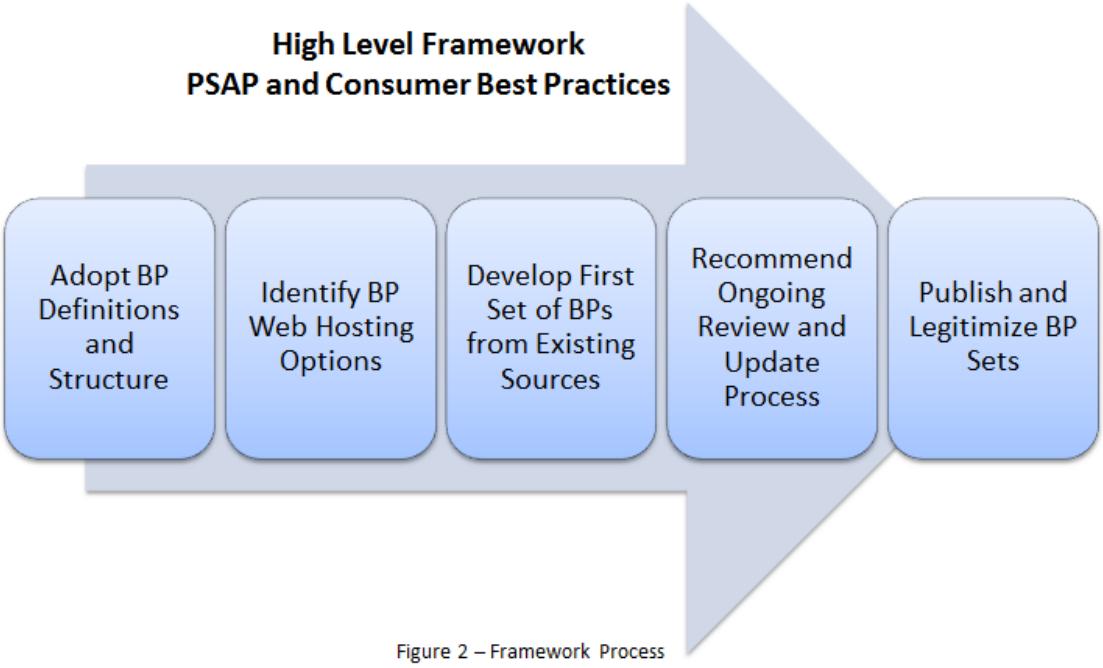


Figure 2 – Framework Process

3.3.1.3 Elements of Best Practice Framework

There were specific framework elements required for the creation of two new non-industry Best Practice categories. This framework is intended to establish an ongoing process similar to that used for industry Best Practices to provide maximum efficiency going forward.

Adopt Best Practice Definitions and Structure:

For each of the new categories, Public Safety Answering Point (PSAP) and Consumer, slightly different approaches were necessary. PSAP Best Practices would follow more closely with industry format both in structure and use. Consumer Best Practices would share structure with both industry and PSAP, however, with an educational theme included could be written as a "good idea" which is generally avoided with industry Best Practices. Generally, development of a Best Practice should meet the following 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

Both categories were able to be closely structured to these guidelines; however, basic industry structure had to be adapted to apply to the new categories. For industry Best Practices the basic structure is listed below in Figure 3.

Industry Best Practice Structure

Number:	8-5-0536
Status:	Highly Important
Description:	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 Types(s):	Cable; Internet/Data; Satellite; Wireless; Wireline
Industry Role(s):	Service Provider; Equipment Supplier; Network Operator
Keywords(s):	Network Elements; Network Operations; Procedures; Software; Technical Support
Reference/Comments:	

Figure 3 – Elements of a Best Practice

To adapt the current structure to meet the needs of the new categories, the sub-team had to address the key structure elements:

- Network Types(s)
- Industry Role(s)
- Status definitions for Critical, Highly Important, and Important
- Best Practice Category
- Keywords

For each new category the sub-team adapted the Best Practice framework to adjust for these items. The importance of these adaptations is explained below.

Network Types(s) – In the Industry Best Practice structure these are used to identify the communications sector(s) that the Best Practice applies to. Currently there are 11 Network Types to choose from that were not appropriate for the new categories and were modified as listed below.

Consumer Best Practices:

Network Type(s) were modified to include:

- 9-1-1 Agencies
- Employees
- Parents/Guardians/Caregivers
- Business Owners
- Government
- Teachers/Trainers
- Children
- Home Owners

PSAP Best Practices:

Network Types(s) were modified to include:

- 9-1-1 Agencies
- Government

Industry Role(s) – In the industry Best Practice structure these are used to identify what industry segment is being identified such as Service Provider, Network Operator, Equipment Provider, Public Safety or Government. Used in a Best Practice for example as "Service Providers and Network Operators shall…" this would not be appropriate for these new categories of Best Practices.

Consumer Best Practices:

Industry Role(s) were modified to include:

- Consumers
- Public Safety Entities
- 9-1-1 Callers
- TTY/TDD Users
- Trainers

PSAP Best Practices:

Industry Role(s) were modified to include:

- PSAPs

Status definitions for Critical, Highly Important, and Important – Developed in CSRIC II by Working Group 6, status definitions categorize each Best Practice to a level of importance to assist users of Best Practices during implementation[4]. The definitions established for industry Best Practices required adaptation to adequately address the categorization needs.

Consumer Best Practice definitions:

Critical Best Practices include those which meet any of the following standards:

- Significantly enhances the potential for a 9-1-1 caller to reach emergency services successfully.

[4] January 2011, CSRIC Working Group 6: Best Practice Implementation Final Report, page 7 Section 3.1 Approach.

- Significantly enhances the ability of consumers to properly set up and use 9-1-1 emergency services.
- Significantly enhances the safety of the general public regarding 9-1-1 emergency services.
- Enhances the accuracy of information transfer between 9-1-1 callers and 9-1-1 call takers.
- Significantly enhances the ability of public safety authorities to locate a 9-1-1 caller.

Highly Important Best Practices include those which meet any of the following standards:

- Reduces the misuse of 9-1-1 emergency services for non-emergencies.
- Reduces unsuccessful 9-1-1 calls by unintentional consumer and 9-1-1 caller actions.
- Enhances the knowledge and safety of consumers and 9-1-1 callers regarding proper 9-1-1 call etiquette.
- Enhances the ability of public safety authorities to locate a 9-1-1 caller.

Important Best Practices include those which meet any of the following standards:

- Promotes education of 9-1-1.
- Enhances awareness to the public on limitations to 9-1-1 services.
- Provides awareness to the risks of using 9-1-1 for non-emergency purposes.
- Promotes steps consumers can take to ensure public safety authorities can locate them during an emergency.
- Provides general guidelines for consumers regarding 9-1-1 emergency services.

PSAP Best Practice definitions:

Critical Best Practices include those which meet any of the following standards:

- Significantly reduces the potential for a catastrophic failure of critical communications network infrastructure and/or services.
- Significantly reduces the duration or severity of critical communications outages.
- Materially limits and/or contains the geographic area affected by a communications failure from cascading to other or adjacent geographic areas.
- Affects critical communications components (e.g., ALI/ANI) for all network configurations.
- Preserves priority communications for key personnel involved in disaster response and recovery.

Highly Important Best Practices include those which meet any of the following standards:

- Improves the likelihood of emergency call completion, with caller information, to the appropriate response agency (i.e., Public Safety Answering Point), ensuring access to emergency communications for all callers.
- Improves the efficiency and promote the availability of networks and the likelihood of call completion and message transmission (e.g., e-mail, instant messaging) for key personnel involved in disaster response and recovery.
- Improves detection of network events by network operators and service providers.

- Implementation has improved network reliability but may not be applicable for all PSAPs.

Important Best Practices include those which meet any of the following standards:

- Promote sound provisioning and maintenance or reliable, resilient networks, services, and equipment, but were not otherwise classified.
- Common sense BPs that entities generally adopt.

Best Practice Category and Keywords – In industry Best Practice structure, this identifies what the Best Practice is primarily addressing and provides keywords for web searching. For the industry there are 38 distinct categories available to select from, many which are not adequate for the new categories. The keywords were most adaptable for the PSAP Best Practices; however, for the Consumer category several new keywords were developed.

Consumer Best Practices:

Category and Keywords were modified to include:

- Alternate Methods
- Device Use
- Next Generation
- Updating Information
- Wireless
- Business
- Family Education
- Residential
- What to Say and Do
- Wireline
- Emergency Personnel
- Knowing Your Location
- Training Methods
- When to Call

PSAP Best Practices:

Category and Keywords were modified to include:

- Access Control
- Cyber Security
- Emergency Preparedness
- Hardware
- Network Elements
- Network Provisioning
- Policy
- Security Systems
- Technical Support
- Buildings
- Disaster Recovery
- Encryption
- Human Resources
- Network Interoperability
- Pandemic
- Power
- Software
- Training and Awareness
- Business Continuity
- Documentation
- Essential Services
- Network Design
- Network Operations
- Physical Security Management
- Procedures
- Supervision

Identify Best Practice Web Hosting Options:

The Working Group addressed how the new Best Practice categories should be made available to the PSAP community and the general public. Industry Best Practices are found on two mirrored web sites, one managed by the FCC and one managed by the Alliance for Telecommunications Industry Solutions (ATIS)[5]. It is recommended by the Working Group that

[5] Both websites can be accessed at http://www.atis.org/nrsc/bpresource.asp.

the new categories be kept separate and unique from the current set of Best Practices and not be integrated due to the different audiences and topics and to prevent general confusion that would result from integrating them with the industry set. The Working Group contacted both the FCC and ATIS regarding their willingness to host these new Best Practice categories. The structure and format were designed to minimize code development needed to bring the new Best Practices online quickly following adoption by CSRIC. Both the FCC and ATIS have agreed to support moving toward hosting these in a similar fashion to the current industry Best Practice set.

It should be noted that although recommendations for hosting the Best Practices are being made in this report, the actual hosting process would not begin until the Council approves this Final Report. Additionally, the FCC/ATIS hosting recommendation does not take into account other options that might be equally acceptable from another industry or public safety entity. One alternative is the National 9-1-1 Program which funds a National 9-1-1 Resource Center, which has a publicly accessible, searchable database of documents of all types related to 9-1-1. The site for the Resource Center can be accessed by going to www.911.gov and clicking on "Resource Center."

Develop First Set of Best Practices from Existing Sources:

The concept of developing the two new Best Practice categories, PSAP and Consumer, originated from the myriad of "best practices" that can be found through numerous documents online. The fundamental problem with these documents, and their insightful best practices, is that as time goes on they become aged, out of date, and become more difficult to find as internet web pages change, priorities change, or search engines index the information deep into queries making them hard to locate. The objective was to preserve these best practices from eventual obscurity and associate them with a time proven process where they could be adequately managed, periodically reviewed, and modernized as needed by subject matter experts.

For the PSAP category, the seeding came from existing government documents and websites particularly the FCC and US Department of Transportation. For the Consumer category, the team used a combination of government sponsored documents and subject matter expertise on the Working Group. It should be noted that the intent was to create the ongoing framework and establish the beginning set of Best Practices for these two new categories. A more inclusive set will need to be developed over time as was the case for the industry set.

Recommend Ongoing Review and Update Process:

The framework being developed for the two new Best Practice categories included ongoing support by appropriate entities and regular review of the Best Practices as needed to keep them current and relevant. Best Practices by their nature change as technology, situations, processes, etc. change. A successful process is one that includes a standard practice for:

1. Periodic reviews.
2. Ability of interested parties to recommend changes to existing Best Practices.
3. Creation of new Best Practices by impacted stakeholders.

Industry Best Practices are cared for by a process that includes CSRIC, the FCC, the ATIS

Network Reliability Steering Committee (NRSC)[6] and Best Practice stakeholders.

Outlined below in Figure 4, the high level process flow for the Industry Best Practices is depicted. For industry this has generally worked well and has resulted in a robust and dependable set of Best Practices. The process begins with defining the need for a review, gap analysis, or other driver. The needs can come from several sources such as a CSRIC Charter, FCC requests to industry, the industry itself, or from other stakeholders. Once the need is defined the Best Practices are reviewed, modified, deleted, created, etc. by a set of experts gathered for that purpose. The next step in the process is acceptance and normally consists of a set of Best Practices being brought by a Focus Group or Working Group to the NRIC/CSRIC Council for a vote. This provides a wide review and public acceptance before any Best Practice is assigned an official identifying number by the FCC. While a Best Practice may be created and used between CSRICs, it is authenticated by the Council vote. Once the Best Practice is accepted and, if required, given an official number it placed on both available websites hosted by the FCC and ATIS.

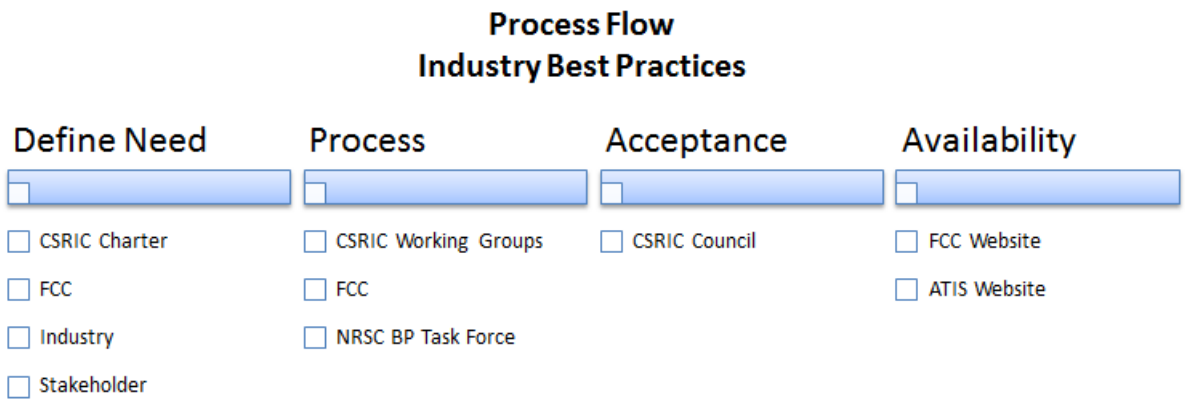


Figure 4 – Industry Best Practice Process Flow

With the introduction of the new categories of PSAP and Consumer Best Practices Working Group 8 is recommending this same process be used with the exception of changes to the define need and acceptance steps (Figure 5). The recommendations only apply to the new categories and not the current industry Best Practice process. When defining the need for a PSAP or Consumer Best Practice the addition of "PSAP" as an valid entity as a source for initial need development is required. Currently a Best Practice that has been modified or newly created is held in a pending status until a CSRIC Council vote is held to accept it. Working Group 8 is recommending that two additional acceptance entities be included for the PSAP and Consumer Best Practices categories in lieu of a full CSRIC Council vote. The FCC Public Safety and Homeland Security Bureau (PSHSB) and the ATIS NRSC have nearly two decades of experience in Best Practice management. The ATIS NRSC also has a standing Best Practice Task Force that regularly reviews industry Best Practices and provides modified or new items to the FCC PSHSB for consideration. These modified or new items are typically forwarded by the

[6] In its 1993 Report to the Nation, the Network Reliability Council (NRC) recommended formation of the Network Reliability Steering Committee (NRSC), under the auspices of ATIS for the purpose of monitoring network reliability on an ongoing basis.

FCC to a current CSRIC to follow the acceptance process.

These new categories, particularly the Consumer category, will not always need to undergo this rigorous process of CSRIC review and voting. By accepting this recommendation the existing CSRIC vote process may be used during any future charter, however, a Best Practice would be permitted to be accepted and placed online outside the CSRIC after a thorough and joint assessment between the FCC and NRSC using expertise already available.

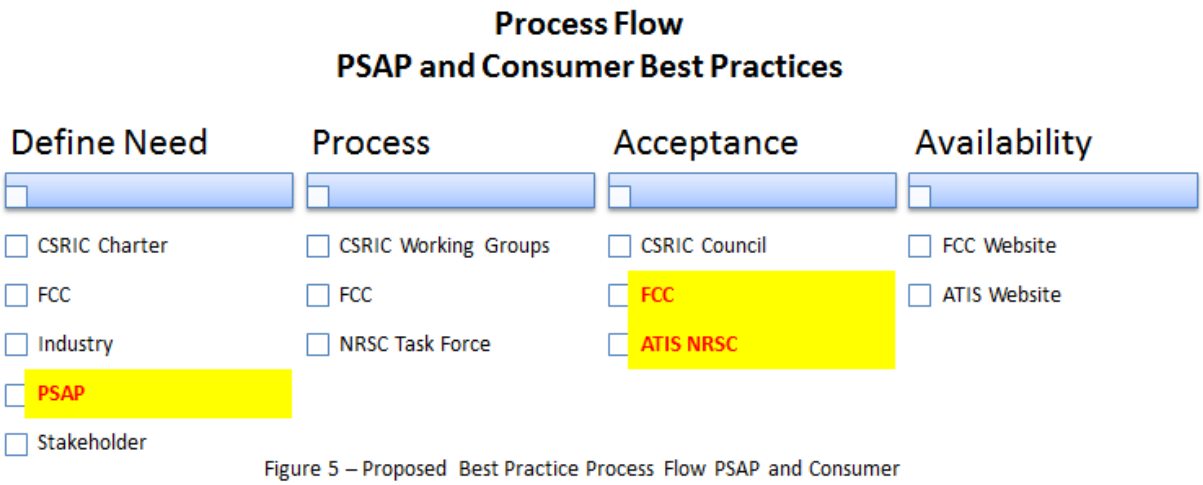


Figure 5 – Proposed Best Practice Process Flow PSAP and Consumer

Publish and Legitimize Best Practice Sets:

Following the acceptance of the new Best Practice categories the publishing to online access status will need to be further implemented. Working Group 8 recommends that this work be provided to the FCC and/or ATIS following the approval of this final report and begin the design and implementation phase onto one or both of the online Best Practice systems.

