



JANUARY 2011

WORKING GROUP 6: BEST PRACTICE
IMPLEMENTATION

FINAL REPORT

Table of Contents

1	Results in Brief.....	3
1.1	Executive Summary	3
2	Introduction	4
2.1	CSRIC Structure.....	4
2.2	Working Group 6 Team Members	5
3	Objective #1: Critical Best Practice Options and Recommendations	6
3.1	Approach	7
3.2	The Network Reliability Steering Committee's Modified & Proposed Best Practices	9
4	Objective #2: Implementation Options and Recommendations	10
4.1	Approach and Recommendations of the Education Awareness Committee	10
4.1.1	Benchmark Survey	10
4.1.2	Web-based Training	11
4.1.3	White Paper	12
4.1.4	Presentations of Information at Industry Conferences and Events	14
4.2	Approach and Recommendations of the Implementation Committee	14
5	Recommendations	16
6	Conclusions	19
7	Appendices	22
	Appendix 1 – Objective #1: Committee Members.....	23
	Appendix 2 – Objective #2: Committee Members.....	24
	Appendix 3 – Educational Awareness Benchmark Survey.....	25
	Appendix 4 – Project Timeline	28
8	Attachments.....	29
	Attachment 1 – Best Practices Ranking Spreadsheets	
	Attachment 2 – NRSC Modified & Proposed Best Practices	
	Attachment 3 – Educational Awareness Benchmark Survey Tables	

1 Results in Brief

1.1 Executive Summary

Working Group 6 of the Communications Security, Reliability and Interoperability Council (CSRIC) developed recommendations for CSRIC's consideration regarding the Critical Best Practices whose implementation would enhance the security, reliability, operability and resiliency of infrastructure for communications industry segments. The report also outlines recommendations to approve 22 of the 23 proposed and modified Best Practices that the Network Reliability Steering Committee submitted to CSRIC for approval.

Working Group 6 also developed recommendations for CSRIC's consideration regarding methods to educate, encourage, and facilitate the implementation where appropriate of those Best Practices by network operators, service providers, equipment suppliers, property managers, and public safety authorities.

To achieve these results, Working Group 6 developed criteria for analyzing over 800 Best Practices that were created and modified by previous Network Reliability and Interoperability Councils. Working Group 6 then applied the criteria and categorized each of the Best Practices as being "Critical," "Highly Important," or "Important" to communications industry segments.

Key recommendations of Working Group 6 include the following:

- Communications organizations should evaluate and implement those Best Practices which they deem appropriate. These organizations should institutionalize the review of Best Practices as part of their planning processes and assess on a periodic basis how implementing selected Best Practices might improve the proficiency and reliability of their operations.
- 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.
- The Federal Communications Commission should continue to endorse the use of Best Practices by communications industry organizations.
- The Best Practices should be reassessed and updated as needed to keep pace with changes and advancements in the communications industry.
- In particular, Best Practices should be developed and revised as appropriate to address emerging risks to the security and reliability of networks.

- Best Practices should be developed to address the interoperability of communications systems.

In addition, Working Group 6 developed recommendations to drive increased familiarity and adoption of the Best Practices into the daily operations and planning for communications organizations. Data about the level of the industry's current awareness and use of the Best Practices was gathered through a custom benchmark survey. Based on the results, Working Group 6 proposed a comprehensive Best Practices web-based training framework, a white paper on the subject to be provided to the industry, and recommendations for live Best Practice presentations at specific industry conferences and events.

In order to have a pulse on implementation of Best Practices in a non-attribution basis, Working Group 6 provided a framework for a possible future industry survey. The goal of such a survey would be to contribute information that could be used in devising techniques that encourage the increased use of the Best Practices by communications industry segments. The decision whether to proceed with a survey, and the obligation to develop and distribute it and to manage the information provided by respondents would be made by a successor group to the current CSRIC. The successor group would need an appropriate complement of participants from diverse elements of the communications industry, along with adequate resources to resolve certain competing considerations and logistical issues identified in the report.

In summary, Working Group 6 believes that the value of having up-to-date Best Practices as a resource for the communications industry is evident and that the goals of the Federal Communications Commission should include (1) assisting the industry in improving the Best Practices databases and (2) supporting communications organizations in maintaining their awareness of the Best Practices and in implementing them as appropriate.

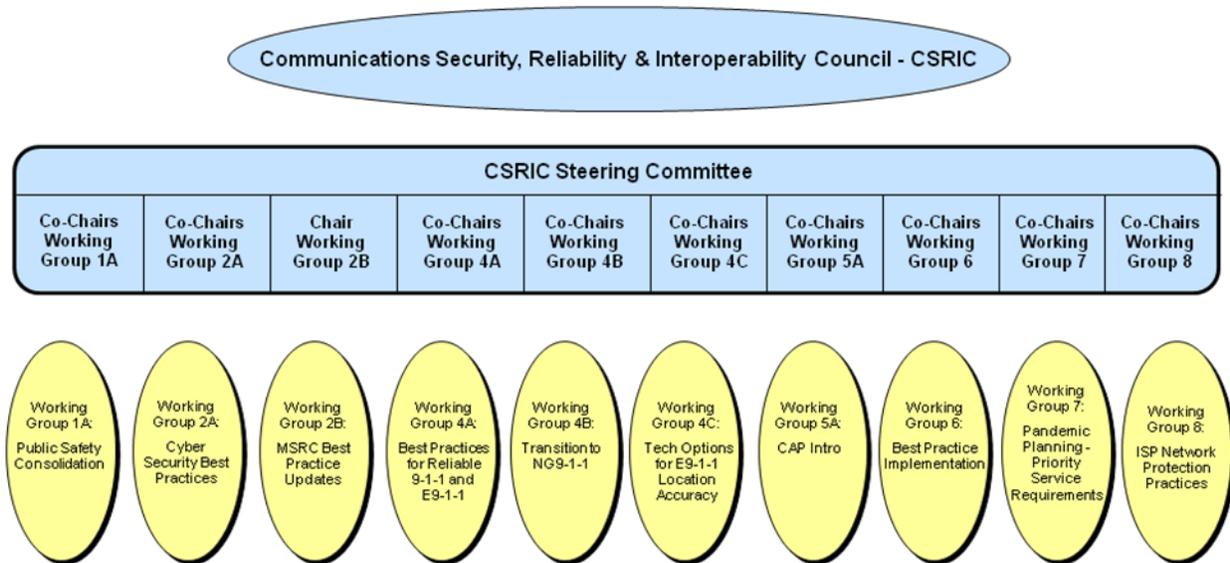
2 Introduction

This report documents the results of the efforts of Working Group 6 (herein, Working Group or WG 6) to develop options and recommendations for approval by CSRIC regarding the subset of the existing 800+ Best Practices that are most critical for enhancing the security, reliability, operability and resiliency of the communication industry's infrastructure¹. The report outlines recommendations regarding the proposed and modified Best Practices (BPs) that the Network Reliability Steering Committee (NRSC) submitted to CSRIC for approval. The report also describes proposals for identifying, contacting, and educating appropriate users within the communications industry about the value of the BPs and how to implement them. Finally, it outlines various approaches that the FCC and communications industry organizations may consider to increase the utilization of the BPs.

2.1 CSRIC Structure

¹ The Federal Communications Commission clarified that this Working Group was not tasked with updating and/or creating new BPs to fill gaps that were identified during the Working Group's review of the existing BPs.

CSRIC was chartered by the Federal Communications Commission (FCC) on March 19, 2009, and was organized into ten working groups for accomplishing its charter. The working groups and their areas of responsibility are listed below.



2.2 Working Group 6 Team Members

The members of WG 6 and their sponsorships or affiliations are listed below:

Name	Organization
Stacy Hartman (Co-Chair)	Qwest
Steve Malphrus (Co-Chair)	Federal Reserve Board of Governors
Jackie Voss	Alliance for Telecommunications Industry Solutions (ATIS)
Jim Runyon	Alcatel-Lucent, Bell Labs
Gordon Barber	AT&T
Doug Peck	California 911 Emergency Communications Office
Mike Giampietro	Cox
Rick Kemper	CTIA
Stephen Hayes	Ericsson
John Healy	Federal Communications Commission (FCC)
Peter Fonash	Federal Reserve Board of Governors
Wayne Pacine	
Thomas Hicks	Intrado
Jim Corry	LightSquared, Satellite Industry Association (SIA)

Karen Eccli ²	Qwest
Cynthia Daily	Sprint Nextel
Richard Zinno	
Spilios Makris	Telcordia Technologies
Uma Chandrashekhar ³	TIA
Jay Naillon	T-Mobile
Harold Salters	
Scott Tollefsen ⁴	USA Mobility, Inc.
Stephen Washburn	US Department of Health and Human Services
Kevin Green	Verizon
Marcia Brooks	WGBH National Center for Accessible Media (NCAM)

Table 1 - List of Working Group 6 Members

The members of WG 6 were divided into several committees in order to accomplish the Working Group's assignments. These committees are described in the appropriate sections below.

