September 2014

WORKING GROUP 7
Legacy Best Practices Updates

Final Report – Legacy Best Practices

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.

The primary objective of Best Practices is to provide guidance, based on assembled industry expertise and experience, to improve network security, reliability and resiliency[1]. In order to provide that guidance, Best Practices must be regularly and expertly reviewed and updated, expanded, or in some cases deleted to provide the most valuable and dependable source of industry guidance. This final report takes a fresh look at 476 legacy Best Practices that have not been reviewed since CSRIC II. In addition a set of proposals made by the Alliance for Telecommunications Industry Solutions (ATIS) Network Reliability Steering Committee (NRSC) were considered and incorporated into the wider body of Best Practices.

In the 1990's the Network Reliability Council (NRC), the predecessor of the Network Reliability Interoperability Council (NRIC) and CSRIC defined Best Practices as "countermeasures (but not the only countermeasures) which go furthest in eliminating the root cause(s) of network outages. It is understood that all countermeasures may not be universally applicable." The FCC currently defines Best Practices as "the most efficient and effective method of accomplishing the tasks in each of our covered areas, based on repeatable procedures that have proven themselves over time for large numbers of people, responses, organizations, or functions.[2]" In this final report Working Group 7 makes every effort to preserve the intent of the original creators of Best Practices in improving and protecting the nation's communications networks by the sharing of expert knowledge in a consistent and voluntary approach. From creation, Best Practices were understood to be a foundation of voluntary guidance for different and unique communication network business models and it remains vital they maintain their intended flexibility and innovation in a non-mandated environment.

One key element in any modification of Best Practices is to use a consistent and repeatable methodology during their assessment. This ensures that analyses are completed in the same manner by multiple teams, and results in a Best Practice that can be applied by the largest audience possible. In this report Working Group 7 addresses legacy Best Practices and speaks to their continued relevance considering that some Best Practices may have become outdated, superseded, duplicative with other Best Practices, or no longer address a current problem. Finally, the wording of a Best Practice should address a single thought and should not promote "pay-for" documents.

In this final report, Working Group 7 provides recommendations on modified and no longer relevant legacy Best Practices and new Best Practices we defined early in the process as "*Best Practices that address categories that are non-cyber security and non-public safety. This*

[1] ATIS Network Reliability Steering Committee (NRSC) Best Practice Tutorial Revised February 2014
[2] http://transition.fcc.gov/pshs/clearinghouse/best-practices.html, last visited August 14, 2014

definition applies to Best Practice network types of Cable, Internet/Data, Satellite, Wireless, and Wireline." Working Group 7 also addressed gaps discovered during analysis with recommendations for future CSRICs to consider. Working Group 7 recommends that the CSRIC Council adopt the Best Practice updates and gap findings as proposed.

2 Introduction

This final report documents the efforts undertaken by the CSRIC IV Working Group 7 with respect to the modernization of 476 legacy Best Practices. The review of Best Practices on a regular basis is essential in providing the communications industry the most comprehensive and up-to-date guidance on network security, reliability, and resiliency. The report outlines recommendations regarding the creation of new Best Practices, modification or deletion of targeted Best Practices, and also includes recommendations regarding the proposed modifications by the NRSC submitted to CSRIC for consideration. The report also describes gaps in the Best Practice process identified by Working Group 7 during their assessment. Finally, the report provides a recommended approach for evaluation of Best Practices by future CSRICs outlining a consistent methodology.

2.1 CSRIC Structure

Communications Security, Reliability, and Interoperability Council (CSRIC) IV									
CSRIC Steering Committee									
Chair or Co-Chairs: Working Group 1	Chair or Co-Chairs: Working Group 2	Chair or Co-Chairs: Working Group 3	Chair or Co-Chairs: Working Group 4	Chair or Co-Chairs: Working Group 5	Chair or Co-Chairs: Working Group 6	Chair or Co-Chairs: Working Group 7	Chair or Co-Chairs: Working Group 8	Chair or Co-Chairs: Working Group 9	Chair or Co-Chairs: Working Group 10
Working Group 1: Next Generation 911	Working Group 2: Wireless Emergency Alerts	Working Group 3: EAS	Working Group 4: Cybersecurity Best Practices Working	Working Group 5: Server-Based DDoS Attacks	Working Group 6: Long-Term Core Internet Protocol Improvements	Working Group 7: Legacy Best Practice Updates	Working Group 8: Submarine Cable Landing Sites	Working Group 9: Infrastructure Sharing During Emergencies	Working Group 10: CPE Powering

Working Group 7 Team Members

Working Group 7 consists of the members listed below.

Name	Company
Kyle Malady - Chair	Verizon
Mary Boyd	Intrado
Tim Collier	Sprint
Shahin Daneshkhah	Sprint
Victor DeVito*	AT&T
Stacy Hartman*	CenturyLink
Robin Howard*	Verizon
Rick Krock*	Alcatel Lucent
John Marinho	CTIA
Bob Oenning	911RP
Andre Savage	Cox Communications
Andy Scott	NCTA
Gigi Smith	APCO
Kathy Whitbeck	Nsight
Christian Vogler	Gallaudet University

Table 1 - List of Working Group Members

*Subteam Leaders

3 Objective, Scope, and Methodology

3.1 Objective

The CSRIC IV Council has been charged with refreshing a subset of industry Best Practices not reviewed since CSRIC II and to modernize, enhance, or clarify them based on changes in technology, practices, or observed reliability trends.

Objective 1: Identify Legacy Best Practices
This objective was to review the current set of industry Best Practices and identify a subset of those to be studied for legacy reliability and resiliency applications. 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.

Objective 2: Review and Modify Legacy Best Practices
This objective was to review the subset of industry Best Practices determined to qualify as legacy Best Practices. Where necessary additional Best Practices would be recommended given changes in technology, practices, or observed reliability trends. The review was performed using a standardized checklist to ensure a consistent assessment was performed on each Best Practice.

Objective 3: Recommend Changes to Existing Best Practices
This objective was to document the recommended changes to qualifying Best Practices, new recommended Best Practices, and Best Practices identified for deletion. The Best Practice recommendations were provided in a standardized format for ease of database entry following approval by CSRIC IV Council.

Objective 4: Incorporate Recommendations by ATIS
This objective was to review revisions to Best Practices proposed by ATIS NRSC and recommend how to incorporate the changes into the wider body of Best Practices. This was accomplished by reviewing the ATIS revisions against Working Group 7 recommendations and blending the suggestions into each Best Practice.

3.2 Scope

This final report analyzes current Best Practices that were originally developed as applicable to legacy networks, systems, and processes. Identified "in scope" Best Practices were to be evaluated for continued relevance, applicability to current network technology where appropriate, as well as structure, wording, and reference updates. Given this scope it was essential to perform an initial review on the full set of 1,022 Best Practices developed by previous NRIC Focus Groups and CSRIC Working Groups. The full Best Practice data set did not qualify under the definition of legacy Best Practices as defined by Working Group 7; therefore it was determined that those Best Practices that weren't relative to the study were out of scope. This report also outlines the development of new Best Practices, and the identification of any gaps, that will provide additional guidance to industry and public safety authorities.

This report reinforces previous guidance that industry Best Practices are voluntary in nature and may not apply in every situation due to the need for flexibility, innovation, and control in the management of different carriers' unique business models, cost, feasibility, resource limitations, or other factors. This guidance is consistent with work completed by previous CSRIC Working Groups in CSRIC II and CSRIC III. CSRIC II Working Group 6 concluded:

Compliance with the Best Practices should not be a regulatory mandate. Attempting to identify which Best Practices might be required of every participant in the communications industry would be very impractical, if not impossible. Mandating compliance with particular Best Practices would impact the ability of organizations, their customers, and other constituents to manage the value proposition, the pricing that defines their business models, and participation in the industry. Compliance with Best Practices should be voluntary in order to allow for co-existence of new and old technologies.[3]"

Similarly, CSRIC III Working Group 8 concluded:

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

[3] CSRIC II Working Group 6 Best Practice Implementation Final Report, January 2011, Key Recommendations, page 3 of 51.

experts who have the overall experience to interpret the individual Best Practice in the manner in which it was intended[4].

3.3 Methodology

The process for determining methodology is often based in theory and can be said to encompass the use of "Best Practices" which are the set of methods applied to address a given issue. In this report Working Group 7 documents the ongoing evolution of industry Best Practices in a consistent and repeatable manner using an assembled team of experts that applied a best practice approach in achieving the objectives. In this section, Working Group 7 outlines the Best Practice methodology used in performing the work entrusted to us. We have confidence that future CSRIC Working Groups would benefit from review and use of this process to more efficiently move Best Practice assessment from concept to implementation.

3.3.1 Best Practice Legacy Identification Process

Working Group 7 decided that legacy NRIC/CSRIC Best Practices would be defined as the subset of the total Best Practice library that was not related to cyber security or applied only to public safety. These Best Practices have a numbering format that typically assigns a single number as a classification code, and then a unique three number reference for each Best Practice. The format for NRIC/CSRIC Best Practices is based on the following format[5]:

X – Y – Z# # #

Where:

X = the current, or most recent, CSRIC Council
Y = the CSRIC Council in which the Best Practice was last edited
Z = 0-4 for Network Reliability and Interoperability
= 1 for Disaster Recovery and Mutual Aid
= 3 for Public Safety
= 5 for Physical Security
= 8 for Cyber Security

= any digits, where every Best Practice has a unique Z# #

Working Group 7 identified a total of 476 of the 1,002 current Best Practices in which to target our initial review, which was broken out as follows:

Best Practices
275 – Network Reliability and Interoperability
25 – Disaster Recovery and Mutual Aid
176 – Physical Security

[4] CSRIC III Working Group 8 E9-1-1 Best Practices, Final Report Part 2, March 2013, Section 3.2 Scope, page 8 of 110.
[5] ATIS Network Reliability Steering Committee (NRSC) Best Practice Tutorial Revised February 2014, Best Practice Numbering Format

3.3.2 Best Practice Review Checklist

In order to perform a consistent review of the Best Practices divided amongst the subteams, a checklist was developed for Working Group 7 to use as an aid. The checklist consisted of 11 checkpoints the subteams were asked to review on each Best Practice. The checklist items were:

Checklist Item	Definition	Choices
In Scope	Best Practice addresses an issue that is not associated specifically to Cybersecurity or Public Safety needs or class of problems.	**Y** = This BP is in-scope for Working Group 7 **N** = This BP is out of scope for Working Group 7
Relevant	Best Practice is still valid and relevant to industry (i.e., it still addresses a current need or class of problems).	**Y** = BP is still relevant to industry **N** = BP does not address current needs, is outdated, or could be recommended for deletion
Wording OK	Best Practice is worded in a way that clearly states the need or class of problems and is OK as written.	**Y** = BP is OK as written and no change is necessary **N** = BP needs to be re-written and/or updated
References OK	Reference material is relevant and worded OK for this Best Practice and does not need to be updated or removed.	**Y** = References are OK as written and no change is necessary **N** = References are no longer accurate and needs to be updated or deleted
Network Types OK	Network Types for the Best Practice are correctly stated and do not need to be updated.	**Y** = Network Types are accurately stated and no change is necessary **N** = Network Types need to be updated to include/exclude one or more
Industry Roles OK	Industry Roles for the Best Practice are correctly stated and do not need to be updated.	**Y** = Industry Roles are accurately stated and no change is necessary **N** = Industry Roles need to be updated to include/exclude one or more
Correct Status OK	Status is correctly stated for this Best Practice as Critically Important, Highly Important, or Important.	**Y** = Status is accurately stated and no change is necessary **N** = Status needs to be updated to a new status
Keywords OK	Keywords are correctly identified for this Best Practice.	**Y** = Keywords are accurately stated and no change is necessary **N** = Keywords needs to be updated to include/exclude one or more
Web links OK	Any Web links embedded in the Best Practice are up to date and go to the correct web site/page.	**Y** = Web link(s) are working and goes to the correct web site/page **N** = Weblink(s) fail or do not go to the correct web site/page **N/A =** Not Applicable for this BP
No reference in Best Practice	There are no documents or web links mentioned in the Best Practice verbiage that could be moved to the References section.	**Y** = No document or weblink references in the BP verbiage **N** = There are document(s) and/or web links in verbiage that need reviewed for movement to reference section **N/A =** Not Applicable for this BP
One Thought	There is only a single thought contained in this Best Practice.	**Y** = There is only a single thought depicted in the BP **N** = There are, or appears to be, multiple thoughts referenced in the BP

Table 2 – Working Group Best Practice Review Checklist

3.3.3 Best Practice Review Process

Working Group 7 performed a review of each Best Practice using a process based on the checklist. At each checkpoint a decision needed to be made regarding the Best Practice. Decisions triggered deeper evaluations, gap analysis, modifications, deletion recommendations, up-to-date and no changes necessary determination, or new Best Practice recommendations. Figure 1 provides a high level flow Working Group 7 followed for each Best Practice reviewed.

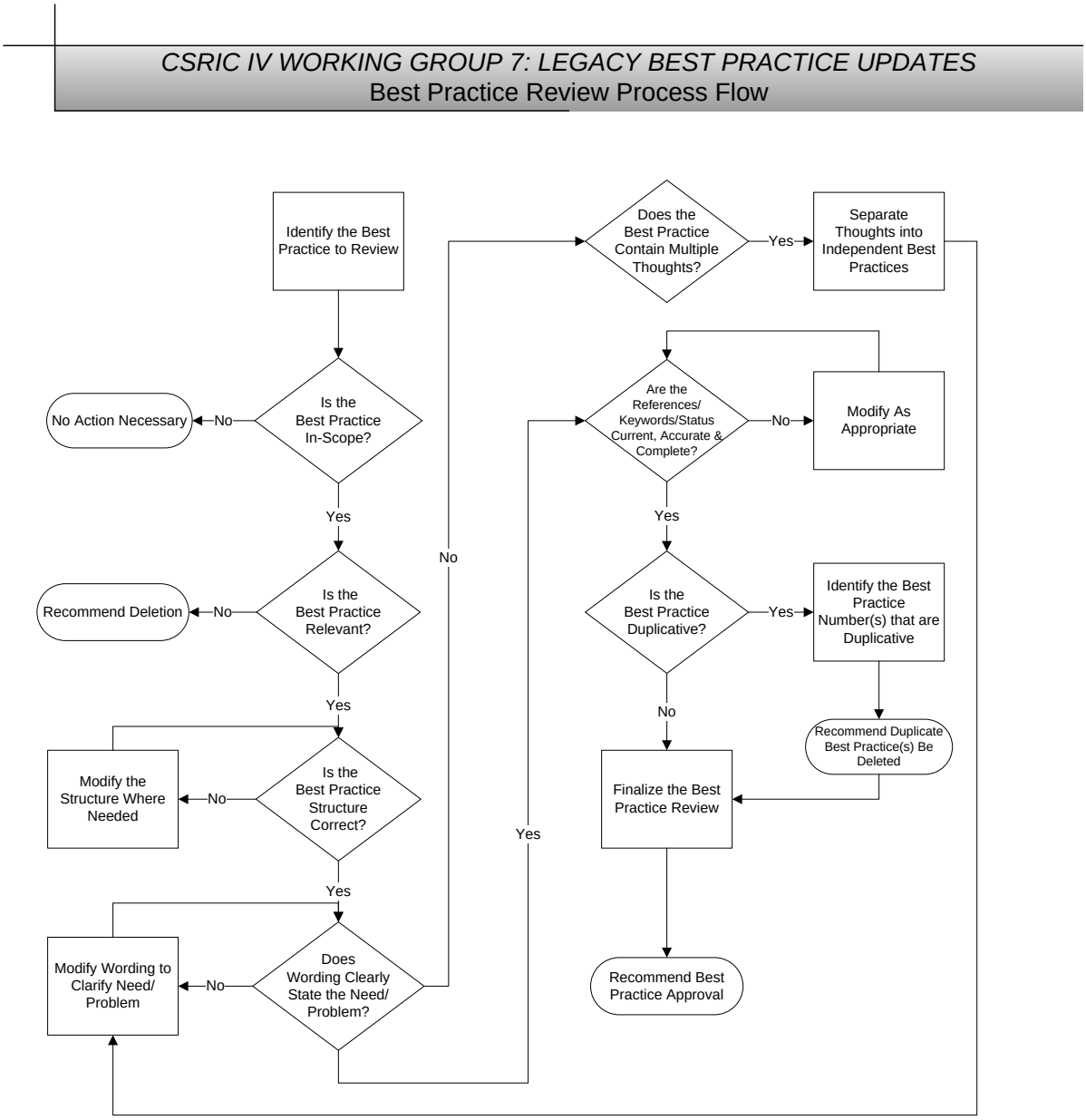

Figure 1 - Best Practice Review Flow

3.3.4 Best Practice Supporting Elements

A Best Practice is made up of two key building blocks – the Best Practice wording and the references – which determine the value and guidance provided by the Best Practice to the largest cross section of the communications industry. To assist users in finding specific Best Practices and knowing how and when to apply them, four supporting elements are associated with each Best Practice and need to be updated whenever a Best Practice is created or modified. The four supporting elements of a Best Practice are; Network Type, Industry Role, Status, and Keywords. Figure 2 represents the building blocks and supporting elements of a Best Practice Working Group 7 used to analyze the targeted set of Best Practices.