Working Group 8 recommends the acceptance of this framework, under the auspices of CSRIC, and should be established and certified by government and industry for the categories of PSAP and Consumer Best Practices.

Working Group 8 recommends that upon the successful online implementation of the new categories on the FCC and/or ATIS Best Practice websites that Public Notices or Press Releases be issued to further support the establishment of the framework.

4 Analysis, Findings and Recommendations

4.1 Analysis

Working Group Subteam 2 (WG8-2) approached the review of current Best Practices by making several assessments of the existing set of 1,023 Critical, Highly Important, and Important Best Practices. During the first review, the team focused on isolating Best Practices that were directly associated with the 9-1-1 network, supported the delivery of 9-1-1, or those that the

team determined needed further study. During this first pass the team identified 730 Best Practices that would constitute the team's workload for the remainder of the project.

The team settled on a two-step process for review and modifying the Best Practices. The first set was those directly related to E9-1-1 and the second those that could impact the E9-1-1 infrastructure indirectly if implemented. It was also agreed that the introduction of the "Public Safety" implementer category approved during the June 2012 CSRIC Council meeting would also need to be added to appropriate Best Practices.

The analysis used the principles set forth in the NRSC Best Practice tutorial regarding proper structure and format. This resulted in the restructuring of several Best Practices to the "One thought one Best Practice" principle and direct enhancements to the Best Practice wording.

WG8-2 established that in numerous cases the Best Practice being reviewed remained relevant and required no alteration other than the addition of the Public Safety implementer category. By updating the Best Practices with this newly approved class it emphasizes the prominence of this group of stakeholders and provides an enhanced set of Best Practices directed toward Public Safety.

WG8-2 also analyzed a group of Best Practices that were not directly related to the 9-1-1 infrastructure. Analysis determined that certain Best Practices if adopted by the appropriate implementer (e.g. Network Operator, Service Provider) could improve the reliability or resiliency of networks that 9-1-1 traffic and data may traverse. Regarding these particular Best Practices the team established that these would not necessitate direct modification based on their content and intent. It was agreed that a special notation in the Best Practice remarks section would serve to alert the user that this Best Practice could impact 9-1-1 operations. The intent of the special notation is to provide an additional search parameter within the Best Practices to identify indirectly related items and provide users additional guidance not previously available.

Working Group Subteam 3 (WG8-3) developed two new categories of Best Practices, PSAP and Consumer. The team began by analyzing the existing Best Practice framework that has been highly successful for the industry. The basic framework of structure, content, standardized format was analyzed to determine if it would appropriately apply to both new categories. The PSAP category was determine to be most closely aligned with industry framework and the general principles that constitute a "Best Practice".

The team concluded that the framework and processes were comprehensive for industry Best Practices, however, modifications were needed as detailed above in Section 3.3.1.3 to adapt to the new PSAP category.

For the Consumer category, however, the team found that the principles of a Best Practice were not fully adaptable. It was determined, for example, that although guidance states that a Best Practice should be "more than a good idea" for this category it was found that this was the case in many instances. This variation was necessary since many of the Consumer Best Practices were educational in nature and focused on the general public. In one new Best Practice it outlines the following good idea:

"*9-1-1 Callers should not hang up if they dial 9-1-1 by mistake. This helps to prevent unnecessary follow-up by the 9-1-1 call center or public safety authorities and allows the caller*

to explain the call was a mistake."

WG8-3 established that for the Consumer category concessions needed to be made to collect and preserve the ideas that were applicable to consumers and the general public. WG8-3 also debated if the new categories should be integrated into the current industry Best Practice set or be standalone. The analysis focused on what implications would result from combining them with industry and what level of effort it would take to duplicate the Best Practice websites for this purpose. It was finally decided that the introduction of these new categories into the current industry set was not practical and recommendations would be made to provide a unique web hosting solution for the new categories.

WG8-3 analyzed a series of documents that were collected throughout the process and also through suggestions conveyed by team members. Items that ultimately became new Best Practice recommendations were in part based on government documents designed to help public safety prepare for pandemics, or general guidelines for the operations of a PSAP. Others were educational documents designed for the public to help understand the proper use of 9-1-1 services. Accordingly there were many best practices and good ideas quoted in these documents, however, most had little common structure and were adaptable to the recommended framework being designed.

4.2 Findings

WORKING GROUP SUBTEAM 8-2

WG8-2 completed their work following an initial review of 730 Best Practices. A total of 10 new Best Practices are being recommended by the team. These were mostly due to restructuring of current Best Practices that were found to have multiple thoughts or concepts contained within the Best Practice. These recommendations are found in Appendix 2 – E9-1-1 Best Practices – *Current Best Practices Changed, Recommended New or Recommended Delete* and are identified by a "New" tag in the CSRIC III (New/Changed/Unchanged/Deleted) column. These Best Practices are labeled for identification purposes only as WG8-2-1 through WG8-2-10 and will require an official Best Practice number following acceptance.

WG8-2 identified 11 Best Practices that were found to be no longer relevant, found to be duplicates of other Best Practices, or was made obsolete by the modification of another Best Practice by the team. These recommendations are found in Appendix 2 – E9-1-1 Best Practices – *Current Best Practices Changed, Recommended New or Recommended Delete* and are identified by a "Delete" tag in the CSRIC III (New/Changed/Unchanged/Deleted) column. The Best Practices being recommended for deletion are 8-7-0413, 8-6-3213, 8-7-0573, 8-7-0632, 8-7-0633, 8-7-3220, 8-7-3221, 8-7-3222, 8-7-5126, 8-7-5247, and 8-8-0903. The explanation for the deletion is included in CSRIC III BP Reference/Comments column.

WG8-2 identified 186 Best Practices that required modification, restructuring, or required the addition of the new implementer class of "Public Safety". These recommendations are found in Appendix 2 – E9-1-1 Best Practices – *Current Best Practices Changed, Recommended New or Recommended Delete* and are identified by a "Changed" tag in the CSRIC III

(New/Changed/Unchanged/Deleted) column. Additional comments, notes, and recommended additions to the Best Practices can be found in the CSRIC III BP Reference/Comments column.

WG8-2 identified 77 Best Practices that did not necessitate direct modification based on their content and intent. A special notation was developed and is to be included in the Best Practice remarks section to alert the user that this Best Practice could impact 9-1-1 operations. The special notation can be found in Appendix 2 – E9-1-1 Best Practices – *Current Best Practices Changed, Recommended New or Recommended Delete* and are identified by an "Unchanged" tag in the CSRIC III (New/Changed/Unchanged/Deleted) column. The special notation "Note: This Best Practice could impact 9-1-1 operations" can be found in the CSRIC III BP Reference/Comments column.

WORKING GROUP SUBTEAM 8-3

WG8-3 completed their work following the development of two new categories, PSAP Best Practices and Consumer Best Practices[7]. A framework was developed for a new set of non-industry voluntary Best Practices one to provide guidance for Public Safety Answering Points (PSAP) and the other to provide education and guidance for consumers of 9-1-1 services.

WG8-3 identified recommendations for web hosting the new Best Practices and discussed this issue with both the FCC and ATIS to determine the level of effort required to develop a unique and standalone hosting solution.

WG8-3 adapted the industry Best Practice elements to fit the framework developed. The team addressed the key structure elements of Network Type, Industry Role, Status definitions, Best Practice categories, and Keywords. These edits can be found in section 3.3.1.3 *Elements of Best Practice Framework* found above.

WG8-3 developed a new set of 65 Consumer Best Practices from data sources collected during the process as well as consulting with experts participating on the team. These new Best Practice can be found in Appendix 3 – *Consumer Best Practices* and are identified by a "New Consumer" tag in the CSRIC III (New/Changed/Unchanged/Deleted) column. These Best Practices are labeled for identification purposes only as WG8-3-1 through WG8-3-65 and will require an official Best Practice number following acceptance.

WG8-3 developed a new set of 117 PSAP Best Practices from government sources identified during the process. These new Best Practice can be found in Appendix 4 – *PSAP Best Practices* and are identified by a "New PSAP" tag in the CSRIC III (New/Changed/Unchanged/Deleted) column. These Best Practices are labeled for identification purposes only as WG8-3-66 through WG8-3-183 and will require an official Best Practice number following acceptance.

WG8-3 determined that the new Best Practice categories should have additional acceptance entities to provide an alternate means of managing changes to the new Best Practices categories when a full council vote is not necessary. The team also developed recommendations for the ongoing support of the new Best Practice categories by expertise already found at the FCC and

[7] During the March 14, 2013 CSRIC Council meeting, a council member recommended that future CSRIC's undertake work efforts to further develop Best Practices to assist the deaf and hard of hearing.

ATIS NRSC.

WG8-3 found that it was important for a recognized governmental entity to publicly endorse and certify the new of PSAP and Consumer Best Practice categories to ensure they are legitimized as official sources of Best Practices.

4.3 Recommendations

Communications organizations, Public Safety, PSAPs, and Consumers 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 and understanding of 9-1-1 services.

Two new categories of Best Practices (i) Public Safety Answering Point (PSAP) and (ii) 9-1-1 Consumer should be established, acknowledged by a recognized government entity, and the recommended new Best Practices should be accepted by CSRIC III and moved to the next step of web hosting. The recommended web hosts are the Federal Communications Commission (FCC) and/or the Alliance for Telecommunications Industry Solutions (ATIS) who are experienced in Best Practice hosting and both who support this initiative.

Recommend that the two new categories of PSAP and Consumer should be kept separate and unique from the current set of Best Practices and not be integrated due to the different audiences and topics and to prevent general confusion that would result from integrating them with the industry set.

Recommend that the same support structure currently used for industry Best Practices be used with the exception of changes to the define need and acceptance steps (Figure 5). This includes future CSRIC charters, FCC generated requests, ATIS NRSC, and appropriate PSAP stakeholders.

Recommend that two additional acceptance entities be included for the PSAP and Consumer Best Practices categories in lieu of a full CSRIC Council vote for ongoing routine review activities. The recommended entities are the FCC and ATIS NRSC both of which are experienced in Best Practice maintenance and is an ongoing activity at the industry level.

Recommend that upon the successful online implementation of the new categories on the FCC and/or ATIS Best Practice websites that Public Notices or Press Releases are issued to further support the establishment of the framework and serve as further endorsement of the process.

Gap Analysis:

Listed below are gaps that were identified during the analysis phase. WG8-2 agreed that the these gaps have developed primarily due to new services that are in an early stage of development and implementation in the industry and sufficient Best Practice development remains difficult until these services have further developed.

1. Hosted Services

2. Cloud Services
3. Text to E9-1-1 Services

5 Conclusions

Working Group 8 – E9-1-1 Best Practices concludes that providing this enhanced and updated set of voluntary industry Best Practices that, if implemented, will strengthen the reliability and resiliency of the 9-1-1 infrastructure for Service Providers, Network Operators, Property Managers, Public Safety, and Government entities. These Best Practices when used by industry and public safety will serve to further harden the nation's 9-1-1 network against outages and disaster situations.

The Working Group also reasoned that preserving 9-1-1 related documents and their valuable insights linked to public safety was important and historic. PSAPs will eventually experience changes in personnel due to turnover, retirements, and new PSAPs. In these instances, incoming personnel will now have a readily available and current source of Best Practices as a valuable reference on day one. Consumers, trainers, parents, guardians, employers, etc. will have an information source that can be accessed instantly and provide expert guidance on the proper use of 9-1-1 to maximize the safety of consumers and the general public.

6 Appendix 1 – CSRIC III Council Considerations

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

Working Group 8 - Recommendations	CSRIC WG 8 Recommendation
Acceptance of this Final report and the recommended changes, new, and deleted Best Practices contained within Appendices 2-4 below.	Approve
Approval of two new categories of Best Practices (i) Public Safety Answering Point (PSAP) and (ii) 9-1-1 Consumer with associated framework under the auspices of CSRIC.	Approve
Acknowledgement that the categories of PSAP and Consumer Best Practices are official sources of Best Practices.	Approve
Recommend that web hosting for the new categories be aligned to the Federal Communications Commission (FCC) and/or the Alliance for Telecommunications Industry Solutions (ATIS) who are experienced in Best Practice hosting and both who support this initiative.	Approve
Recommend that PSAP and Consumer Best Practices be kept separate and unique from the current set of industry Best Practices.	Approve
Recommend that the same support structure currently used for industry Best Practices be used for the new PSAP and Consumer categories with the exception of changes to the define need and acceptance steps outlined in section 3.3.1.3 and Figure 5.	Approve
Recommend that two additional acceptance entities be included for the PSAP and Consumer Best Practices categories in lieu of a full CSRIC Council vote for routine review activities. The recommended entities are the FCC and ATIS NRSC.	Approve
Recommend that gaps identified by Working Group 8 be considered for a future CSRIC charter to provide time for Hosted Services, Cloud Services, and Text to E9-1-1 Services to develop to a stage where sufficient Best Practices can be identified.	Approve

7 Appendix 2 – E9-1-1 Best Practices

CSRIC III Best Practice Number	CSRIC III Best Practice	CSRIC III BP Reference/Comments	Best Practice Status	CSRIC III (New/Changed/ Unchanged/ Deleted)
CURRENT BEST PRACTICES CHANGED, RECOMMENDED NEW OR RECOMMENDED DELETE				
WG8-2-1	Network Operators, Service Providers, and Public Safety should establish mechanisms in Next Generation 9-1-1 (NG9-1-1) applications to handle call congestion and outages through diversion of calls to alternate Public Safety Answering Points (PSAP) that have the capabilities to effectively answer and provide assistance during periods of extreme overload or network failure scenarios.	**Network Types(s):** Cable; Internet/Data; Wireline **Industry Role(s):** Service Provider; Network Operator ; Public Safety **Keywords(s):** Essential Services; Network Operations; Pandemic; Procedures; Public Safety Service; Supervision	Critical	**New**
WG8-2-2	Network Operators, Service Providers, and Public Safety should design Emergency Services IP Networks (ESInets) with redundant interconnectivity to Online Service Providers (OSPs) and Public Safety Answering Points (PSAP) to maintain connectivity in the face of extensive disaster damage using the characteristics of IP routing to provide assistance in ensuring 9-1-1 calls will reach a PSAP if there is any path possible.	**Network Types(s):** Cable; Internet/Data; Wireline **Industry Role(s):** Service Provider; Network Operator ; Public Safety **Keywords(s):** Essential Services; Network Operations; Pandemic; Procedures; Public Safety Service; Supervision	Critical	**New**
WG8-2-3	Network Operators, Public Safety, and Equipment Suppliers should have procedures in place to allow for manual configuration in the event of a failure of automatic synchronization systems.	**Network Types(s):** Cable; Internet/Data; Satellite; Wireless; Wireline **Industry Role(s):** Equipment Supplier; Network Operator; Public Safety **Keywords(s):** Information Protection; Network Operations; Network Provisioning; Procedures; Software; Supervision; Training and Awareness	Highly Important	**New**
WG8-2-4	Network Operators, Public Safety, and Equipment Suppliers should consider restricting provisioning technicians from all	**Network Types(s):** Cable; Internet/Data; Satellite; Wireless; Wireline	Highly Important	**New**

	commands except those that are needed for their work (least privileges) and avoid any "global" commands or unauthenticated, privileged access that may have the potential for significant impact.	**Industry Role(s):** Equipment Supplier; Network Operator; Public Safety **Keywords(s):** Information Protection; Network Operations; Network Provisioning; Procedures; Software; Supervision; Training and Awareness		
WG8-2-5	Network Operators, Service Providers, and Public Safety should consider using wireless public or private networks as a backup to dedicated trunks for the 9-1-1 network during periods of network failure. In cases where the ability to deliver 9-1-1 calls to the Public Safety Answering Point (PSAP) through normal routing is interrupted by a failure (not all trunks busy conditions) consider forwarding the call over wireless public, private networks, or satellite-based services to provide an additional alternate path to the PSTN, providing IP multimedia connectivity for next generation networks, or used solely as an alternate call delivery path for the voice component of 9-1-1 calls.	**Network Types(s):** Cable; Internet/Data; Wireline **Industry Role(s**): Service Provider; Network Operator; Public Safety **Keywords(s):** Essential Services; Facilities Transport; Network Design; Network Interoperability; Network Operations; Procedures; Public Safety Service	Highly Important	**New**
WG8-2-6	Network Operators, Service Providers, and Public Safety should implement testing and verification processes for 9-1-1 pseudo Automatic Number Identification (pANI) to prevent bad data from being entered into the wrong routing databases typically occurring at the Automatic Location Information (ALI) or Selective Router (SR) stage of the provisioning process.	**Network Types(s):** Cable; Internet/Data; Wireless; Wireline **Industry Role(s):** Network Operator; Service Provider; Public Safety **Keywords(s):** Network Provisioning; Public Safety Service	Highly Important	**New**
WG8-2-7	Network Operators, Service Providers, and Public Safety should establish an assignment accuracy process to send a list of all applicable Master Street Address Guide (MSAG) ranges to Virtual Private Cloud (VPC) and Mobile Positioning Center (MPC) operators to ensure pseudo Automatic Number Identification (pANI) shell records are built correctly during original pANI provisioning to reduce negative impact of errors related to data entry.	**Network Types(s):** Cable; Internet/Data; Wireless; Wireline **Industry Role(s):** Network Operator; Service Provider; Public Safety **Keywords(s):** Network Provisioning; Public Safety Service	Highly Important	**New**
WG8-2-8	Network Operators and Service Providers using IP-based	**Network Types(s):** Cable; Internet/Data;	Highly	**New**

	connection arrangements for routing to a 9-1-1 system Service Provider (SSP) or Public Safety agency should ensure those transport facilities are diverse private facilities or their functional equivalent (e.g., generic routing encapsulation (GRE) tunneling, virtual private network (VPN), or equally secure industry protocols) and where appropriate and necessary supported by service level agreements.	Satellite; Wireless; Wireline **Industry Role(s):** Service Provider; Network Operator; Public Safety **Keywords(s):** Network Design; Public Safety Service	Important	
WG8-2-9	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should work together to jointly perform cause analysis, and meet periodically with the specific agenda of sharing the failure and outage information to develop corrective measures.	**Network Types(s):** Cable; Internet/Data; Satellite; Wireless; Wireline **Industry Role(s):** Equipment Supplier; Network Operator; Public Safety **Keywords(s):** Network Elements; Network Operations	Highly Important	**New**
WG8-2-10	Service Providers, Network Operators, and Public Safety should coordinate and perform necessary testing of all new call paths between their network and the emergency services network (e.g., Selective Routers, or the Emergency Services IP Network (ESInet)) that includes a test call using all routing elements.	**Network Types(s):** Cable; Internet/Data; Wireless; Wireline **Industry Role(s):** Service Provider; Network Operator; Public Safety **Keywords(s):** Network Provisioning; Public Safety Service	Highly Important	**New**
8-7-0413	Maintenance Notification: Network Operators and Service Providers should communicate information on service affecting maintenance activities and events to their customers, as appropriate.	Delete, this is a duplicate of BP 8-7-0403		**Delete**
8-6-3213	Network Operators, Service Providers, Equipment Suppliers and Public Safety Service and Support providers should work together to establish reliability and performance objectives in the field environment.	Delete, doesn't solve a problem, highly general statement with no real guidance. Does not create a gap by deletion		**Delete**
8-7-0573	Network Operators, Service Providers and Public Safety Authorities, should consider providing local loop diversity to the PSAP including the use of alternate technologies, (e.g., wireless, broadband). PSAPs should consider the availability of diverse local loop connections in the site selection for new	Delete, this is a duplicate of BP 8-8-0569 and CSRIC III new BP WG8-2-3.		**Delete**