WG 6 began holding regular meetings by video conference and telephone on March 4, 2010⁵. Meetings of the entire Working Group were held monthly. Meetings of the WG 6 Co-Chairs, Committee Co-Chairs, and other designated members also were held monthly. Committees met as often as weekly while completing their assignments. WG 6 also held four face-to-face meetings in Washington, D.C. at the offices of the Board of Governors of the Federal Reserve System.

3 Objective No. 1: Critical Best Practice Options and Recommendations

The first objective of WG 6 was to develop options and recommendations for CSRIC's approval regarding the critical BPs that communications industry segments should consider implementing (if they have not already done so) in order to enhance the security, reliability, operability, and resiliency of communications infrastructure and performance.

The BPs that the Working Group assessed came from two sources. The majority were created and modified over a 14-year period by a series of Network Reliability and Interoperability Councils (NRIC), which were federal advisory committees that preceded CSRIC. The former NRICs were comprised of representatives of communications companies, communications

² Actively participated on the Working Group and Co-Chaired the Business Continuity and Disaster Recovery Committee from December 2009 through July 2010, when she retired from Qwest

³ Works for Bell Labs, Alcatel Lucent

⁴ The Working Group Co-Chairs would like to recognize and thank Scott Tollefsen for the significant amount of time and effort that he contributed in drafting and editing this Report.

⁵ The Working Group's project timeline is in Appendix 4.

industry associations, and government entities. The NRICs existed for 14 years (January 1992 through December 2005) operating under the authority of successive charters established by the FCC. The NRICs developed over 800 BPs, and WG 6 reviewed and assessed each of these BPs. Prior to the assessment by CSRIC Working Group 6, the NRIC BPs had not been reviewed or updated since 2005.

In addition, WG 6 reviewed, evaluated and provided recommendations regarding the 23 modified and new BPs which had been developed by the Network Reliability Steering Committee (NRSC), a committee of the Alliance for Telecommunications Industry Solutions (ATIS).

WG 6 did not review, evaluate, or provide recommendations related to any of the practices and/or guidelines which were developed by the other CSRIC Working Groups chartered under this CSRIC. However, WG 6 recommends that any BP modified or first developed under this CSRIC be reviewed and ranked by a successor CSRIC.

3.1 Approach

WG 6 adopted a five-step process to accomplish the task of developing options and recommendations regarding the critical BPs.

First, WG 6 developed criteria for use in categorizing each BP as being either “Critical,” “Highly Important,” or “Important” to communications industry organizations. Those BPs categorized as “Critical” are those which the Working Group assessed as being most vital to the various communications network operators, service providers, equipment suppliers, property managers, and public safety authorities. The guidelines adopted for the three categories were the following:

Critical Best Practices include those which met 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.).
- Significantly reduce the duration or severity of critical communications outages.
- 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 Best Practices include those which met 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 Best Practices include those which met any of the following standards:

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

Second, after establishing the criteria for categorizing the BPs, the BPs were sorted by the Working Group's FCC Liaison into five groups corresponding to the names of the committees listed below. The primary reasons for segmenting the BPs in this manner were that many companies provide products or services relating to more than one of these topic areas, and many companies are vitally concerned with more than one of the topic areas in their day-to-day operations. A secondary objective of the sorting process was to assign each committee roughly the same number of BPs for review. In cases where a given BP related significantly to the interests of two committees, that BP was included among the BPs assigned to both committees.

Third, the Working Group formed the following four committees and assigned each of its members to serve on at least one of the committees to evaluate the BPs:

- Business Continuity and Disaster Recovery
- Cyber Security
- Network Reliability
- Physical Security and E911 (two separate topic areas)⁶

The members of these committees are listed in Appendix 1.

As a result of the sorting process described above, the Business Continuity and Disaster Recovery Committee was assigned 217 BPs, the Cyber Security Committee was assigned 205, the Network Reliability Committee was assigned 251, and the Physical Security and E911 Committee was assigned a total of 175 BPs (124 and 51, respectively).

Fourth, each of the committees reviewed their assigned BPs, applying the guidelines described above to establish a view of the relative significance of each assigned BP to the industry. The committees then completed a comprehensive review and ranking of their assigned BPs.

In performing this work, each committee member reviewed the assigned BPs and determined the ranking which each person considered appropriate for every BP. The rankings were aggregated on a spreadsheet that displayed the rankings, which was distributed to the other members of the

⁶ Separate groups of BPs were sorted and assigned for the topics of Physical Security and E911.

given committee. Each committee subsequently held between six and 10 face-to-face meetings or conference calls to compare, discuss, and assign the appropriate ranking for each BP.

The committees determined that they could best serve the interests of CSRIC and the communications industry by reaching the largest consensus when ranking each BP. If the individual rankings within a committee were unanimous for a BP, that ranking was assigned. For BPs where unanimity was not reached in the initial individual rankings, the committees either discussed the issues until consensus on a ranking was achieved or used a voting arrangement to settle on a ranking supported by all committee members.

The committees also considered the data provided in “Best Practices Mentioned in Final Outage Reports” presented by Whitey Thayer (FCC Public Safety and Homeland Security Bureau) and how the FCC reportable outage reports could be utilized as a source for assigning rankings.

Some of the BPs required lengthier discussion than others, reflecting the variety of perceptions that stem from the knowledge and experience of participants who occupy different roles in the communications industry. Appropriate comments about particular BPs are included in Attachment 1.

Fifth, the members of WG 6 performed a final review to the ranking and participant comments produced for each BP and collaborated in the development of recommendations for CSRIC’s approval. These recommendations appear in Section 5 below.

Best Practice Review & Ranking	
Category	# of Best Practices
Critical	114
Highly Important	348
Important	341

Table 2 – Working Group 6 Best Practice Ranking Results

A complete copy of the ranking is attached in the form of a spreadsheet as Attachment 1.

3.2 The Network Reliability Steering Committee’s Modified & Proposed Best Practices

Working Group 6’s description was expanded to include reviewing and providing recommendations regarding the 23 proposed and modified BPs that the NRSC submitted to CSRIC for approval. In order to accomplish this task, the Working Group collectively reviewed the modified and proposed BPs while tracking any recommended revisions and/or issues with the BPs. After this comprehensive review was completed, the WG 6 leadership met with the NRSC

to review the changes and concerns. During this meeting, the WG 6 leadership and the NRSC collaborated to finalize a list of 22 of the 23 BP's to recommend for approval.

A complete list of the BPs recommended for approval are attached in the form of a spreadsheet in Attachment 2.

While the NRSC's BP were not categorized as "Critical," "Highly Important," or "Important," Working Group 6 recommends that they be categorized during a subsequently chartered CSRIC.

4 Objective No. 2: Implementation Options and Recommendations

The second objective of WG 6 was to develop options and recommendations for CSRIC's approval regarding how communications industry segments can reliably and accurately self measure implementation of key BPs.

WG 6 determined that, based upon the shared experience of its members, and given that this evaluation of the BPs is occurring approximately five years after the last NRIC, the FCC's primary focus should be on educating the appropriate users of BPs, specifically about what BPs are, why they are important, and how to access and use them effectively. An education plan appears to be the appropriate step, in view of the previously described efforts to (a) to identify and highlight the most critically important BPs and (b) ensure the BPs are worded clearly to reflect current communications industry capabilities and policy goals.

To address these tasks, and having already reviewed and ranked the BPs as to their relative importance, the Working Group formed two additional committees:

- Education and Awareness
- Implementation

The members of these two committees are listed in Appendix 2.

4.1 Approach and Recommendations of the Education and Awareness Committee

The objective of the Education and Awareness Committee was to develop recommendations for a plan that, upon implementation, would drive familiarity and adoption of the BPs into the daily operations and planning of the communications industry. The committee's plan was comprised of four elements: (1) a benchmark survey to determine the industry's current awareness and use of the BPs; (2) comprehensive web-based training on the use of the BPs; (3) a "white paper" informational document intended for wide circulation among appropriately targeted readers within the industry; and (4) recommendations for presenting information about the BPs at industry conferences and events. To inform these recommendations, the committee conducted and discussed online research into how communications industry websites reflect BPs and potential industry conferences/events to target.

4.1.1 Benchmark Survey

The committee recognized at the outset of this task that it would be useful to gauge the industry's current degree of familiarity with and use of the BPs, and that the best way to measure awareness and use would be to conduct a non-attribution survey. As such, the committee developed survey questions and arranged for the Alliance for Telecommunications Industry Solutions (ATIS), a third-party industry representative, to conduct the survey in order to take advantage of the long-term working relationships fostered by ATIS with many companies and organizations in the communications services industry.

A copy of the survey and data summarizing the survey responses are found in Appendix 3 and Attachment 3 (respectively).

This survey was provided to over 300 executives and employees of communications organizations, and 62 recipients responded to the survey. Over 70% of the respondents identified themselves as telecommunications companies or wireless carriers. Two-thirds of the persons responding for their organizations identified themselves as regulatory affairs and compliance analysts, general analysts, network operations staff, or engineering design and architecture staff. Nearly two-thirds of responding organizations were not obligated to file FCC outage reports or were unaware if they were obligated.