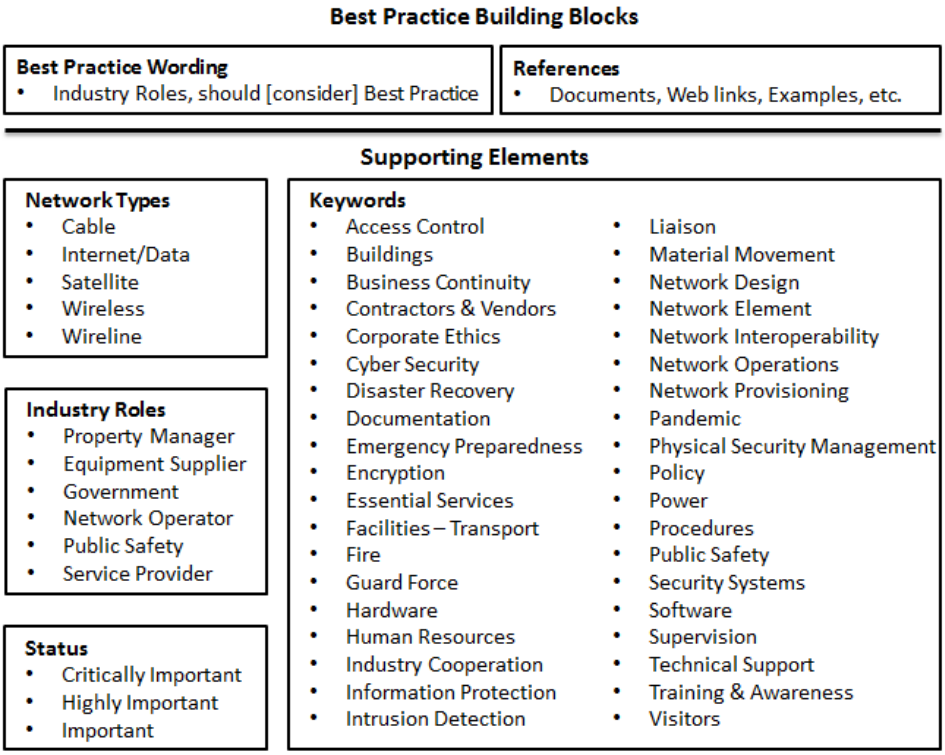

Figure 2 - Building Blocks and Supporting Elements of a Best Practice

Each supporting element has several options available, each having a written definition to ensure consistency in their application. When considering edits, the reviewer must review and update the supporting element choices as appropriate, using the definitions as a guide. Individuals or teams modifying Best Practices should have sufficient knowledge on the Best Practice subject matter in order to select the proper elements. Short of this level of detail, a modification can unintentionally change the original intent of the Best Practice and result in unreasonable and/or inappropriate guidance to industry. In some cases it may also become necessary to look back to the NRIC/CSRIC Final Report that first recommended the Best Practice to understand the original intent.

Best Practice references are another consideration needing study to ensure they are not overly narrow in focusing on particular documents where in fact multiple document options may exist. When wording Best Practices, the inclusion of pay-for–use documents, web links, or highly selective documents into the verbiage runs the risk of premature obsolescence or limiting the

applicability of the Best Practice. Pay-for documents are those that a user of the Best Practice would be required to acquire at a cost. Using pay-for documents as examples in the reference section is acceptable, but they should be avoided in the main body of the Best Practice.

Appendix 2 includes the list of the supporting element definitions used by Working Group 7 during analysis of targeted Best Practices.

3.3.5 Best Practice Wording Structure

Best Practice wording is vital to the understanding, the passing of meaning, and the intent of the authors. Figure 3 demonstrates the recommended ATIS NRSC Best Practice format that Working Group 7 agrees is consistent in delivering the most concise and understandable guidance. Best Practices that were structured in this format, in Working Group 7's opinion, were more to the point and had a better flow than those that did not follow this structure.

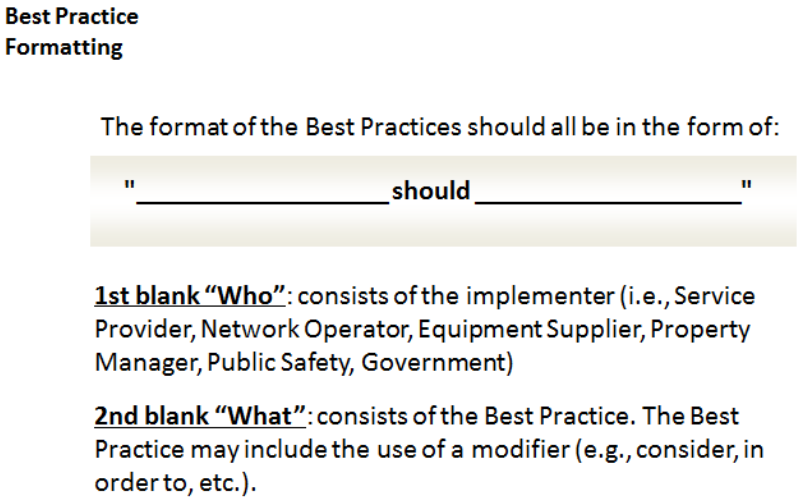

Figure 3 - Best Practice Wording Structure

3.3.6 Best Practice Implementation to Production

Working Group 7 agreed that one issue that has been often overlooked by other CSRIC Working Groups is the format used when offering Best Practice recommendations to the CSRIC Council for consideration. Following a successful adoption of a set of Best Practice recommendations it is desirable for those Best Practices to move as quickly as possible into the two online production databases used by industry[6]. Delivering new or modified Best Practices for consideration without all of the supporting elements addressed can significantly delay their introduction into the databases managed by the FCC and ATIS and, in turn, delay their adoption by industry. Using past team experience with implementing CSRIC Best Practices, Working Group 7 adopted a presentation format that has proven successful in providing an efficient

[6] FCC Best Practice website: https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm and ATIS Best Practice website: http://www.atis.org/bestpractices/Default.aspx, last visited August 4, 2014.

means for database entry.

Figure 4 shows the format Working Group 7 used to present recommendations to the CSRIC Council in this report that can be used to expedite the inclusion of the Best Practices into the on-line databases. In this example a modified Best Practice is shown. Each of the four supporting elements of a Best Practice as discussed earlier in the report is addressed in this format.

CSRIC IV Best Practice Number	CSRIC IV Best Practice	CSRIC IV BP Reference/Comments	Best Practice Status	CSRIC IV (New/Changed/ Unchanged/ Deleted)
9-7-5164 (1)	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should establish and enforce a policy to immediately report stolen or missing company vehicles and trailers to the appropriate authorities. (2)	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Public Safety Service **Reference(s):** No Change (3) **Status:** Changed	Important (4)	**Changed** (5)

Figure 4 - Presenting Best Practices

1. Current Best Practice number. The FCC is responsible for updating the Best Practice number following Council approval or assigning a number for all newly created Best Practices.

2. Best Practice verbiage recommendation, as modified and being presented for vote and approval.

3. Detailed changes to the supporting elements of the Best Practice and reference sections of the Best Practice. In the case of a recommended deletion, the explanation for the deletion is provided.

4. Recommended Best Practice status following approval process of Best Practice (e.g., Critically Important, Highly Important, or Important).

5. Overall change being made to the Best Practice (e.g., New, Changed, Delete, or Unchanged).

4 Analysis, Findings and Recommendations

4.1 Analysis

Working Group 7 divided the 476 legacy Best Practices identified as the targeted data set into four smaller data sets. Teams A-D were assigned 120 Best Practices each to review and in turn provided their initial recommendations to the full Working Group 7 team for consideration. Each of the teams had a team leader who was well versed in Best Practice development. This ensured that each team had an expert resource available to lead the team in discussions and to provide periodic reports to the full team on any concerns or gaps identified. Prior to the reviews beginning, training was provided using the Best Practice tutorial created by the ATIS NRSC. Teams were asked to complete the 11 point checklist for each Best Practice reviewed and document rationale for changes as necessary. Best Practice changes proposed by ATIS NRSC were blended in alongside the team reviews to provide the best overall recommendations.

A monthly measure was established to keep teams on course and to make certain milestones set by the full team were met. On 3/19/14 the full team met face-to-face in Washington, DC to finalize the first half of the Best Practice recommendations. A total of three sets of Best Practices were eventually analyzed with Round 1 review completed on 3/19/14, Round 2 completed on 5/27/14, and Round 3 completed on 6/13/14.

The full Working Group 7 team met on a regular basis through May 2014 to review overall process. Upon completion of the final data set, the team met as necessary to complete the final report. Working Group 7 full team meetings were held on 9/19/13, 9/26/13, 11/1/13, 11/26/13, 12/18/13, 1/15/14, 1/29/14, 2/12/14, 3/19/14, 4/9/14, 5/21/14, and 8/22/14. Between full team calls, email was used to provide status updates and complete Best Practice reviews. Teams A-D established their individual schedules of team meetings to review their subset of Best Practices. Working Group 7 provided status readouts at CSRIC Council meetings on 9/12/13, 12/4/13, 3/20/14, 6/18/14, and 9/24/14.

4.2 Findings

Working Group 7 concluded an analysis of an initial set of 476 Best Practices. Through this analysis using processes outlined earlier in this report, a total of 458 Best Practices were found to be relevant and in scope and classified as legacy. A total of 18 were rejected as out of scope and review was concluded. A total of four new Best Practices were created and one new NRSC recommended Best Practice supporting elements were completed and 22 were found to be no longer relevant or duplicative and were targeted for deletion. At the conclusion of the analysis, a total of 396 Best Practices were updated with one or more changes and 40 were found to be satisfactory as written and no changes were necessary.

During the analysis there were several key findings that had had a recurring theme. These issues appeared at the highest rate and warrant further clarification:

Best Practice Taglines
A tagline is the short two to four word introduction found on many Best Practices. Working

Group 7 assessed the value of taglines and considered if they should be officially removed from all current and future Best Practices. Due to the lack of consistency of taglines and because existing search engines on the FCC and ATIS databases provide more than adequate search options, Working Group 7 concluded they add no value and should be discontinued. Below are two examples to demonstrate the ambiguity in taglines:

> Tagline Examples (in red):
> National Security and Emergency Preparedness: Government, Network Operators and Service Providers of critical services to National Security and Emergency Preparedness (NS/EP) users should be familiar with the Telecommunications Service Priority (TSP) program and support / promote it as applicable. **(Could also be "Telecommunications Service Priority")**
>
> Network Element Support: Network Operators and Service Providers should provide duplicated, non-co-located maintenance administration, surveillance and support for network elements. **(Could also be "Duplicated Support Sites")**

Public Safety Industry Role

In CSRIC III, a new Industry Role of *Public Safety* was established to appropriately recognize the importance of this key contributor to E9-1-1 reliability and resiliency[7]. This Industry Role was found to be applicable to many legacy Best Practices in light of the fact that many Public Safety organizations maintain their own communications networks. This Industry Role had not been applied to the larger set of Best Practices since its approval in June of 2012. Where applicable, Working Group 7 has updated in scope Best Practices to include this new Industry Role.

Best Practice References

Working Group 7 discovered a number of Best Practices where information contained in the body of the Best Practice was better aligned as reference support material. In these cases, the Best Practice was found to be just as effective once specific standard documents, pay-for documents, or web link references were moved to the reference support section. In other cases it seemed that the authors of the Best Practices were unaware of the reference section and included references as part of their development processes. Working Group 7 revised the Best Practices to maintain the original intent of the Best Practice while preserving the reference materials.

Best Practice Gaps

During the analysis phase, Working Group 7 documented several gaps that are being documented for future CSRIC consideration.

> **Best Practice Creation Guide**
> The development and editing of Best Practices for the purpose of having the greatest value for industry should be done in a tightly controlled and constant manner. The mishandling of a Network Type, Industry Role, Status, or Keyword can overinflate or devalue the Best Practice resulting in it not being widely adopted by industry. This can also lead to confusion as to why a particular Best Practice has or has not been adopted. For example, several Best Practices that Working Group 7 analyzed using the definitions

[7] CSRIC III Working Group 8 – E9-1-1 Best Practices, Final Report – Part 1, Appendix 1, page 19 of 112, Non-Best Practice recommendations, June 2012.

provided in Appendix 2 led to addition or deletion of supporting elements such as Network Types or Industry Roles, expanding or reducing their scope. Working Group 7 concluded that with Working Group members changing with every CSRIC, if a Best Practice creation guide existed outlining the necessary and standard steps when creating or editing Best Practices, the overall quality and accuracy would improve. Working Group 7, as well as other Working Groups, is dependent on the independent knowledge of team members to locate process and definition documents which leads to inconsistency in the process. In section 4.3 of this report, Working Group 7 recommends a solution to this process gap to ensure references to definition documents are included for future CSRIC Working Groups.

Best Practice Overlap

Working Group 7 considered that there is ongoing risk that multiple Working Groups may unintentionally choose to edit the same Best Practices, or create similar Best Practices in parallel. Uncoordinated changes between Working Groups may come into conflict within various final reports. The overlap and conflict issues appear when Working Groups pull overlapping lists of Best Practices using the same keywords, or active Working Groups plan to cite Best Practices that are being modified by another Working Group leading to duplicated efforts and conflicts.

For Purchase Documents

Working Group 7 believes that Best Practices should not contain references or advertise documents that a user must pay for as a condition of implementing the Best Practice. Working Group 7 has made every effort to move occurrences of pay-for documents to the reference section and redefine as examples of available documents. However, there remain many Best Practices that were out of scope for Working Group 7 that still contain these references.

Non-Core Best Practices

Working Group 7 reviewed a number of Best Practices that did not clearly support the underlying theme of addressing reliability, security, or interoperability issues. These non-core Best Practices should be actively searched out, reviewed, and deleted if necessary. In one example, Working Group 7 concluded the Best Practice appeared to be sales related or setting of customer expectations and provided no real guidance to industry.

Recommendations

1. Working Group 7 recommends Best Practice edits outlined in Appendix 1 of this final report should be adopted and approved by CSRIC IV Council. Following approval, the FCC should incorporate the modified Best Practices into production online websites for general use of industry.

2. Working Group 7 recommends that the FCC establish a Best Practice clearing house function in all future CSRIC's. This clearing house will ensure multiple Working Groups are not modifying the same Best Practices preventing duplication of effort and conflicting final reports. The clearing house should be used too as a resource for Working Groups to ensure all supporting elements of a Best Practice have been properly addressed to avoid any delays in their implementation. This clearing house can be part of the CSRIC or an external industry organization with expertise in Best Practice structure and design.

3. Working Group 7 recommends that the use of Best Practice taglines be permanently eliminated and be removed from all remaining Best Practices. Taglines can be removed either in bulk by the FCC or at the time a Best Practice is modified/reviewed in future CSRIC activities. Any new Best Practices recommended in the future should not contain a tagline and, if one is provided, should be removed before being placed in production.

4. Working Group 7 recommends that a future CSRIC be tasked with the creation of a documented process outlining a consistent and standard process for Best Practice creation. This document should incorporate the supporting elements of a Best Practice, standard structure, and standard definitions to be used as a resource by creators/editors of Best Practices. This document should be made available at the beginning of all future CSRIC's to provide Working Group guidance. The FCC may consider consigning this recommendation to an external party (e.g., ATIS NRSC) experienced in the creation and structure of Best Practices.

5. Working Group 7 recommends that the FCC promote the process used to develop these Best Practices as part of a Best Practices education effort. This educational effort could incorporate a discussion on how the telecommunications industry utilizes Best Practices in their operational environment.

6. Working Group 7 recommends that a future CSRIC address the issue of pay-for documents referenced in Best Practice verbiage. A review of all remaining Best Practices should be scheduled with the goal of moving *pay-for* documents to the reference section of Best Practices as examples. Use of Best Practices should not be contingent on the purchase of a specific document. The FCC may consider consigning this recommendation to an external party (e.g., ATIS NRSC) experienced in the creation and structure of Best Practices.

7. Working Group 7 recommends that a future CSRIC consider reviewing all Best Practices to identify those that do not meet the core definition of clearly supporting the reliability, security, or interoperability of the communication network. Once identified, consider

targeting these non-core Best Practices for removal.

8. Working Group 7 recommends that a future CSRIC consider chartering a Working Group to revisit all the Best Practices that deal with locating buried facilities and reconcile those with current 811 programs, including suggestions for collaboration with other industries.

5 Conclusions

Best Practices are guidelines for industry that are the aggregated experiences of many experts who, through their use, have demonstrated a high level of benefit in the reliability, security, or interoperability of the nation's communications networks. Best Practices are not intended to be applicable in all situations; however, corporations should regularly review Best Practices and consider adoption into their individual organizations.

The continued periodic review of Best Practices by experts for relevance, content, and accuracy is paramount for providing the highest level of value to the industry. Best Practices should never be restrictive in a manner that requires the purchase of additional documents in order to fully implement the practice. These types of restrictions dilute the overall value of Best Practices and their adoption by industry. Every communications organization will benefit from the evaluation of Best Practices even if resources do not permit their adoption. The ability to develop alternatives to voluntary Best Practices that are tailored to the individual organization is an important part of what makes Best Practices so valuable.

Based on the efforts of Working Group 7 several recommendations have been presented in this report that improve on Best Practices and the Best Practice process. Ongoing creation and periodic expert reviews should be held to the highest standards possible to ensure the greatest value to industry. Consistency in Best Practice creation and editing guidelines are paramount to their continued adoption. Best Practices that do not measure up to these strict quality guidelines should be reconsidered, modified if possible, or deleted if necessary.

In this final report, Working Group 7 performed the following:

- Reviewed over 470 Best Practices and provided edits to modernize and refresh based on changes in technology, practices, or observed reliability trends.
- Created four new Best Practices to address new classes of problems or to divide existing Best Practices into multiple individually focused Best Practices.
- Updated one new NRSC recommended Best Practice with supporting elements for approval.
- Recommended the deletion of 22 Best Practices found to be no longer relevant or needed.
- Developed recommendations and proposals intended to provide ongoing guidance to future CSRICs and external parties on maintaining a quality process and consistency in the Best Practice process.