	PSAP facilities.			
8-7-0632	Network Operators and Service Providers that use soldering irons in the provision or maintenance of service should periodically review the work processes and safety precautions applicable to safe operations of these work tools.	Delete, this Best Practice should be sunset based on the issue it refers to and the change in technology and use of tools.		**Delete**
8-7-0633	Network Operators, Service Providers, Equipment Suppliers, and Property Managers should prohibit smoking in buildings.	Delete.		**Delete**
8-7-3220	E9-1-1 Selective Router Database (SRDB) Diversity: Network Operators and Service Providers that operate E9-1-1 Selective Router Databases (SRDBs) should deploy SRDBs with redundancy and geographic diversity.	Delete, this Best Practice replaced by modified Best Practice 8-7-0571		**Delete**
8-7-3221	Selective Router Database (SRDB) Update Frequency: Network Operators and Service Providers that operate E9-1-1 Selective Router Databases (SRDBs) should maintain SRDBs with as current E9-1-1 routing information as is feasible.	Delete, this Best Practice replaced by modified Best Practice 8-7-0571		**Delete**
8-7-3222	E9-1-1 Selective Router (SR) to Public Safety Answering Point (PSAP) Trunking Architecture: Network Operators, Service Providers and Public Safety Answering Points (PSAPs) should provide, where appropriate, at least one additional trunk between the E9-1-1 Selective Router (SR) and the PSAP than the switching entity source with the largest total number of trunks serving that PSAP.	Delete, this Best Practice replaced by modified Best Practice 8-7-0571		**Delete**
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).	Delete, covered by BP 8-7-5160		**Delete**
8-7-5247	Network Operators, Service Providers, Equipment Suppliers and Property Managers should take into account failed security systems after an event when determining restoration priorities.	Delete, combined this Best Practice with 8-7-5240		**Delete**
8-8-0903	Public Safety Authorities should be allowed access to Department of Homeland Security—National Geospatial-	Delete, does not meet the definition of a Best Practice. Following team review it was		**Delete**

	Intelligence Agency (DHS—NGA) data, which can be provided on a monthly basis or as needed. The importance of 9-1-1 for Public Safety and for national intelligence should be emphasized. Common baseline imagery should be used to align GIS maps with streets and Public Safety Authority jurisdictional boundaries. One way to achieve that goal is to grant Public Safety Authorities access to federal or military imagery databases such as DoD–NGA and/or DHS–GMO (Department of Defense—Geospatial Management Office) that can be provided monthly or as-needed. This access should be justified through acknowledgement that 9-1-1 is of importance for public safety and national intelligence.	determined to generally be a "good idea" but does not address an issue in a proactive way in order to minimize negative consequences of a particular action.		
8-5-0570	Network Operators, Service Providers, and Public Safety should implement procedures that allow for 9-1-1 traffic to be rerouted to an alternate 9-1-1 answering location such as a fixed, mobile, or temporary PSAP (automatically, based on policy rules or with minimal manual intervention). For example situations where a network condition causes 9-1-1 call delivery to be disrupted or PSAP personnel must be evacuated for safety reasons.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-6-0762	Network Operators should engineer networks supporting VoIP applications to provide redundant and highly available application layer services.	**Remarks/Comments section:** 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.	Highly Important	**Changed**
8-6-0803	Network Operators, Service Providers, Public Safety, 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.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-6-1017	Network Operators, Service Providers, and Public Safety should have documented plans or processes to assess damage to network elements, outside plant, facility infrastructure, etc. for implementation immediately following a disaster.	**Add Industry Role(s):** Public Safety	Critical	**Changed**

8-6-1022	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider the development of a vital records program to protect vital records that may be critical to restoration efforts.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-6-1038	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider during all hazard and preplanned events, communicating the response status frequently and consistently to all appropriate employees detailing what processes have been put in place to support customers and what priorities have been established in the response.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-6-3204	Public Safety and Government should work with Service Providers to educate the public on the proper use of N11 Access codes (e.g., 211, 311, 411 or 511 services) where available, such that it enables the 9-1-1 network and personnel to be exclusively focused on emergencies.	**Remarks/Comments section:** Proper use of all N11 codes, including 9-1-1, prevents exhaustion of resources of emergency personnel on non-emergency situations. **Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-6-5012	Network Operators, Service Providers, Public Safety and Equipment Suppliers should limit access to areas of critical infrastructure to essential personnel.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-6-5073	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should perform risk assessment on significant network changes (e.g., technology upgrades).	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-6-5131	Network Operators and Public Safety should provide appropriate security for emergency mobile units (both pre- and post-deployment) in order to protect against a coordinated terrorist attack on emergency communications capabilities.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-6-5132	Network Operators and Public Safety should identify primary and alternate transportation (e.g., air, rail, highway, boat) for emergency mobile units and other equipment and personnel.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-6-5133	Network Operators and Public Safety should minimize availability of information to a need to know basis regarding	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**

	locations where emergency mobile units and equipment are stored.			
8-6-5162	Network Operators, Service Providers, Public Safety and Equipment Suppliers should ensure adequate physical protection for facilities/areas that are used to house certificates and/or encryption key management systems, information or operations.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-6-5200	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should establish and implement procedures for the proper disposal and/or destruction of hardware (e.g., hard drives) that contain sensitive or proprietary information.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-6-5228	Network Operators, Service Providers and Equipment Suppliers should consider including cross-subsidiary (e.g. A LEC and its Wireless Business Unit) resource sharing and communications in business continuity plans to support emergency response and restoration.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-6-5231	Network Operators, Service Providers, Public Safety, and 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.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-6-8037	Network Operators, Service Providers, and Public Safety 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.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-6-8038	For Network Operators and Service Providers, a formal process during system or service development should exist in which a review of security controls and techniques is performed by a group independent of the development group, prior to deployment.	**Remarks/Comments section:** This review should be based on an organization's policies, standards, and guidelines, as well as best practices. In instances where exceptions are noted, mitigation techniques should be designed and	Highly Important	**Changed**

		deployed and exceptions should be properly tracked.		
8-7-0400	Network Operators, Service Providers, and Public Safety should establish measurements to monitor their network performance.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0401	Network Operators, Service Providers, and Public Safety should monitor their network to enable quick response to network issues.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-0402	Network Operators, Service Providers, and Public Safety should, where appropriate, design networks (e.g., Time Division Multiplexing (TDM) or Internet Protocol (IP)) to minimize the impact of a single point of failure (SPOF).	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-0403	Network Operators, Service Providers, and Public Safety should communicate maintenance windows to appropriate entities so proper methods of procedures can be invoked.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-0405	Network Operators, Service Providers, and Public Safety should periodically examine and review their networks to ensure that they meet the current design specifications.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0406	Network Operators, Service Providers, and Public Safety should, where appropriate, establish a process to ensure that spares inventory is kept current to at least a minimum acceptable release (e.g., hardware, firmware or software version).	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0412	Network Operators, Services Providers, and Public Safety to enhance security, should, by default, disable ICMP (Internet Control Message Protocol) redirect messages and IP source routing.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-0414	Network Operators, Service Providers, and Public Safety should establish plans for internal communications regarding maintenance activities and events that impact customers.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**

8-7-0415	Network Operators, Service Providers, and Public Safety should test the restoral process associated with critical data back-up, as appropriate. .	**Remarks/Comments section:** The goal is to demonstrate that data restoration is complete and works as expected **Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0416	Network Operators, Service Providers, and Public Safety should design and implement procedures for traffic monitoring, trending and forecasting so that capacity management issues may be addressed.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0417	Network Operators, Service Providers, and Public Safety should design and implement procedures to evaluate failure and emergency conditions affecting network capacity.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-0422	Network Operators, Service Providers, and Public Safety should collect failure-related data to perform cause analysis, impact and criticality analysis and failure trending.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0425	Network Operators, Service Providers, and Public Safety should maintain software version deployment records, as appropriate.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0428	Service Providers, Network Operators, and Public Safety should monitor software and hardware vulnerability reports and take the recommended action(s) to address problems, where appropriate. Reports and recommendations are typically provided by equipment suppliers and Computer Emergency Response Teams (CERTs).	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0442	Service Providers and Public Safety should consider measuring end-to-end path performance and path validity for both active and alternate routes.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0476	Network Operators, Public Safety, 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.	**Add Industry Role(s):** Public Safety	Critical	**Changed**

8-7-0504	Network Operators, Service Providers, and Public Safety, in order to facilitate asset management and increase the likelihood of having usable spares in emergency restorations, should consider maintaining "hot spares" (e.g., circuit packs electronically plugged in and interfacing with any element management system) as opposed to being stored in a cabinet for mission critical elements.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0505	Network Operators, Service Providers, and Public Safety should have procedures in place to process court orders and subpoenas for wire taps or other information.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0510	Network Operators, Service Providers, Public Safety and Equipment Suppliers should, by design and practice, manage critical Network Elements (e.g., Domain Name Servers, Signaling Servers, Gateway Servers) that are essential for network connectivity and subscriber service as critical systems (e.g., secure, redundant, alternative routing).	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-0513	Network Operators and Service Providers should maintain a 24x7x365 contact list of other providers and operators for service restoration of inter-connected networks and as appropriate share with Public Safety and Support providers.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0530	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should participate in interoperability testing (including services), as appropriate, to maintain reliability across connected networks.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0532	Network Operators and Public Safety should periodically audit the physical and logical diversity called for by network design of their network segment(s) and take appropriate measures as needed.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0541	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should store multiple software versions for critical network elements and be able to fallback to earlier versions.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**

8-7-0550	Network Operators, Public Safety, and Equipment Suppliers should implement procedures to ensure synchronization and security of databases.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0566	Network Operators, Service Providers and Public Safety should consider placing and maintaining 9-1-1 TDM or IP based networks 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).	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-0568	Network Operators, Service Providers and Public Safety should establish a routing plan so that in the case of lost connectivity or disaster impact affecting a Public Safety Answering Point (PSAP), 9-1-1 calls are routed to an alternate PSAP answering point.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-0571	Network Operators and Public Safety should consider deploying dual active 9-1-1 selective routing architectures to enable circuits from the serving end office to be split between two selective routers or Emergency Service Routing Proxies (ESRP) in order to eliminate single points of failure (SPOF) taking diversity between Selective Routers (SR) or ESRP and PSAP into consideration.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-0576	Network Operators and Service Providers should minimize impact from pre-planned high volume call events by invoking network management and congestion controls for affected end offices to maximize 9-1-1 call throughput.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0577	Network Operators, Service Providers and Public Safety responsible for Public Safety Answering Point (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.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-0578	Network Operators, Service Providers and Public Safety should actively engage in public education efforts aimed at informing the public of the capabilities and proper use of 9-1-	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**

	1.			
8-7-0579	Network Operators, Service Providers and Public Safety should routinely team to develop, implement, test, evaluate and update, as needed, plans for managing 9-1-1 disruptions (e.g., share information about network and system security and reliability where appropriate).	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-0580	Network Operators and Public Safety Authorities should apply redundancy and diversity where feasible, to all network links considered vital to a community's ability to respond to emergencies.	**Remarks/Comments section:** Security practices and concepts should be applied to the critical systems supporting Link Redundancy and Diversity. **Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-0581	Network Operators and Service Providers should include Automatic Location Identification (ALI) data for both traditional and alternate providers (e.g., Private Switch, Competitive Local Exchange Carrier (CLEC), Voice over Internet Protocol (VoIP)) in the ALI systems, where required.	**Modifications:** Acronyms defined and added additional clarity.	Critical	**Changed**
8-7-0603	Network Operators, Service Providers and Public Safety should establish policies and procedures that outline how critical network element databases will be backed up onto a storage medium (e.g., tapes, optical diskettes) on a scheduled basis.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0616	Network Operators and Service Providers should design and implement procedures to evaluate failure and emergency conditions affecting network capacity.	**Remarks/Comments section**: Note: This Best Practice could impact 9-1-1 operations.	Highly Important	**Changed**
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.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0622	Network Operators, Service Providers, Property Managers and Public Safety should use approved industry standards for Telecommunications Environmental Protection, DC Power Systems for key equipment locations (e.g., routers, central	**Remarks/Comments section:** Example ANSI T1.311-1998 **Add Industry Role(s):** Public Safety	Highly Important	**Changed**

	office switches, and other critical network elements) to reduce fires associated with DC power equipment.			
8-7-0635	Network Operators, Service Providers, Property Managers and Public Safety should ensure that AC surge protection is provided at the power service entrance to minimize the effects caused by lightning or extremely high voltages.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-0644	Network Operators, Service Providers, Property Managers and Public Safety should use over-current protection devices and fusing.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-0655	Network Operators, Service Providers, Property Managers and Public Safety should coordinate hurricane and other disaster restoration work with electrical and other utilities as appropriate.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-0657	Network Operators, Service Providers, Property Managers and Public Safety should design standby generator systems for fully automatic operation and for ease of manual operation, when required.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-0658	Network Operators, Service Providers, Property Managers and Public Safety should ensure generator life support systems (e.g., radiator fan, oil cooler fan, water transfer pumps, fuel pumps, engine start battery chargers) are on the essential Alternating Current (AC) buss of the generator they serve.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-0660	Network Operators, Service Providers, Property Managers and Public Safety should have a plan that is periodically verified for providing portable generators to offices with and without stationary engines.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0662	Network Operators, Service Providers, Property Managers and Public Safety should exercise power generators on a routine schedule in accordance with manufacturer's specifications. For example, a monthly 1 hour engine run on load, and a 5 hour annual run.	**Add Industry Role(s):** Public Safety	Critical	**Changed**

8-7-0668	Network Operators, Service Providers, Equipment Suppliers, Property Managers and Public Safety should clearly label the equipment served by each circuit breaker and fuse.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-0669	Network Operators, Service Providers, Property Managers and Public Safety should develop and/or provide appropriate emergency procedures for Alternating Current (AC) transfer.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0671	Network Operators, Service Providers, Property Managers and Public Safety should design and implement a preventive maintenance and inspection program for electrical systems.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0689	Network Operators, Service Providers and Public Safety should provide a separate "battery discharge" alarm for all critical infrastructure facilities, and where feasible, periodically (e.g., every 15 minutes) repeat the alarm as long as the condition exists.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-0690	Network Operators, Property Managers and Public Safety should consider providing power alarm redundancy so that no single point alarm system failure will lead to a network power outage.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-0695	Network Operators, Service Providers, Property Managers and Public Safety 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).	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0697	Network Operators, Service Providers, Equipment Suppliers and Public Safety should employ an "Ask Yourself" program as part of core training and daily operations.	**Remarks/Comments section:** This initiative is intended to reinforce the responsibility every employee has to ensure flawless network service. **Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-0699	Network Operators, Service Providers, Equipment Suppliers, Property Managers and Public Safety should design standby systems (e.g., power) to withstand harsh environmental conditions.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**