The majority of respondents were familiar with BPs; two-thirds of the respondents routinely access the BPs via the FCC's website (www.fcc.gov/nors/outage/bestpractice/BestPractice/cfm), while the remainder generally access the BPs using the Bell Labs website (www.bell-labs.com/USA/NRICbestpractices/). Users of the FCC site appear to visit the site more often than users of the Bell Labs site. In addition, survey data also established that a higher percentage of users successfully found the information they were seeking on the FCC site than on the Bell Labs site. Information returned on the first inquiry attempt on the FCC site was more likely to be helpful than information returned on the first inquiry attempt on the Bell Labs site. Output produced by the FCC site was compatible with the users' computer systems more frequently than output produced by the Bell Labs site.

Based on the survey results, the Working Group was able to conclude that most of those persons providing data on behalf of respondent organizations were those that used the BPs as a resource for completing FCC outage reports. The Working Group also believes it is preferable for communications organization staff from disciplines such as network operations and design, network capacity planning, and network architecture to use the BPs to enhance the probability that networks will be built in a manner that makes them more robust and hardened against failure.

Additional recommendations arising from the survey process and results appear in Section 5 below.

4.1.2 Web-based Training

The online training component of the plan was focused on developing a framework for an electronic BP reference resource that would be available for use by network operators, service providers, equipment suppliers, property managers, and public safety authorities. Working

Group 6 believes that an online training program should be presented in the form of a tutorial and that the content should minimally be reviewed and updated annually.

The intent of the BP tutorial should be to inform and guide the user by posing a series of questions for the user to answer; if incorrect answers are given by the user, the tutorial should respond by providing the correct answer. Taking the tutorial should be a positive and productive experience in all respects. In order to maximize the utilization of the training, each user should be guided through the tutorial, provided with explanations about the process, and thanked for participating.

In addition, WG 6 believes that the tutorial should be hosted by an industry association such as ATIS, CTIA, the United States Telecom Association, or another similar organization. The Working Group determined that this would be preferable to the FCC developing and/or hosting the website, because it would eliminate any unintended assumption by potential users that their tutorial performance is being monitored by a regulatory agency and/or that poor performance may be detrimental to them or their respective organization(s). Apart from these concerns, the FCC should be encouraged to promote utilization of such tutorial.

While the FCC has the option to develop a tutorial of this nature, the Working Group recommends that the tutorial be developed by a third party having expertise in designing such programs and not necessarily by the host organization, unless such organization demonstrates that it has the required expertise. The development process should take into account the results of the BP benchmark survey described above, along with any other input the developer recommends. The target audience of the tutorial should be those persons in the industry that have significant impact on their respective organizations through the education and implementation of appropriate BPs. The developer should assist in identifying appropriate industry websites and contacting those sites to request the inclusion of the link to this tutorial.

WG 6 further believes that the format of the tutorial should consist of training modules for the key decision-making areas involved in overseeing, implementing, and maintaining the functions and activities addressed by the BPs. Each module should be structured to be brief (e.g. taking 20 minutes to complete) and the program should allow for users to complete each module in multiple sessions.

WG 6 further believes that a webinar approach may be another efficient and useful tool for training target users on the BPs. A webinar may be more expensive to develop, maintain and present than an automated electronic tutorial. However, a webinar could potentially be scaled at different levels in relation to demonstrated interest and available funding. As such, a webinar could be provided by the FCC, the host organization, other interested industry groups, or on a per-user fee basis.

4.1.3 White Paper

Working Group 6 also recommends that the following framework for a white paper be utilized to develop a document that explains to appropriate users the value of the BPs and how to access and use them. The white paper should encourage the use of the BPs by providing examples of their value and emphasize the availability of the training resources that are referenced above.

WG 6 believes that the chief responsibility for developing the white paper should be assigned to a willing industry organization, such as the ATIS NRSC, rather than to the FCC. Such an industry group should have the following qualifications: it should recognize the value of such a white paper, have the expertise to create a white paper of high quality, and be comprised of members or representatives of entities with sufficient financial resources to support the development and maintenance of the paper. The Working Group further believes that a subsequently chartered CSRIC and/or the FCC's Public Safety and Homeland Security Bureau (PSHSB) should partner with the developer to review and update the white paper as necessary.

Regardless of which industry group is assigned to this project, the Working Group believes that the white paper should target executives, network architects, software engineers, and other personnel within network operators, service providers, equipment designers, manufacturers, and suppliers, facility and property managers, and public safety authorities that (i) have operational responsibility for the activities and facilities addressed by the BPs and (ii) assess the BPs for incorporation into their organizations' procedures and work plans.

Once the white paper is developed, it should be made available to members of the appropriate audience in the following ways:

- Post a link to the document on the websites of selected industry associations and government agencies.
- E-mail a link and a short summary to people identified as target audience members, such as those in radiofrequency licensing records, industry association membership lists, and publication circulation databases.
- Distribute copies at industry conferences and other events.
- Include copies in mailings made periodically available by the FCC (e.g. to licensees in connection with maintenance of their licenses) or by industry organizations/associations.
- Advertise or publicize the availability of the white paper and a general description of the BPs in industry magazines and newsletters.

WG 6 recommends that the white paper include the following:

- An overview of what the BPs are, how they came to be established, and how they are revised and updated to keep pace with industry policy and technology developments.
- A statement of where the BPs can be found and how to use the online library or database.
- An explanation of how persons can be trained in using the BPs quickly and effectively, including the following:
 - Description of the 24/7 web-based training
 - Announcement of periodic webinars
- Some case studies or examples of how the BPs have assisted communications providers by adding value, including:
 - Higher quality and reliability in operations.
 - Differentiation in the marketplace.
 - Employee safety, including the reduced risk of liability for personal injury or loss of life.
 - Asset protection, including the reduction of property damage and nonperformance of contracts.

- Directions for users to provide input, feedback, suggested changes, and/or proposed new BPs.

4.1.4 Presentations of Information at Industry Conferences and Events

The committee completed a comprehensive review of the broad array of trade shows, conventions, and exhibits held across the country each year for the communications industry. Several of the largest are the Consumer Electronics Show sponsored by the Consumer Electronics Association; the National Association of Broadcasters' convention; the Wireless Show (sponsored by CTIA); the Inside the Network show (sponsored by the Telecommunications Industry Association); the Alliance for Telecommunications Industry Solutions (ATIS) Annual Meeting of the Committees (AMOC); the annual meeting of the National Telecommunications Cooperative Association (NTCA); the Institute of Electrical and Electronics Engineers (IEEE) Reliability and Maintainability Symposium – Product Quality & Integrity; the International IEEE Communications Quality and Reliability (CQR) Workshop; and the EastWest Institute Worldwide Cybersecurity Summit. These events are geared primarily to the marketing of products and services. Among the attendees of these shows are the key decision makers within communications industry segments who determine the policies for network design, service standards, and product development that their organizations' engineering and operations groups follow.

The Working Group believes that information on BPs should be presented live and in-person to intended users at some or all of the industry events listed above and that this should be accomplished in innovative ways that underscore the importance and value of the BPs. Panels and "break-out sessions" at industry trade shows are ideal mechanisms for such presentations. To be effective, the presentations must be coordinated with the event producer(s) and promoted in advance to the target attendees. For example, at CES, the FCC or an industry group could work with the sponsor to place the BP training program on an education track that will cause it to be noticed by engineering and operations specialists. Such a presentation should be conducted by an effective speaker and facilitator. For example, at the NTCA show, a business owner could explain to fellow owners how implementing BPs has improved the financial performance and service quality of their operations.

4.2 Approach and Recommendations of the Implementation Committee

To augment the education plan described above, the Implementation Committee considered approaches for organizations to self measure their respective implementation of the critical BPs identified in this report. After considerable thought and discussion, the Working Group resolved that a survey would be the only mechanism that could deliver statistically valid information about the implementation of BPs. The committee believed that a survey may attempt to identify specific BPs that had not been implemented by organizations and to determine what factors may block or hamper their use. The committee also thought that a survey might somehow seek to assess the degree of BP implementation in different sectors of the industry. The process of analyzing how to design an appropriate survey led to the recognition that attempting to gather information from communications organizations that would yield the foregoing results would be difficult for reasons of logistics and would be unlikely to produce the type of data desired.

Any sharing of survey results with others is fraught with potential problems. First, the information sought would not lie solely with organizations such as those which are members of CSRIC and its Working Groups but would also require input from organizations including applications, content development, and other web-based functions; as well as vendors which provide managed services to network providers. Second, many communications companies likely would be reluctant to jeopardize their competitive standing by disclosing proprietary data or creating a security risk by disclosing information about possible system vulnerabilities. Third, entities subject to FCC regulation would question whether making disclosures in such a survey would amount to subjecting themselves to Commission inquiries or enforcement actions.