6 Appendix 1 – Best Practice Recommendations

CSRIC IV Best Practice Number	CSRIC IV Best Practice	CSRIC IV BP Reference/Comments	Best Practice Status	CSRIC IV (New/Changed/ Unchanged/ Deleted)
BEST PRACTICES - NEW				
WG7-1-2	Network Operators, Service Providers and Property Managers should utilize Transfer Switch Equipment that conforms to industry standards.	**Network Types(s):** Cable, Internet, Satellite, Wireless, Wireline **Industry Role(s):** Property Manager, Network Operator, Service Provider **Keywords(s):** Buildings, Network Design, Network Operations, Power, Procedures **Reference(s):** Add: http://www.ul.com/global/eng/pages/solutions/standards/accessstandards/	Important	**New**
WG7-1-3	Network Operators, Equipment Suppliers and Property Managers should consider marking or modifying copper bars and cable to deter theft, to make them easier to identify at scrap yards, and/or to reduce their value.	**Network Types(s): Add:** Cable, Internet, Satellite Wireless, Wireline **Industry Role(s):** Add: Network Operators, Equipment Suppliers, Property Managers **Keywords(s):** Add: Facilities Transport, Hardware, Power, Physical Security Management **Reference(s):** Add: This may include stamping copper ground bars with "Registered Property" and "Recycling Prohibited", tinning copper ground bars or coating them with cold galvanizing spray, and marking cable with identifying markings.	Important	**New**

CSRIC IV Best Practice Number	CSRIC IV Best Practice	CSRIC IV BP Reference/Comments	Best Practice Status	CSRIC IV (New/Changed/ Unchanged/ Deleted)
WG7-1-4	Network Operators, Service Providers, Public Safety, and Property Managers should utilize a UL standard for Transfer Switch Equipment.	**Network Types(s):** Cable, Internet, Satellite, Wireless, Wireline **Industry Role(s):** Property Manager, Network Operator, Service Provider, Public Safety **Keywords(s):** Buildings, Network Design, Network Operations, Power, Procedures **Reference(s):** http://www.ul.com/global/eng/pages/solutions/standards/accessstandards/ **Status:** New	Important	**New**
WG7-1-5	Network Operators, Service Providers, Public Safety, and Property Managers should mechanically and electrically interlock transfer breaker systems when they are utilized.	**Network Types(s):** Add: Cable, Internet, Satellite, Wireless, Wireline **Industry Role(s):** Add: Property Manager, Network Operator, Service Provider, Public Safety **Keywords(s):** Add: Buildings, Network Design, Network Operations, Power, Procedures **Reference(s):** No Change **Status:** New	Highly Important	**New**

CSRIC IV Best Practice Number	CSRIC IV Best Practice	CSRIC IV BP Reference/Comments	Best Practice Status	CSRIC IV (New/Changed/ Unchanged/ Deleted)
WG7-1-6	Network Operators, Service Providers, Public Safety, and Property Managers should verify that protector size does not exceed cable rated current capacity.	**Network Types(s):** Add: Cable, Internet, Satellite, Wireless, Wireline **Industry Role(s):** Property Manager, Network Operator, Service Provider, Public Safety **Keywords(s):** Fire, Hardware, Network Operations, Power **Reference(s):** No Change **Status:** New	Important	**New**

BEST PRACTICES - DELETIONS				
9-7-0817	For the deployment of Residential Internet Access Service, Broadband Network Operators should select, implement and locate equipment within the operators architecture to provide residential internet access to the most users where economically and technically feasible.	**Delete BP:** This Best Practice is not in scope as far as Security, Reliability or Interoperability is concerned.	Highly Important	**Delete**
9-9-0823	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.	**Delete BP:** This Best Practice is not in scope as far as Security, Reliability or Interoperability is concerned. This is performance related and more appropriate for service level agreements with users.	Highly Important	**Delete**
9-8-0811	Specified Rate Services: Service Providers should make available meaningful information about expected performance with respect to upstream and downstream throughput and any limitations of the service. Specified rate services (such as those covered by QoS or similar systems) should be handled by an SLA between the parties.	**Delete BP:** This BP appears to be sales/setting customer expectations, not Cyber Security	Important	**Delete**
9-7-1025	Network Operators and Service Providers should consider using a team to quickly determine appropriate actions both pro-active and re-active to address potential or real threats.	**Delete BP:** Best Practice is too vague, does not recommend specific action that would be of value for Network Operators or Service Providers. Believe this function would be integral to any security process or procedure.	Highly Important	**Delete**
9-6-5023	Network Operators, Service Providers and Equipment Suppliers should establish and enforce a policy that requires all individuals to properly display company identification (e.g., photo ID, visitor badge) while on company property. Individuals not properly displaying a badge should be challenged and/or reported to security.	**Delete BP:** Best Practice 9-7-5021 covers access procedures more broadly. Delete this BP and added a brief note to 9-7-5021 stating, “Processes should include challenging non-badged personnel."	Important	**Delete**

9-6-5253	Network Operators, Service Providers and Equipment Suppliers should use lessons learned from restoration efforts to update recovery plans for transponder loss, satellite payload failure and satellite failure.	**Delete BP:** This thought is captured in BP 9-9-5227 which has more details and useful reference	Highly Important	**Delete**
9-6-5254	During restoration efforts, Network Operators and Service Providers should not permit unsecured wireless access points for the distribution of critical data or operating system upgrades.	**Delete BP:** This Best Practice was combined with 9-6-5172	Important	**Delete**
9-7-5115	Network Operators, Service Providers, Equipment Suppliers and Property Managers should provide and reinforce as appropriate mail screening procedures to relevant employees and contractors to increase attention to security.	**Delete BP:** This Best Practice was combined with 9-7-5114	Important	**Delete**
9-7-5123	Network Operators should maintain and control access to accurate location information of critical network facilities in order to identify physical locations hosting critical infrastructure assets.	**Delete BP:** This Best Practice is a duplicate of 9-7-5022.	Highly Important	**Delete**
9-7-5238	Network Operators, Service Providers who are tenants in multi-tenant facilities (e.g., telecom hotels) should coordinate security and restoration efforts with the Property Manager.	**Delete BP:** This Best Practice was combined with 9-7-5236 and should be deleted.	Important	**Delete**
9-7-5262	Network Operators, Service Providers and Equipment Suppliers should evaluate the vulnerability of storage locations in an effort to protect critical spares.	**Delete BP:** This Best Practice is duplicative of 9-7-5030 and should be deleted.	Important	**Delete**
9-7-0468	Antenna Structure Sharing: Network Operators and Property Managers should consider agreements to share in-building cellular antenna infrastructure between multiple service providers in order to make it more feasible to deploy in-building systems.	**Delete BP:** Not related to reliability, security, or interoperability issue.	Important	**Delete**

9-7-0583	Reporting and Tracking Outages: Network Operators, Service Providers and Equipment Suppliers should adopt an industry uniform method of reporting and tracking significant service outages.	**Delete BP:** Outage Reporting is mandatory and does not require a BP to comply.	Highly Important	**Delete**
9-7-0597	Network Technician Training: Network Operator and Service Provider network technicians should be trained in (1) detection of conditions requiring intervention, (2) escalation procedures, and (3) manual recovery techniques.	**Delete BP:** This Best Practice was combined with 9-5-0511.	Highly Important	**Delete**
9-6-1041	Disaster Recovery: Equipment Suppliers should consider providing a "Disaster Recovery Services Checklist" to all of the Service Providers they support. The checklist would assist the Service Provider in identifying equipment needs and professional services during an event.	**Delete BP:** This Best Practice was combined with 9-6-1044.	Highly Important	**Delete**
9-7-5028	Access Control Exceptions: Network Operators, Service Providers, Property Managers, and Equipment Suppliers should establish policies and procedures related to access control to provide exception access (e.g., emergency repair or response, forgotten credential, etc.).	**Delete BP:** This Best Practice has been combined with 9-6-5021.	Highly Important	**Delete**
9-7-0434	Employee Training: Network Operators, Service Providers, Equipment Suppliers and Property Managers should provide appropriate training and periodic refresher courses for their employees.	**Delete BP:** Duplicate of modified BP 9-5-0511 as well as covered in several other BPs.	Important	**Delete**
9-7-0479	Network Operators should take into consideration fundamental technology differences when operating multiple RF technologies in an existing system. Radio Frequency Interference (RFI) sources (e.g., intermodulation, out of band emissions, receiver overload), link budgets, and performance metrics (e.g., data rates, latency, capacity) should be evaluated.	**Delete BP:** This Best Practice is common sense versus solving a problem or class of problems.	Highly Important	**Delete**

9-6-0810	Service Providers should make available meaningful information about expected performance with respect to upstream and downstream throughput and any limitations of the service; best effort services up to or unspecified bit rate services should be specified as such in a clearly identifiable manner.	**Delete BP:** This Best Practice doesn't support reliability, security, or interoperability and seems to be more sales or marketing based.	Important	**Delete**
9-7-0460	Network Operators should ensure that equipment is installed in accordance with equipment suppliers' stated environmental specifications.	**Delete BP:** This Best Practice combined with 9-7-0815 and deleted as a duplicate.	Important	**Delete**
9-7-0728	Standard Cable Markings: Network Operators should use industry standard markings for outside plant cables.	**Delete BP:** This Best Practice combined with 9-7-0706 and deleted as a duplicate.	Important	**Delete**
9-7-0740	One-Call Center Legislation: Network Operators should implement internal processes needed to support the One-Call Notification legislation.	**Delete BP:** This Best Practice combined with 9-7-0725 and deleted as a duplicate.	Important	**Delete**

BEST PRACTICES - REVISIONS				
9-5-0511	Operators, Service Providers, Public Safety, and Equipment Suppliers should ensure that appropriate operations personnel involved in the direct operation, maintenance, provisioning, security, troubleshooting, repair, and support of network elements are provided periodic training.	**Network Types(s):** No Change **Industry Role(s):** Add: Equipment Suppliers, Public Safety **Keywords(s):** Add: Essential Services, Network Elements, Technical Support, Emergency Preparedness Delete: Industry Cooperation, Network Interoperability **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-5-0514	Network Operators and Service Providers should, when available, utilize a device management architecture that provides a single interface with access to alarms and monitoring information from all critical network elements.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Security Systems **Reference(s):** Examples of device management architectures that support multiple platforms are Common Object Request Broker Architecture (CORBA) and Simple Network Management Protocol (SNMP). **Status:** No Change	Highly Important	**Changed**

9-5-0524	Network Operators and Service Providers should operate an information-only route database containing the routing advertisement source and cannot be changed by peers, customers, and other users, should be highly secure, and should not affect or impact the actual routing table.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Cyber Security **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-5-0526	Network Operators and Service Providers should operate a route registry database of all the routes advertised by their network with the source of that advertisement, with which outside entities can communicate with.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Cyber Security Add: Network Provisioning **Reference(s):** This database might be used as the source for interface configurations as well as troubleshooting problems. These outside entities may be central, regional, or global in nature. **Status:** No Change	Highly Important	**Changed**
9-5-0531	Network Operators, Service Providers, and Public Safety should require staff to use grounding straps when working with equipment where appropriate.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**

9-7-0411	Network Operators, Service Providers, and Public Safety should consider developing and implementing cable labeling standards.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Transport Facilities **Reference(s):** Delete current reference **Status:** Changed	Important	**Changed**
9-9-0418	Network Operators, Service Providers, and Public Safety should, where appropriate, have a documented back-out plan as part of a Method of Procedure (MOP) for scheduled and unscheduled maintenance activities.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-0419	Network Operators and Service Providers should design and capacity-manage EMSs (Element Management Systems) and OSSs (Operational Support Systems) to accommodate changes in network element capacity.	**Network Types(s):** No Change **Industry Role(s):** Add: Network Operators **Keywords(s):** Delete: Pandemic **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0420	Network Operators and Service Providers should periodically measure EMS (Element Management System), NMS (Network Management System) and OSS (Operational Support System) performance using a benchmark or applicable requirements to verify that internal or vendor performance objectives are being met.	**Network Types(s):** No Change **Industry Role(s):** Add: Service Providers **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-9-0447	Network Operators and Service Providers should consider establishing a customer advocacy function to take part in the development and scheduling of network change activity in order to minimize impact.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Policy Add: Liaison **Reference(s):** Delete statement "See BP 0600" **Status:** No Change	Highly Important	**Changed**
9-7-0448	Equipment Suppliers should, where feasible, provide a memory management capability to reconfigure or expand memory without impacting stable calls or other critical processes (e.g., billing).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-0464	Network Operators and Government should cooperate on zoning issues that affect reliability of communication networks serving the public good.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Essential Services **Reference(s):** Add: Examples: noise from emergency backup power generators, aesthetics of tower placement, public safety and health concerns. **Status:** No Change	Important	**Changed**

9-7-0465	Network Operators and Public Safety should account for the effects of environmental changes on attenuation, shadowing, and multipath (e.g., new buildings, tree growth, construction materials) during initial design and through periodic reviews of cell site coverage.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-0466	Network Operators should take into account link budget impacts due to propagation differences between various frequencies when planning network coverage.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change. **Status:** No Change	Highly Important	**Changed**
9-7-0467	Network Operators should give consideration to the degree of balance between RF (Radio Frequency) channels on uplinks and downlinks, for both control and traffic for air interface reliability.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-0486	Network Operators should have an ongoing RF (Radio Frequency) performance improvement process to reduce air interface issues related to blocks, drops, and access failures.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Procedures **Reference(s):** No Change	Highly Important	**Changed**

9-7-0487	Network Operators and Property Managers should have procedures in place to identify and correct degradations in cell site performance resulting from defects in feedlines and antennas (e.g., moisture, vandalism, kinking).	**Network Types(s):** No Change **Industry Role(s):** Add: Property Manager **Keywords(s):** Add: Industry Cooperation **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0488	Network Operators, Service Providers, and Public Safety should consider registering critical circuits with Telecom Service Priority (TSP).	**Network Types(s):** Add: Cable, Internet/Data, Satellite, Wireline **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** Delete remark "Also, see BP 0587" Add: http://www.dhs.gov/telecommunications-service-priority-tsp http://transition.fcc.gov/pshs/services/priority-services/tsp.html **Status:** No Change	Important	**Changed**
9-7-0489	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider provisions in labor contracts to provide for cooperation between union and non-union personnel during disaster recovery situations.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** Delete Reference **Status:** No Change	Important	**Changed**

9-7-0490	Network Operators, Service Providers, and Public Safety should consult NFPA (National Fire Prevention Association) Standards for guidance in the design of fire suppression systems, and, when building code regulations require sprinkler systems, should seek an exemption for the use of non-destructive systems.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** Modify: ~~Communications equipment can be easily damaged by water from sprinkler systems.~~ Reference NFPA 75 and 76. When zoning regulations require sprinkler systems, an exemption should be sought for the use of non-destructive systems. **Status:** No Change	Important	**Changed**
9-7-0565	Equipment Suppliers should identify key areas and establish and use metrics to measure progress in improving quality, reliability, and security during product development and field life cycle.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Cybersecurity **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-9-0587	Government, Network Operators and Service Providers of critical services to National Security and Emergency Preparedness (NS/EP) users should be familiar with the Telecommunications Service Priority (TSP) program and support / promote it as applicable.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Public Safety Service **Reference(s):** Replace: Reference: The TSP Program is a FCC program used to identify and prioritize telecommunication services that support NSEP missions. The TSP Program also provides a legal means for the telecommunications industry to provide preferential treatment to services enrolled in the program. More information on the TSP Program can be obtained from the National Communications System (NCS) Office of Priority Telecommunications, Manager National Communications System, Attn: OPT/N3, 701 South Courthouse Road, Arlington, Virginia 22204-2198, on telephone 703-607-4932 or at http://www.dhs.gov/telecommunications-service-priority-tsp **Status:** No Change	Important	**Changed**
9-7-0564	Equipment Suppliers should develop and update training for their products with a clear understanding of customer needs and human factors.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Procedures **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0582	Public Safety and Government should use 911 as the standard access code for emergency services (e.g., PSAP, law enforcement, fire, EMS, hazardous materials).	**Network Types(s):** Add: Satellite **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**
9-9-0584	Service Providers, Network Operators and Equipment Suppliers and Government representatives should work together to support appropriate industry and international organizations to develop and implement NS/EP standards in networks.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0588	Network Operators, Service Providers and Equipment Suppliers should provide awareness training that stresses the services impact of network failure, the risks of various levels of threatening conditions and the roles components play in the overall architecture.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Modify: Reference: Training should be provided for personnel involved in the direct operation, maintenance, provisioning, security and support of network elements. A successful program should educate its target audience on the technology, its benefits and risks, and the magnitude of traffic carried. The training might include the functionality and the network impact of failure of active and standby (protect) equipment in processors, interfaces, peripheral power supplies, and other related components, and the identification of active and standby (protect) units. Special emphasis should focus on the systematic processes for trouble isolation and repair. **Status:** No Change	Highly Important	**Changed**

9-7-0589	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should establish a minimum set of work experience and training courses which must be completed before personnel may be assigned to perform maintenance activities on production network elements, especially when new technology is introduced in the network.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** Modify: References: This training should reinforce the importance of following procedures at all times and emphasize the steps required to successfully detect problems and to isolate the problem systematically and quickly without causing further system degradation. Lack of troubleshooting experience and proper training in trouble detection and isolation usually prolongs the trouble detection and isolation process. **Status:** No Change	Highly Important	**Changed**
9-9-0592	Network Operators and Service Providers should provide duplicated, non-co-located maintenance administration, surveillance and support for network elements.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Add: Monitoring and administration locations should be minimized to provide consistency of operations and overall management. **Status:** No Change	Highly Important	**Changed**

9-9-0594	Network Operators and Service Providers should follow industry guidelines for validating SS7 link diversity, which 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.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-9-0595	Network Operators, Service Providers, and Public Safety 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.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Training and Awareness **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-9-0596	Network Operators and Service Providers should carefully review all re-home procedures, undertake pre-planning before execution, and ensure that re-home procedures are carefully followed.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-9-0600	Network Operators and Service Providers should establish and document a process to plan, test, evaluate and implement major change activities in their network.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-9-0601	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.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Network Provisioning, Supervision **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-9-0602	Network Operators and Service Providers should establish procedures to reactivate alarms after provisioning or maintenance activities (when alarms are typically deactivated).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Training and Awareness **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-9-0605	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.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Network Elements, Network Provisioning **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-0607	Inter-Provider Fault Isolation: Network Operators and Service Providers should ensure that bilateral technical agreements between interconnecting networks address the issue of inter-provider fault isolation.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Policy **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-9-0608	Network Operators and Service Providers should utilize network surveillance and monitoring to keep overflow traffic conditions from adversely affecting networks.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Network Provisioning **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0609	Network Operators and Service Providers should provide and maintain the contact information for mutual aid coordination for inclusion in mutual aid processes.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Delete: See also http://www.ncs.gov/ncc/nccmaa/nccmaa_toc.html) **Status:** No Change	Highly Important	**Changed**