8-7-0701	Network Operators, Service Providers, Property Managers, and Public Safety should provide security for portable generators.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0758	Network Operators, Service Providers and Public Safety should, upon restoration of service in the case of an outage where 9-1-1 call completion is affected, make/request multiple test calls to the affected PSAP(s) to ensure proper completion.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-0760	Network Operators, Service Providers and Public Safety should maintain records that accurately track the diversity of internal wiring for office synchronization, including timing leads and power.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-0773	Network Operators, Service Providers, Property Managers, and Public Safety should perform annual capacity evaluation of power equipment, and perform periodic scheduled maintenance, including power alarm testing.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-0774	Network Operators, Service Providers , Equipment Suppliers, and Public Safety should provide warning signs to indicate precautions to be taken when powering on circuits that require special procedures	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-0780	Network Operators, Service Providers, and Public Safety should consider including coordination information of each other when developing disaster restoration and prioritization plans.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-1001	Network Operators, Service Providers, Equipment Suppliers, Property Managers, and Public Safety 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.	**Add Industry Role(s):** Public Safety	Critical	**Changed**

8-7-1004	Network Operators, Service Providers, Equipment Suppliers, Property Managers, and Public Safety 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.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-1005	Network Operators, Service Providers, Equipment Suppliers, and Public Safety should perform a Business Impact Analysis (BIA) to assess the impact of the loss of critical operations, support systems and applications.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-1009	Network Operators, Service Providers, Equipment Suppliers, and Public Safety 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).	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-1010	Network Operators, Service Providers, Equipment Suppliers, and Public Safety should designate personnel responsible for maintaining Business Continuity and Disaster Recovery Plans.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-1011	Network Operators, Service Providers, Equipment Suppliers, and Public Safety should establish alternative methods of communication for critical personnel.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-1015	Network Operators, Service Providers, and Public Safety should make available to the disaster recovery team "as-built" drawings of network sites.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-1018	Network Operators, Service Providers ,Equipment Suppliers and Public Safety should emphasize employee and public safety during a disaster and all phases of disaster recovery	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-1020	Network Operators, Service Providers, Public Safety 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.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**

8-7-1023	Network Operators, Service Providers, Public Safety 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.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-1024	Network Operators, Service Providers, Public Safety and Equipment Suppliers should plan for the possibility of a disaster occurring during a work stoppage.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-1026	Network Operators, Public Safety and Service Providers should consider creating a policy statement that defines a remote system access strategy, which may include a special process for disaster recovery.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-1028	Network Operators, Service Providers, Public Safety 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.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-1029	Network Operators, Public Safety and Service Providers should periodically review their portable power generator needs to address changes to the business.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-1031	Network Operators, Public Safety 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.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-1032	Network Operators, Public Safety 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.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**

8-7-1034	Network Operators and Public Safety 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.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-1035	Network Operators, Public Safety and Service Providers should include trial deployment of emergency mobile assets in disaster response exercises to evaluate level of personnel readiness.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-1037	Network Operators, Public Safety, 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.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-1058	Network Operators, Service Providers, Public Safety 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.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-1063	Network Operators, Public Safety 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., 9-1-1, GETS) receive proper priority during national emergency situations. Implementation in all networks should be in accordance with ANSI T1.111.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-1067	Network Operators, Public Safety, 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).	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
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	**Add Industry Role(s):** Public Safety	Important	**Changed**

	procedure to notify all impacted network operators, prior to launching an alert event.			
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).	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-3211	Network Operators, Public Safety 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 9-1-1 services.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-3212	Network Operators and Service Providers should consider including notification of Public Safety Authorities, as appropriate, in their trouble notification plans.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-3214	Public Safety Answering Points should avoid deploying an automatic ALI rebid function for wireless E9-1-1 calls. However, where deemed necessary, an automatic ALI rebid function should only be deployed for the initial bid to retrieve the Phase II location.	**Modifications:** Removed tagline and minor grammatical corrections.	Important	**Changed**
8-7-3215	For Network Operators that operate Mobile Switching Centers ("MSCs"), the MSC should default route 9-1-1 calls based on cell sector/tower location to the proper serving Public Safety Answering Point (PSAP) when necessary and where feasible.	**Modifications:** Removed tagline.	Important	**Changed**
8-7-3216	For Network Operators that cannot default route 9-1-1 calls based on cell sector/tower location, switch level defaulted calls should be routed to a "fast busy" tone or to an appropriate recorded announcement.	**Modifications:** Removed tagline.	Important	**Changed**
8-7-3217	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.	**Modifications:** Removed tagline.	Important	**Changed**

8-7-3218	Public Safety should provide Training to educate PSAP personnel as to the process to obtain E9-1-1 Phase II data.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-3219	Public Safety should provide training to educate PSAP personnel as to the proper meaning and interpretation of the E9-1-1 Phase II display parameters.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-3223	Network Operators, Public Safety and Service Providers should implement dedicated trunk groups between the Mobile Switching Center (MSC) end office or similar source and the E9-1-1 Selective Router (SR), based on the geography served by the default Public Safety Answering Points (PSAPs).	**Remarks/Comments section:** This should be done rather than aggregating traffic from centralized switching architectures serving wide spread geographic areas onto a single trunk group to the E9-1-1 Selective Router. This should be done in conjunction with the local PSAP jurisdictional authorities to ensure that correct choices are made. **Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-3225	Network Operators, Public Safety and Service Providers that deploy geographically diverse 9-1-1 Mobile Positioning Centers (MPC) with dual load sharing nodes should ensure that the utilization on either node is less than half of each node's capacity so that if one node fails the other node will absorb the load.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-3226	Network Operators, Public Safety and Service Providers operating Mobile Positioning Centers (MPC) should provide 24x7 network operations support.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-3227	Network Operators, Service Providers, Public Safety and Equipment Suppliers should deploy location solutions such that the E9-1-1 related data traffic between the Position Determining Entity (PDE) and the mobile subscriber associated with location determination should not interfere with the voice traffic, when feasible.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-3228	Network Operators, Service Providers, Public Safety and Equipment Suppliers that use Global Positioning System (GPS) enabled Phase II location solutions should ensure that	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**

	the GPS satellite location information (e.g., GPS ephemeris, almanac, etc.) is as current as is feasible to assist the handset in providing improved accuracy of the GPS fix, aiding in the reduction of the time of database responses and reduction of the number of database query rebids.			
8-7-3229	Network Operators, Public Safety and Service Providers that operate Mobile Positioning Centers (MPC)/ Gateway Mobile Location Centers (GMLC) should maintain local storage of record logs for a minimum of 7 days showing incoming successful requests from Emergency Services Message Entity (ESME) and outgoing responses to ESME.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-3230	Network Operators, Public Safety and Service Providers that produce location event records that include time-stamped call detail transactions should store these records for a minimum of 3 days.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-3231	Network Operators, Public Safety and Service Providers that use Global Positioning System (GPS) enabled Phase II location solutions should ensure that the GPS satellite location identification information (e.g., GPS ephemeris, almanac, etc.) is transmitted to the Phase II Mobile Subscriber or Position Determining Entities (PDE) as soon as is feasible after the E9-1-1 call commences in order to reduce the number of database query rebids.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-3233	Service Providers and Public Safety deploying wireless Phase II should work to ensure that Phase II accuracy is optimized and the performance trouble resolution process is followed as needed.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-5113	Network Operators, Service Providers, Public Safety and Property Managers, when feasible, should provide multiple cable entry points at critical facilities (e.g., copper or fiber conduit) avoiding single points of failure (SPOF).	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-5127	Network Operators, Service Providers, Equipment Suppliers and Public Safety should provide a Government Emergency Telecommunications Service (GETS) card to essential staff	**Add Industry Role(s):** Public Safety	Critical	**Changed**

	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).			
8-7-5128	Network Operators, Service Providers, Equipment Suppliers and Public Safety should maintain accurate records for Government Emergency Telecommunications Service (GETS) cards and Wireless Priority Service (WPS) phone assignments as staff changes occur.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-5130	Network Operators, Service Providers, Public Safety, Equipment Suppliers and the Government should conduct public and media relations in such a way as to avoid disclosing specific network or equipment vulnerabilities that could be exercised by a terrorist.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-5139	Network Operators, Service Providers, Public Safety and Equipment Suppliers should consider establishing procedures for managing personnel who perform functions at disaster area sites.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-5160	Public Safety, Network Operators, Service Providers, Equipment Suppliers and Property Managers should have contingency plans in place for the possible absence of critical personnel in their business continuity plan.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-5175	Network Operators, Service Providers, Public Safety and Equipment Suppliers should establish a proprietary information protection policy to protect proprietary information in their possession belonging to the company, business partners and customers from inadvertent, improper or unlawful disclosure. The policy should establish procedures for the classification and marking of information; storage, handling, transfer and transmission of information, retention guidelines and disposal/deletion of information.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-5196	Network Operators, Public Safety and Service Providers should ensure that contractors and Equipment Supplier	**Add Industry Role(s):** Public Safety	Critical	**Changed**

	personnel working in critical network facilities follow the current applicable MOP (Method of Procedures), which should document the level of oversight necessary.			
8-7-5204	Service Providers, Network Operators, Public Safety 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.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-5206	Network Operators, Service Providers, Public Safety and Property Managers should maintain sufficient fuel supplies for emergency/backup power generators running at full load and ensure contracted refueling is in place.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-5207	Network Operators, Service Providers, Public Safety 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).	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-5208	Network Operators, Service Providers, Equipment Suppliers, Public Safety and Property Managers should ensure that electrical work (e.g., AC and high current DC power distribution) is performed by licensed technicians.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-5223	Network Operators, Service Providers, Public Safety and Equipment Suppliers should establish a technical support plan that prevents the loss of one facility or location from disabling their ability to provide support.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-5225	Network Operators, Service Providers, Equipment Suppliers, Public Safety and Property Managers should ensure that Business Continuity Plan(s) are restricted to those with a	**Add Industry Role(s):** Public Safety	Important	**Changed**

	need-to-know.			
8-7-5227	Network Operators, Service Providers, Equipment Suppliers, Pubic Safety and Property Managers should perform after-action reviews of emergency response and restoration of major events to capture lessons learned (e.g., early warning signs) and to enhance emergency response and restoration plans accordingly. A process similar to NRIC VII, Focus Group 2B Report Appendices Appendix Z "Recovery Incident Response (IR) Post Mortem Checklist" can be used to capture and identify countermeasures to prevent or mitigate the impact of future incidents and to quickly and effectively restore service from such events in the future.	**Remarks/Comments section:** http://www.nric.org/meetings/docs/meeting_20041206/NRICVII_FG2B_December2004_BPs_Appendices.pdf **Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-5232	Network Operators, Service Providers, Pubic Safety 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.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-5234	Network Operators, Service Providers, Pubic Safety 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.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-5237	Network Operators, Service Providers, Pubic Safety and Equipment Suppliers should verify the integrity of system spares and replenish spares, as appropriate, as part of a disaster response and at the conclusion of a disaster response at a facility.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-5240	Network Operators, Service Providers, Equipment Suppliers, Pubic Safety and Property Managers should have a plan for responding to malfunctioning access control equipment to include determining restoration priorities for failed security systems after an event.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-5241	Network Operators, Service Providers, Pubic Safety and Equipment Suppliers should consider placing access and	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**

	facility alarm points to critical or sensitive areas on backup power.			
8-7-5258	Network Operators, Service Providers, Pubic Safety 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.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-5259	Network Operators, Service Providers, Equipment Suppliers, Pubic Safety 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.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-5260	Network Operators, Service Providers, Equipment Suppliers, Pubic Safety and Property Managers should provide any significant changes to access control procedures to affected personnel involved in a restoration.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-5281	Network Operators, Service Providers, Pubic Safety and Property Managers with buildings serviced by more than one emergency generator, should design, install and maintain each generator as a standalone unit that is not dependent on the operation of another generator for proper functioning, including fuel supply path.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-8030	For Network Operators, Service Providers, Public Safety and Equipment Suppliers, all Operations, Administration, Maintenance, and Provisioning (OAM&P) applications, systems, and interfaces should use session timers to disconnect, terminate, or logout authenticated sessions that remain inactive past some preset (but ideally configurable by the Administrator) time limit that is appropriate for operational efficiency and security.	**Add Industry Role(s):** Public Safety	Important	**Changed**

8-7-8065	Network Operators, Service Providers, Public Safety 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.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-8083	Authentication databases/files used by Network Operators, Service Providers, Public Safety, and Equipment Suppliers must be protected from unauthorized access, and must be backed-up and securely stored in case they need to be restored.	**Remarks/Comments section:** Filter access to the TCP and/or UDP ports serving the database at the network border. Use strong authentication for those requiring access. Prevent users from viewing directory and file names that they are not authorized to access. Enforce a policy of least privilege. Build a backup system in the event of loss of the primary system. Document and test procedures for backup and restoral of the directory. **Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-8086	Network Operators, Service Providers, Public Safety, and Equipment Suppliers based on the principles of least–privilege (the minimum access needed to perform the job) and separation of duties (certain users perform certain tasks) should develop capabilities and processes to determine which users require access to a specific device or application.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-7-8121	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should conduct regular audits of their Information Security practices.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-7-8131	Network Operators, Service Providers, and Public Safety Business Continuity and Recovery Plans should factor in potential Information Security threats of a plausible likelihood or significant business impact.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-7-8510	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should upon an occurrence of compromise or trust violations conduct a forensic analysis to determine the extent of compromise, revoke compromised keys, and establish new crypto keys as soon as possible, and	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**

	review crypto procedures to re-establish trust.			
8-8-0567	Network Operators, Service Providers, and Public Safety should spread 9-1-1 and Next Generation 9-1-1 access connections across similar equipment to avoid single points of failure and clearly mark plug-in level components and termination points as critical essential services that are to be treated with a high level of care.	**Remarks/Comments section:** This service provider equipment identification applies to E9-1-1 and may apply to some elements of NG9-1-1. **Add Industry Role(s):** Public Safety	Important	**Changed**
8-8-0569	Network Operators, Service Providers, and Public Safety should consider using the Public Switch Telephone Network (PSTN) as a backup to dedicated trunks for the 9-1-1 network during periods of network failure. In cases where the ability to deliver 9-1-1 calls to the Public Safety Answering Point (PSAP) through normal routing is interrupted by a failure (not all trunks busy conditions) consider forwarding the call over the PSTN to a telephone number specified and answered by Public Safety authorities. It is desirable for that specified telephone number to be a type that can provide the original Caller ID/Automatic Number Identification (ANI).	**Remarks/Comments section:** 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. **Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-8-0574	Network Operators, Service Providers, and Public Safety should actively 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.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-8-0575	Network Operators, Service providers, and Public Safety 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).	**Remarks/Comments section:** These include, but are not limited to, ALI, MPC/GMLC, VPC systems, and LIS. **Add Industry Role(s):** Public Safety	Critical	**Changed**
8-8-0599	Network Operators, Service Providers, and Public Safety should conduct exercises periodically to test a network's	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**

	operational readiness for various types of events (e.g., hurricane, flood, nuclear, biological, and chemical), through planned, simulated exercises being as authentic as practical including scripts prepared in advance with team members playing their roles as realistically as possible.			
8-8-0674	Network Operators, Service Providers, Property Managers, and Public Safety should initiate or continue a modernization program to ensure that outdated power equipment is phased out of plant considering capabilities of smart controllers, local and remote monitoring and control, alarm systems when updating power equipment, and being integrated into engineering and operational strategies.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-8-0786	Network Operators, Service Providers, and Public Safety should consider allowing Equipment Suppliers or third party Service Providers remote secured access to vital hardware components.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-8-0797	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider creating a workforce augmentation plan prior to a pandemic or other crisis situation.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-8-0900	Network Operators and Service Providers operating a Virtual Private Cloud (VPC), Mobile Positioning Center (MPC), or Gateway Mobile Location Center (GMLC) should strive to reduce bad shell record data routing errors for 9-1-1 pseudo Automatic Number Identification (pANI) due to incorrect Master Street Address Guide (MSAG) to Emergency Service Number (ESN) to Public Safety Answering Point (PSAP) relationship (MSAG-ESN-PSAP) by following National Emergency Number Association (NENA) 56-504 "NENA VoIP 9-1-1 Deployment and Operational Guidelines" to fully test routing for every pANI placed in service.	**Remarks/Comments section:** See Testing in Section 5.1.4 of NENA 56-504 "NENA VoIP 9-1-1 Deployment and Operational Guidelines".	Highly Important	**Changed**
8-8-3224	Network Operators, Service Providers, and Public Safety should use dedicated Signaling System 7 (SS7) or Multi-Frequency (MF) controlled trunk groups for the normal routing of 9-1-1 calls from originating switching entities to 9-	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**