Due to the constraints set forth above, the Working Group determined that any such survey would be of limited value and that the primary focus should rather be on educating the users of BPs about what BPs are, why they are important, and how to access and use them effectively. That said, if the FCC or an industry group were to move forward with the development of a survey, Working Group 6 believes that the survey framework and considerations outlined in this report should be utilized. Further, if a survey were developed, WG 6 believes that a non-governmental trade or professional association should be charged with the development and management of the survey on behalf of the industry.

The committee determined that an implementation survey could be utilized to gather some statistically meaningful data that could be analyzed for the purpose of devising techniques to encourage the increased study and use of the BPs within an organization. A survey could gather information on the cost incurred by different types of organizations to implement BPs, and/or the views of organizations on the effectiveness of particular BPs and the respective risks of not implementing them.

Where organizations decline to use the BP guidelines and the websites which contain them, a survey could seek explanation of why that is the case. Questions could ask whether a cost/benefit analysis is seen as not justifying implementation of one or more BPs, whether implementation is beyond the scope of the organization's business plan and commitment to customers or users, or whether any state or local regulatory factors, such as zoning, emissions or hazardous materials restrictions, preclude implementation of BPs.

A survey could inquire whether an organization would be more likely to use the BP website(s) if they were designed differently or if the content were to be presented in a different way. For example, with respect to BPs relating to Cybersecurity, would organizations prefer that a website be organized by function (e.g., signaling, routing, protocols, DNS, etc.) or by capability (e.g., whether the BP addresses prevention of an outage or a security breach, detection of the same, or response to or recovery from an outage)? A survey might also inquire whether communications organizations concur with what WG 6 has defined as the category of "Critical" BPs or whether the BPs that are defined as having the most significance should be those which relate to emerging risks to the integrity of network performance and the most crucial vulnerabilities of such networks.

The committee also determined that a number of inherent logistical matters must be resolved prior to the development of such a survey. One consideration is the source of the funding to produce and evaluate the survey. A second is identifying what body or bodies should deliver the

survey and interface with the responding organizations in regard to it. A third consideration is determining what organizations to survey and how to arrange for respondents in the organizations with appropriate knowledge and appreciation of the importance of the information. A fourth matter is who or what organization should analyze the results, bearing in mind that such provider of analysis must have the requisite expertise and that the confidentiality interests of respondent organizations be protected in the process of analyzing and reporting results. A fifth issue is determining the standards by which the survey – whatever its results – is to be judged on whether it a successful process. That is are the results significant and reliable; how many responses should be solicited; and how many must be received and analyzed, in order to warrant a high level of confidence in the results?

The committee believes that the determination of whether to proceed with developing and distributing a survey devoted to the foregoing implementation issues is best made by a successor to CSRIC that has an appropriate complement of participants from more of the affected communications industry constituencies and has the resources to resolve the logistical issues described above.

A survey addressing the foregoing matters would seek more information than that collected by the Education and Awareness Committee's benchmark survey (see Section 4.1.1). The data that the implementation survey would generate should help inform the initial or future versions of the other education initiatives proposed by the Working Group.

5 Recommendations

The recommendations of the Working Group are as follows:

- 5.1 All types of communications organizations for which the BPs are intended – network operators, service providers, equipment suppliers, property managers, and public safety organizations – should evaluate the BPs and implement those which they deem appropriate. Communications organizations are strongly encouraged to institutionalize the review of BPs into their planning and operations processes and periodically assess how implementing selected BPs might improve the proficiency and reliability of their respective operations. Each organization should determine which area(s) of its structure should be charged with evaluating the BPs for implementation. Areas likely to be considered for this activity are risk management, network management, engineering, compliance, and policy development.
- 5.2 Compliance with BPs should not be a regulatory mandate, for a variety of reasons.
 - First, not every BP is appropriate for every sector of the communications industry as network and system designs, technologies, and capabilities differ and are continually evolving.
 - Second, within each sector, not every BP is appropriate for every network operator, service provider, equipment supplier, property manager, and public safety authority, since the scope of activities, the resources, and the capabilities of these entities vary.

- Third, while most of the BPs are distinct operational practices, some of the BPs are briefly worded and may be mere admonitions or statements of aspiration, and as such it would not be appropriate to attempt to enforce compliance with the latter in a manner that could result in sanctions such as monetary fines or license revocation.
- Fourth, the resource burdens of implementing BPs not currently in use by a given operator or provider may be significant and are a factor in the decision process of whether or not to implement a particular BP.

In summary, (i) attempting to identify which BPs might be required of each participant in the communications industry would be very impractical, if not impossible, and (ii) mandating compliance with particular BPs would impact the ability of organizations and their customers and other constituents to determine the appropriate value proposition and pricing that define their business models and participation in the industry.

- 5.3 The FCC should continue to endorse the use of BPs by communications industry organizations. The FCC has a long history of supporting industry's development and utilization of BPs through its previously chartered Advisory Committees, including NRIC and the Media Security and Reliability Council (MSRC). The FCC should maintain this support based upon the work of CSRIC during its current and any future chartered terms.
- 5.4 Some of the BPs should be revised to take into account advances and other changes in the communications industry that have occurred since the BPs were initially drafted. As examples, the BPs should take into consideration technologies that enable multiple communication modalities presently used by consumers, the evolution from Time-Division Multiplexed (TDM) networks to Internet Protocol (IP)-based networks, and the use of next-generation IP-networks to facilitate equal access to 9-1-1 services for people with disabilities. With this in mind, the Working Group has offered comments on some of the BPs. These comments are included in Attachment 1.
- 5.5 Moreover, the pace of advancement in communication theory and in system design, fabrication, and operation is accelerating. In response to this, the existing BPs for security and reliability of communications systems should be reassessed and updated with a corresponding increase in frequency. A future CSRIC charter should provide for such reassessment and updating by representatives of communications companies, communications industry associations, government entities, and people with disabilities no less frequently than every two years⁷ to ensure that the BPs address state-of-the-art industry capabilities.
- 5.6 The BPs reviewed by the Working Group did not address interoperability of communications systems using different systems designs, frequencies, and user equipment. This can be explained by the fact that during the time period when the BPs were being devised, communications operators and government regulators were not devoting attention or resources to the development of interoperability capabilities to the extent that they are

⁷ This recommendation and several others include a reference to defining a task in a "future CSRIC charter." In all such cases, WG 6 recommends that the tasks be included in the next available CSRIC charter, because the issues should be addressed as promptly as possible.

today. Given the current policy preference for encouraging interoperability of communications systems for various purposes (including increasing the functionality and utility of communications systems generally and strengthening the ability of emergency responders to communicate more effectively during crises), new BPs should be developed to address concerns arising in the field of communications system interoperability.

- 5.7 Certain risks to the security and reliability of communications networks have existed in the same form for many years and are well understood. Emerging risks to networks present greater uncertainty and compel fresh assessment. The BPs as a whole should be assessed and augmented under a future CSRIC charter by a team of experts who have experience dealing with new forms of risks and threats that are presented by (i) persons who use today's knowledge and tools in seeking to disrupt network performance and (ii) any inherent weaknesses in newer network architecture and equipment.
- 5.8 The BPs relating to E-911 performance address voice interruption more than data interruption. An appropriate team of experts should be tasked in a future CSRIC charter to solicit and modify existing BPs or establish new BPs relating to avoidance of interruptions in data transmission, minimization of the duration of such interruptions, and speed restoration of service.
- 5.9 None of the BPs pertaining to E-911 performance addresses accessibility considerations, gaps, or compliance with the Americans with Disabilities Act. A team of experts representing a wide spectrum of interested constituencies, including people with disabilities, should be convened under a future CSRIC charter (or in some other way with the support of the FCC) to identify and address accessibility gaps in the BPs to ensure that persons with disabilities have direct access to 9-1-1 services in their preferred communication modalities⁸. BPs should be modified and/or newly developed to advance the findings of the Emergency Access Advisory Committee (EAAC) and the Video Programming and Emergency Access Advisory Committee (VPEAAC), both of which the FCC established on December 7, 2010 to assist the FCC in implementing the 21st Century Communications and Video Accessibility Act of 2010⁹.
- 5.10 A team of experts should be convened under a future CSRIC charter to reconcile and merge the phrasing and organization of the BPs assessed by WG 6 with those BPs that have been developed by other working groups operating under the current CSRIC charter.

⁸ The National Emergency Number Association (NENA) Accessibility Committee keeps an updated list of communication modalities (<http://www.nena.org/operations-committee-accessibility>).

⁹ The purpose of the EAAC is to determine the most effective and efficient technologies and methods by which to enable access to Next Generation 911 emergency services by individuals with disabilities, and many of the recommendations which it has been directed to provide pertain to achieving reliable and interoperable communication that will ensure access to emergency services by people with disabilities. The purpose of the VPEAAC is to develop recommendations concerning, *inter alia*, (i) the compatibility between video programming delivered using Internet protocol and devices capable of receiving and displaying such programming in order to facilitate access to captioning, video description, and (ii) emergency information, and accessible emergency information on television programming delivered using Internet protocol or digital broadcast television. As emergency communications systems, including those for people with disabilities, migrate to Internet protocol-based systems, the security, reliability, and interoperability of these systems become essential to the safety and well-being of all.