9-7-0611	Equipment Suppliers and Service Providers should provide secure electronic distribution of documentation and software, where feasible.	**Network Types(s):** No Change **Industry Role(s):** Add: Service Provider **Keywords(s):** Add: Software **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-9-0612	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.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Network Elements **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-0614	Network Operators, Service Providers and Equipment Suppliers should position the equipment designation information (e.g., location, labels, RFID tags) so that they are securely affixed and not on removable parts.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Add: The equipment designation should not be placed on removable parts such as covers, panels, doors, or vents that can be removed and mistakenly installed on a different network element. **Status:** No Change	Important	**Changed**

9-9-0615	Network Operators, Service Providers, and Public Safety should verify complex configuration changes before committing them and test after the change to ensure the appropriate and expected results.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-9-0617	Network Operators and Service Providers should ensure that routing controls are implemented and managed to prevent adverse routing conditions.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Network Provisioning **Reference(s):** Modify link to: http://www.rfc-editor.org/info/rfc1918 **Status:** No Change	Highly Important	**Changed**
9-7-0618	Network Operators and Service Providers should establish mutually agreed upon reliability thresholds with Equipment Suppliers for new hardware (e.g., routers, switches, call servers, signaling servers) brought into service on the network.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Procedures, Network Provisioning **Reference(s):** Delete Reference **Status:** No Change	Highly Important	**Changed**

9-7-0621	Network Operators and Service Providers should consider abandoning and / or removing existing cable that does not meet New Equipment Building System (NEBS) standards, if it is economically feasible and safe to do so.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Add: http://192.4.253.70/services/testing/nebs/index.html **Status:** No Change	Important	**Changed**
9-7-0623	Network Operators and Service Providers using Valve Regulated Lead Acid (VRLA) batteries should perform annual maintenance by performing a discharge test or by using an ohmic test instrument.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Procedure, Fire **Reference(s):** Modify: The aging properties of these batteries can lead to thermal runaway that may cause a fire. See GR-4228, VRLA Battery String Certification Levels Based on Requirements for Safety and Performance and http://telecom-info.telcordia.com/site-cgi/ido/docs.cgi?DOCUMENT=gr-4228&KEYWORDS=&TITLE=&ID=097222093SEARCH Delete: http://telecom-info.telcordia.com/site-cgi/ido/docs2.pl?ID=170086171&page=home) **Status:** No Change	Important	**Changed**

9-7-0624	Network Operators, Service Providers, and Property Managers are encouraged to establish rectifier case history files, by equipment category to facilitate decisions to replace equipment with more efficient equipment based on failure trends.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Procedures, Documentation, Network Elements, Network Operations, Network Provisioning **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-0625	Network Operators, Service Providers, Public Safety, and Property Managers should consider placing electric utility transformers external to buildings.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0626	Network Operators, Service Providers, Public Safety, and Property Managers should regularly inspect building mechanical equipment (e.g., air handling fans, air compressors, pumps).	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Buildings, Procedures **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0627	Network Operators, Service Providers, Public Safety, and Property Managers should exercise, service, and calibrate AC circuit breakers per manufacturers' recommendations.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Procedures **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0628	Network Operators and Service Providers should develop and implement defined procedures for removal of unused equipment and cable (e.g., cable mining) if it is economically feasible and safe to do so.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0629	Network Operators, Service Providers and Property Managers should implement a training program for contractors working in critical equipment locations to ensure they understand the need to protect the continuity of service and all fire safety requirements applicable to the facility.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-9-0630	Network Operators, Service Providers, Equipment Suppliers and Property Managers should develop and execute standard Methods of Procedure (MOP) for all vendor work in or external to equipment locations with emphasis on service continuity and safety precautions.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Fire, Training and Awareness **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-0631	Network Operators, Service Providers, Equipment Suppliers, and Property Managers should develop a comprehensive Site Management and/or Building Certification Program to ensure that critical equipment locations have carefully documented procedures to ensure fire safety.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Buildings, Training and Awareness **Reference(s):** Add: These procedures should include, among other things, guidance for the safe operation of all electrical appliances at this facility, including space heaters which are a frequent source of fires. **Status:** No Change	Important	**Changed**
9-7-0634	Network Operators, Service Providers, Public Safety, and Property Managers together with the Power Company should verify that aerial power lines are not in conflict with hazards that could produce a loss of service during high winds or icy conditions.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Network Design, Network Operations, Network Provisioning Delete: Buildings **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0640	Network Operators, Service Providers, Public Safety, and Property Managers should ensure proper air filtration.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Network Operations, Procedures **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-9-0649	Network Operators, Service Providers, Public Safety, and Property Managers should ensure critical network facilities have appropriate fire detection and alarm systems.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Critically Important	**Changed**
9-7-0650	Network Operators, Service Providers, Public Safety, and Property Managers should place strong emphasis on activities related to the operation of power systems (e.g., maintenance procedures, alarm system operation, response procedures, and training).	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**
9-7-0651	Network Operators, Service Providers, Public Safety, and Property Managers should consider providing diversity within power supply and distribution systems so that a single point of failure (SPOF) is not catastrophic in critical network locations.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Network Operations **Reference(s):** Add: For large battery plants in critical offices, dual AC feeds should be considered. **Status:** Changed	Highly Important	**Changed**

9-7-0652	Network Operators, Service Providers, Equipment Suppliers and Property Managers should adhere to applicable power engineering design standards.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Network Operations, Network Provisioning Delete: Building **Reference(s):** Modify: See http://telecom-info.telcordia.com/site-cgi/ido/docs2.pl?ID=170086171&page=home, (Delete: and) http://www.atis.org/docstore, and Add: Telcordia GR-513-CORE (Power - LSSGR section 13), Telcordia GR-63-CORE (NEBS), Telcordia GR-295-CORE (Isolated Ground Planes), Telcordia GR-1089-CORE (Electromagnetic Compatibility), and ATIS-0600311.2007 (DC Power Systems - Telecommunications Environment Protection). **Status:** No Change	Highly Important	**Changed**
9-9-0653	Network Operators, Service Providers, Public Safety, and Property Managers should retain complete control concerning when to transfer from the electric utility and operate standby generators.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-9-0654	Network Operators, Service Providers and Property Managers should generally avoid entering into power curtailment or load shedding contracts with electric utilities.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-9-0656	Network Operators, Service Providers, and Public Safety should establish a requirement for power conditioning, monitoring and protection for sensitive equipment.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Procedures **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-9-0663	Network Operators, Service Providers, Public Safety, and Property Managers should coordinate scheduled power generator tests with all building occupants to avoid interruptions.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Documentation **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0673	Network Operators and Service Providers should provide some method to detect/prevent thermal runaway on rectifiers when valve regulated batteries are used.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Network Design, Procedures **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0675	Network Operators, Service Providers and Property Managers should, for new installations, consider using multiple small battery plants in place of single very large plants, and consider using multiple battery strings in each plant.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Network Design, Procedures, Hardware **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-9-0679	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 the network.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Network Elements **Reference(s):** No Change **Status:** Changed	Critically Important	**Changed**
9-7-0680	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should provide protective covers on vulnerable circuit breakers which power critical equipment.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0682	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should ensure that power wire, cable, and signaling cables used in communications locations meet Network Equipment Building Systems (NEBS) compliance.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Network Provisioning **Reference(s):** Add: http://192.4.253.70/services/testing/nebs/index.html **Status:** No Change	Important	**Changed**
9-7-0683	Network Operators, Service Providers, Property Managers, Public Safety, and Equipment Suppliers should not mix Direct Current (DC) power cables, Alternating Current (AC) power cables and telecommunications cables wherever possible.	**Network Types(s):** No Change **Industry Role(s):** Add: Property Manager, Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0815	Network Operators, Service Providers, Property Managers, and Public Safety should deploy hardware in accordance with equipment suppliers' stated environmental specifications.	**Network Types(s):** No Change **Industry Role(s):** Add: Service Provider, Property Manager, Public Safety **Keywords(s):** Add: Network Provisioning **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0816	Service Providers that deploy Internet Access Service in a shared media environment should design Broadband systems that provide appropriate privacy and access restriction to the data packet information.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0818	Network operators and service Providers that deploy Internet Access Service should deploy network equipment that report alarms.	**Network Types(s):** No Change **Industry Role(s):** Add: Service Provider, Government **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-9-0819	Service Providers, Network Operators and Property Managers should periodically evaluate the need for and feasibility of providing back up power at cell sites and broadband network equipment, at remote locations where economically and technically practical taking into consideration the criticality of the site or location, as well as local zoning laws, statutes, and contractual obligations.	**Network Types(s):** No Change **Industry Role(s):** Add: Property Manager and Service Provider **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**

9-7-0820	Network Operators and Service Providers should deploy networks and services in a manner that mitigates the effects of harmful interference from other sources, and mitigates harmful interference into other services.	**Network Types(s):** No Change **Industry Role(s):** Add: Service Provider **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0821	Network Operators, Service Providers and Property Managers should coordinate to ensure that network deployment and equipment installation, including equipment moves, adds or changes (MACs), do not physically impair the operation of other collocated communications networks/equipment.	**Network Types(s):** No Change **Industry Role(s):** Add: Property Managers, Service Providers **Keywords(s):** Add: Network Provisioning **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0822	Network operators and service providers should incorporate multilevel security schemes for network data integrity in the network design, as applicable, to prevent user traffic from interfering with network operations, administration, and management.	**Network Types(s):** No Change **Industry Role(s):** Add: Service Provider **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-8-0472	Network Operators, Public Safety, and Equipment Suppliers should consider connector choices and color coding to prevent inappropriate combinations of cables.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Network Element **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-8-0551	Network Operators should design their SS7 network components and interfaces consistent with industry base security guidelines to reduce the risk of potentially service affecting security compromises of the signaling networks supporting the public telephone network.	**Network Types(s):** Add: Wireless **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Add: See NIIF Reference document Part 3, Appendix I. This document provides guidance for desirable security features for any network element (call agent, feature server, soft switch, cross connect, gateway, database). It identifies security functionality, which should be in place by design, device or procedure. It includes an assessment framework series of checklists. **Status:** No Change	Important	**Changed**
9-8-0731	Network Operators and Service Providers should provide physical diversity on critical inter-office and wireless backhaul routes when justified by a risk or value analysis.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Emergency Preparedness **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-8-0755	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should document and communicate their installation and maintenance guidelines (e.g., MOP) and the expectation of compliance by all involved parties.	**Network Types(s):** No Change **Industry Role(s):** Add: Equipment Suppliers, Public Safety **Keywords(s):** Add: Supervision **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-8-0782	Network Operators and Service Providers should detect transport simplex events and restore the duplex protective path expeditiously by executing appropriate incident response and escalation processes.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-8-0784	Network Operators, Service Providers, and Public Safety should utilize appropriate fiber/cable management equipment or racking systems to provide cable strain relief and ensure that bend radius is maintained to avoid micro-bends (e.g., pinched fibers).	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Documentation, Hardware, Contractors and Vendors. **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-8-0785	Network Operators and Service Providers should consider secured remote access to critical network management systems for network management personnel working from distributed locations (e.g., back-up facility, home) in the event of a situation where the NOC cannot be staffed (e.g., pandemic).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Information Protection, Procedures, Network Operations **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**
9-8-0787	Network Operators, Service Providers, and Property Managers should consider the use of fixed alternate fuel generators (e.g., natural gas) connected to public utility supplies to reduce the strain on refueling.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-8-0790	Personal Protective Equipment: Network Operators, Service Providers, Equipment Suppliers and Public Safety should consider providing personal protective equipment (PPE) for infection control (e.g., masks, disposable gloves, and sanitizers) in locations where multiple employees are located.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Public Safety and Government **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-8-0791	Network Operators, Service Providers, Equipment Suppliers, Government, and Public Safety should consider providing personnel training in the use of personal protective equipment (PPE) specific to a pandemic or other crisis situations and the employee's particular job.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety, Government **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-8-0792	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider modifying attendance guidelines during a pandemic, or other crisis situations.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-8-0793	Network Operators, Service Providers, and Equipment Suppliers should, as part of business continuity planning, identify employees that can perform their tasks from alternate locations and consider provisions for enabling them to do so.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**

9-8-0794	Network Operators, Service Providers, and Equipment Suppliers should, as part of business continuity planning, provide for elevated /increased utilization of remote access capabilities for telecommuting purposes by employees during a pandemic, or other crisis situations.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Business Continuity **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-8-0795	Network Operators, Service Providers, and Equipment Suppliers should as part of business continuity planning, plan for elevated/increased utilization of virtual collaboration and remote meetings capabilities during pandemics or other crisis situations.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Business Continuity **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-8-0796	Network Operators, Service Providers, and Equipment Suppliers should, as part of business continuity planning, consider developing guidelines for the deferral of specific maintenance or provisioning activities during certain situations (e.g., pandemic, holiday, National Special Security Event).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Business Continuity **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-8-0798	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider, as part of business continuity/disaster recovery, alternate transportation and delivery methods for equipment, spares, and personal protective equipment to prepare for situations where transportation and delivery may be delayed (e.g., pandemic, other crisis situations).	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Business Continuity **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-8-0799	Service Providers, Network Operators and Property Managers should periodically evaluate the need for and feasibility of providing back up power at cell sites and broadband network equipment, at remote locations where economically and technically practical taking into consideration the criticality of the site or location, as well as local zoning laws, statutes, and contractual obligations.	**Network Types(s):** No Change **Industry Role(s):** Add: Property Manager and Service Provider **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-6-1044	Equipment Suppliers should consider providing a "Disaster Recovery Services Checklist" to all of the Service Providers they support to assist the Service Provider in identifying equipment needs and professional services during an event.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Industry Cooperation and Materials Movement. **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-6-1051	Network Operators, Service Providers, Equipment Suppliers, and Government should work together to identify criteria for developing procedures to handle network elements affected by nuclear attack or nuclear accidents (e.g., shock wave, Electro-magnetic Pulse (EMP), Thermal, Fallout, fiber darkening of phosphorous based fiber cable).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-1052	Network Operators, Service Providers, and Public Safety should assess the functionality of network critical systems during disaster exercises.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-1002	Network Operators, Service Providers and Equipment Suppliers should consider establishing a business continuity executive steering committee (composed of executive managers and business process owners) to ensure executive support and oversight.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Disaster Recovery, Policy **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-1008	Network Operators, Service Providers, and Equipment Suppliers should use the Incident Command System for incident coordination and control in the emergency operations center and at the incident site.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Procedures **Reference(s):** Modify: See the National Incident Management System (NIMS) http://www.fema.gov/national-incident-management-system. See also National Fire Protection Association Standard 1600. http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=1600 (Free but requires registration) **Status:** No Change	Important	**Changed**

9-6-1043	Equipment Supplies should, during major disasters, make it easy for customers to contact them by providing an Interactive Voice Response (IVR) option or dedicated contact information.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Industry Cooperation **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-1047	Network Operators, Service Providers, and Public Safety should develop a process to routinely archive critical system backups and provide for storage in a secure off-site facility which would provide geographical diversity.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Software **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-1048	Network Operators and Service Providers should consider supplementing media backup storage with full system restoral media and documented restoration procedures that can be utilized at an alternate hot site, in case of total failure of the primary service site.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-1049	Service Providers should consider utilizing multiple network carriers for internet backbone connectivity if required to prevent isolation of service nodes.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-1050	Network Operators and Service Providers should consider alternative carrier/transport methods such as satellite, microwave or wireless to further reduce point of failures or as hot transport backup facilities.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Disaster Recovery **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**
9-6-5024	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should include physical security as an integral part of the strategic business planning and decision making process to ensure that security risks are properly identified and appropriately mitigated.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-6-5025	Network Operators, Service Providers and Equipment Suppliers should include physical security as an integral part of the merger, acquisition and divestiture process to ensure that security risks are proactively identified and appropriate plans are developed to facilitate the integration and migration of organizational functions (e.g., Due Diligence investigations, integration of policy and procedures).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-6-5049	Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider a strategy of using technology (e.g., access control, CCTV, sensor technology, person traps, turnstiles) to supplement the guard force.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Visitors **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-6-5050	Network Operators, Service Providers, Equipment Suppliers and Property Managers utilizing guard services should have a supervision plan that requires supervisory checks for all posts.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-6-5051	Network Operators, Service Providers and Equipment Suppliers utilizing guard services should consider establishing incentives and recognition programs to increase morale and reduce turnover.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-6-5119	Equipment Suppliers of critical network elements should document the technical specifications of their electronic hardware, including characteristics such as tolerance limitations to electromagnetic energy, vibration, voltage spikes and temperature ranges.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-6-5143	Network Operators responsible for satellite operations should maintain access to a back-up or secondary uplink site to provide tracking, telemetry and control (T.T.&C.) support for all operational communications spacecraft. The back-up or secondary site must be geographically diverse from the primary uplink facility, active and tested on a regular schedule to insure readiness and timely response.	**Network Types(s):** No Change **Industry Role(s):** Delete: Service Provider **Keywords(s):** No Change **Reference(s):** Delete Reference **Status:** Changed	Highly Important	**Changed**