	1-1 Selective Routers (SRs) rather than using shared Public Switched Telephone Network (PSTN) trunk arrangements and where appropriate and necessary supported by service level agreements.			
8-8-8008	Network Operators, Service Providers, and Public Safety should implement architectures that partition or segment networks and applications using means such as firewalls, demilitarized zones (DMZ), or virtual private networks (VPN) so that contamination or damage to one asset does not disrupt or destroy other assets. In particular, where feasible, it is suggested user traffic networks, network management infrastructure networks, customer transaction system networks, and enterprise communication/business operations networks be separated and partitioned from one another.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-8-8035	Network Operators, Service Providers, and Public Safety should include steps to appropriately test all patches/fixes in a test environment prior to distribution into the production environment in their patch/fix policy and process guidelines.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-8-8039	Service Providers, Network Operators, and Public Safety should perform a verification process to ensure that patches/fixes are actually applied as directed throughout the organization. Exceptions should be reviewed and the proper patches/fixes actually applied.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-8-8061	Service Providers, Network Operators, and Public Safety should establish a set of standards and procedures for dealing with computer security events that should be part of the overall business continuity/disaster recovery plan, exercised periodically and revised as needed, and cover likely threats to those elements of the infrastructure which are critical to service delivery/business continuity. See Appendix X and Y of the NRIC VII, Focus Group 2B Report Appendices.	**Remarks/Comments section:** http://www.nric.org/meetings/docs/meeting_20041206/NRICVII_FG2B_December2004_BPs_Appendices.pdf **Add Industry Role(s):** Public Safety	Critical	**Changed**
8-8-8064	Service Providers, Network Operators, and Public Safety should generate and collect security-related event data for critical systems (i.e., syslogs, firewall logs, IDS alerts, remote access logs, etc.). Where practical, this data should be	**Add Industry Role(s):** Public Safety	Critical	**Changed**

	transmitted to secure collectors for storage and should be retained in accordance with a data retention policy. A mechanism should be enabled on these systems to ensure accurate timestamps of this data (e.g., Network Time Protocol).			
8-8-8068	Service Providers, Network Operators, Public Safety, and Equipment Suppliers should develop and practice a communications plan as part of the broader Incident response plan identifying key players to include as many of the following items as appropriate: contact names, business telephone numbers, home telephone 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 (e.g., alpha pagers, internet, satellite phones, VOIP, private lines, smart phones) balancing the value of any alternate method against the security and information loss risks introduced.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-8-8073	Service Providers, Network Operators, and Public Safety should deploy Intrusion Detection/Prevention Tools (IDS/IPS) 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.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-8-8103	Service Providers, Network Operators, and Public Safety should deploy malware protection tools where feasible, establish processes to keep signatures current, and establish procedures for reacting to an infection.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-8-8136	Service Providers, Network Operators and Public Safety 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.	**Add Industry Role(s):** Public Safety	Important	**Changed**

8-8-8139	Service Providers, Network Operators and Public Safety should review and analyze security-related event data produced by critical systems on a regular basis to identify potential security risks and issues. Automated tools and scripts can aid in this analysis process and significantly reduce the level of effort required to perform this review.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-8-8502	When a compromise occurs, or new exploits are discovered, Service Providers, Network Operators and Public Safety 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.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-8-8506	Following a compromise and reestablishment of lost service, Service Providers, Network Operators and Public Safety 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.	**Add Industry Role(s):** Public Safety	Highly Important	**Changed**
8-8-8508	Immediately following incident recovery, Service Providers, Network Operators, and Public Safety should re-evaluate the adequacy of existing security architecture and implement revisions as needed.	**Remarks/Comments section:** 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. **Add Industry Role(s):** Public Safety	Important	**Changed**
8-8-8522	Upon discovery of an unsanctioned device on the organizational network, Service Providers, Network Operators, and Public Safety should investigate to determine ownership and purpose/use of the device. Where possible, this phase should be non-alerting (i.e., log reviews, monitoring of network traffic, review of abuse complaints for suspect IP address) to determine if the use is non-malicious or malicious/suspect. If use is determined to be non-malicious, employ available administrative tools to correct behavior and educate user. Conduct review of policies to determine:	**Add Industry Role(s):** Public Safety	Important	**Changed**

	1. If additional staff education regarding acceptable use of network/computing resources is required 2. If processes should be redesigned / additional assets allocated to provide a sanctioned replacement of the capability. Was the user attempting to overcome the absence of a legitimate and necessary service the organization was not currently providing so that s/he could perform their job? If the use is deemed malicious/suspect, coordinate with legal counsel: 1. Based on counsel's advice, consider collecting additional data for the purposes of assessing 2. Depending on the scope of the misuse, consider a referral to law enforcement.			
8-8-8554	Insomuch as is possible without disrupting operational recovery, Service Providers, Network Operators and Public Safety should handle and collect information as part of a computer security investigation in accordance with a set of generally accepted evidence-handling procedures.	**Remarks/Comments section:** Example evidence handling processes are provided in Appendix X, Section 2f of the NRIC VII, Focus Group 2B Report Appendices. **Add Industry Role(s):** Public Safety	Critical	**Changed**
8-8-8564	After responding to a security incident or service outage, Service Providers, Network Operators and Public Safety should follow processes similar to those outlined in Appendix X of the NRIC VII, Focus Group 2B Report Appendices to capture lessons learned and prevent future events.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-8-8629	Equipment Suppliers, Service Providers, Network Operators, and Public Safety should have processes in place to ensure that all third party software (e.g. operating system) have been properly patched with the latest security patches and that the system works correctly with those patches installed.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-8-8727	Network Operators, Service Providers and Public Safety should implement industry guidelines for validating physical diversity, and consider performing signaling link diversification validation on a scheduled basis (e.g., twice a year).	**Remarks/Comments section:** Processes and procedures should exist for tracking discrepancies and maintaining a historical record. Re: PBX & statewide networks - sonic ring could be influenced by this.	Important	**Changed**

		Add Industry Role(s): Public Safety		
8-8-8748	Service providers, Network Operators, Equipment Vendors and Public Safety should test new devices to identify unnecessary services, outdated software versions, missing patches, and misconfigurations, and validate compliance with or deviations from an organization's security policy prior to being placed on a network.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-8-8755	Service Providers, Network Operators, Equipment Suppliers and Public Safety should utilize automated (where possible) Patch Management to quickly deploy patches for known vulnerabilities. PSAP software version control is important for backroom PSAP systems	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-8-8756	Network Operators and Public Safety 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.	**Add Industry Role(s):** Public Safety	Critical	**Changed**
8-8-8757	Service Providers, Network Operations and Public Safety should set policy within each corporation or agency to provide guidance when there is a security breach.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-8-8771	Service Providers, Network Operators, and Public Safety should consider implementing a control-signaled (i.e. SIP) network 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.	**Add Industry Role(s):** Public Safety	Important	**Changed**
8-8-8772	Service Providers, Network Operators, Equipment Suppliers and Public Safety 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.	**Add Industry Role(s):** Public Safety	Critical	**Changed**

8-8-0901	Voice over Internet Protocol (VoIP) Service Providers (VSP) 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) to immediately reduce the risk of misrouting a block of callers at a particular facility and in turn reduce the liability for those same entities.	**Remarks/Comments section:** 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.	Important	**Changed**
8-8-0902	Service Providers and Network Operators when reconfiguring their network (e.g., changes to Virtual Private Cloud (VPC), Mobile Position Center (MPC), Gateway Mobile Location Center (GMLC), or Emergency Services Gateway (ESGW)) should assess the impact on the routing of 9-1-1 calls.	**Modifications:** Acronyms defined and BP re-structured into two BPs (see New WG8-2-10).	Highly Important	**Changed**
UNCHANGED BEST PRACTICES WITH NOTE ADDITION ONLY				
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.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0418	Back-out MOPs: Network Operators and Service Providers should, where appropriate, have a documented back-out plan as part of a Method of Procedure (MOP) for scheduled and unscheduled maintenance activities.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0423	Cable Management: Equipment Suppliers should provide cable management features and installation instructions for network elements that maintain cable bend radius, provide strain relief to prevent cable damage, ensure adequate cable connector spacing for maintenance activities, and provide clear access for cable rearrangement (i.e. moves/add/deletes) and FRU (Field Replaceable Unit) swaps.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**

8-7-0447	Network Operators and Service Providers should consider establishing a customer advocacy function to take part in the development and scheduling of changes in order to minimize impact.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0449	Network Operators and Service Providers should, where feasible, deploy SPAM controls in relevant nodes (e.g., message centers, email gateways) in order to protect critical network elements and services.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
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).	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0519	Capacity Monitoring: Network Operators and Service Providers should engineer and monitor networks to ensure that operating parameters are within capacity limits of their network design (e.g., respect limitations of deployed packet switches, routers and interconnects, including "managed networks" and "managed CPE"). These resource requirements should be re-evaluated as services change or grow.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0529	Network Operators, Service Providers and Equipment Suppliers should support sharing of appropriate information pertaining to outages as an effort to decrease the potential of further propagation (e.g., ATIS NIIF reference document).	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
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).	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
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	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**

	distributed locations to provide service assurance (e.g., maintainability, connectivity, security, reliability) consistent with other critical network elements.			
8-7-0548	Post Mortem Review: Network Operators and Service Providers should have an internal post mortem process to complete root cause analysis of major network events with follow-up implementation of corrective and preventive actions to minimize the probability of recurrence. Network Operators and Service Providers should engage Equipment Suppliers and other involved parties, as appropriate, to assist in the analysis and implementation of corrective measures.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0584	Service Providers, Network Operators and Equipment Suppliers and Government representatives [of the National Security Emergency Preparedness (NS/EP) community] should work together to support appropriate industry and international organizations to develop and implement NS/EP standards in packet networks.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
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.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0592	Network Operators and Service Providers should provide duplicated, non-co-located maintenance administration, surveillance and support for network elements. Monitoring and administration locations should be minimized to provide consistency of operations and overall management.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0594	Maintaining SS7 Link Diversity: Network Operators and Service Providers should follow industry guidelines for validating SS7 link diversity. SS7 link diversification validation should be performed at a minimum of twice a year, and at least one of those validations should include a physical validation of equipment compared to the recorded documentation of diversity.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**

8-7-0595	Network Operators and Service Providers should be aware of the dynamic nature of peak traffic periods and should consider scheduling potentially service-affecting procedures (e.g., maintenance, high risk procedures, growth activities) so as to minimize the impact on end-user services.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0596	Network Operators and Service Providers should carefully review all re-home procedures, undertake meticulous pre-planning before execution, and ensure that re-home procedures are carefully followed.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0600	Network Operators and Service Providers should establish and document a process to plan, test, evaluate and implement major change activities onto their network.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0601	Network Operators and Service Providers should restrict commands available to technicians to ensure authorized access and use, and maintain, manage and protect an audit trail.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0602	Network Operators and Service Providers should establish procedures to reactivate alarms after provisioning or maintenance activities (when alarms are typically deactivated).	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0605	Network Operators and Service Providers should assess the synchronization needs of the network elements and interfaces that comprise their networks to develop and maintain a detailed synchronization plan.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0608	Network Operators and Service Providers should utilize network surveillance and monitoring to keep overflow traffic conditions from adversely affecting networks. Interconnecting companies should address the control of overflow conditions in their bilateral agreements.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0612	Network Operators and Service Providers should verify both local and remote alarms and remote network element maintenance access on all new critical equipment installed in the network, before it is placed into service.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**

8-7-0615	Network Operators and Service Providers should test complex configuration changes before and after the change to ensure the appropriate and expected results.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0617	Route Controls: Network Operators and Service Providers should ensure that routing controls are implemented and managed to prevent adverse routing conditions.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0630	Network Operators, Service Providers, Equipment Suppliers and Property Managers should develop and execute standard Method of Procedure (MOP) for all vendor work in or external to equipment locations with emphasis on service continuity and safety precautions.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0649	Network Operators and Service Providers and Property Managers should ensure critical network facilities have appropriate fire detection and alarm systems.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
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.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0654	Network Operators, Service Providers and Property Managers should not normally enter into power curtailment or load sharing contracts with electric utilities.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0656	Network Operators and Service Providers should establish a general requirement for power conditioning, monitoring and protection for sensitive equipment.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0663	Network Operators, Service Providers and Property Managers should coordinate scheduled power generator tests with all building occupants to avoid interruptions.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0664	Network Operators, Service Providers and Equipment Suppliers should provide indicating type control fuses on the front of the power panels, including smaller distribution panels.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**

8-7-0665	Network Operators, Service Providers and Property Managers should provide and maintain accurate single line drawings of AC switch equipment on-site.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0667	Network Operators, Service Providers and Property Managers should keep circuit breaker racking/ratchet tools, spare fuses, fuse pullers, etc. readily available.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
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.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0693	Network Operators, Service Providers and Property Managers should emphasize the use of Methods Of Procedures (MOPs), vendor monitoring, and performing work on in-service equipment during low traffic periods.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0694	Network Operators and Service Providers should check for current flow in cables with AC/DC clamp-on ammeters before removing the associated fuses or opening the circuits during removal projects.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0700	Network Operators, Service Providers and Equipment Suppliers should consider the need for power expertise/power teams.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0736	Network Operators should develop and implement a rapid restoration program for cables and facilities.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0745	Equipment Suppliers should design equipment so that changes and upgrades are non-service impacting.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0750	Equipment Suppliers should provide a mechanism for feature activation or deactivation that is not service impacting to end-users (e.g., avoid re-boot, re-start or re-initialization).	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**

8-7-0759	Network Operators and Service Providers should ensure that engineering, design, and installation processes address how new network elements are integrated into the office and network synchronization plan(s).	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0766	Service Providers should consider using a minimum interoperable subset for VoIP coding standards (for example, TI 811 mandates the use of G.711) in a VoIP-to-PSTN gateway configuration in order to achieve interoperability and support all types of voiceband communication (e.g., DTMF tones, facsimile, TTY/TDD).	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0775	Network Operators and Service Providers should consult and update the synchronization plan whenever facility (e.g., intra-/inter-office or inter-provider interconnect circuits) rearrangements, additions, deletions, or consolidations are planned. Verify the completed changes against the synchronization plan.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0805	Service Providers, Network Operators and Equipment Suppliers should work to establish operational standards and practices that support broadband capabilities and interoperability (e.g., video, voice, data, wireless).	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0819	For the deployment of Residential Internet Access Service, Network Operators should provide backup power for broadband network equipment when economically and technically practical.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-7-0823	For the deployment of Residential Internet Access Service, Network Operators, Service Providers and Equipment Suppliers should design, build, and operate broadband networks considering performance aspects of the data facilities employed, such as: packet loss ratio, Bit Error Ratio, latency, and compression, where feasible.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
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,	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**

	HVAC units, etc. for emergency use or service augmentation for planned events (e.g., National Special Security Event (NSSE)).			
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).	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
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.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-8-8005	Document Single Points of Failure: Service Providers and Network Operators should implement a continuous engineering process to identify and record single points of failure and any components that are critical to the continuity of the infrastructure. The process should then pursue architectural solutions to mitigate the identified risks as appropriate.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-8-8018	Hardening OAM&P User Access Control: Service Providers, Network Operators, and Equipment Suppliers should, for OAM&P applications and interfaces, harden the access control capabilities of each network element or system before deployment to the extent possible (typical steps are to remove default accounts, change default passwords, turn on checks for password complexity, turn on password aging, turn on limits on failed password attempts, turn on session inactivity timers, etc.). A preferred approach is to connect each element or system's access control mechanisms to a robust AAA server (e.g., a RADIUS or TACAS server) with properly hardened access control configuration settings.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-8-8019	Hardening OSs for OAM&P: Service Providers, Network Operators, and Equipment Suppliers with devices equipped with operating systems used for OAM&P should have	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**

	operating system hardening procedures applied. Harding procedures include (a) all unnecessary services are disabled; (b) all unnecessary communications pathways are disabled; (c) all critical security patches have been evaluated for installations on said systems/applications; and d) review and implement published hardening guidelines, as appropriate. Where critical security patches cannot be applied, compensating controls should be implemented.			
8-8-8026	Distribution of Encryption Keys: When Service Providers, Network Operators, and Equipment Suppliers use an encryption technology in the securing of network equipment and transmission facilities, cryptographic keys must be distributed using a secure protocol that: a) Ensures the authenticity of the sender and recipient, b) Does not depend upon secure transmission facilities, and c) Cannot be emulated by a non-trusted source.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-8-8032	Patching Practices: Service Providers, Network Operators, and Equipment Suppliers should design and deploy a patching process based on industry recommendations, especially for critical OAM&P systems.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-8-8034	Software Patching Policy: Service Providers and Network Operators should define and incorporate a formal patch/fix policy into the organization's security policies.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
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.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
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	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**

	rate limiting traffic. Network engineers must understand the capabilities of the devices and how to employ them to maximum effect. Wherever practical, mission critical systems should be deployed in clustered configuration allowing for load balancing of excess traffic and protected by a purpose built DoS/DDoS protection device. Operators of critical infrastructure should deploy DoS survivable hardware and software whenever possible.			
8-8-8079	Use Strong Passwords: Service Provider, Network Operators, and Equipment Suppliers should create an enforceable policy that considers different types of users and requires the use of passwords or stronger authentication methods. Where passwords can be used to enhance needed access controls, ensure they are sufficiently long and complex to defy brute force guessing and deter password cracking. To assure compliance, perform regular audits of passwords on at least a sampling of the systems.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-8-8080	Change Passwords on a Periodic Basis: Service Providers, Network Operators, and Equipment Suppliers should change passwords on a periodic basis implementing a policy which considers different types of users and how often passwords should be changed. Perform regular audits on passwords, including privileged passwords, on system and network devices. If available, activate features across the user base which force password changes.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-8-8081	Protect Authentication Methods: Service Providers, Network Operators, and Equipment Suppliers should develop an enforceable password policy, which considers different types of users, requiring users to protect, as applicable, either (a) the passwords they are given/create or (b) their credentials for two-factor authentication.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
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	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**

	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.			
8-8-8111	Protect Sensitive Data in Transit for Externally Accessible Applications: Service Providers and Network Operators should encrypt sensitive data from web servers, and other externally accessible applications, while it is in transit over any networks they do not physically control.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
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.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
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.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
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.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-8-8509	Recover from Poor Network Isolation and Partitioning: When, through audit or incident, a co-mingling of data or violation of a trust relationship is discovered, Service Providers and Network Operators should, as part of a post-	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**

	mortem process, review segmentation design to evaluate adequacy of the architecture and data isolation.			
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.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-8-8540	Recover from Unauthorized Remote OAM&P Access: When an unauthorized remote access to an OAM&P system occurs, Service Providers and Network Operators should consider terminating all current remote access, limiting access to the system console, or other tightened security access methods. Continue recovery by re-establishing new passwords, reloading software, running change detection software, or other methods, continuing quarantine until recovery is validated, as practical.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
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 Security Focus Mailing Lists.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-8-8647	Service Standards: Service Providers should develop and implement security event logging systems and procedures to allow for collection of security related events.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**

8-8-8648	General: Service Providers and Network Operators [that provide or manage Customer Premise Equipment (CPE)] should ensure that initial configurations are secure.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-8-8725	Signaling DoS Protection: Network Operators should establish alarming thresholds for various message types to ensure that DoS conditions are recognized. Logs should be maintained and policies established to improve screening and alarming thresholds for differentiating legitimate traffic from DoS attacks.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-8-8729	Signaling Services Requested Changes: Network Operators should establish policies and processes for adding and configuring network elements, that include approval for additions and changes to configuration tables (e.g., screening tables, call tables, trusted hosts, and calling card tables). Verification rules should minimize the possibility of receiving inappropriate messages.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-8-8759	Recover from Unauthorized Use: Network Operators and Service Providers should remove invalid records whenever it is determined that a network element has been modified without proper authorization, or rollback to the last valid version of record. The attack should be investigated to identify potential security changes.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
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.	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**
8-8-8773	Social Engineering: Network Operators, Service Providers and Equipment Suppliers should establish policies in preventing socially engineered attacks, but perhaps the most important step is educating employees to make them aware of the danger of social engineering. Source: http://www.windowsecurity.com/articles/Social_Engineers.ht	**Remarks/Comments section:** Note: This Best Practice could impact 9-1-1 operations.		**Unchanged**

	ml • Training the front-line employees through case studies and understanding the need to recognize social engineering threats and its harmful consequences. The training must include: 1- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company. 2- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information. 3- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email. 4- Don't send sensitive information over the Internet before checking a website's security (see Protecting Your Privacy for more information). 5- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).			