- 5.11 Many BPs included multiple concepts or were in need of re-wording to make the intent of the BP clearer. This complicated the process of seeking consensus on the relative significance of those BPs and, more importantly, was seen as diminishing the value of these BPs as sources of guidance for the industry. The Working Group has offered suggestions to improve the standardization and clarity of some of the BPs and also to improve their utility by identifying some considerations for reorganizing them. The process of generating revisions and additions to the BPs in the future should emphasize clarity of expression (e.g., standardized language and format) in light of then-current industry standards. Additionally, the ATIS NRSC has developed a brief tutorial on BPs that outlines guidelines for the development of these practices as well as their format. These guidelines would serve well as the basis for the development of future BPs and should be further distributed throughout the industry. Additionally, as experts in this area, the NRSC could undertake an effort to revisit previously developed BPs to ensure clarity, conciseness, and relevancy with new technologies.
- 5.12 The search engine used in organizing and locating BPs on particular topics is understood to have gone unchanged since 2001. Based on assessing the data gathered in the Benchmark Survey and on advancements in the communications industry during the past 10 years, it would be beneficial for CSRIC, in a future term, to reassess the design and operation of the search engine to determine if it should be refined so as to deliver enhanced performance
- 5.13 Web-based training in the form of a tutorial should be developed to assist communications industry organizations in learning about the BPs and how to use them, and the tutorial should be updated as needed in order to keep pace with relevant changes. More specific recommendations concerning the tutorial appear in Section 4.1.2.
- 5.14 A White Paper that explains the value of the BPs and how to access and use them should be prepared and distributed to key executives and operations personnel of communications organizations. More specific recommendations concerning the framework of the White Paper appear in Section 4.1.3.
- 5.15 Presentations about the BPs should be made at selected communications industry events. More specific recommendations concerning proposed venues and other facets of these presentations appear in Section 4.1.4.
- 5.16 A survey may be considered to gather data as how to encourage the increased study and use of the BPs. More specific recommendations concerning how this survey should be designed and what information it should elicit from responding organizations appear in Section 4.2.

6 Conclusions

Working Group 6 performed the following:

- Reviewed over 800 Best Practices (developed over a 14-year period by a predecessor FCC advisory committee) and classified each as Critical, Highly Important, or Important.

- Identified 114 of these BPs as the most critical for enhancing the security, reliability, operability, and resiliency of the communications industry's infrastructure and operations.
- Developed recommendations and proposals to educate executives and staff of network operators, service providers, equipment suppliers, property managers, and public safety authorities about the availability of the BPs, to encourage their use, and to assist with their implementation.

The communications industry supports the vital activities of federal, state, local and tribal governments and nearly all areas of the economy. Disruption of communications affecting the nation's financial system, the military, emergency responders, the energy industry, and similar critical infrastructures can threaten national security as well as personal safety and wellbeing.

There is no shortage of good reasons for communications organizations to take steps to ensure continued delivery of their mission-critical services in less-than-optimal conditions, whether those conditions are predicted or arise as emergencies and whether they occur naturally or are man-made. Where business continuity preparation cannot prevent interruption of service, communications organizations should have arrangements in place to restore service as quickly as possible.

Best Practices are guidelines that emerge from the aggregation of analyses by many trained experts who study the experiences of their organizations and determine the actions that have been shown to be of the greatest benefit in conducting or restoring operations during any and all conditions. Best Practices are not "one size fits all" procedures for any given business or profession and this rule certainly holds true for the communications industry.

It is of paramount importance that all communications organizations incorporate a recurring review of the Best Practices into their respective operations. Circumstances will dictate which Best Practices are implemented by individual organizations, and when that will occur in each case. A tone must be set by the top management of each communications organization that when the appropriate Best Practices are implemented, there is great value and that Best Practices can enhance the security, reliability and operations of the communications network.

Every communications organization will benefit by periodically assessing how its operations and overall network security, reliability, operability, and resiliency might be improved by adopting additional Best Practices and whether its resources will permit their adoption. Such reviews may be carried out by the functional areas including risk management, network management, engineering, compliance, or by policy development. The duties may be distributed or shared according to the subject matter and the organization's internal governance.

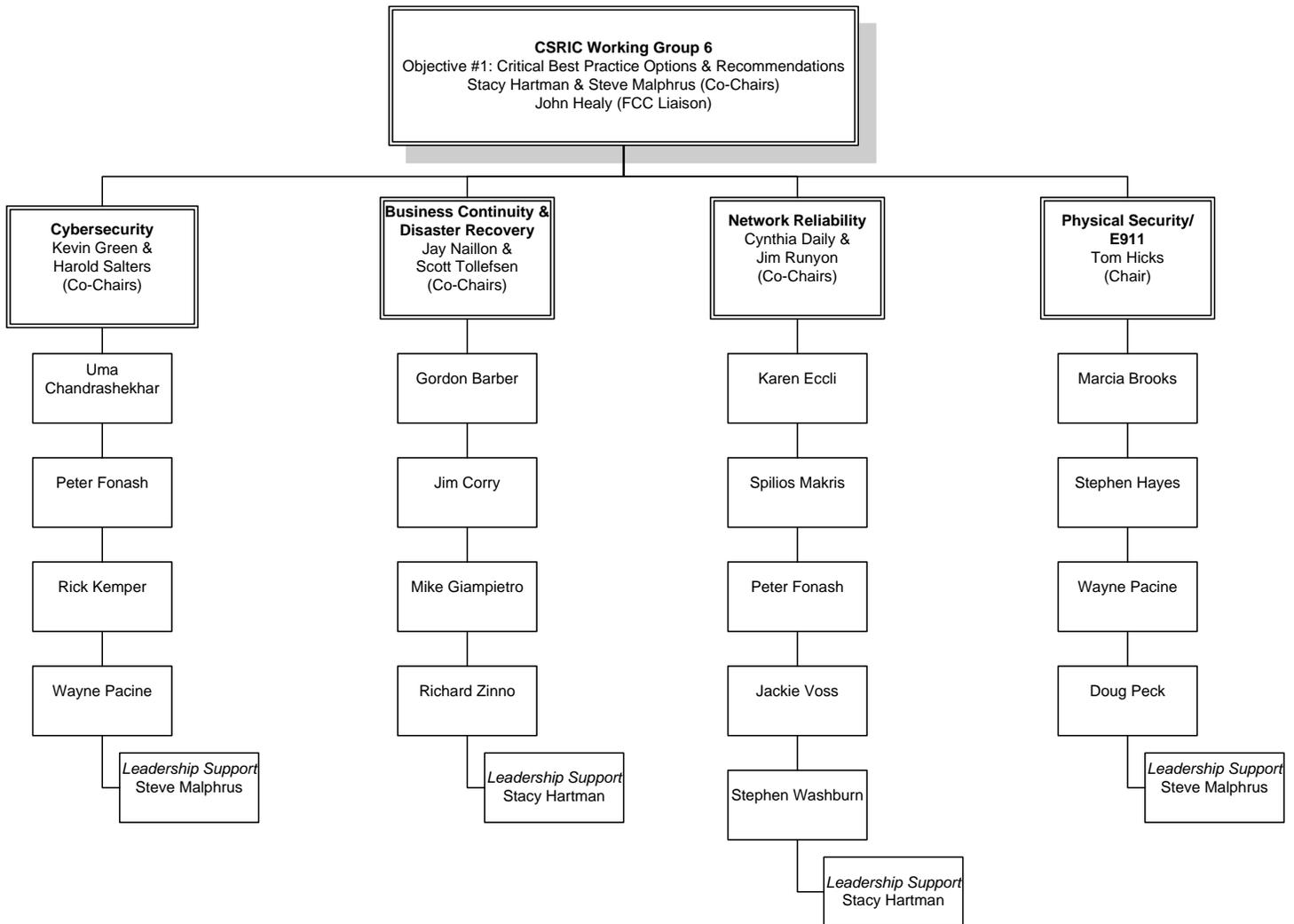
Based on its efforts, Working Group 6 recommends that the charter for CSRIC's next term include a number of tasks related to Best Practices. Among those tasks are to update the Best Practices, develop new Best Practices that address additional areas of concern, and enhance the functionality of the Best Practice databases. The value of the Best Practices to the communications industry cannot be fully realized until these additional tasks are performed.

The capabilities and architecture of communications systems are constantly evolving. These changes are accompanied by new and different vulnerabilities to the security and reliability of the systems. Consequently, the systems must be managed to identify those vulnerabilities and to reduce or eliminate their negative impacts. The communications industry must continue to develop and share new Best Practices that address these evolving issues, and the CSRIC can assist the industry in that important activity by adopting the recommendations proposed by Working Group 6.