9-6-5144	Network Operators should maintain a current database of all satellite transmit and receive sites (i.e. uplink and downlink facilities) that are operational and/or support their services and networks.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Add: The database information should list location (i.e. street address, latitude and longitude), service provider/phone number, site manager contact/phone number, control point if remotely controlled, and equipment type used at the site. **Status:** No Change	Important	**Changed**
9-6-5146	Network Operators and Service Providers should develop and manage Satellite service recovery plans to ensure the timely restoration of services in the event of transponder loss, payload failure, and satellite failure.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Delete Reference **Status:** No Change	Highly Important	**Changed**
9-6-5165	Network Operators, Service Providers and Equipment Suppliers should ensure that teleworkers have the equipment and support necessary to secure their computing platforms and systems at an equivalent level of those within company office facilities (e.g., Security software, firewalls and secure documents storage).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-6-5168	Network Operators, Service Providers and Equipment Suppliers should review personnel background information prior to assignment to sensitive roles, to ensure there are no security risks, or risk of compromising processes as they evolve.	**Network Types(s):** No Change **Industry Role(s):** Add: Network Operator and Service Providers **Keywords(s):** Add: Access Control, Information Protection, Procedures **Reference(s):** Delete Reference **Status:** Changed	Highly Important	**Changed**
9-6-5169	Network Operators, Service Providers and Equipment Suppliers should establish and implement an information protection process to control and manage the distribution of critical R&D documentation and the revisions thereto (e.g., serialize physical and electronic documentation to maintain audit trails).	**Network Types(s):** No Change **Industry Role(s):** Add: Network Operator, Service Providers **Keywords(s):** No Change **Reference(s):** Delete Reference **Status:** Changed	Highly Important	**Changed**
9-6-5171	Equipment Suppliers should design network equipment to reduce the likelihood of malfunction due to failure of the connected devices (i.e. in order to reduce the potential for cascade failures; software or system damage).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Delete Reference **Status:** No Change	Highly Important	**Changed**

9-6-5179	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should establish policies and procedures that prevent or reduce workplace violence.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Visitors **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-6-5194	Equipment Suppliers should design electronic hardware to minimize susceptibility to electrostatic discharge.	**Network Types(s):** Add: Satellite **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-6-5195	Network Operators, Service providers and Equipment Suppliers should keep track of network product identification (e.g., circuit pack serial number), repair, modification and decommissioning records.	**Network Types(s):** Add: Satellite **Industry Role(s):** Add: Network Operator, Service Provider **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-6-5239	Property Managers of multi-tenant facilities should maintain crisis management plan(s) for incident resolution and restoration.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-6-5243	Network Operators, Service Providers and Equipment Suppliers should consider restricting, supervising, and/or prohibiting tours of critical network facilities, restoration sites and operations.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-6-5248	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should perform risk assessment on significant network changes (e.g., technology upgrades, temporary or permanent changes due to restoration efforts).	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-6-5255	Network Operators, Service Providers and Equipment Suppliers should ensure that temporary wireless networks (e.g., terrestrial microwave, free-space optical, satellite, point-to-point, multi-point, mesh) used during an incident are subsequently disabled or secured.	**Network Types(s):** No Change **Industry Role(s):** Add: Equipment Supplier **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-6-5265	Network Operators, Service Providers, Public Safety, Equipment Suppliers and Property Managers' senior management should actively support compliance with established corporate security policies and procedures.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Security Systems **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-6-5274	Network Operators, Service Providers, Public Safety, Equipment Suppliers and Property Managers should, in facilities using automated access control systems, install one mechanical lock to permit key override access to the space(s) secured by the access control system in the event the system fails in the locked mode. An appropriate procedure should be followed to track and control the keys.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5001	Network Operators, Service Providers and Equipment Suppliers should establish additional access control measures that provide two factor identification (e.g., cameras, PIN, biometrics) in conjunction with basic physical access control procedures at areas of critical infrastructure, as appropriate, to adequately protect the assets.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Procedures **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5021	Network Operators, Service Providers, Public Safety, Equipment Suppliers and Property Managers should establish procedures for access control, exception access, and identification for all individuals (including visitors, contractors, and vendors) that provide for the issuing of ID badges, sign-in and escorting where appropriate, with challenging of non-badged personnel.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Training and Awareness **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-6-1006	Network Operators, Service Providers and Equipment Suppliers should consider establishing a designated Emergency Operations Center. This center should contain tools for coordination of service restoral including UPS, alternate means of communications, maps, and documented procedures to manage business interruptions and/or disasters.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Procedures **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-6-5054	Network Operators, Service Providers, Equipment Suppliers, and Property Managers utilizing guard services should develop a process to quickly disseminate information to all guard posts. This process should be documented and should clearly establish specific roles and responsibilities.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Supervision **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-6-5055	Network Operators, Service Providers and Equipment Suppliers should establish and maintain (or contract for) a 24/7 emergency call center for internal communications. Ensure staff at this center has access to all documentation pertinent to emergency response and up to date call lists to notify appropriate personnel. The number to this call center should be appropriately published so personnel know where to report information.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Contractors & Vendors **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**
9-6-5069	Property Managers should require all tenants to adhere to the security standards set for colocation sites.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-6-5210	Network Operators, Service Providers and Property Managers should discourage use of Emergency Power Off (EPO) switches between the primary battery supplies and the main power distribution board. EPO switches are not recommended for use in traditional -48V DC battery plants.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Hardware **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-6-5235	Network Operators and Service Providers should ensure that impacted alarms and monitors associated with critical utility vaults are operational after a disaster event.	**Network Types(s):** No Change **Industry Role(s):** Delete: Equipment Suppliers **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-6-5244	Network Operators, Service Providers and Equipment Suppliers should make all employees, contractors, and others with access to critical infrastructure during restoration, aware of changes to security posture resulting from the incident, and the need for increased vigilance.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**

9-6-5249	Network Operators and Service Providers should consider geographic separation of network redundancy during restoration, and address losses of redundancy and geographic separation following restoration.	**Network Types(s):** No Change **Industry Role(s):** Add Service Provider **Keywords(s):** Add: Hardware, Network Elements, Procedures **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-6-5250	Network Operators and Service Providers should develop an engineering design for critical network elements and inter-office facilities that addresses diversity, and utilize management systems to provision, track, and maintain and restore that inter-office and intra-office diversity.	**Network Types(s):** No Change **Industry Role(s):** Add: Service Provider **Keywords(s):** Add: Buildings, Transport Facilities, Network Provisioning, Policy, Power **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5002	Network Operators, Service Providers, Public Safety, Equipment Suppliers and Property Managers should develop and implement periodic physical inspections and maintenance as required for all critical security systems.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-5003	Network Operators, Service Providers, Public Safety, Equipment Suppliers and Property Managers should periodically audit compliance with physical security policies and procedures.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5005	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should conduct electronic surveillance (e.g., CCTV, access control logs, alarm monitoring) at critical access points and preserve the data for investigation.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5009	Network Operators, Service Providers, Public Safety, Equipment Suppliers and Property Managers should ensure that access control records are retained in conjunction with company standards.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Visitors **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5010	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should deploy security measures in proportion to the criticality of the facility or area being served.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-5011	Network Operators, Service Providers, Public Safety, Equipment Suppliers and Property Managers should alarm and monitor critical facility access points to detect intrusion or unsecured access (e.g., doors being propped open).	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5013	Network Operators, Service Providers, Public Safety, Equipment Suppliers and Property Managers in facilities where master key systems are used should consider establishing hierarchical key control system(s) (e.g., Master Key Control systems) with record keeping databases. Master Key Control system should be implemented so that keys are distributed only to those with need for access into the locked space (e.g., perimeter doors, offices, restricted areas).	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-5014	Network Operators, Service Providers, Public Safety, Equipment Suppliers and Property Managers should establish and maintain inventory control measures to protect all media associated with Master Key Control (MKC) systems and access control systems (e.g. master keys, key blanks, cards, tokens, fobs).	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** Delete Reference **Status:** Changed	Highly Important	**Changed**
9-7-5018	Network Operators, Service Providers and Equipment Suppliers should periodically conduct reviews to ensure that proprietary information is protected in accordance with established policies and procedures.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Cybersecurity **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-6-5172	Network Operators, Service Providers and Equipment Suppliers should not permit unsecured wireless access points for the distribution of data or operating system upgrades during normal operations or system restoration efforts.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Procedures **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-6-5185	Network Operators, Service Providers, Public Safety, Equipment Suppliers and Property Managers should ensure the inclusion of fire stair returns in their physical security designs with consideration that there should be no uncontrolled re-entry paths into areas of critical infrastructure, where permitted by code.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-5022	Network Operators, Service Providers, Equipment Suppliers, Property Managers, and Public Safety should internally identify locations of critical infrastructure for emergency planning and security, and protect it as highly sensitive proprietary information.	**Network Types(s):** No Change **Industry Role(s):** Add: Property Managers, Public Safety **Keywords(s):** Add: Business Continuity **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-5026	Network Operators, Service Providers, Equipment Suppliers, Property Managers, and Public Safety should include security as an integral part of the facility construction process to ensure that security risks are proactively identified and appropriate solutions are included in the design of the facility.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** Add: Where appropriate, this review may include elements such as facility location selection, security system design, configuration of the lobby, limitation of outside access points (both doors and windows), location of mailroom, compartmentalization of loading docks, design of parking setbacks, placement and protection of air handling systems and air intakes, structural enhancements, and ramming protection. Consider sign off authority for security and safety on all construction projects. **Status:** Changed	Important	**Changed**
9-7-5027	Network Operators, Service Providers, Equipment Suppliers, and Property Managers should collaborate during major events (e.g., hiring, downsizing, outsourcing, labor disputes, civil disorder).to ensure that security risks are identified and plans are developed to protect the company's personnel and assets.	**Network Types(s):** No Change **Industry Role(s):** Add: Property Managers **Keywords(s):** Add: Access Control, Buildings, Contractors & Vendors, Disaster Recovery, Industry Cooperation, **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-5029	Network Operators, Service Providers, Equipment Suppliers and Property Managers should facilitate the availability of security related hardware and media (e.g., spare hardware) and/or a contingency plan for its availability in the event of a disaster.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Access Control **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5030	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should provide a level of security protection over critical inventory (i.e., spares) that is proportionate to the criticality of the equipment.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Access Control, Material Movement **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5031	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should establish a role for the security function (i.e., physical and cyber) in business continuity planning, including emergency response plans and periodic tests of such plans.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Cyber Security **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-5032	Network Operators, Service Providers, Property Managers, Public Safety, and Equipment Suppliers should establish a procedure governing the assignment of facility access levels.	**Network Types(s):** No Change **Industry Role(s):** Add: Property Managers, Public Safety **Keywords(s):** Add: Contractors & Vendors, Guard Forces, Disaster Recovery, Information Protection **Reference(s):** Add: This could include, but is not limited to buildings, equipment rooms, and access points. **Status:** No Change	Important	**Changed**
9-7-5033	Network Operators, Service Providers, Equipment Suppliers, Public Safety and Property Managers should consider establishing and implementing background investigation policies that include criminal background checks of employees.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Delete: Physical Security, Management, Contractors & Vendors **Reference(s):** Add: The policy should detail elements of the background investigation as well as disqualification criteria. **Status:** No Change	Important	**Changed**
9-7-5034	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should consider establishing contractual obligations requiring contractors, subcontractors and vendors to conduct background investigations of all personnel who require unescorted access to areas of critical infrastructure or who require access to sensitive information related to critical infrastructure.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**

9-7-5040	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should install environmental emergency response equipment (e.g., fire extinguishers, high rate automatically activated pumps) where appropriate, and periodically inspect the equipment.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5041	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should establish and implement policies and procedures to secure and restrict access to power, environmental, security, and fire protection systems.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5042	Network Operators, Service Providers, Public Safety, and Property Managers should establish and implement policies and procedures to secure and restrict access to fuel supplies.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Emergency Preparedness **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-5043	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should comply with security standards for perimeter lighting.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-5044	Network Operators, Service Providers, Equipment Suppliers, Public Safety, or Property Managers should plan and maintain landscaping at facilities to enhance the overall level of building security wherever possible.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** Add: Landscaping at critical facilities should not obstruct necessary security lighting or camera views of ingress and egress areas, and landscaping should also avoid creating fire hazards or hiding places. **Status:** No Change	Important	**Changed**
9-7-5046	Network Operators, Public Safety, and Property Managers should ensure critical infrastructure utility vaults are secured from unauthorized access.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5048	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should implement a policy that requires approval by senior member(s) of the security department for security related goods and services contracts.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Contractors & Vendors **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-5052	Network Operators, Service Providers, Equipment Suppliers and Property Managers using guard services should ensure that each post has written detailed post orders including site specific instructions, up to date emergency contact information and ensure that on the job training occurs.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Documentation **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5053	Network Operators, Service Providers, Equipment Suppliers and Property Managers should periodically audit guard services to ensure satisfactory performance, and compliance with organizational contractual requirements.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Access Control **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5057	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider an enhanced level of emergency response for locations supporting critical functions.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Disaster Recovery, Public Safety Services **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-5058	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should ensure that all critical infrastructure facilities, including the security equipment, devices and appliances protecting it, are supported by backup power systems (e.g., batteries, generators, fuel cells).	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Delete: Essential Services **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**
9-7-5061	Equipment Suppliers should consider ergonomics and human-centric factors when designing user interfaces (e.g., hardware labeling, software, documentation).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-5062	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should staff critical functions at appropriate levels, considering human factors such as workload and fatigue.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-5064	Network Operators, Service Providers, Public Safety, and Property Managers should alarm and monitor critical electronic equipment areas to detect parameters that are outside operating specifications (e.g., temperature, humidity).	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-5066	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should ensure that sensitive information pertaining to critical infrastructure is considered proprietary and access is restricted appropriately, both internally and externally.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Cyber Security **Reference(s):** Add: Appropriate markings are required to qualify for exemption from disclosure under FOIA. **Status:** No Change	Highly Important	**Changed**
9-7-5068	Network Operators, Service Providers and Property Managers should establish standards, policies and procedures that, where feasible, restrict equipment access to authorized personnel where co-location exists.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5070	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider establishment of a senior management function for a chief security officer (CSO) or functional equivalent to direct and manage both physical and cyber security.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-5071	Network Operators, Service Providers and Property Managers should maintain liaison with local law enforcement, fire department and other security and emergency agencies to exchange critical information related to threats, warnings and mutual concerns.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Public Safety Service **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-5072	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should perform risk assessments on key network facilities and control areas on a regular basis, taking into account natural disasters and unintentional or intentional acts of people impacting the facility or nearby structures.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Buildings **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5074	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should document in a Disaster Recovery Plan the process for restoring physical security control points for critical infrastructure facilities.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Disaster Recovery **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**
9-7-5075	Network Operators, Service Providers, and Public Safety should ensure that networks built with redundancy are also built with geographic separation where feasible (e.g., avoid placing mated pairs in the same location and redundant logical facilities in the same physical path).	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-5078	Network Operators, Service Providers, and Public Safety should be automatically notified upon the loss of alarm data and react accordingly.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Delete: Emergency Preparedness **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5080	Network Operators, Service Providers, and Public Safety should identify and track critical network equipment, location of spares, and sources of spares to ensure the long term continuity and availability of communication service.	**Network Types(s):** No Change **Industry Role(s):** Add: Service Provider, Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5083	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should maintain the availability of spares for critical network systems.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-5084	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider ensuring that outsourcing of hardware and software includes a quality assessment, functional testing and security testing by an independent entity.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**
9-7-5089	Service Providers, Network Operators, Property Managers, Public Safety, and Equipment Suppliers should establish, implement and enforce appropriate procedures for the storage and movement of equipment and material, including trash removal, to deter theft.	**Network Types(s):** No Change **Industry Role(s):** Add: Property Managers, Public Safety **Keywords(s):** Add: Hardware **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-5091	Network Operators, Service Providers and Equipment Suppliers should develop and implement, as appropriate, travel security awareness training and briefings before traveling internationally.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Physical Security Management **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-5092	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should establish an incident reporting mechanism and investigations program so that security or safety related events are recorded, analyzed, and investigated as appropriate.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** Delete Reference **Status:** No Change	Important	**Changed**
9-7-5095	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should implement a security response plan for communications facilities that recognizes the threats identified in the National Terrorism Advisory System.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** Modify: In order to prevent terrorist/criminal access and activity. ~~Homeland Security's Physical Security Alert Status Program. See http://www.dhs.gov/files/programs/ntas.shtm#current~~ http://www.dhs.gov/.national-terrorism-advisory-system **Status:** No Change	Highly Important	**Changed**
9-7-5096	Network Operators, Service Providers and Equipment Suppliers should require compliance with corporate security standards and programs for contractors (and their subcontractors), vendors and others as appropriate.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Information Protection **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-5099	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should consider keeping centralized trash storage outside the building and dumpsters located away from the building to reduce the potential for fire and access to the building.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5100	Network Operators, Service Providers and Equipment Suppliers should interact with federal, state, and local agencies to identify and address potential adverse security and service impacts of new laws and regulations (e.g., exposing vulnerability information, required security measures, fire codes).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Information Protection **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5105	Network Operators, Service Providers, and Equipment Suppliers should consider the security implications of equipment movement both domestically and internationally, including movement across borders and through ports of entry.	**Network Types(s):** No Change **Industry Role(s):** Add: Service Providers **Keywords(s):** Add: Hardware **Reference(s):** Delete: TAPA - Technology and Asset Protection Association. **Status:** No Change	Important	**Changed**

9-7-5110	Network Operators and Public Safety should not share information pertaining to the criticality of individual communication facilities or the traffic they carry, except with trusted entities for justified specific purposes with appropriate protections against further disclosure.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5111	Network Operators, Service Providers, Public Safety, Government, and Equipment Suppliers should not share information regarding the location, configuration or composition of the telecommunication infrastructure without proper information protection measures.	**Network Types(s):** No Change **Industry Role(s):** Add: Service Providers, Public Safety, Equipment Suppliers, and Government **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5114	Network Operators, Service Providers, Equipment Suppliers and Property Managers should establish, implement and enforce mailroom and delivery screening procedures that recognize changes in threat conditions and increase attention to security as appropriate.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-5116	Network Operators, Service Providers, Public Safety, Equipment Suppliers, and Property Managers should provide periodic briefings on guidance to personnel (employees or contractors) involved in shipping, receiving or mailroom activities for identifying suspicious letters or parcels and protocols for handling any suspicious items.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-5117	Equipment Suppliers of critical network elements should consider designing electronic hardware to industry requirements to minimize susceptibility to electromagnetic energy, shock, vibration, voltage spikes, and temperature.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Modify: See GR-1089, Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment, Telcordia at http://telecom-info.telcordia.com/site-cgi/ido/docs.cgi?DOCUMENT=1089&KEYWORDS=&TITLE=&ID=298454680SEARCH~~GR-1089 Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment, Telcordia, http://telecom-info.telcordia.com/site-cgi/ido/docs2.pl?ID=170086171&page=home~~. or See EN 300 386-2 Electromagnetic Compatibility and Radio Spectrum Matters (ERM); Telecommunication Network Equipment; Electromagnetic Compatibility (EMC) Requirements; Part 2: Product Family Standard, ETSI, ~~Feb 27, 1999,~~ http://webapp.etsi.org/WorkProgram **Status:** No Change	Highly Important	**Changed**