	6- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).			

8 Appendix 3 – Consumer Best Practices

CSRIC III Best Practice Number	CSRIC III Best Practice	CSRIC III BP Reference/Comments	Best Practice Status	CSRIC III (New/Changed/ Unchanged/ Deleted)
NEW CATEGORY - CONSUMER BEST PRACTICES				
WG8-3-1	Consumers should dial 9-1-1 if they are unsure of whether their situation is an emergency requiring Police, Fire, Emergency Medical Services or other emergency agency response or assistance.	**Network Types(s):** Children; Employees; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Business; Family Education; What to Say and Do	Critical	**New Consumer**
WG8-3-2	9-1-1 Callers should know the location of their emergency and should be able to provide it to the 9-1-1 call taker when asked.	**Network Types(s):** Children; Employees; Parents/Guardians/Caregivers **Industry Role(s):** 9-1-1 Callers **Keywords(s):** Business; Family Education; Knowing Your Location; Residential; What to Say and Do	Critical	**New Consumer**
WG8-3-3	Consumers should install telephones so that all potential 9-1-1 callers are able to physically reach at least one phone at their location.	**Network Types(s):** Business Owners; Home Owners **Industry Role(s):** Consumers **Keywords(s):** Business; Device Use; Residential; Wireless; Wireline	Critical	**New Consumer**
WG8-3-4	Consumers should teach children their name, parents name, telephone number, address, etc., and to provide that to the 9-1-1 call taker when asked.	**Network Types(s):** Children; Home Owners; Parents/Guardians/Caregivers; Teachers/Trainers **Industry Role(s):** Consumers **Keywords(s):** Family Education; Knowing Your	Critical	**New Consumer**

		Location; Residential; Training Methods; What to Say and Do		
WG8-3-5	Consumers should teach children to stay on the line with a 9-1-1 operator until instructed to hang up as long as it is safe to do so.	**Network Types(s):** Children; Home Owners; Parents/Guardians/Caregivers; Teachers/Trainers **Industry Role(s):** Consumers **Keywords(s):** Family Education; Knowing Your Location; Residential; Training Methods; What to Say and Do	Critical	**New Consumer**
WG8-3-6	Consumers should report missing street signs or other directional marking to appropriate authorities when noted.	**Network Types(s):** Business Owners; Employees; Government; Home Owners **Industry Role(s):** Consumers **Keywords(s):** Business; Family Education; Residential; When to Call	Critical	**New Consumer**
WG8-3-7	9-1-1 Callers should stay calm when calling 9-1-1 and clearly provide information about their emergency when asked.	**Network Types(s):** Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** 9-1-1 Callers **Keywords(s):** Business; Family Education; Knowing Your Location; Residential; What to Say and Do	Critical	**New Consumer**
WG8-3-8	TTY/TDD users without access to Relay Services should dial 9-1-1, preferably from a landline phone.	**Network Types(s):** Business Owners; Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** TTY/TDD Users **Keywords(s):** Alternate Methods; Business; Device Use; Family Education; What to Say and Do; Wireline	Critical	**New Consumer**

WG8-3-9	9-1-1 Callers should not hang up when calling from a wireless device and unable to speak. Keeping the phone line open allows 9-1-1 call takers to obtain approximate location and/or hear background noises.	**Network Types(s):** 9-1-1 Agencies; Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** 9-1-1 Callers **Keywords(s):** Business; Emergency Personnel; Device Use; Family Education; Residential; What to Say and Do; Wireless	Critical	**New Consumer**
WG8-3-10	TTY/TDD Users should remain calm, and remember to place the phone handset in the TTY receiver before dialing 9-1-1.	**Network Types(s):** Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** TTY/TDD Users **Keywords(s):** Alternate Methods; Business; Device Use; Family Education; Residential; What to Say and Do	Critical	**New Consumer**
WG8-3-11	TTY/TDD Users should communicate to the 9-1-1 call taker what is needed (e.g., Police, Fire, or Emergency Medical Services (EMS)) and provide their name, phone number, and the address of the emergency.	**Network Types(s):** Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** TTY/TDD Users **Keywords(s):** Alternate Methods; Business; Device Use; Family Education; Knowing Your Location; Residential; What to Say and Do	Critical	**New Consumer**
WG8-3-12	9-1-1 Callers should be aware when using Video Relay Service (VRS) or Internet Protocol (IP) Relay that a call may take several minutes to connect before a conversation can be started and hanging up may prevent a connection to 9-1-1 call takers.	**Network Types(s):** Business Owners; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** 9-1-1 Callers **Keywords(s):** Alternate Methods; Business; Device Use; Family Education; Next Generation; Residential; What to Say and Do	Critical	**New Consumer**
WG8-3-13	9-1-1 Callers should be aware that location information through a Video Relay Service (VRS) or Internet Protocol	**Network Types(s):** Business Owners; Employees; Home Owners;	Critical	**New Consumer**

	(IP) Relay may not always be provided to 9-1-1 call takers and should be prepared to provide an address, cross streets, or landmarks as necessary.	Parents/Guardians/Caregivers **Industry Role(s):** 9-1-1 Callers **Keywords(s):** Alternate Methods; Business; Device Use; Family Education; Next Generation; Residential; What to Say and Do		
WG8-3-14	Consumers should register and provide their physical address with their service provider when using Voice over Internet Protocol (VoIP) whenever activating, updating, or moving services to keep their 9-1-1 emergency services location accurate.	**Network Types(s):** Business Owners; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Business; Device Use; Family Education; Next Generation; Residential; Updating Information; Wireless; Wireline	Critical	**New Consumer**
WG8-3-15	Consumers should be aware that 9-1-1 centers, in most cases, cannot receive text messages, photos, or video and when needing 9-1-1 emergency assistance and should dial 9-1-1 on their phone for help.	**Network Types(s):** 9-1-1 Agencies; Business Owners; Employees; Home Owners; Parents/Guardians/Caregivers; Teachers/Trainers **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Emergency Personnel; Device Use; Family Education; Next Generation; Residential; Training Methods; When to Call	Critical	**New Consumer**
WG8-3-16	Consumers should limit calls during periods of natural or man-made disasters to reduce network congestion.	**Network Types(s):** 9-1-1 Agencies; Business Owners; Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Business; Device Use; Family Education; Residential; When to Call; Wireless; Wireline	Critical	**New Consumer**
WG8-3-17	Consumers should attempt to communicate via other mechanisms such as text, e-mail, or other social media in	**Network Types(s):** Business Owners; Children; Employees; Home Owners;	Critical	**New Consumer**

	cases where non-emergency calls cannot be completed during disaster situations.	Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Business; Device Use; Family Education; Residential; When to Call; Wireless; Wireline		
WG8-3-18	9-1-1 callers should wait at least 10 seconds if disconnected before redialing 9-1-1 to provide time for the call taker to attempt to call back.	**Network Types(s):** Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** 9-1-1 Callers **Keywords(s):** Business; Device Use; Family Education; Residential; What to Say and Do	Critical	**New Consumer**
WG8-3-19	Consumers with disabilities should check with local law enforcement officials to see if they have additional systems to inform public safety agencies of pertinent information or needs for the caller.	**Network Types(s):** Business Owners; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Device Use; When to Call	Critical	**New Consumer**
WG8-3-20	Consumers with disabilities should ensure that any additional information databases that they update with law enforcement officials are kept current.	**Network Types(s):** Business Owners; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Residential; Updating Information	Critical	**New Consumer**
WG8-3-21	Consumers with personal care assistants should work with that person to decide on how they will communicate during an emergency or if they become separated.	**Network Types(s):** Children; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Device Use; Family Education; Knowing Your Location; Residential; What to Say and Do; When to Call	Critical	**New Consumer**

WG8-3-22	Consumers with special medical needs should give consideration to the use of a medical alert system to contact emergency service providers on their behalf if they need to contact emergency services.	**Network Types(s):** Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Device Use; Family Education; Knowing Your Location; Residential; When to Call	Critical	**New Consumer**
WG8-3-23	Consumers should be aware that most 9-1-1 centers do not currently have the ability to receive any type of multi-media or text messaging.	**Network Types(s):** Business Owners; Employees; Home Owners; Parents/Guardians/Caregivers; Teachers/Trainers **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Device Use; Family Education; Residential; Training Methods	Critical	**New Consumer**
WG8-3-24	Consumers should always contact 9-1-1 directly rather than rely on a friends or family notification feature to obtain help during an emergency.	**Network Types(s):** Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Device Use; Family Education; Residential	Critical	**New Consumer**
WG8-3-25	Consumers with traditional landline phone service should keep at least one phone (e.g., a non-cordless phone) that does not require external AC power to be available in emergencies.	**Network Types(s):** Business Owners; Home Owners **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Device Use; Residential; Wireline	Critical	**New Consumer**
WG8-3-26	Consumers should limit use of their mobile devices to watch streaming videos during, or immediately after a disaster to help reduce network congestion and to allow potential	**Network Types(s):** Business Owners; Children; Employees; Home Owners; Parents/Guardians/Caregivers	Critical	**New Consumer**

	emergency traffic (e.g. 9-1-1) to use the network.	**Industry Role(s):** Consumers **Keywords(s):** Business; Device Use; Family Education; Residential		
WG8-3-27	Consumers should dial the 3-1-1 non-emergency number for information and non-emergencies if available in their community.	**Network Types(s):** Business Owners; Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Device Use; Family Education; Residential; When to Call; Wireless; Wireline	Highly Important	**New Consumer**
WG8-3-28	Consumers should be aware that Smart Phone Applications may not work properly if a user has location services disabled on their phone to conserve power.	**Network Types(s):** Business Owners; Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Device Use; Family Education; Residential; When to Call; Wireless	Highly Important	**New Consumer**
WG8-3-29	Consumers (e.g., business, multiple tenant locations, campus environments, medical campuses, schools, etc.) should determine if there are special laws governing the location identification of 9-1-1 callers upon their property.	**Network Types(s):** Business Owners; Government **Industry Role(s):** Consumers **Keywords(s):** Business; Device Use; Wireless; Wireline	Highly Important	**New Consumer**
WG8-3-30	Consumers using "smart phones" should call 9-1-1 directly rather than attempting to use a smart phone application service.	**Network Types(s):** Business Owners; Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers	Highly Important	**New Consumer**

		Keywords(s): Alternate Methods; Business; Device Use; Family Education; Residential; What to Say and Do; When to Call; Wireless		
WG8-3-31	Consumers should maintain a list of emergency numbers (i.e., In Case of Emergency [ICE]) in their mobile phones to assist Emergency Service Providers if necessary.	**Network Types(s):** Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Business; Device Use; Family Education; Residential; Updating Information	Highly Important	**New Consumer**
WG8-3-32	9-1-1 Callers should not hang up if they dial 9-1-1 by mistake. This helps to prevent unnecessary follow-up by the 9-1-1 call center or public safety authorities and allows the caller to explain the call was a mistake.	**Network Types(s):** Children; Employees; Parents/Guardians/Caregivers **Industry Role(s):** 9-1-1 Callers **Keywords(s):** Business; Family Education; Residential; What to Say and Do	Highly Important	**New Consumer**
WG8-3-33	9-1-1 Callers should remain calm and promptly answer all of the call taker questions.	**Network Types(s):** Children; Employees; Parents/Guardians/Caregivers **Industry Role(s):** 9-1-1 Callers **Keywords(s):** Business; Family Education; Knowing Your Location; Residential; What to Say and Do	Highly Important	**New Consumer**
WG8-3-34	Consumers should never make prank phone calls to 9-1-1.	**Network Types(s):** Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Business; Family Education; Residential	Highly Important	**New Consumer**
WG8-3-35	Consumers should post their address clearly and prominently so that it is visible to emergency service providers.	**Network Types(s):** Business Owners; Home Owners	Highly Important	**New Consumer**

		Industry Role(s): Consumers **Keywords(s):** Alternate Methods; Business; Knowing Your Location		
WG8-3-36	Consumers should install Address Markers so that they are locatable both during daylight and nighttime hours in order to assist emergency service providers.	**Network Types(s):** Business Owners; Home Owners **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Knowing Your Location	Highly Important	**New Consumer**
WG8-3-37	Consumers should not assume that marking their mailbox is sufficient for emergency personnel to locate a 9-1-1 Caller's location.	**Network Types(s):** Business Owners; Home Owners **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Knowing Your Location	Highly Important	**New Consumer**
WG8-3-38	Consumers should not dial the number 9-1-1 for information, directory assistance, or non-emergencies.	**Network Types(s):** Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Business; Family Education; Residential; When to Call	Highly Important	**New Consumer**
WG8-3-39	Consumers should not dial the number 9-1-1 for contacting non-emergency city, county, or municipal services.	**Network Types(s):):** Business Owners; Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Business; Family Education; Residential; When to Call	Highly Important	**New Consumer**
WG8-3-40	9-1-1 Callers should speak clearly and distinctly to the 9-1-1 call taker when providing their name, number, and address of	**Network Types(s):** Children; Employees; Home Owners; Parents/Guardians/Caregivers	Highly Important	**New Consumer**

	their emergency.	**Industry Role(s):** 9-1-1 Callers **Keywords(s):** Business; Family Education; Knowing Your Location; Residential; What to Say and Do		
WG8-3-41	9-1-1 Callers and TTY/TDD Users should stay on the line if it is safe to do so, until instructed to hang up.	**Network Types(s):** Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** 9-1-1 Callers **Keywords(s):** Alternate Methods; Business; Family Education; Residential; What to Say and Do	Highly Important	**New Consumer**
WG8-3-42	Consumers should register and provide their address when using Video Relay Service (VRS) or Internet Protocol (IP) Relay and keep that address updated regularly.	**Network Types(s):** Business Owners; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Device Use; Next Generation; Residential; Updating Information; What to Say and Do	Highly Important	**New Consumer**
WG8-3-43	9-1-1 Callers should be prepared to promptly and accurately respond to all 9-1-1 call taker questions when using Video Relay Service (VRS), Internet Protocol (IP) Relay service and/or TTY/TDD.	**Network Types(s):** Business Owners; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** 9-1-1 Callers **Keywords(s):** Alternate Methods; Business; Family Education; Next Generation; Residential; What to Say and Do	Highly Important	**New Consumer**
WG8-3-44	9-1-1 Callers should be aware that when using Video Relay Service (VRS) or Internet Protocol (IP) Relay the call may need to be transferred by the 9-1-1 call taker to another 9-1-1 center and they should stay on the call if it is safe to do so.	**Network Types(s):** Business Owners; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** 9-1-1 Callers	Highly Important	**New Consumer**

		Keywords(s): Alternate Methods; Business; Device Use; Family Education; Next Generation; Residential; What to Say and Do		
WG8-3-45	Consumers should be familiar with and keep handy their Voice over Internet Protocol (VoIP) service provider's procedures for updating information for 9-1-1 emergency services in the event a change or update is necessary.	**Network Types(s):** Business Owners; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Business; Device Use; Family Education; Next Generation; Residential; Updating Information; Wireless; Wireline	Highly Important	**New Consumer**
WG8-3-46	Consumers should have a clear understanding of any potential limitations regarding 9-1-1 emergency services (e.g., location identification) when considering or subscribing to a Voice over Internet Protocol (VoIP) service.	**Network Types(s):** Business Owners; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Business; Device Use; Family Education; Next Generation; Residential; Wireless; Wireline	Important	**New Consumer**
WG8-3-47	Consumers should educate children, babysitters, and visitors about any 9-1-1 emergency service limitations, if any, if the household uses a Voice over Internet Protocol (VoIP) service.	**Network Types(s):** Children; Home Owners; Parents/Guardians/Caregivers; Teachers/Trainers **Industry Role(s):** Consumers **Keywords(s):** Device Use; Family Education; Next Generation; Residential; Wireless; Wireline	Important	**New Consumer**
WG8-3-48	Consumers should be aware their Voice over Internet Protocol (VoIP) service may not operate if power is out or their internet connection is down and may want to consider installing a backup power supply or have an alternate means of calling 9-1-1 (e.g., traditional phone line, cell phone, satellite phone) if necessary.	**Network Types(s):** Business Owners; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business;	Important	**New Consumer**