7 Appendices

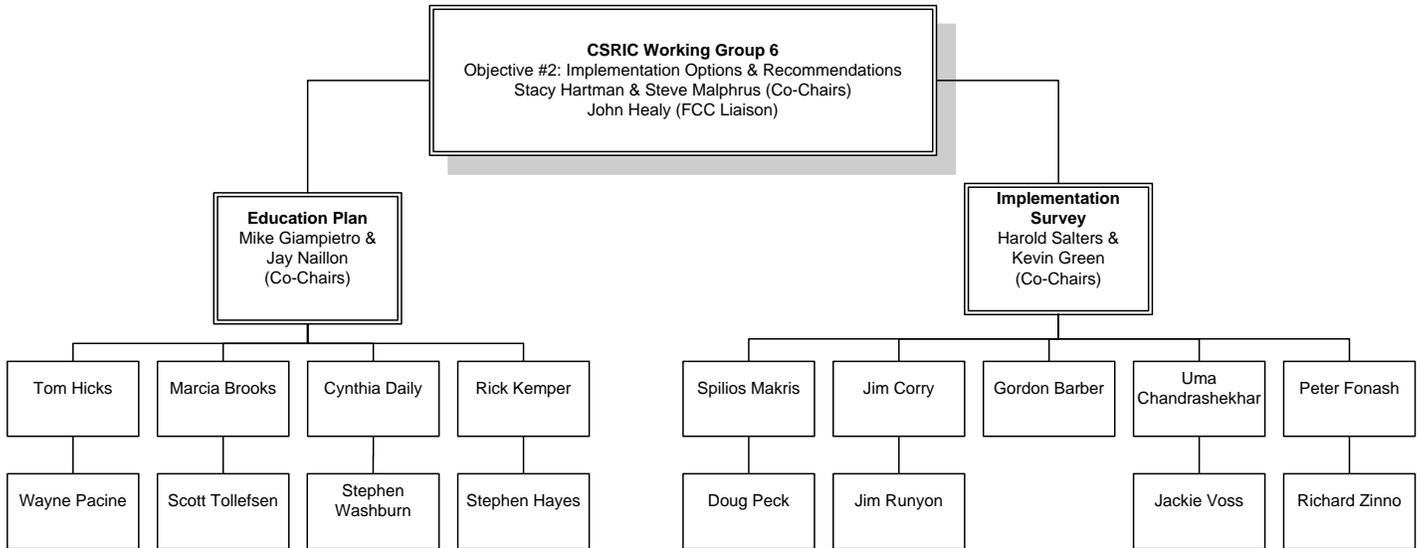
Appendix 1

Working Group 6 Committees that developed options and recommendations for CSRIC's consideration regarding the critical BPs that each communications industry organization should consider for implementation in order to enhance the security, reliability, operability, and resiliency of their communications infrastructure:



Appendix 2

Working Group 6 Committees that developed proposals for identifying, contacting, and educating intended users about the value of the BPs and for considering approaches for organizations to self measure implementation of critical BPs:



Appendix 3

Educational Awareness Benchmark Survey

Best Practice Webpage Survey

ATIS' Network Reliability Steering Committee (NRSC) is asking for your assistance in completing this survey regarding how Communications Best Practices websites are being used. Our request is to not only take the survey yourself, but to forward the survey to the appropriate people within your organization that may be familiar with these websites and request their participation in completing the survey. We would suggest inviting both individual contributors and managers who are responsible for Network Operations, Capacity Planning, System Design, Emergency Management, or Business Continuity.

Individual results will be kept confidential; however, they will be aggregated, provided to the NRSC and the Communications Security Reliability and Interoperability Council (CSRIC)'s Best Practice Implementation Team. This information will aid CSRIC in their report/recommendation to the Council regarding what education and training material may be useful to the industry.

If you have questions or are interested in obtaining a copy of the aggregated results, please contact Jackie Voss, ATIS Manager-Standards Development, at jvoss@atis.org.

Background information.

1. What industry are you from?

(Drop down? Check box?)

a) Wireless Carrier

b) Satellite

c) Cable

d) Telco

e) Telecommunications

Manufacturing Vendor (OEM)

f) Industry

g) Public Safety / E911

h) Internet Service Provider

i) Broadcasting

j) Industry Consortium

k) Industry Consultant

l) Emergency Management

m) Other _____

2. Are you obligated to report communications outages to the Federal Communications Commission (FCC)?

Yes

No

3. How familiar are you with Communications Best Practices?

Very

Somewhat

Not at all (if no, then skip to end)

Familiarity with Communications Best Practice Websites

4. Do you visit the Communication Best Practices websites maintained by (select all that apply):

FCC (<https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm>)

Bell Labs (<http://www.bell-labs.com/USA/NRICbestpractices/>)

Other. Please describe and/or provide link : _____

(if neither of first two is selected, skip to end)

5. How often do you use the FCC or Bell Labs Communications Best Practice website?

Bell Labs website

- a. never
- b. 1-2 times per year
- c. 1-2 times per quarter
- d. > 1- 2 per quarter

FCC website

- a. never
- b. 1-2 times per year
- c. 1-2 times per quarter
- d. > 1- 2 per quarter

6. How often are you able to find the information you are seeking using the retrieval options listed on the websites?

Bell Labs website

- a. Every time
- b. Most of the time
- c. Sometimes
- d. Never

FCC website

- a. Every time
- b. Most of the time
- c. Sometimes
- d. Never

7. Are you aware you can use the “Shift and Left Click” function to select a serial list of Types and Keywords?

Bell Labs website

- Yes
- No
- I don't use this website

FCC website

- Yes
- No
- I don't use this website

The following questions pertain to the search functionality of the websites.

8. When using the search functionality, is the information provided to you in a timely manner (server response time)?

Bell Labs website

- Yes
- No
- I don't use the Search function (skip to question 12)**

FCC website

- Yes
- No
- I don't use the Search function (skip to question 12)**

9. Is the information provided on the first search attempt helpful, if not how many searches on average does it take to obtain the information you are seeking?

Bell Labs website

- Yes
- No Number of Searches _____

FCC website

Yes

No Number of Searches _____

10. Does the timing for the data retrieval vary depending on what you've searched by? (i.e. "Number", "Text" etc.)

Bell Labs website

No

I don't know

Yes.

If yes, please explain

FCC website

No

I don't know

If Yes. Please explain

11. Is the output file compatible with your PC/MAC/Operating system for viewing and manipulation?

Bell Labs website

Yes

No

FCC website

Yes

No

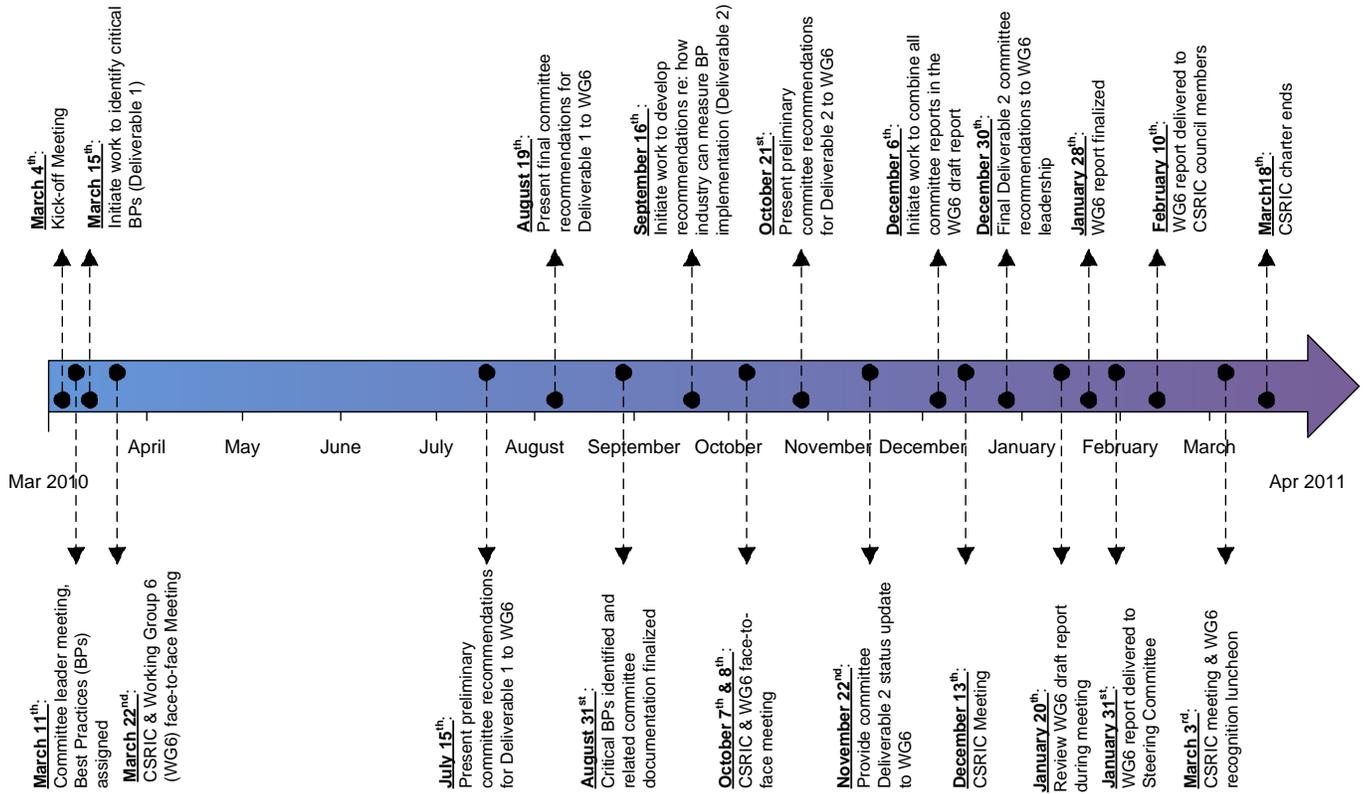
Other suggestions or comments:

12. Do you have any suggestions of how the BP websites could be more useful?

13. Other comments?

Please provide your email address in case of questions (**this information will not be transmitted to the FCC**): _____. If you have questions, please contact Jackie Voss, ATIS Manager-Standards Development, at jvoss@atis.org.