9-7-5118	Equipment Suppliers of critical network elements should test electronic hardware to ensure its compliance with design criteria for tolerance to electromagnetic energy, shock, vibration, voltage spikes, and temperature.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Modify: GR-1089, Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment, Telcordia at http://telecom-info.telcordia.com/site-cgi/ido/docs.cgi?DOCUMENT=1089&KEYWORDS=&TITLE=&ID=298454680SEARCH or See EN 300 386-2 Electromagnetic Compatibility and Radio Spectrum Matters (ERM); Telecommunication Network Equipment; Electromagnetic Compatibility (EMC) Requirements; Part 2: Product Family Standard, ETSI, http://webapp.etsi.org/WorkProgram **Status:** No Change	Highly Important	**Changed**
9-7-5120	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should evaluate the potential benefits and security implications when making decisions about building and facility signage, both internally and externally.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-5121	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should develop and consistently implement software delivery procedures that protect the integrity of the delivered software in order to prevent software loads from being compromised during the delivery process.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5129	Network Operators and Service Providers who file outage reports for major network outages should ensure that such reports do not unnecessarily contain information that discloses specific network vulnerabilities, to prevent such information from being available to public access.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-5134	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider establishing a policy to manage the risks associated with key personnel traveling together.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Delete: Physical Security Management Add: Business Continuity, Human Resources **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-5135	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should participate in the Communications Security, Reliability and Interoperability Council (CSRIC) and its working groups in order to develop industry Best Practices for addressing and mitigating public communications infrastructure vulnerabilities.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** Delete Reference **Status:** No Change	Important	**Changed**
9-7-5138	Network Operators and Public Safety should plan for the possibility that impacted network nodes cannot be accessed by company personnel for an extended period of time and define the corporate response for restoration of service.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5141	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider restricting, supervising, and/or prohibiting tours of critical network facilities, systems and operations.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Delete: Supervision **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5145	Network Operators and Public Safety should establish plans to perform interference analysis and mitigation to ensure timely resolution of all cases of interference (e.g., caused by equipment failure, intentional act/sabotage or frequency overlap), and, where feasible, identify the type and general location of the interference source.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Delete: Emergency Preparedness **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-5151	Network Operators, Service Providers and Property Managers located in the same facility should coordinate security matters and include all tenants in the overall security and safety notification procedures, as appropriate.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Emergency Preparedness **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5152	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider performing targeted sweeps of critical infrastructures and network operations centers for listening devices when suspicion warrants.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Delete: Intrusion detection **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5153	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should ensure that critical information being provided to other companies as part of bid processes is covered under non-disclosure agreements and limited to a need to know basis.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Contractors & Vendors **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5158	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider unannounced internal security audits at random intervals to enforce compliance with company security policies.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Guard Force **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**

9-7-5163	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should consider establishing procedures for security video equipment and recording, (e.g., storage, accurate time/date stamping, privacy protection, and regular operational performance checks).	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** Delete Reference **Status:** No Change	Important	**Changed**
9-7-5164	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should establish and enforce a policy to immediately report stolen or missing company vehicles and trailers to the appropriate authorities.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Public Safety Service **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-5166	Equipment Suppliers should, wherever feasible, isolate R&D and software manufacturing of Network Elements from general office systems to prevent unauthorized access.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Access Control Add: Cyber Security **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-5167	Network Operators, Service Providers and Equipment Suppliers should provide secured methods, both physical and electronic, for the internal distribution of software development and production materials.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Cyber Security **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5174	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should utilize a coordinated physical security methodology that incorporates diverse layers of security in direct proportion to the criticality of the site.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5187	Property Managers of collocation and telecom hotel facilities should be responsible and accountable for common space, critical shared areas (e.g., cable vault, power sources) and perimeter security for the building in accordance with industry standards and Best Practices.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Guard Force, Visitors **Reference(s):** Modify: GR-63, NEBS Requirements: Physical Protection, Telcordia at http://telecom-info.telcordia.com/site-cgi/ido/docs2.pl?ID=170086171&page=home; NRIC - ~~http://www/nric/org~~; GSA - http://www.gsa.gov/portal/content/104821; DOD - http://www.wbdg.org/; PCCIP - ~~http://www.iwar.org.uk/cip/resources/pccip/info.html~~ **Status:** No Change	Highly Important	**Changed**

9-7-5188	Network Operators and Service Providers in multi-tenant communications facilities (e.g., telecom hotels) should provide or arrange security for their own space with consideration of CSRIC Best Practices and in coordination with the existing security programs for the building.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-5191	Network Operators, Service Providers that are tenants within telecom hotels should plan accordingly to protect their own facilities from potential risks within the building complex (e.g., fire suppression system, plumbing, hazardous materials).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Hardware **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5192	Network Operators and Service Providers that are tenants of a telecom hotel should provide a current list of all persons authorized for access to the Property Manager, provide periodic updates to this list, and provide instructions for exceptions (e.g., emergency restoration personnel).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Guard Force **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5197	Network Operators, Service Providers, Public Safety, and Property Managers should periodically inspect, or test as appropriate, the grounding systems in critical network facilities.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Hardware **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**

9-7-5199	Network Operators, Service Providers, and Public Safety should provide appropriate protection for outside plant equipment (e.g., Controlled Environmental Vault, remote terminals) against tampering and should, where practicable, monitor locations for intrusion.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Network Operations **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5203	Network Operators, Service Providers, Public Safety, and Property Managers should develop, maintain and administer a comprehensive program to sustain a reliable power infrastructure.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Delete: Disaster Recovery Add: Business Continuity **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**
9-7-5209	Network Operators, Service Providers, Public Safety, and Property Managers should restrict access to the AC transfer switch housing area, ensure that scheduled maintenance of the transfer switch is performed, and ensure that spare parts are available.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Emergency Preparedness **Reference(s):** No Change **Status:** Changed	Critically Important	**Changed**

9-7-5211	Network Operators, Service Providers, Public Safety, and Property Managers should, under normal conditions, disable power equipment features that allow switching off of power equipment from a remote location (i.e. dial up modem), but may consider activating such features during severe service conditions, to allow a degree of remote control.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Emergency Preparedness **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5212	Network Operators, Service Providers, Public Safety, and Property Managers should consider placing generator sets and fuel supplies for critical sites within a secured area to prevent unauthorized access, reduce the likelihood of damage and/or theft, and to provide protection from explosions and weather.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5213	Network Operators, Service Providers, Public Safety, and Property Managers should, where feasible, place fuel tanks in a secured and protected area restrict access to fill pipes, fuel lines, vents, manways, to reduce the possibility of unauthorized access.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** Add: Restricting access may be accomplished via such things as fencing, walls, or burying. **Status:** No Change	Highly Important	**Changed**

9-7-5214	Network Operators, Service Providers, Public Safety, and Property Managers should consider placing all power and network equipment in a location that affords physical protection from potential vulnerabilities based on risk of the location.-	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Hardware **Reference(s):** Add: Examples include floods, broken water mains, fuel spillage. In storm surge areas, consider placing all power related equipment above the highest predicted or recorded storm surge levels. **Status:** No Change	Highly Important	**Changed**
9-7-5216	Network Operators, Service Providers, Public Safety, and Property Managers should consider providing secure pre-constructed exterior wall pathways for mobile generator connections or tap box connections.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-5217	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should raise awareness of appropriate personnel regarding possible secondary events immediately after an incident, including the importance of promptly reporting any suspicious conditions.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Disaster Recovery **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-5218	Equipment Suppliers should implement a comprehensive security program for protecting hardware, firmware and software from malicious code insertion or tampering during development and delivery, taking into consideration that some developmental environments around the world present a higher risk level than others.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Cyber Security **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5220	Network Operators, Service Providers and Equipment Suppliers who utilize foreign sites should establish and implement a comprehensive physical security program for protecting corporate assets, including personnel, at those sites.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Corporate Ethics **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-5221	Network Operators, Service Providers and Equipment Suppliers should consider limiting the dissemination of information relating to future locations of key leadership.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Information Protection **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5222	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider providing trouble call centers with a physically diverse back-up capability that can quickly be configured to receive the incoming traffic and take appropriate action.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Public Safety Service **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-5226	Network Operators, Service Providers and Property Managers should maintain liaison with local law enforcement, fire department, other utilities and other security and emergency agencies to ensure effective coordination for emergency response and restoration.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-5229	Network Operators, Service Providers, Public Safety, and Property Managers should have controlled access to comprehensive facility cabling documentation (e.g., equipment installation plans, network connections, power, grounding and bonding) and keep a backup copy of this documentation at a secured off-site location.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Delete: Disaster Recovery **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5233	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should verify proper functioning of electronic surveillance equipment (e.g., CCTV, access control logs, alarm monitoring) at critical access points after any incident that may impact such equipment.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Delete: Intrusion Detection Add: Fire **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-5236	Property Managers should take the lead in restoration efforts of the base building infrastructure for an incident at a multi-tenant facility, ensuring that they have points of contact for each tenant to allow for coordination, support, security, and additional resources as necessary.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Liaison, Emergency Preparedness, Physical Security Management **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5242	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should reassess the criticality of associated facilities following a catastrophic incident (i.e. loss of one facility may make others more critical).	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5245	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should document the use of non-standard equipment or cable during restoration to review and/or replace those devices or cable as appropriate.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**

9-9-5252	Network Operators and Public Safety 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.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5256	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should monitor temporary connections of network test equipment that are established for restoration to prevent access by unauthorized personnel.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5261	Network Operators, Service Providers, Public Safety, and Property Managers should identify carrier interconnection points and coordinate restoral plans, as appropriate.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5263	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should use cables with adequate reliability and cable signal integrity, (e.g., flammability, strain reliefs, signal loss) and should mark as temporary and replace with standard cables as soon as practical any non-standard cables used because of an emergency restoration.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**

9-6-5264	Network Operators and Service Providers who utilize satellite backhaul as part of providing services should maintain an alternate recovery facility (Such as an Earth Station) that would duplicate necessary satellite backhaul operations. The alternate recovery facility should be geographically diverse from the primary facility, maintained and tested on a regular schedule to ensure readiness and timely response.	**Network Types(s):** No Change **Industry Role(s):** Add: Service Provider **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5267	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should ensure that operating procedures are clearly defined and followed by personnel during emergency situations in order to avoid degradation of cyber and physical security due to a diversion.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Delete: Business Continuity, Corporate Ethics Add: Guard Forces, Network Operations **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5269	Network Operators, Service Providers, Equipment Suppliers and Property Managers should incorporate various types of diversionary tactics into exercises to assess the security response.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Guard Force **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-5270	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers personnel should authenticate and cross-verify information, knowing that terrorists or malicious groups may use false information to divert attention and resources away from their intended physical or cyber target.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-5271	Network Operators, Service Providers, and Public Safety should consider physical and cyber security issues in Mutual Aid Agreements (e.g., authorization, access control, badging).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Delete Reference **Status:** No Change	Important	**Changed**
9-7-5272	Network Operators, Service Providers, Public Safety and Equipment Suppliers should include security considerations in disaster recovery plans for critical infrastructure sites.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-5275	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider backup power capabilities for Command and Control (Crisis Teams) so that communications and access to critical systems can be maintained in the event of a significant disruption to commercial power.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Delete: Security Systems Add: Disaster Recovery **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**
9-7-5277	Network Operators, Service Providers and Equipment Suppliers who develop hardware, software or firmware should ensure that appropriate security programs are in place for protecting the product from theft or industrial espionage, taking into consideration that some developmental environments around the world present a higher risk level than others.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Add: See Best Practice 5218 **Status:** No Change	Highly Important	**Changed**
9-7-5279	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider site specific (e.g., location, region, country) threat information during security program development.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**

9-7-5280	Network Operators, Service Providers, Equipment Suppliers, Public Safety, and Property Managers should instruct security personnel to confirm the authenticity of directions to supersede existing security processes or procedures before implementing changes.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Access Control, Disaster Recovery, Procedures **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-5282	Network Operators and Service Providers should coordinate with Property Managers to ensure adequate growth space.	**Network Types(s):** No Change **Industry Role(s):** Add: Network Operators **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-8-5067	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should make security an ongoing priority and implement an annual compliance requirement for the completion of a security awareness program.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Delete: Public Safety Service **Reference(s):** Delete Reference **Status:** No Change	Important	**Changed**

9-7-0814	Network Operators and Service Providers should design broadband networks with the ability to take active measures to detect and restrict or inhibit any network activity that adversely impacts performance or security.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Network Operations **Reference(s):** No Change **Status:** Changed	Critically Important	**Changed**
9-7-0561	Equipment Providers should provide timely documentation that is complete and easy-to-use.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-0559	Service Providers, Network Operators, and Public Safety should consider validating upgrades, new procedures and commands in a lab or other test environment that simulates the target network and load prior to the first application in the field.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**
8-5-0540	Equipment Suppliers should share countermeasures resulting from analysis of an outage with Network Operators and Public Safety using the same equipment.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**

8-5-0620	Equipment Suppliers should endeavor to meet requirements outlined in Industry Standards regarding Network Equipment-Building System (NEBS) practices for Power and Communication Cables (e.g., power, fire, temperature, humidity, vibration).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
8-6-0761	Network Operators, Service Providers, and Public Safety should conduct periodic verification of the office synchronization plan and the diversity of timing links, power feeds and alarms.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Essential Services **Reference(s):** No Change **Status:** No Change	Important	**Changed**
8-6-0763	Service Providers implementing DNS (Domain Name System) servers in support of VoIP (Voice over Internet Protocol) telephone number mapping applications such as ENUM should provision those servers per Industry Standards for operation of DNS name servers.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Add: Reference IETF Best Current Practices for operation of DNS nameservers: BCP 40 (RFC 2182) and BCP 16 (RFC 2870). **Status:** No Change	Highly Important	**Changed**

9-6-0764	Network Operators and Service Providers should implement congestion control mechanisms for transporting VoIP data on IP networks.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Add: See RFC 2309, RFC 2914, and RFC 3155 for examples **Status:** No Change	Highly Important	**Changed**
9-6-0767	Network Operators and Service Providers should consider using media gateway controllers to achieve interoperability with SS7/ISUP-signaled TDM voice networks.	**Network Types(s):** Delete: Satellite **Industry Role(s):** Add: Network Operator **Keywords(s):** No Change **Reference(s):** Add: See IETF RFC 3372, BCP 63 for examples. **Status:** No Change	Highly Important	**Changed**
9-6-0768	Network Operators and Service Providers implementing a SIP-signaled VoIP network should consider using media gateway controllers that map ISUP-to-SIP and SIP-to-ISUP messages in order to achieve a consistent interpretation of ISUP-to-SIP messaging industrywide.	**Network Types(s):** No Change **Industry Role(s):** Add: Network Operator **Keywords(s):** No Change **Reference(s):** Add: See IETF RFC 3398, Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping. **Status:** No Change	Highly Important	**Changed**

9-6-0769	Network Operators and Service Providers implementing a Bearer Independent Call Control (BICC)-signaled network should implement industry standards to achieve interoperability between an SS7/ISUP signaled TDM voice network and a SIP-signaled VoIP network.	**Network Types(s):** No Change **Industry Role(s):** Add: Network Operator **Keywords(s):** No Change **Reference(s):** Add: See ITU-T Recommendation Q.1912.5, "Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control Protocol or ISDN User Part," or 3GPP TS 29.163, "Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks," **Status:** No Change	Highly Important	**Changed**
9-6-0770	Network Operators and Service Providers who have deployed IS-41 or GSM Mobility Application Part (MAP) signaling networks should consider implementing and using the network management controls of SS7 within their networks.	**Network Types(s):** No Change **Industry Role(s):** Add: Network Operator. **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0404	Service Providers, Network Operators, Public Safety, and Equipment Suppliers should incorporate methodologies that continually improve network or equipment performance.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0407	Network Operators and Service Providers should establish processes for NOC-to-NOC (Network Operations Center) peer communications for critical network activities (e.g., scheduled maintenance, upgrades and outages).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Critically Important	**Changed**
9-7-0409	Service Providers should use virtual interfaces (i.e. a router loopback address) for routing protocols and network management to maintain connectivity to the network element in the presence of physical interface outages.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Cyber Security **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0421	Equipment Suppliers should design network elements intended for critical hardware and software with recovery mechanisms to minimize restoration times.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0424	Network Operators and Public Safety should whenever possible require specific applicable safety standards for network elements that they plan to purchase, procure or implement.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0427	Equipment Suppliers should maintain software documentation including revision change history and associated release notes.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-0429	Equipment Suppliers should provide for appropriate storage and retrieval mechanisms of system operational data to support analysis after a hardware or software crash.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0430	Equipment Suppliers should be able to recreate supported software from source including, where feasible, software obtained from third parties.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Business Continuity **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-0431	Equipment Suppliers should provide capacity and performance data for network elements.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**