		Device Use; Family Education; Next Generation; Residential; Wireless; Wireline		
WG8-3-49	Consumers should contact their service provider if they are unsure if they are receiving their phone service over Voice over Internet Protocol (VoIP).	**Network Types(s):** Business Owners; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Device Use; Next Generation; Residential; Wireless; Wireline	Important	**New Consumer**
WG8-3-50	Consumers should keep phones charged to reduce disconnections and loss of communication during a 9-1-1 call.	**Network Types(s):** Business Owners; Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Business; Device Use; Family Education; Residential; What to Say and Do	Important	**New Consumer**
WG8-3-51	9-1-1 Callers in vehicles should attempt to place emergency calls while the vehicle is stationary.	**Network Types(s):** Business Owners; Employees; Parents/Guardians/Caregivers **Industry Role(s):** 9-1-1 Callers **Keywords(s):** Device Use; Family Education; What to Say and Do; Wireless	Important	**New Consumer**
WG8-3-52	Consumers should listen to broadcast TV and/or radio news for important Public Safety Alerts (e.g., PDAs, text radio systems, NOAA radio, etc.) and/or additional instructions during times of man-made or natural disasters.	**Network Types(s):** Business Owners; Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Family Education; What to Say and Do	Important	**New Consumer**
WG8-3-53	Consumers should visit websites with additional information about 9-1-1 (e.g., NENA, APCO, FEMA, 9-1-1forkids).	**Network Types(s):** Business Owners; Children; Employees; Home Owners;	Important	**New Consumer**

		Parents/Guardians/Caregivers; Teachers/Trainers **Industry Role(s):** Consumers **Keywords(s):** Business; Family Education; Training Methods		
WG8-3-54	Consumers should be aware that 9-1-1 centers do not generally provide 9-1-1 call takers with access to the internet.	**Network Types(s):** Business Owners; Employees; Home Owners; Parents/Guardians/Caregivers; Teachers/Trainers **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Device Use; Family Education; Residential; Training Methods	Important	**New Consumer**
WG8-3-55	Consumers should contact their local public safety authorities to determine if their 9-1-1 center has the ability to accept multi-media or text messaging.	**Network Types(s):** 9-1-1 Agencies; Business Owners; Government; Home Owners; Parents/Guardians/Caregivers; Teachers/Trainers **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Device Use; Family Education; Residential; Training Methods	Important	**New Consumer**
WG8-3-56	Consumers should not program devices (e.g., smart phones, tablets, building alarm systems) for automated calling to 9-1-1 as that practice may violate local, state, or federal laws.	**Network Types(s):** Business Owners; Home Owners **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Device Use; Residential; When to Call	Important	**New Consumer**
WG8-3-57	Consumers should notify their "in case of emergency" (ICE) emergency contacts that they may be contacted on their behalf, and inform them of any medical issues or special needs that they may have.	**Network Types(s):** Employees; Parents/Guardians/Caregivers **Industry Role(s):** Consumers	Important	**New Consumer**

		Keywords(s): Updating Information; What to Say and Do		
WG8-3-58	Consumers without cell phones should consider purchasing a prepaid phone card to use during or after a disaster.	**Network Types(s):** Business Owners; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Device Use; Family Education; Residential; When to Call	Important	**New Consumer**
WG8-3-59	Consumers should consider subscribing to text alert services (e.g., school boards, local or state governments) if available to receive alerts in the event of a disaster.	**Network Types(s):** Business Owners; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** Consumers **Keywords(s):** Alternate Methods; Business; Device Use; Residential	Important	**New Consumer**
WG8-3-60	Consumers should teach Children on how to call 9-1-1 from their location.	**Network Types(s):** Children; Home Owners; Parents/Guardians/Caregivers; Teachers/Trainers **Industry Role(s):** Consumers **Keywords(s):** Device Use; Family Education; Knowing Your Location; Residential; Training Methods; When to Call	Important	**New Consumer**
WG8-3-61	Consumers should teach employees on how to call 9-1-1 from their location.	**Network Types(s):** Business Owners; Employees; Teachers/Trainers **Industry Role(s):** Consumers **Keywords(s):** Business; Device Use; Knowing Your Location; Training Methods; When to Call	Important	**New Consumer**
WG8-3-62	Consumers should teach children to answer call taker questions.	**Network Types(s):** Children; Home Owners; Parents/Guardians/Caregivers; Teachers/Trainers	Important	**New Consumer**

		Industry Role(s): Consumers **Keywords(s):** Family Education; Knowing Your Location; Residential; Training Methods; What to Say and Do		
WG8-3-63	Consumers should know and understand the operation of the phones that they may own or use.	**Network Types(s):** Business Owners; Children; Employees; Home Owners; Parents/Guardians/Caregivers; Teachers/Trainers **Industry Role(s):** Consumers **Keywords(s):** Business; Device Use; Family Education; Residential; Training Methods; Wireless; Wireline	Important	**New Consumer**
WG8-3-64	Consumers should look under public education tabs on various websites for additional information and training regarding 9-1-1.	**Network Types(s):** Business Owners; Children; Employees; Home Owners; Parents/Guardians/Caregivers; Teachers/Trainers **Industry Role(s):** Consumers **Keywords(s):** Business; Family Education; Training Methods	Important	**New Consumer**
WG8-3-65	TTY/TDD Users should provide the 9-1-1 call taker some time to connect the TTY, and if necessary, repeat the step of pressing keys to alert the 9-1-1 call taker to the need for a TTY/TDD conversation.	**Network Types(s):** 9-1-1 Agencies; Children; Employees; Home Owners; Parents/Guardians/Caregivers **Industry Role(s):** TTY/TDD Users **Keywords(s):** Alternate Methods; Business; Device Use; Family Education; Residential; What to Say and Do	Important	**New Consumer**

9 Appendix 4 – PSAP Best Practices

CSRIC III Best Practice Number	CSRIC III Best Practice	CSRIC III BP Reference/Comments	Best Practice Status	CSRIC III (New/Changed/ Unchanged/ Deleted)
NEW CATEGORY - PSAP BEST PRACTICES				
WG8-3-66	PSAPs should develop comprehensive plans to address day-to-day operations, emergencies, and mutual aid with other PSAPs and jurisdictions.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Documentation; Emergency Preparedness; Essential Services; Human Resources; Network Operations; Policy; Procedures	Critical	**New PSAP**
WG8-3-67	PSAPs should plan for all types of events including those that range from large-scale loss of communications infrastructure requiring network restoration and repair, through those for which communications is largely left intact resulting in higher PSAP call volumes.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Documentation; Emergency Preparedness; Essential Services; Network Operations; Policy; Procedures	Critical	**New PSAP**
WG8-3-68	PSAPs should plan for increased call volumes caused by large scale disasters by ensuring that they have adequate facilities, functional equipment, appropriate amount of personnel, and rerouting plans needed to handle increased call volumes and overflow situations.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Documentation; Emergency Preparedness; Human Resources; Network Design; Network Interoperability; Supervision; Technical Support	Critical	**New PSAP**
WG8-3-69	PSAPs should develop mutual aid plans for adequate response and coverage for disasters that may have a regional impact	**Network Types(s):** 9-1-1 Agencies; Government	Critical	**New PSAP**

	and encompass large geographical areas.	**Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Documentation; Emergency Preparedness; Policy; Procedures		
WG8-3-70	PSAPs should develop contingency plans that include appropriate strategies for sharing call load and load balancing among multiple call centers during emergency situations.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Documentation; Emergency Preparedness; Procedures	Critical	**New PSAP**
WG8-3-71	PSAPs should work with local governments and medical teams to consider 9-1-1 personnel and technical staff in priority planning for vaccinations.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Pandemic; Policy; Procedures	Critical	**New PSAP**
WG8-3-72	PSAPs should ensure that emergency plans and activities are consistent with the phases of pandemic influenza as defined by both the World Health Organization (WHO) and the U.S. Federal Government's Response Stages.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Pandemic; Policy; Procedures	Critical	**New PSAP**
WG8-3-73	PSAPs should use call-taking protocols that provide for specific influenza-symptom monitoring, triage and priority dispatch of EMS and public safety resources. The proper legal and medical authority, in coordination with the emergency medical services system, should be predetermined in the planning process.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Pandemic; Policy; Procedures	Critical	**New PSAP**
WG8-3-74	PSAPs should coordinate with public health, law enforcement and emergency management agencies to identify mechanisms for freedom of movement of PSAP personnel when faced	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs	Critical	**New PSAP**

	with restricted travel laws, isolation/quarantine or security measures during a pandemic.	**Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Human Resources; Pandemic		
WG8-3-75	PSAPs should develop processes to be used during recovery from an emergency that include impact assessment, repair/restoration, alternate solutions, post-incident analysis, and the updating of the emergency management plan.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Disaster Recovery; Network Operations; Power; Procedures	Critical	**New PSAP**
WG8-3-76	PSAPs should establish an alternate operations site capable of supporting critical Information Technology (IT) and communications functions for emergency situations.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Disaster Recovery; Emergency Preparedness; Network Design; Network Interoperability; Network Operations; Network Provisioning	Critical	**New PSAP**
WG8-3-77	PSAPs should identify and establish safe locations for communications systems that require redundancy and back-up configurations.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Disaster Recovery; Emergency Preparedness; Network Design; Network Interoperability; Network Operations; Network Provisioning	Critical	**New PSAP**
WG8-3-78	PSAPs should have plans that identify specific vulnerabilities (e.g., power outages, high wind, flooding) that are most likely to occur in that specific region and provide resources to overcome them.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness	Critical	**New PSAP**
WG8-3-79	PSAPs should evaluate the resiliency, redundancy, and interoperability of systems while performing inventory and risk assessment analysis.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs	Critical	**New PSAP**

		Keywords(s): Network Design; Network Elements; Network Interoperability; Network Operations; Network Provisioning; Power;		
WG8-3-80	PSAPs should consider obtaining a last-resort backup means of communication (e.g., Wireless, WIFI, satellite) in response to adverse conditions, even if technical signal quality is substantially degraded under such conditions, for communicating with employees, police, fire department officials, emergency medical personnel and others in the community as needed.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness	Critical	**New PSAP**
WG8-3-81	PSAPs should consider High Frequency (HF) radio as an option, recognizing that HF usually requires a skilled operator such as a licensed Amateur Radio (HAM) radio operator.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness	Critical	**New PSAP**
WG8-3-82	PSAPs should consider the use of divergent routes (e.g., an office across the street that may be fed from a different cable or transformer) which is best accomplished through discussions with telecommunications service providers.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Network Design; Network Interoperability; Network Operations; Network Provisioning	Critical	**New PSAP**
WG8-3-83	PSAPs should consider obtaining interoffice diversity from its provider even in cases where end-to-end diversity is not available (e.g., there is only one loop route to the PSAP).	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Network Design; Network Interoperability; Network Operations; Network Provisioning	Critical	**New PSAP**
WG8-3-84	PSAPs should consider arranging with another PSAP for backup and support in the event of total failure or abandonment of the PSAP.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs	Critical	**New PSAP**

		Keywords(s): Business Continuity; Disaster Recovery; Essential Services; Policy		
WG8-3-85	PSAPs should consider maintaining vital communications and Information Technology (IT) equipment in protected locations with authorized only access.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Access Control; Buildings; Business Continuity; Physical Security Management; Security Systems	Critical	**New PSAP**
WG8-3-86	PSAPs should consider securing key facilities with experienced personnel and/or video surveillance cameras.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Access Control; Buildings; Business Continuity; Physical Security Management; Security Systems	Critical	**New PSAP**
WG8-3-87	PSAPs should protect communication and Information Technology (IT) systems from malicious cyber-attacks and viruses by implementing security measures such as the regular updating of virus protection and other software security programs.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Cyber Security; Encryption; Network Elements; Policy;	Critical	**New PSAP**
WG8-3-88	PSAPs should consider activating backup power automatically through the use of a power source having a low risk of being interrupted during a power outage to maintain continuity of operations (i.e. a power generator).	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Emergency Preparedness; Essential Services; Hardware; Network Design; Power	Critical	**New PSAP**
WG8-3-89	PSAPs should deploy, maintain, and frequently test emergency generators at secure, elevated locations in cases where it is essential to maintaining daily operations.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Emergency Preparedness; Essential Services; Hardware;	Critical	**New PSAP**

		Network Design; Power		
WG8-3-90	PSAPs should ensure that sufficient levels of fuel are available at all times and periodically check those levels.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Emergency Preparedness; Essential Services; Network Design; Power	Critical	**New PSAP**
WG8-3-91	PSAPs should ensure that battery backup is available for critical communications in case emergency generators fail to function taking into consideration that batteries are good for short term outages but often do not power HVAC equipment and may not adequately cool other equipment (e.g., computers) which may be damaged or shutoff when overheated.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Network Design; Network Interoperability; Network Operations; Power	Critical	**New PSAP**
WG8-3-92	PSAPs should establish sources for obtaining fuel to refill generators.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Network Operations; Power	Critical	**New PSAP**
WG8-3-93	PSAPs should ensure backup systems are operating properly and are performing their function when activated.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Network Interoperability; Network Operations	Critical	**New PSAP**
WG8-3-94	PASPs should include in risk modeling inclusions that test fail over for lost facilities, loss of human services, current structure and building designs, tower locations, and National Institute of Standards for Technology.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Access Control; Buildings;	Critical	**New PSAP**

		Business Continuity; Disaster Recovery; Emergency Preparedness; Network Design; Network Interoperability; Network Operations; Physical Security Management; Policy; Power; Procedures; Security Systems; Software		
WG8-3-95	PSAPs should perform an analysis that includes single point of failure studies and action prioritization to mitigate failures using a steady and repeatable process that allows for a gap analysis of the systems and their functions.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Access Control; Business Continuity; Disaster Recovery; Emergency Preparedness; Network Design; Network Interoperability; Network Operations; Physical Security Management; Policy; Power; Procedures; Security Systems; Software	Critical	**New PSAP**
WG8-3-96	PASPs should include in risk modeling studies of current design and standards, as well as recovery based upon current service level agreement response intervals.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Access Control; Business Continuity; Disaster Recovery; Emergency Preparedness; Network Design; Network Interoperability; Network Operations; Physical Security Management; Policy; Power; Procedures; Security Systems; Software	Critical	**New PSAP**
WG8-3-97	PSAPs should develop a means of personnel identification to insure access during emergency situations for employees and any mutual aid agencies that may be assisting.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Access Control; Disaster Recovery; Emergency Preparedness; Human Resources; Physical Security Management; Policy; Procedures; Security Systems	Critical	**New PSAP**
WG8-3-98	PSAPs should develop procedures to communicate with callers that are not using a native language of an available call taker.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs	Critical	**New PSAP**

		Keywords(s): Business Continuity; Essential Services; Human Resources; Policy; Training and Awareness		
WG8-3-99	PSAPs should have a training program for new call takers including both call handling and the operation of their system and equipment.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Essential Services; Human Resources; Policy; Training and Awareness	Critical	**New PSAP**
WG8-3-100	PSAPs should register all critical circuits with Telecommunications Service Priority (TSP service) with their telecommunications carriers.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Network Interoperability; Network Operations; Policy	Critical	**New PSAP**
WG8-3-101	PSAPs should design their networks to utilize concepts such as diverse facilities, routes, and self-healing topologies when possible.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Hardware; Network Design; Network Elements; Network Interoperability; Network Operations; Network Provisioning; Power; Security Systems; Software	Critical	**New PSAP**
WG8-3-102	PSAPs should reroute traffic and network access from congested network components during surge events that accompany an emergency.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Disaster Recovery; Emergency Preparedness; Essential Services; Network Interoperability; Network Operations; Network Provisioning; Policy	Critical	**New PSAP**

WG8-3-103	PSAPs should work with communication providers to obtain commitments for tabletop exercises, and development of disaster plans, then put those procedures in place prior to large-scale disasters that disrupt communications.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Documentation; Emergency Preparedness; Essential Services; Human Resources; Network Operations; Policy; Procedures; Training and Awareness	Highly Important	**New PSAP**
WG8-3-104	PSAPs should routinely practice emergency plans, and procedures, and update them to include lessons learned ensuring training exercises are realistic and challenge the comprehensiveness of the emergency plan.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Documentation; Emergency Preparedness; Training and Awareness	Highly Important	**New PSAP**
WG8-3-105	PSAPs should practice emergency plans jointly with communications providers and review them on an agreed upon schedule.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Documentation; Emergency Preparedness; Training and Awareness	Highly Important	**New PSAP**
WG8-3-106	PSAPs should develop standard operating procedures for call takers to respond to callers.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Policy; Procedures; Supervision; Training and Awareness	Highly Important	**New PSAP**
WG8-3-107	PSAPs should develop standard operating procedures for call takers to improve accessibility for special needs of people with hearing and speech disabilities.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Essential Services; Policy; Procedures; Supervision; Training and Awareness	Highly Important	**New PSAP**