Appendix 4: Project Timeline



8 Attachments

Physical Security Committee			
Best Practice Number	Best Practice Description	Final Priority	Notes
7-7-5107	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.	Critical	It is critical that network operators, service providers and equipment suppliers perform risk assessments of their communications networks for all configurations and develop risk mitigation procedures/processes to reduce the duration or severity of future critical communications outages. This is of particular importance where there is a concentration of equipment, circuits, facilities, etc. and the impact of a major failure could cascade to a larger geographic region.
7-7-5196	MOPs: Network Operators and Service Providers should ensure that contractors and Equipment Supplier personnel working in critical network facilities follow the current applicable MOP (Method of Procedures), which should document the level of oversight necessary.	Critical	Any time a technical change is made to equipment that supports critical and essential emergency services, a detailed step-by step procedure needs to be written and followed explicitly in order to preclude unplanned service failures that may be caused by technical ignorance, carelessness, accident and/or incomplete work activity.
7-7-5084	Hardware & Software Quality Assurance: Network Operators, Service Providers 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.	Critical	Employing an additional independent entity to provide independent verification and validation adds an additional layer of protection from a separate set of technical experts in order to ensure that critical essential emergency services remain operational.
7-7-5113	Network Operators, Service Providers and Property Managers, when feasible, should provide multiple cable entry points at critical facilities (e.g., copper or fiber conduit) avoiding single points of failure (SPOF).	Critical	While it is not uncommon for communications service providers to diversely route emergency or critical communications from the service provider's location over diverse transport facilities (i.e. cables), the transport facilities commonly enter the building structure where such communications are utilized at one entry point to the building/structure. Thus the cable entry point to the building itself becomes a potential "single point for failure" should an excavation crew or others accidentally severe the cables) entering the building.
7-7-5197	Network Operators, Service Providers, and Property Managers should periodically inspect, or test as appropriate, the grounding systems in critical network facilities.	Critical	Power surges and/or transients can lead to a loss of critical communications , as well as costly damage to low voltage electronic equipment if grounding systems are not properly installed or have been compromised. Further, improperly grounded equipment experiencing a power surge can result in component degradations that may result in latent failures that can be extremely difficult to isolate and resolve. Periodic inspections and/or routine testing of grounding systems can minimize the potential for interruptions to critical communications.
7-6-5170	Network Operators, Service Providers and Equipment Suppliers should control or disable all administrative access ports (e.g., manufacturer) into R&D or production systems (e.g., remap access ports, require callback verification, add second level access gateway).	Critical	To ensure that only authorized personal can manage the communications systems, there should be no back-doors or remote access with weak security. Having such access may lead to confusion with multiple parties updating the systems or in a worst case, may be used as a basis for a malicious attack against the communications system.
7-7-5074	Network Operators, Service Providers, and Equipment Suppliers should document in a Disaster Recovery Plan the process for restoring physical security control points for critical infrastructure facilities.	Critical	During times of a natural or man-made disaster, it will be critical to ensure the physical security control points are fully operational. This is particularly important when the situation has resulted from a man-made or terrorist attack and the possibilities of additional actions are unknown.

Physical Security Committee

Best Practice Number	Best Practice Description	Final Priority	Notes
7-7-5071	In order to prepare for contingencies, 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.	Critical	In order to be ready to address various contingencies that may arise at any time, it is necessary to maintain close liaison with and to maintain priority communications with appropriate emergency operations centers, disaster relief and key government personnel. Once an emergency occurs, it will be difficult to try to develop the appropriate contacts in the various organizations that must be coordinated with.
7-7-5112	Network Operators, Service Providers and Equipment Suppliers should, at the time of the event, coordinate with the appropriate local, state, or federal agencies to facilitate timely access by their personnel to establish, restore or maintain communications, through any governmental security perimeters (e.g., civil disorder, crime scene, disaster area).	Critical	During the week of Sep 11 following terrorists attacks and also following Hurricane Katrina events in New Orleans, restoration efforts were hampered by personnel identification practices and the lack of clear plans relative to who may or may not gain access to the blighted areas. Furthermore, the personal safety of restoration personnel and emergency responders can affect the timeliness of service restoration and delivery of aid.
7-6-5162	Network Operators, Service Providers and Equipment Suppliers should ensure adequate physical protection for facilities/areas that are used to house certificates and/or encryption key management systems, information or operations.	Critical	Certificates and key management systems are used to generate the credentials for access to various critical components of the communications system. If the certificates and systems used to generate keys are damaged or unavailable, then the systems they govern will eventually fail due to authentication failures. Furthermore, stolen information can be used a basis for malicious attacks against the system by reconfiguring key systems.
7-7-5126	Network Operators, Service Providers and Equipment Suppliers should plan for contingency staffing to perform critical functions in response to crisis situations (e.g., natural disasters, labor strike, terrorist attack).	Critical	
7-7-5046	Network Operators and Property Managers should ensure critical infrastructure utility vaults are secured from unauthorized access.	Highly Important	
7-7-5199	Network Operators and Service Providers should provide appropriate protection for outside plant equipment (e.g., Controlled Environmental Vault, remote terminals) against tampering and should consider monitoring certain locations against intrusion.	Highly Important	
7-7-5028	Network Operators, Service Providers 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.).	Highly Important	
7-7-5229	Network Operators, Service Providers and Property Managers should have controlled access to comprehensive facility cabling documentation (e.g., equipment installation plans, network connections, power, grounding and bonding) and keep a backup copy of this documentation at a secured off-site location.	Highly Important	
7-7-5041	Network Operators, Service Providers, Equipment Suppliers and Property Managers should establish and implement policies and procedures to secure and restrict access to power, environmental, security, and fire protection systems.	Highly Important	
7-6-5142	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 through assured communications protocols in order to prevent sabotage.	Highly Important	

Physical Security Committee

Best Practice Number	Best Practice Description	Final Priority	Notes
7-6-5173	Network Operators and Equipment Suppliers should design wireless networks (e.g., terrestrial microwave, free-space optical, satellite, point-to-point, multi-point, mesh) to minimize the potential for interception.	Highly Important	Providers of services to people who are deaf (e.g. phone/video relay/ASL interpretation) need to retain secure access to appropriate wireless networks
7-7-5187	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 with consideration of industry standards and best practices.	Highly Important	
7-6-5274	Network Operators, Service Providers, 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.	Highly Important	
7-7-5005	Network Operators, Service Providers and Equipment Suppliers should conduct electronic surveillance (e.g., CCTV, access control logs, alarm monitoring) at critical access points.	Highly Important	
7-7-5026	Network Operators, Service Providers, Equipment Suppliers and Property Managers 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. 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.	Highly Important	
7-7-5034	Network Operators, Service Providers, Equipment Suppliers 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.	Highly Important	
7-7-5123	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.	Highly Important	
7-7-5164	Network Operators, Service Providers and Equipment Suppliers should establish and enforce a policy to immediately report stolen or missing company vehicles and trailers to the appropriate authorities.	Highly Important	
7-7-5217	Network Operators, Service Providers, Equipment Suppliers and Property Managers should raise awareness of appropriate personnel regarding possible secondary events immediately after an incident and promptly report any suspicious conditions.	Highly Important	