9-7-0432	Equipment Suppliers should support standardized MIBs (Management Information Bases) and maintain documentation of private and enterprise MIBs.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Update: Enterprise MIBs are those written by vendors for their particular object. The managed object can furnish both standard MIB and enterprise MIB information. The standard MIBs are those that have been approved by the IAB (Internet Architecture Board, http://www.iab.org) Equipment and software vendors define the private MIBs unilaterally. **Status:** No Change	Highly Important	**Changed**
9-7-0435	Network Operators, Service Providers, Public Safety, Equipment Suppliers and Property Managers should assess the functions of their organization and identify those critical to ensure network reliability.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**
9-7-0436	Network Operators, Service Providers, and Public Safety should have a process to ensure smooth handling and clear ownership of problems that transition work shifts or organizational boundaries.	**Network Types(s):** No Change **Industry Role(s):** Add: Network Operator, Public Safety **Keywords(s):** Delete: Business Continuity **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-0437	Network Operators and Service Providers should aggregate routes where appropriate (e.g., singly-homed downstream networks) in order to minimize the size of the global routing table taking care to not disrupt engineered circuit diversity.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0438	Network Operators and Service Providers should enable CIDR (Classless Inter-Domain Routing) by implementing classless route prefixes on routing elements.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Cyber Security **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0440	Network Operators and Service Providers should set and periodically review situation-specific limits on numbers of routes imported from peers and customers in order to lessen the impact of misconfigurations.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Cyber Security **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-9-0449	Network Operators, Service Providers, and Public Safety should, where feasible, deploy fraudulent traffic (e.g., SPAM) controls in relevant nodes (e.g., message centers, email gateways) in order to protect critical network elements and services.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**

9-7-0450	Property Managers should maintain current documentation that ensures that the tower loading is consistent with the engineering design (e.g., antenna loading, feedline loading, ice or wind loading).	**Network Types(s):** Add: Cable, Wireline **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-0451	Property Managers should conduct a periodic physical site audit to update and maintain accurate antenna and tower engineering documentation in order to positively identify every item on the tower structure (e.g., identifying rogue antennas).	**Network Types(s):** Add: Cable, Wireline **Industry Role(s):** Delete: Network Operators, Service Providers **Keywords(s):** Add: Buildings **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-0452	Network Operators, Service Providers, Public Safety, and Property Managers should post emergency contact number(s) and unique site identification in an externally visible location at unmanned communication facilities (e.g., towers, cell sites, Controlled Environment Vault (CEV), satellite earth stations), but should not reveal additional information about the facility, except when necessary.	**Network Types(s):** Add: Wireline, Satellite, Cable **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-0453	Network Operators, Service Providers, and Public Safety should prepare for HVAC or cabinet fan failures by ensuring that conventional fans are available to cool heat-sensitive equipment, as appropriate.	**Network Types(s):** Add: Wireline, Satellite, Cable, Internet **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-0454	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider establishing technical and managerial escalation policies and procedures based on the service impact, restoration progress and duration of the issue.	**Network Types(s):** Add: Wireline, Satellite, Cable, Internet **Industry Role(s):** Add: Equipment Supplier, Public Safety **Keywords(s):** Add: Network Operations, Procedures **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0455	Equipment Suppliers and Network Operators should consider a program to remove cards or modules from circulation that have a history of failure even if tests indicate “No Trouble Found”.	**Network Types(s):** Add: Wireline, Satellite, Cable, Internet **Industry Role(s):** Add: Network Operator **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**

9-9-0456	Network Operators, Service Providers, and Public Safety should maintain records of pertinent information related to a cell site for its prioritization in disaster recovery and key coverage areas (e.g., emergency services, government agencies, proximity to hospitals).	**Network Types(s):** No Change **Industry Role(s):** Add: Service Provider, Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**
9-7-0457	Network Operators and Service Providers should develop a process to identify Radio Frequency (RF) dead spots and, where feasible, provide a solution to fill the dead spot with RF coverage.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-0458	Network Operators should verify that calls handoff between cells when a new cell site is added to the network.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Procedures **Reference(s):** No Change **Status:** Changed	Important	**Changed**

9-7-0459	Equipment Suppliers and Property Managers should design outdoor equipment to operate in expected environmental conditions (e.g., weather, earthquakes).	**Network Types(s):** No Change **Industry Role(s):** Add: Property Manager **Keywords(s):** Delete: Transport Facilities **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-0461	Equipment Suppliers should provide the capability to test failover routines of redundant network elements.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Transport Facilities **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0462	Network Operators should work in conjunction with Government to anticipate Radio Frequency (RF) capacity needs driven by changes in vehicle traffic patterns or other demographics.	**Network Types(s):** Add: Government **Industry Role(s):** No Change **Keywords(s):** Add: Network Design **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0463	Network Operators and Service Providers should consider establishing agreements so that mobile customers can roam on other providers' networks.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Emergency Preparedness **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0469	Network Operators and Property Managers should consider the use of cable support (e.g., H-Frames, Ice Bridges) in tower and shelter designs.	**Network Types(s):** Add: Cable, Internet, Wireline **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0470	Network Operators and Property Managers should consider tower and antenna designs that do not attract bird and animal nesting (e.g., no platforms, flush mounted panels, smooth radome).	**Network Types(s):** Add: Cable, Internet, Wireline **Industry Role(s):** No Change **Keywords(s):** Delete: Network Design **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-8-0789	Network Operators, Service Providers, and Equipment Suppliers should consider modifying travel guidelines/policies for use during a pandemic or other crisis situations.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Business Continuity **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-6-1013	Service Providers, Network Operators, Property Managers, and Equipment Suppliers should review their insurance requirements in order to maintain business continuity in the event of massive property damage or loss, incapacitation of senior officers, and other interruptive situations.	**Network Types(s):** No Change **Industry Role(s):** Add: Property Managers **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-6-1016	Network Operators, Service Providers, Equipment Suppliers, and Government, should develop processes or plans to quickly account for all employees (e.g. field techs) in or near the impact area of a disaster.	**Network Types(s):** No Change **Industry Role(s):** Add: Equipment Supplier, Government **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**
9-9-1033	Network Operators should develop a strategy for deployment of emergency mobile assets such as Cell on Wheels (COWs), cellular repeaters, Switch on Wheels (SOWs), transportable satellite terminals, microwave equipment, power generators, HVAC units, etc. for emergency use or service augmentation for planned events (e.g., National Special Security Event (NSSE)).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Pandemic **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**

9-7-1036	Network Operators should determine in advance if they will use wireless alternate backhaul systems (microwave radio, free space optics, and satellite communications systems) to re-establish communications and if these technologies are to be deployed it is recommended that path designs be developed for each critical area in advance of deployment with personnel trained to install and optimize the systems.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Network Elements **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-1039	Equipment Suppliers should develop support processes that include interfaces with those internal organizations (e.g., sales, logistics, and manufacturing) that have a potential role in assisting Network Operators and Service Providers in disaster response efforts.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Contractors and Vendors, Materials Movement **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-1045	Network Operators and Service Providers should use their escalation process, as needed, to address resource issues identified through damage and resource assessments.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Human Resources, Industry Cooperation **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-1054	Network Operators, Service Providers, Public Safety, and Property Managers should install fire detection systems and consider the use of suppression systems or devices at buildings supporting network functionality.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-1061	Service Provider, Network Operators, Equipment Suppliers, and Public Safety should ensure that Telecommunication Service Priority (TSP) records and data bases are reconciled annually.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** Add: http://www.dhs.gov/telecommunications-service-priority-tsp **Status:** No Change	Important	**Changed**
9-7-1065	Network Operators and Service Providers should identify and manage critical network elements and architecture that are essential for network connectivity and subscriber services considering security, functional redundancy and geographical diversity.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Business Continuity **Reference(s):** Delete Reference **Status:** No Change	Important	**Changed**

9-6-5097	Network Operators, Service Providers and Equipment Suppliers should establish and implement corporate standards for physical and system security requirements in consideration of the Best Practices of the communications industry.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Security System **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-6-5098	Network Operators, Service Providers and Equipment Suppliers should ensure that all network infrastructure equipment meets the minimum industry standards for fire resistance.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Add: Example: ATIS-0600319.2014, April 2014 **Status:** No Change	Important	**Changed**
9-6-5106	Network Operators, Service Providers, and Equipment Suppliers should consider participating in and complying with industry organizations that develops standards for security, logistics and transportation practices.	**Network Types(s):** No Change **Industry Role(s):** Add: Network Operator, Service Provider **Keywords(s):** No Change **Reference(s):** Delete Reference **Status:** No Change	Important	**Changed**

9-6-5142	Network Operators, Service Providers and Equipment Suppliers should work together to deploy safeguards to protect the software (i.e. generic or upgrade releases) being loaded to network elements in order to prevent sabotage.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-5019	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider establishing an employee awareness training program to inform employees who create, receive or transfer proprietary information of their responsibilities for compliance with proprietary information protection policies and procedures.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-9-0665	Network Operators, Service Providers and Property Managers should provide and maintain accurate single line drawings of AC switch equipment on-site.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Procedures **Reference(s):** No Change **Status:** Changed	Critically Important	**Changed**
9-7-0471	Network Operators, Property Managers, and Public Safety should consider remote, electronic antenna aiming and utilize tower-mounted equipment that minimizes the need for tower top maintenance where conditions prevent climbs (e.g., osprey nest, weather conditions).	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0473	Network Operators, Property Managers, and Public Safety should consider maintaining a list of authorized climbers and a log of authorized tower climbs.	**Network Types(s):** No Change **Industry Role(s):** Add: Network Operator, Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-0474	Network Operators, Property Managers, and Public Safety should periodically perform grounds maintenance at cell site facilities (e.g., pest control, mow grass, fence maintenance, snow removal).	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0475	Network Operators, Property Managers, and Public Safety should have agreements in place to ensure necessary and timely access to cell sites.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0477	Network Operators and Public Safety should consider the potential of electromagnetic coupling when designing cell sites with high voltage FAA beacons and, if present, take appropriate steps to mitigate the interference (e.g., squelch, physical separation, shielding).	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-0478	Network Operators and Public Safety should allow for deviation in elevation angle and azimuth resulting from deflection of the supporting structure (e.g., sun, load distribution, wind) during the design of a cell site.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0480	Network Operators, Property Managers, and Public Safety should periodically inspect antennas, waveguide, and ancillary hardware to insure physical integrity and the absence of physical movement which can create intermittent and localized intermodulation interference generators (e.g., rusty joints) and/or alter predicted antenna radiation patterns (e.g., antennas swinging around in the wind) potentially creating interference.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0481	Network Operators, Property Managers, and Public Safety should ensure appropriate spacing between all antennas at a cell site in order to avoid interference, intermodulation, or other detrimental effects.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0482	Network Operators and Public Safety should utilize RF propagation and other modeling tools to analyze and optimize designs to avoid interference and improve network performance.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-0483	Network Operators and Public Safety should have a master cell site database with configuration parameters, connectivity, and performance statistics that can be used to analyze and audit cell site performance.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0484	Network Operators and Public Safety should have a program (e.g., automated drive test equipment, network probes) to monitor and detect network performance anomalies.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0492	Network Operators, Property Managers, and Public Safety should provide back-up power (e.g., some combination of batteries, generator, fuel cells) at cell sites and remote equipment locations, consistent with the site specific constraints, criticality of the site, the expected load and reliability of primary power.	**Network Types(s):** No Change **Industry Role(s):** Add: Property Manager, Public Safety **Keywords(s):** Add: Emergency Preparedness Delete: Access Control **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**

9-7-0493	Network Operators, Property Managers, and Public Safety should consider placing fixed power generators at cell sites, where feasible.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**
9-7-0494	Network Operators, Property Managers, and Public Safety should consider including a provision in cell-site contracts for back-up power.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Industry Cooperation **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0495	Network Operators, Property Managers, and Public Safety should consider pre-arranging contact information and access to restoral information with local power companies.	**Network Types(s):** Add: Cable, Internet, Satellite, Wireline **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**

9-7-0496	Network Operators, Property Managers, and Public Safety should consider storing their portable generators at critical sites that are not otherwise equipped with stationary generators.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-0498	Network Operators, Property Managers, and Public Safety should consider alternative measures for cooling network equipment facilities (e.g., powering HVAC on generator, deploying mobile HVAC units) in the event of a power outage.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Emergency Preparedness, Disaster Recovery **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0499	Network Operators, Service Providers, and Public Safety should consider ensuring that the back-haul facility equipment located at the cell site is provided with backup power duration equal to that provided for the other equipment at the cell site.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**

9-7-0501	Network Operators, Service Providers, and Public Safety should report problems discovered from their operation of network equipment to the Equipment Supplier whose equipment was found to be the cause of problem.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Delete: Documentation **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0508	Network Operators and Service Providers should establish company-specific interconnection agreements, and where appropriate, utilize existing interconnection templates and existing data connection trust agreement.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** FCC URL(s) needs added to this reference when available to provide user's access to older NRIC Final Reports and supporting documents. **Status:** No Change	Important	**Changed**
9-7-0512	Network Operators, Service Providers, Public Safety, and Property Managers should perform periodic inspections of fire and water stops where cable ways pass through floors and walls (e.g., sealing compounds).	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0517	Equipment Suppliers should design network elements and associated network management elements with the combined capability to dynamically handle peak load and overload conditions gracefully and queue or shed traffic as necessary (e.g., flow control).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Network Provisioning, Network Operations **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-9-0529	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.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0542	Equipment Suppliers should include steps to prevent and detect malicious code insertion from Original Equipment Manufacturers (OEMs), contractors, and disgruntled employees.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-0543	Network Operators and Service Providers should establish agreements with Property Managers for both regular and emergency power.	**Network Types(s):** No Change **Industry Role(s):** Add: Network Operator **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-9-0546	Network Operators, Service Providers, and Public Safety should consider minimizing single points of failure (SPOF) in paths linking network elements deemed critical to the operations of a network.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Delete: Business Continuity **Reference(s):** Add: With this design, two or more simultaneous failures or errors need to occur at the same time to cause a service interruption. **Status:** Changed	Highly Important	**Changed**
9-9-0547	Network Operators, Service Providers, and Public Safety should place critical network databases (e.g., directory server, feature server, Service Control Point (SCP)) in a secure environment across distributed locations to provide service assurance (e.g., maintainability, connectivity, security, reliability) consistent with other critical network elements.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-9-0548	Network Operators, Service Providers, and Public Safety should have an internal post mortem process, which engages Equipment Suppliers and other involved parties as appropriate, 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 Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0552	Equipment Suppliers should perform software fault insertion (including simulating network faults such as massive failures) as a standard part of the development process.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-0553	Equipment Suppliers should perform hardware fault insertion testing (including simulating network faults such as massive failures) as a standard part of the development process.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-0554	Equipment Suppliers should converge hardware and software fault recovery design processes early in the development cycle.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0557	Equipment Suppliers should take steps to minimize the possibility of having a silent failure on any system component, especially critical components, throughout the life of the product.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Important	**Changed**
9-7-0645	Network Operators, Service Providers, Public Safety, and Property Managers should inspect and maintain heating, venting, air conditioning (HVAC) areas.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0648	Network Operators, Service Providers, Public Safety, and Property Managers should ensure certified inspection of boilers & fuel storage units.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-9-0667	Network Operators, Service Providers, Public Safety, and Property Managers should keep circuit breaker racking/ratchet tools, spare fuses, fuse pullers, etc. readily available.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Network Provisioning, Hardware **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0672	Network Operators and Service Providers should provide a minimum of 3 hours battery reserve for central offices equipped with fully automatic standby systems.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** Changed	Highly Important	**Changed**
9-7-0681	Network Operators, Service Provider, Equipment Suppliers and Property Managers should ensure that fuses and breakers meet quality reliability standards.	**Network Types(s):** No Change **Industry Role(s):** Add: Service Provider **Keywords(s):** Add: Network Provisioning **Reference(s):** Add: Refer to Technical Reference (SR-332), Reliability Prediction Procedure for Electronic Equipment, and http://telecom-info.telcordia.com/site-cgi/ido/docs.cgi?ID=SEARCH&DOCUMENT=SR-332& **Status:** Changed	Highly Important	**Changed**