WG8-3-108	PSAPs should ensure that 9-1-1 services are accessible to all people, including those with hearing and speech disabilities.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Essential Services; Policy; Procedures	Highly Important	**New PSAP**
WG8-3-109	PSAPs should implement processes and technology to support Telecommunications Relay Service (TRS) calls.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Essential Services; Policy; Procedures	Highly Important	**New PSAP**
WG8-3-110	PSAPs should have accurate, up-to-date information to be effective in call taking, dispatching and relaying information to the public.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Policy; Procedures	Highly Important	**New PSAP**
WG8-3-111	PSAPs should be integrated into the local, regional, and state incident command structures in order to be fully engaged as a collaborative partner in the response to any pandemic outbreaks (e.g., influenza).	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Pandemic	Highly Important	**New PSAP**
WG8-3-112	PSAPs should have personnel follow infection control measures and industrial hygiene practices as a standard part of daily practices, and reinforce these measures and practices with continuing education.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Pandemic; Policy; Procedures; Training and Awareness	Highly Important	**New PSAP**
WG8-3-113	PSAPs and their staff should be included along with elected officials and others, in community drills, with a focus on reinforcement of the clear delineation of authority and responsibility in the simulations.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster	Highly Important	**New PSAP**

		Recovery; Emergency Preparedness; Policy; Procedures; Training and Awareness		
WG8-3-114	PSAPs should include specifics in emergency plans that consider accommodations for those with special needs (e.g., mental health, limited English proficiency, children, and elderly, home health care) or individuals with disabilities.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Training and Awareness	Highly Important	**New PSAP**
WG8-3-115	PSAPs should include procedures in emergency plans to identify callers who are likely afflicted by the influenza virus or another pandemic outbreak and to assign the appropriate resource to provide assistance.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Pandemic; Training and Awareness	Highly Important	**New PSAP**
WG8-3-116	PSAPs should consider the use of automated emergency alerts in the form of pre-recorded phone messages and through other media in the overall strategy for delivering information to the public.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Essential Services; Policy; Procedures	Highly Important	**New PSAP**
WG8-3-117	PSAPs should have procedures during pandemic situations to manage and/or prioritize other non-influenza related requests for help, and appropriately matching need to resource.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Pandemic; Training and Awareness	Highly Important	**New PSAP**
WG8-3-118	PSAPs should have procedures during pandemic situations to tell callers if no response is available or will be delayed.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Documentation; Emergency	Highly Important	**New PSAP**

		Preparedness; Pandemic; Procedures		
WG8-3-119	PSAPs should have pre-established links with other types of call centers (e.g., 2-1-1 or nurse assist lines) or alternate care centers to ensure those resources can effectively be utilized in transferring or referring callers during a pandemic influenza.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Documentation; Emergency Preparedness; Pandemic; Procedures	Highly Important	**New PSAP**
WG8-3-120	PSAPs should ensure emergency plans for pandemic influenza events are in concert with the appropriate medical and legal authority.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Documentation; Emergency Preparedness; Pandemic; Procedures	Highly Important	**New PSAP**
WG8-3-121	PSAPs should identify and transfer responsibilities that can be handled by non-PSAP staff during a pandemic influenza to manage workload.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Essential Services; Human Resources; Pandemic; Supervision	Highly Important	**New PSAP**
WG8-3-122	PSAPs should include in pre-plans existing tools and resources needed to support the PSAP during a pandemic.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Documentation; Emergency Preparedness; Pandemic; Policy; Procedures; Technical Support	Highly Important	**New PSAP**
WG8-3-123	PSAPs should ensure all 9-1-1 personnel are aware of the overall emergency action plan.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs	Highly Important	**New PSAP**

		Keywords(s): Business Continuity; Disaster Recovery; Emergency Preparedness; Training and Awareness		
WG8-3-124	PSAPs should address infection control training for 9-1-1 personnel in pre-planning for pandemic influenza.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Pandemic; Training and Awareness	Highly Important	**New PSAP**
WG8-3-125	PSAPs should address how they will staff different positions based on the skill levels needed in the pre-planning process. More routine tasks within the PSAP may be handled with alternative staffing, with the goal to have trained call takers available to interface with the public for the most critical 9-1-1 calls.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Human Resources; Pandemic; Training and Awareness	Highly Important	**New PSAP**
WG8-3-126	PSAPs should identify staffing alternatives (e.g., retirees, former employees, staff from other departments) in the pre-planning process to free up trained staff and supervisors to answer critical 9-1-1 calls.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Human Resources; Pandemic; Training and Awareness	Highly Important	**New PSAP**
WG8-3-127	PSAPs should identify infection control procedures specifically for the pandemic influenza virus in their emergency plans.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Emergency Preparedness; Pandemic; Procedures	Highly Important	**New PSAP**
WG8-3-128	PSAPs should identify isolation and quarantine policies and procedures to be used during a pandemic influenza.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Emergency	Highly Important	**New PSAP**

		Preparedness; Pandemic; Procedures		
WG8-3-129	PSAPs should identify in pre-plans how to limit the exposure of 9-1-1 staff, identify isolation and lock-down procedures and identify on-site treatment areas for those who have become infected during a pandemic influenza.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Human Resources; Pandemic; Training and Awareness	Highly Important	**New PSAP**
WG8-3-130	PSAPs should consider and evaluate how Next Generation technology and the IP-enabled PSAP could allow each community to be served by a remotely run PSAP or to more effectively exchange information with the public and the many groups involved in a pandemic response.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Hardware; Network Design; Network Provisioning; Pandemic; Software; Technical Support	Highly Important	**New PSAP**
WG8-3-131	PSAPs should develop a team that will take action during and following an emergency with clearly defined employee roles and responsibilities with a chain of command for operational functions and maintenance of communications infrastructure and IT services.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Disaster Recovery; Emergency Preparedness; Policy; Supervision; Technical Support	Highly Important	**New PSAP**
WG8-3-132	PSAPs should prepare contact information for service providers, Information Technology (IT), Internet, and telecommunications services including circuit numbers, diagrams and Telecommunication Service Priority (TSP) codes as appropriate.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Emergency Preparedness; Procedures	Highly Important	**New PSAP**
WG8-3-133	PSAPs should plan for and perform periodic testing of systems (e.g. land mobile radio system, repeaters, Private Branch Exchange (PBX), Local Area Network (LAN) or data network, email) to make sure they will work in an emergency.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Emergency Preparedness	Highly Important	**New PSAP**

WG8-3-134	PSAPs should identify employees with disabilities and special needs and work with these employees to develop strategies for keeping them informed during an emergency (i.e., some employees may be unable to see or hear workplace announcements).	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Disaster Recovery; Emergency Preparedness; Procedures	Highly Important	**New PSAP**
WG8-3-135	PSAPs should develop plans for evacuating employees with special needs (e.g., those in wheelchairs).	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Disaster Recovery; Emergency Preparedness; Procedures	Highly Important	**New PSAP**
WG8-3-136	PSAPs should consider limiting access to Information Technology (IT) systems to appropriate staff using login/password and other security measures.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Access Control; Buildings; Business Continuity; Security Systems	Highly Important	**New PSAP**
WG8-3-137	PSAPs should develop a testing schedule (e.g., daily, weekly, or monthly) to ensure that batteries for radios, flashlights, fire detectors and other communications and safety devices are working, charged, and ready.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Disaster Recovery; Emergency Preparedness; Procedures	Highly Important	**New PSAP**
WG8-3-138	PSAPs should plan to have necessary test equipment available when an emergency occurs.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Disaster Recovery; Emergency Preparedness; Network Operations; Technical Support	Highly Important	**New PSAP**
WG8-3-139	PSAPs should have test equipment that works with both commercial and battery power if necessary.	**Network Types(s):** 9-1-1 Agencies; Government	Highly Important	**New PSAP**

		Industry Role(s): PSAPs **Keywords(s):** Disaster Recovery; Emergency Preparedness; Network Operations; Technical Support		
WG8-3-140	PSAPs should work with local public utilities (e.g., telephone, wireless phone, electric, and water) to develop a critical infrastructure priority restoration plan for their locality.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Disaster Recovery; Emergency Preparedness; Network Interoperability; Network Operations	Highly Important	**New PSAP**
WG8-3-141	PSAPs should establish a procedure and develop emergency contact information with local public utilities (e.g., telephone, wireless phone, electric, and water) as well as any other party necessary to support or assist in the restoration of their system.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Disaster Recovery; Emergency Preparedness; Network Interoperability; Network Operations	Highly Important	**New PSAP**
WG8-3-142	PSAPs should make arrangements to meet and establish relationships with key individuals in public utilities (e.g., telephone, wireless phone, electric, and water) before the need arises.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Network Interoperability; Network Operations	Highly Important	**New PSAP**
WG8-3-143	PSAPs should consider establishing a three-tiered priority list for assets (i.e., Mission Critical, Important, and Minor) that will help identify the impact of losing a given asset and will allow them to better communicate their needs for assistance when necessary.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Network Interoperability; Network Operations; Policy; Procedures	Highly Important	**New PSAP**

WG8-3-144	PSAPs should identify what communications systems that they can repair on their own and which systems will need repairs by commercial vendors or telephone companies for when any of their lines or services have been impacted by an emergency.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Network Interoperability; Network Operations	Highly Important	**New PSAP**
WG8-3-145	PSAPs should develop risk modeling against first responder infrastructure and response; based upon the possible or likely disasters their jurisdiction is prone to, and upon likely severity of the failure, up to and including a total loss of systems.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Access Control; Building; Business Continuity; Emergency Preparedness; Network Operations; Policy; Procedures; Security Systems; Software	Highly Important	**New PSAP**
WG8-3-146	PSAPs should instruct 9-1-1 call takers to follow standard operating procedures when a silent or open call is received, and dispatch appropriate services or call the caller back per PSAP protocol.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Essential Services; Policy; Procedures; Training and Awareness	Highly Important	**New PSAP**
WG8-3-147	PSAPs should develop training programs that help reduce the incidences of silent, inadvertent or misdialed calls in order to help reduce the workload on the agency in dealing with that type of call.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Essential Services; Policy; Procedures; Training and Awareness	Highly Important	**New PSAP**
WG8-3-148	PSAPs should develop procedures for when friends or family call them looking for information and provide responses that meet local, state, federal, and/or privacy laws, with regard to what information can be provided.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Essential Services; Policy; Procedures; Training and Awareness	Highly Important	**New PSAP**

WG8-3-149	PSAPs should review and follow National Emergency Number Association (NENA) recommended standards as applicable.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Policy; Procedures	Highly Important	**New PSAP**
WG8-3-150	PSAPs should provide periodic training and re-training for call takers.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Essential Services; Human Resources; Policy; Training and Awareness	Highly Important	**New PSAP**
WG8-3-151	PSAPs should plan for alternate alerting procedures to the public in the case of an outage of their primary alerting procedures or system.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Documentation; Emergency Preparedness; Policy; Procedures	Important	**New PSAP**
WG8-3-152	PSAPs should obtain written commitments from communication providers describing what they will provide in a joint emergency plan (e.g., points of contact and staging points).	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Documentation; Emergency Preparedness; Policy; Procedures	Important	**New PSAP**
WG8-3-153	PSAPs should standardize equipment and procedures at local, state, regional, and federal levels to facilitate mutual aid and emergency backup.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Hardware;	Important	**New PSAP**

		Network Design; Network Elements; Network Interoperability		
WG8-3-154	PSAPs should, support the National Emergency Number Association (NENA) and Association of Public Safety Communications Officials (APCO) Telecommunicator Emergency Response Team (TERT) program when appropriate.	**Remarks/Comments section:** TERT includes assistance to individual states in developing programs to establish predetermined and selected trained teams who can mobilize quickly and deploy to assist communications centers during disasters. **Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Procedures; Training and Awareness	Important	**New PSAP**
WG8-3-155	PSAPs should have in place standard operating procedures for all types of emergency calls to include medical emergencies.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Policy; Procedures	Important	**New PSAP**
WG8-3-156	PSAPs should institute procedures to allow the immediate dissemination of information to call takers during a pandemic situation or incident.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Pandemic	Important	**New PSAP**
WG8-3-157	PSAPs should use standardized 9-1-1 protocols and data that capture symptoms specific to a pandemic along with other possible indictors (e.g., recent travel to affected areas) that can assist in this process.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Pandemic; Policy; Procedures	Important	**New PSAP**

WG8-3-158	PSAPs should provide employee training in incident command per the requirements of the National Incident Management System (NIMS).	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Training and Awareness	Important	**New PSAP**
WG8-3-159	PSAPs should focus on what may be the same, as well as what is different, about influenza or other pandemic outbreaks that will require a response unlike that needed for past hazards.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Pandemic; Policy; Procedures	Important	**New PSAP**
WG8-3-160	PSAPs should incorporate recommendations of the Department of Homeland Security Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources when planning their response to influenza or other pandemic outbreaks.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Pandemic; Policy; Procedures	Important	**New PSAP**
WG8-3-161	PSAPs should identify policies related to paid and unpaid leave and care of the families of PSAP staff during a pandemic influenza event.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Human Resources; Pandemic	Important	**New PSAP**
WG8-3-162	PSAPs should identify those with key communications and Information Technology (IT) components that are critical to the continuation of essential services in an emergency.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Disaster Recovery; Emergency Preparedness; Human Resources; Technical Support	Important	**New PSAP**

WG8-3-163	PSAPs should specify procedures to be followed in the hours preceding a storm to protect computers, paper records (e.g., securing equipment, placing garbage bags over files, or moving files upstairs) and identify which, if any, databases to be backed up at the last possible moment.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Buildings; Business Continuity; Disaster Recovery; Documentation; Emergency Preparedness; Procedures	Important	**New PSAP**
WG8-3-164	PSAPs should consider cross training between communications team members to be able to compensate for personnel shortages that may occur taking into account specialized training for employees with disabilities.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Human Resources; Training and Awareness	Important	**New PSAP**
WG8-3-165	PSAPs should conduct leader training for those responsible for coordinating communications operations during major emergency events.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness; Human Resources; Training and Awareness	Important	**New PSAP**
WG8-3-166	PSAPs should develop employee contact lists that include office/home numbers, work/home cell numbers, and office/personal email addresses that are continually updated and maintained in paper format and at offsite location using removable media (e.g., USB drive).	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Emergency Preparedness; Procedures	Important	**New PSAP**
WG8-3-167	PSAPs should develop a list of employees with disabilities, giving instructions on how to contact them in an emergency (e.g., how to send a text message to a deaf employee's pager).	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Emergency Preparedness; Procedures	Important	**New PSAP**
WG8-3-168	PSAPs should develop a plan for how to keep employees with disabilities informed in case of an emergency.	**Network Types(s):** 9-1-1 Agencies; Government	Important	**New PSAP**

		Industry Role(s): PSAPs **Keywords(s):** Business Continuity; Emergency Preparedness; Procedures		
WG8-3-169	PSAPs should establish public education campaigns and work with schools, parents, or many others to promote the proper use of 9-1-1.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Policy; Training and Awareness	Important	**New PSAP**
WG8-3-170	PSAPs should be well knowledgeable of the capabilities of systems and be proficient in their use so as to maximize their value and readiness during times of emergency.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness	Important	**New PSAP**
WG8-3-171	PSAPs should consider including Amateur Radio (HAM) radio operators in emergency operations plan and when activated, identify where they will be assigned. It is important to include all known HAM, Amateur Radio Emergency Service (ARES), and SHARES operating personnel in the area to maximize their assistance during critical times.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Emergency Preparedness	Important	**New PSAP**
WG8-3-172	PSAPs should consider using a number of notification systems such as building-wide intercom, wireline phone messages, email notifications, and person-to-person communications for crisis management instructions (e.g., for full evacuation or relocation to a designated area of the building).	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Disaster Recovery; Emergency Preparedness; Procedures	Important	**New PSAP**
WG8-3-173	PSAPs should ensure that notification systems (e.g., public address) can function in the event of a power failure.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Emergency Preparedness; Network Elements; Power	Important	**New PSAP**

WG8-3-174	PSAPs should consider when ordering a new generator installation, the use of dual fuel sources, such as Natural Gas and Diesel.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Emergency Preparedness; Essential Services; Network Design; Power	Important	**New PSAP**
WG8-3-175	PSAPs should consider purchasing new radios that can be powered by off-the-shelf alkaline batteries using appropriate adapters taking into consideration they could present a HAZMAT issue in disposal.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Disaster Recovery; Emergency Preparedness; Procedures	Important	**New PSAP**
WG8-3-176	PSAPs should consider entering into mutual aid or lend-lease agreements with similar organizations both inside and outside of their jurisdiction to enable organizations to share specialized resources rather than duplicate them in every jurisdiction.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Disaster Recovery; Hardware; Network Interoperability; Network Operations; Technical Support	Important	**New PSAP**
WG8-3-177	PSAPs should conduct situational awareness surveys/analyses and provide updates and reports to leadership and emergency management teams, and, when appropriate, to the public.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Network Operations; Policy	Important	**New PSAP**
WG8-3-178	PSAPs should establish post-incident analysis review procedures that utilize a lessons learned approach to emergencies following completion of all repairs.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Network Operations; Policy	Important	**New PSAP**
WG8-3-179	PSAPs should add lessons learned in post incident analysis to future procedures	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs	Important	**New PSAP**

		Keywords(s): Business Continuity; Network Operations; Policy		
WG8-3-180	PSAPs should consider holding a debriefing session with employees or visitors with disabilities or special needs to determine how well emergency procedures worked for them and what, if anything can be improved.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Network Operations; Policy	Important	**New PSAP**
WG8-3-181	PSAPs should develop procedures regarding internet access that are in line with network and system security and access of information over the internet.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Business Continuity; Cyber Security; Human Resources; Policy; Security Systems	Important	**New PSAP**
WG8-3-182	PSAPs should consider offering tours of their PSAP or location to help train children/students/the public about how 9-1-1 calls are handled.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Policy; Training and Awareness	Important	**New PSAP**
WG8-3-183	PSAPs should maintain training records for their staff.	**Network Types(s):** 9-1-1 Agencies; Government **Industry Role(s):** PSAPs **Keywords(s):** Human Resources; Policy; Training and Awareness	Important	**New PSAP**