9-7-0684	Network Operators, Service Providers, Equipment Suppliers, and Property Managers should verify DC fusing levels throughout the power supply and distribution system, especially at the main primary distribution board, to ensure that fuses and breakers are not loaded at more than 80% of their rated ampacity.	**Network Types(s):** No Change **Industry Role(s):** Add: Equipment Supplier **Keywords(s):** Add: Hardware **Reference(s):** Add: Diode OR'ed arrangements require additional special overcurrent protection considerations **Status:** No Change	Important	**Changed**
9-7-0685	Network Operators and Service Providers should have detailed methods and procedures to identify the protection required for energized DC buses.	**Network Types(s):** No Change **Industry Role(s):** Add: Service Provider **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0692	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider using fail-safe alarm points (i.e., alarm point that does not require power to operate) for critical alarms.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Hardware **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-9-0693	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 (i.e., maintenance window).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Power **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0696	Network Operators and Service Providers should use infrared thermography to check power connections and cabling in central offices when trouble shooting, during installation test and acceptance, and as otherwise appropriate.	**Network Types(s):** No Change **Industry Role(s):** Delete: Property Manager **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-9-0700	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider the use of power expertise/power teams.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0702	Network Operators and Service Providers should minimize dependence on equipment requiring AC power feeds in favor of DC-powered components.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Network Operations **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0703	Network Operators, Service Providers, Public Safety, and Property Managers should secure remote power maintenance systems to prevent unauthorized use.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Cyber Security **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0705	Network Operators should place warning tape 12 inches above buried cable facilities.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0706	Network Operators should use visible cable markings on buried facilities and outside plant cables (unless prone to vandalism).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0707	Network Operators should ensure timely response once they receive notification from the One Call Center for all locate requests.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0708	Network Operators should use appropriate technologies for locating buried facilities and consider upgrading as technologies evolve.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Procedures **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0709	Network Operators should compare outside plant drawings relative to marking cable route maps when locating buried facilities and resolve any discrepancies.	**Network Types(s):** Delete: Satellite **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0710	Network Operators should use 'dig carefully' concepts and utilize guidance from industry sources for the protection of underground facilities when excavation is to take place within the specified tolerance zone.	**Network Types(s):** Delete: Satellite **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0719	Network Operators should use 'dig carefully' concepts and utilize guidance from industry sources when installing underground facilities.	**Network Types(s):** Delete: Satellite **Industry Role(s):** No Change **Keywords(s):** Add: Network Operations **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0722	Network Operators, Service Providers, Public Safety, and Property Managers should consider pest control measures to protect cables where appropriate.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Procedures **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0725	Network Operators and Government should increase stakeholder coordination and cooperation to improve the effectiveness of state one-call (811) legislation efforts.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0726	Network Operators should consider partnering with excavators, locators, and municipalities in a cable damage prevention program (811).	**Network Types(s):** Delete: Satellite **Industry Role(s):** No Change **Keywords(s):** Add: Industry Cooperation **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0729	Network Operators should establish training, qualification and performance standards for internal utility locators and establish performance standards with external utility locators.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Industry Cooperation **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0733	Network Operators should coordinate activities with other right-of-way occupants to minimize the potential for damage when they are relocating buried facilities in a common right-of-way area.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Liaison **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0735	Network Operators should evaluate the performance of their contracted excavators and internal excavators to foster improved network reliability.	**Network Types(s):** Delete: Satellite **Industry Role(s):** No Change **Keywords(s):** Add: Supervision **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-9-0736	Network Operators should develop and implement a rapid restoration program for cables and facilities.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Policy **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-0741	Network Operators and Service Providers should review, and adopt as appropriate, Best Practices aimed at reducing damage to underground facilities that are maintained by the Common Ground Alliance.	**Network Types(s):** Delete: Satellite **Industry Role(s):** No Change **Keywords(s):** Add: Documentation, Policy, Procedures, Training & Awarness **Reference(s):** Update: The Common Ground Alliance Best Practices document (www.commongroundalliance.com) provides comprehensive guidance in the areas of Planning & Design, One-Call Centers, Locating & Marking, Excavation, Mapping, Compliance, Public Education, Reporting & Evaluation, and Homeland Security. Many of the Best Practice are applicable to the activities of Service Providers and Network Operators. **Status:** No Change	Important	**Changed**
9-9-0745	Equipment Suppliers should design equipment so that changes and upgrades are non-service impacting.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Technical Support **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0746	Equipment Suppliers should emphasize human factors during design and development to reduce human errors and the impact of these errors. Automated systems should be considered to reduce operating errors.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** Modify: See GR 2914 at http://telecom-info.telcordia.com/site-cgi/ido/docs.cgi?ID=287618448SEARCH&DOCUMENT=GR-2914 **Status:** No Change	Important	**Changed**
9-7-0747	Network Operators, Service Providers and Equipment Suppliers should work together to establish reliability and performance objectives in the field environment.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Policy Delete: Hardware **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0748	Equipment Suppliers should provide troubleshooting job aids, with updates as appropriate, to assist operations support personnel during fault isolation and recovery.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Disaster Recovery, Training & Awareness **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0749	Equipment Suppliers should prevent critical systems from accepting or allowing service affecting activity without appropriate confirmation.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Procedures **Reference(s):** No Change **Status:** No Change	Critically Important	**Changed**
9-7-0751	Equipment Suppliers should provide clear and specific engineering guidelines, ordering procedures, and installation documentation in support of their products.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Hardware, Software **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0752	Network Operators, Service Providers, and Public Safety should evaluate support documentation as an integral part of the equipment selection process.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Procedures **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0753	Network Operators, Service Providers, and Public Safety should be familiar with support documentation provided with the equipment.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Procedures **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0754	Network Operators, Service Providers, Public Safety, and Property Managers should have documented installation guidelines for equipment deployment in their network or buildings.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Hardware **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0756	Network Operators, Service Providers, Public Safety, Equipment Suppliers and Property Managers should consider including a quality review based on the installation guidelines as part of the on-site installation acceptance.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Procedures **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0757	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should have procedures for pre-qualification or certification of installation vendors.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-9-0759	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).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Network Operations **Reference(s):** Delete: Best Practice recommended by the NRSC Timing Outage Task Force Report - March 6, 2002 **Status:** No Change	Important	**Changed**
9-7-0765	Network Operators should configure their TCP algorithm parameters in order to optimize the performance of TCP/IP data transport for VoIP over wireless networks.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-9-0766	Service Providers should consider using a minimum interoperable subset for VoIP coding standards in a VoIP-to-PSTN gateway configuration in order to achieve interoperability and support all types of voice band communication (e.g., DTMF tones, facsimile, TTY/TDD).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Cyber Security **Reference(s):** Add: For example, TI 811 mandates the use of G.711 **Status:** No Change	Highly Important	**Changed**

9-7-0771	Network Operators, Service Providers and Equipment Suppliers should have a procedure for pre-notification of visits to critical facilities.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Procedures, Physical Security Management **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0772	Collocated Service Providers should coordinate with Network Operators and Property Managers on equipment moves, adds or changes which could impact other occupants.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-9-0775	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, and then verify the completed changes against the synchronization plan.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**

9-7-0776	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should conduct and periodically re-validate physical security assessments on critical network facilities.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** Add: Procedures **Reference(s):** No Change **Status:** No Change	Highly Important	**Changed**
9-7-0777	Equipment Suppliers should optimize equipment initializations to minimize service impact.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Hardware, Software **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0778	Network Operators, Service Providers, Public Safety, Equipment Suppliers and Property Managers should ensure that handling installation/interconnection of circuit and signal paths continues to be performed by qualified communications technicians.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0779	Network Operators, Service Providers and Equipment Suppliers should establish a means to allow for coordination between cyber and physical security teams supporting preparedness, response, investigation and analysis.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Business Continuity **Reference(s):** No Change **Status:** No Change	Important	**Changed**

9-7-0781	Network Operators, Service Providers, Public Safety, and Property Managers should evaluate the use of automatic notification mechanisms to the local fire department at critical facilities.	**Network Types(s):** No Change **Industry Role(s):** Add: Public Safety **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-7-0804	Service Providers should consider appropriate means for providing their customers with information about their traffic policies so that users may be informed when planning and utilizing their applications.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Delete: Cyber Security **Reference(s):** No Change **Status:** No Change	Important	**Changed**
9-9-0805	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).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** Add: Documentation Delete: Cyber Security **Reference(s):** No Change **Status:** No Change	Important	**Changed**

BEST PRACTICES – UNCHANGED (TAGLINES REMOVED)				
9-9-0423	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.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Unchanged**
9-7-0426	Equipment Suppliers should use software change control to manage changes to source material used in the production of their products.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Unchanged**
9-7-0433	Equipment Suppliers should support, clearly define and document environmental variables in Management Information Bases (MIB).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Unchanged**

9-7-0562	Equipment Suppliers should use a change control and release planning process to keep track of the changes to the product and the corresponding documentation.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**
9-7-0604	Network Operators and Service Providers should establish synchronization coordinator(s) who has responsibility for the network synchronization. The synchronization coordinator(s) should be accessible to their Network Operations Centers.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Unchanged**
9-9-0664	Network Operators, Service Providers and Equipment Suppliers should provide indicating type control fuses on the front of the power panels, including smaller distribution panels.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**
9-7-0676	Network Operators and Service Providers should not use low voltage disconnects or battery disconnects at central office battery plants.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**

9-7-0677	Network Operators, Service Providers and Property Managers should only use rectifier sequence controllers where necessary to limit load on the backup power generator.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**
9-8-0590	Network Operators, Service Providers, and Equipment Suppliers should develop Methods of Procedure (MOP) for core infrastructure hardware and software growth and change activities and periodically review and update as appropriate.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**
9-7-1064	Network Operators, Service Providers and Equipment Suppliers should implement minimum network management controls in order to promote reliability of the interconnected network.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Unchanged**
9-7-5006	Network Operators, Service Providers, Equipment Suppliers and Property Managers should have policies and procedures that address tailgating (i.e. following an authorized user through a doorway or vehicle gateway). At critical sites, consider designing access points to minimize tailgating.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**

9-7-5015	Network Operators, Service Providers and Equipment Suppliers should establish separation policies and procedures that require the return of all corporate property and invalidate access to all corporate resources (physical and logical) to coincide with the separation of employees, contractors and vendors.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Unchanged**
9-7-5020	Network Operators, Service Providers and Equipment Suppliers should consider establishing corporate standards and practices to drive enterprise-wide access control to a single card and single system architecture to mitigate the security risks associated with administering and servicing multiple platforms.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**
9-6-5081	Equipment Suppliers should provide serial numbers on critical network components (e.g., circuit packs, field replaceable units).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Unchanged**
9-6-5086	Equipment Suppliers should consider electronically encoding a unique identifier into non-volatile memory of critical elements (e.g., Field Replaceable Units, FRUs) for integrity and tracking.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**

9-7-5076	Network Operators and Service Providers should ensure and periodically review intra-office diversity of critical resources including power, timing source and signaling leads (e.g., SS7).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Unchanged**
9-7-5079	Network Operators and Service Providers should, where feasible, provide both physical and logical diversity of critical facilities links (e.g., nodal, network element). Particular attention should be paid to telecom hotels and other concentration points.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Unchanged**
9-7-5088	Equipment Suppliers should ensure appropriate physical security controls are designed and tested into new products and product upgrades (e.g., tamper resistant enclosures).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**
9-7-5107	Network Operators, Service Providers and Equipment Suppliers should evaluate and manage risks (e.g., alternate routing, rapid response to emergencies) associated with a concentration of infrastructure components.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Critically Important	**Unchanged**

9-9-5112	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).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**
9-7-5198	Equipment Suppliers should design their products to take into consideration protection against the effects of corrosion and contamination.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**
9-7-5283	Equipment Suppliers should provide network element thermal specifications or other special requirements in order to properly size Heating, Ventilation, and Air Conditioning (HVAC) systems.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**
9-6-1007	Network Operators, Service Providers and Equipment Suppliers should consider establishing a geographically diverse back-up Emergency Operations Center.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Unchanged**

9-7-1040	Network Operators, Service Providers and Equipment Suppliers should consider using lab, demonstration or training equipment if replacement equipment is unavailable in disaster situations.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**
9-7-0485	Network Operators should optimize cell sites, including relationships between neighboring cells, using a combination of drive testing and network statistics.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**
9-7-0491	Network Operators, Service Providers and Equipment Suppliers should, where programs exist, coordinate with local, state and/or federal emergency management and law enforcement agencies for pre-credentialing to help facilitate access by technicians to restricted areas during an event.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Critically Important	**Unchanged**
9-7-0497	Network Operators and Property Managers should consider connecting the power load to portable generators stored at critical sites, and configuring them for auto-engage in the event of a failover.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Unchanged**

9-7-0515	Network Operators and Service Providers should, for easy communication with subscribers and other operators and providers, use specific role-based accounts (e.g., abuse@provider.net, ip-request@provider.net) versus general accounts (e.g., noc@provider.net) which will help improve organizational response time and also reduce the impact of Spam.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**
9-7-0516	Network Operators and Service Providers should manage the volatility of route advertisements in order to maintain stable IP service and transport. Procedures and systems to manage and control route flapping at the network edge should be implemented.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Unchanged**
9-7-0538	Equipment Suppliers' network element (including OSS) software should be backward compatible.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Unchanged**
9-7-0539	Equipment Suppliers should share trend information (availability, etc.) with their Network Operators and Service Providers.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**

9-7-0549	Network Operators should develop an engineering design for critical network elements and inter-office facilities that addresses diversity, and utilize management systems to provision, track and maintain that inter-office and intra-office diversity.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Unchanged**
9-7-0555	Equipment Suppliers should continually enhance their software development methodology to ensure effectiveness by employing modern processes of assessment.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**
9-7-0686	Network Operators, Service Providers and Equipment Suppliers should verify front and rear stenciling on equipment during installation for accurate identification.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**
9-9-0694	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.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**

9-7-0715	Network Operators should proactively communicate with land owners regarding rights-of-way or easements near critical buried facilities to prevent accidental service interruption.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**
9-7-0716	Network Operators should encourage employees to become proactive in preventing buried facilities damages.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**
9-7-0738	Network Operators and Service Providers should track and analyze facility outages taking action if any substantial negative trend arises or persists.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**
9-7-0744	Equipment Suppliers should periodically review the results of root cause analysis to ensure that the least impacting methods for fault recovery are being used.	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Important	**Unchanged**

9-9-0750	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).	**Network Types(s):** No Change **Industry Role(s):** No Change **Keywords(s):** No Change **Reference(s):** No Change **Status:** No Change	Highly Important	**Unchanged**

7 Appendix 2 – Best Practice Supporting Element Definitions

BEST PRACTICES NETWORK ROLES:

- **Cable:**
  An entity that provides terrestrial communications through direct connectivity, predominantly by coaxial cable or optical fiber, between the serving central office and end user location(s).

- **Internet/Data:**
  An entity that provides terrestrial internet and/or data communications through direct connectivity, predominantly by wire, coaxial cable, or optical fiber, between facilities-based and non-facilities-based serving networks and end user location(s).

- **Satellite:**
  An entity that provides telephony, internet, and/or paging communications through satellite connectivity, predominantly by satellite beams, inter-satellite links, or MSS gateway earth stations between a terrestrially-based control center and end user location(s).

- **Wireless:**
  An entity that provides terrestrial communications through radio spectrum allocation, predominantly by cellular architecture and/or CMRS paging between the terrestrially-based mobile switching center and end user location(s).

- **Wireline:**
  An entity that provides terrestrial communications through direct connectivity, predominantly by wire or optical fiber, between the serving central office and end user location(s).

BEST PRACTICES INDUSTRY ROLES:

- **Property Manager**
  The responsible party for the day-to-day operation of any facility including a facility owner or "landlord", the majority owner of a shared facility, the owner's representative, a professional property management company, a realty management company, tenant representative, a facility provider, or a facility manager, usually involved in facility operations and providing service to a communications enterprise.

- **Equipment Supplier**
  An organization whose business is to supply network operators and service providers with equipment or software required to render reliable network service.

- **Government**

Any government agency at federal, state or local level.

- **Network Operator**
  The entity responsible for the development, provision and maintenance of real-time networking services and for operating the corresponding networks.

- **Public Safety**
  An organization that is a key contributor to E9-1-1 reliability and resiliency in the Public Safety sector.

- **Service Provider**
  An organization that provides services for content providers and for users of a computer network. The services may include access to the computer network, content hosting, server of a private message handling system, news server, etc. A company, organization, administration, business, etc., that sells, administers, maintains, charges for, etc., the service. The service provider may or may not be the operator of the network.

BEST PRACTICES RATING & RANKING:

- ***Critical*** **(1)** Best Practices include those which meet any of the following standards:
  - Significantly reduce the potential for a catastrophic failure of critical communications network infrastructure and/or services (e.g., telecommunication, public safety, energy sector, financial, etc.).
  - Materially limit and/or contain the geographic area affected by a communications failure from cascading to other or adjacent geographic areas.
  - Affect critical communications networks (e.g., SS7) for all network configurations, independent of size.
  - Preserve priority communications for key personnel involved in disaster response and recovery.
- ***Highly Important*** **(2)** Best Practices include those which meet any of the following standards:
  - Improve 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.
  - Improve 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.
  - Improve detection of network events by network operators and service providers.

  - Implementation has improved network reliability but may not be applicable for all networks or companies.

- ***Important*** **(3)** 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 PRACTICES RECOMMENDED KEYWORDS:

- **Access Control**
  Limiting and/or documenting physical access to buildings, equipment and/or systems.

- **Buildings**
  Physical structures that house communications equipment or employees.

- **Business Continuity**
  Corporate wide program that has been established for the purpose of internal planning for and responding to emergency situations impacting services, employees or assets.

- **Contractors & Vendors**
  Non-employees working on behalf of the company or providing goods/services (not visitors).

- **Corporate Ethics**
  Corporate values and integrity for organizations supporting public communications infrastructure.

- **Cyber Security**
  The protection of information and systems against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

- **Disaster Recovery**
  Steps taken after an emergency event has occurred to recover from the event.

- **Documentation**
  Information concerning the operation/location of communications equipment and networks. This DOES NOT necessarily include everything written but may include information in a draft format.

- **Emergency Preparedness**
  Steps taken prior to an emergency event occurring that will facilitate the restoration from the event.

- **Encryption**
  Steps taken to make data unusable to any other person(s) or system(s) other than for

whom it is intended.

- **Essential Services**
  Ensuring the continued operation of vital services (911, priority circuits).

- **Facilities – Transport**
  Interoffice facilities used to carry communications (e.g., copper, fiber, free space).

- **Fire**
  Preventing, controlling, or extinguishing combustion of materials at or near telecommunications equipment.
- **Guard Force**
  People tasked for safeguarding facilities, physical assets, and personnel.

- **Hardware**
  Equipment used to support communications networks.

- **Human Resources**
  Processes and procedures relating to personnel within a company.

- **Industry Cooperation**
  Collaboration between separate business entities.

- **Information Protection**
  Safeguarding the confidentiality and integrity of a company's proprietary information.

- **Intrusion Detection**
  Actions taken to alert users or administrators when an unauthorized entity has attempted or has succeeded in accessing a system or database. This denotes cyber intrusion and does not cover physical intrusion.

- **Liaison**
  Maintaining communications through a working relationship with other entities.

- **Material Movement**
  Physical movement of materials (i.e., logistics).

- **Network Design**
  Planning and configuration of communication networks.

- **Network Element**
  Unique equipment that is a component of a network.

- **Network Interoperability**
  Interaction of networks that must work together to provide communications.

- **Network Operations**
  Tasks required to operate a network.

- **Network Provisioning**
  Steps taken to activate equipment/services in a network.

- **Pandemic**
  Related to the preparation or reaction to wide-spread epidemic or epidemic in a specific area.

- **Physical Security Management**
  Anything having to do with safeguarding the physical assets of the corporation.

- **Policy**
  High level management statements of a desired condition (not detailed procedures).

- **Power**
  Electrical systems (AC/DC) used to operate communications equipment.

- **Procedures**
  Instructions for specific tasks.

- **Public Safety**
  Related to emergencies and 9-1-1 services used by individuals or corporations.

- **Security Systems**
  Hardware/Software devices specifically used to monitor and control security.

- **Software**
  Code specific to running communications equipment.

- **Supervision**
  Direct management of tasks workers.

- **Technical Support**
  Providing assistance in installing, maintaining, or restoring equipment.

- **Training & Awareness**
  Company provided instruction or other means of education on specific topics.

- **Visitors**
  Individuals who are not employees/contractors/vendors.