Physical Security Committee

Best Practice Number	Best Practice Description	Final Priority	Notes
7-7-5022	Network Operators, Service Providers and Equipment Suppliers should internally identify and document areas of critical infrastructure as part of security and emergency response planning. This documentation should be kept current and protected as highly sensitive proprietary information.	Highly Important	
7-7-5001	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.	Highly Important	
7-7-5010	Network Operators, Service Providers and Equipment Suppliers should deploy security measures in proportion to the criticality of the facility or area being served.	Highly Important	
7-7-5011	Network Operators, Service Providers, 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).	Highly Important	
7-6-5012	Network Operators, Service Providers and Equipment Suppliers should limit access to areas of critical infrastructure to essential personnel.	Highly Important	
7-7-5015	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.	Highly Important	
7-7-5021	Network Operators, Service Providers, Equipment Suppliers and Property Managers should establish and enforce access control and identification procedures for all individuals (including visitors, contractors, and vendors) that provide for the issuing of ID badges, and the sign-in and escorting procedures where appropriate.	Highly Important	
7-6-5024	Network Operators, Service Providers and Equipment Suppliers should include 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.	Highly Important	
7-7-5027	Security and Human Resources (for Network Operators, Service Providers or Equipment Suppliers) should partner on major issues to ensure that security risks are identified and plans are developed to protect the company's personnel and assets (e.g., hiring, downsizing, outsourcing, labor disputes, civil disorder).	Highly Important	
7-7-5029	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.	Highly Important	
7-7-5030	Network Operators, Service Providers 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.	Highly Important	
7-7-5031	Network Operators, Service Providers 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.	Highly Important	

Physical Security Committee

Best Practice Number	Best Practice Description	Final Priority	Notes
7-7-5040	Network Operators, Service Providers, Equipment Suppliers 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.	Highly Important	
7-7-5066	Network Operators, Service Providers, Equipment Suppliers, and Property Managers should ensure that sensitive information pertaining to critical infrastructure is considered proprietary and access is restricted appropriately, both internally and externally. Appropriate markings are required to qualify for exemption from disclosure under FOIA.	Highly Important	
7-7-5095	Network Operators, Service Providers, Equipment Suppliers and Property Managers should implement a tiered security response plan for communications facilities that recognizes the threat levels identified in the Homeland Security Advisory System.	Highly Important	
7-7-5096	Network Operators, Service Providers and Equipment Suppliers should require compliance with corporate security standards and programs for contractors, vendors and others, as appropriate. This requirement should be included as part of the terms and conditions of the contract that the contractor or vendor has with the company, and should also be made to apply to their subcontractors.	Highly Important	
7-6-5097	Network Operators, Service Providers and Equipment Suppliers should establish and implement corporate security standards and requirements in consideration of the best practices of the communications industry (e.g., NRIC Best Practices).	Highly Important	
7-7-5110	Network Operators 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.	Highly Important	
7-7-5111	Network Operators should not share information regarding the location, configuration or composition of the telecommunication infrastructure where this information would be aggregated at an industry level without proper protection measures acceptable to the information provider.	Highly Important	
7-6-5131	Network Operators should provide appropriate security for emergency mobile trailers (both pre- and post-deployment) in order to protect against a coordinated terrorist attack on emergency communications capabilities.	Highly Important	
7-6-5133	Network Operators should protect the identity of locations where emergency mobile trailers and equipment are stored.	Highly Important	
7-7-5160	Network Operators, Service Providers, Equipment Suppliers and Property Managers should account for the possible absence of critical personnel in their business continuity plan.	Highly Important	
7-6-5172	Network Operators, Service Providers and Equipment Suppliers should not permit unsecured wireless access points for the distribution of data or operating system upgrades.	Highly Important	
7-7-5174	Network Operators, Service Providers, Equipment Suppliers 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.	Highly Important	

Physical Security Committee

Best Practice Number	Best Practice Description	Final Priority	Notes
7-7-5220		Highly Important	
7-7-5277	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.	Highly Important	
7-7-5279	Network Operators, Service Providers and Equipment Suppliers should consider site specific (e.g., location, region, country) threat information during security program development.	Highly Important	
7-7-5116	Network Operators, Service Providers, Equipment Suppliers and Property Managers should provide periodic briefings and/or make available industry/Government guidance for identifying suspicious letters or parcels, to personnel (employees or contractors) involved in shipping, receiving or mailroom activities at major locations or critical sites. Protocols for handling any suspicious items should be established in advance and implemented upon the receipt of any suspicious letter or parcel.	Highly Important	
7-6-5165	Network Operators, Service Providers and Equipment Suppliers should ensure that teleworkers (e.g., remote software developers) have the equipment and support necessary to secure their computing platforms and systems to the equivalent level of those on-site. Security software, firewalls and locked file cabinets are all considerations.	Highly Important	
7-7-5070	Network Operators, Service Providers 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.	Highly Important	
7-6-5200	Network Operators, Service Providers and Equipment Suppliers should establish and implement procedures for the proper disposal and/or destruction of hardware (e.g., hard drives) that contain sensitive or proprietary information.	Highly Important	
7-7-5048	Network Operators, Service Providers and Equipment Suppliers should establish and implement a policy that requires approval by senior member(s) of the security department for security related goods and services contracts.	Important	
7-7-5121	Network Operators, Service Providers 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.	Important	
7-7-5262	Network Operators, Service Providers and Equipment Suppliers should evaluate the vulnerability of storage locations in an effort to protect critical spares.	Important	
7-7-5020	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.	Important	

Physical Security Committee

Best Practice Number	Best Practice Description	Final Priority	Notes
7-7-5088	Equipment Suppliers should ensure appropriate physical security controls are designed and tested into new products and product upgrades (e.g., tamper resistant enclosures).	Important	
7-7-5032	Network Operators, Service Providers and Equipment Suppliers should establish a procedure governing the assignment of facility access levels.	Important	
7-7-5002	Network Operators, Service Providers, Equipment Suppliers and Property Managers should develop and implement periodic physical inspections and maintenance as required for all critical security systems.	Important	
7-7-5003	Network Operators, Service Providers, Equipment Suppliers and Property Managers should periodically audit compliance with physical security policies and procedures.	Important	
7-7-5014	Network Operators, Service Providers, 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.	Important	
7-7-5019	Network Operators, Service Providers 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.	Important	
7-6-5069	For Network Operators, Service Providers collocation sites, the Property Manager should require all tenants to adhere to the security standards set for that site.	Important	
7-6-5149	Network Operators, Service Providers and Equipment Suppliers should, where feasible, ensure that intentional emissions (e.g., RF and optical) from network equipment and transmission facilities are secured sufficiently to ensure that monitoring from outside the intended transmission path or beyond facility physical security boundaries cannot lead to the obtaining of critical network operations information.	Important	
7-7-5033	Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider establishing and implementing background investigation policies that include criminal background checks of employees. The policy should detail elements of the background investigation as well as disqualification criteria.	Important	
7-7-5006	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.	Important	
7-7-5009	Network Operators, Service Providers, Equipment Suppliers and Property Managers should ensure that access control records are retained in conjunction with company standards.	Important	

Physical Security Committee

Best Practice Number	Best Practice Description	Final Priority	Notes
7-7-5013	In facilities where master key systems are used, Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider establishing hierarchical key control system(s) (e.g., Master Key Control systems) with record keeping data bases and implemented so that keys are distributed only to those with need for access into the locked space (e.g., perimeter doors, offices, restricted areas).	Important	
7-7-5018	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.	Important	
7-6-5023	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.	Important	
7-6-5025	Network Operators, Service Providers and Equipment Suppliers should include 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).	Important	
7-7-5042	Network Operators, Service Providers and Property Managers should establish and implement policies and procedures to secure and restrict access to fuel supplies.	Important	
7-7-5043	Network Operators, Service Providers, Equipment Suppliers and Property Managers should comply with security standards for perimeter lighting.	Important	
7-7-5044	Network Operators, Service Providers, Equipment Suppliers or Property Managers should plan and maintain landscaping at facilities to enhance the overall level of building security wherever possible. 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.	Important	
7-6-5049	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.	Important	
7-6-5050	When guard services are utilized by Network Operators, Service Providers, Equipment Suppliers and Property Managers, a supervision plan should be established that requires supervisory checks for all posts.	Important	
7-6-5051	When guard services are utilized by Network Operators, Service Providers and Equipment Suppliers, consider establishing incentives and recognition programs to increase morale and reduce turnover.	Important	
7-7-5052	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.	Important	

Physical Security Committee

Best Practice Number	Best Practice Description	Final Priority	Notes
7-7-5053	Network Operators, Service Providers, Equipment Suppliers and Property Managers should periodically audit guard services to ensure satisfactory performance, and compliance with organizational contractual requirements.	Important	
7-6-5054	When guard services are utilized by Network Operators, Service Providers, Equipment Suppliers or Property Managers, a process should be developed to quickly disseminate information to all guard posts. This process should be documented and should clearly establish specific roles and responsibilities.	Important	
7-7-5067	Network Operators, Service Providers and Equipment Suppliers should make security an ongoing priority and provide periodic, at least annually, security awareness information to all personnel. Where appropriate, include contractors and other regular visitors.	Important	
7-7-5068	Network Operators, Service Providers and Property Managers should establish standards, policies and procedures that, where feasible, separate Inter-connector equipment and personnel access from ILEC floor space.	Important	
7-7-5089	Service Providers, Network Operators 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.	Important	
7-7-5091	Network Operators, Service Providers and Equipment Suppliers should develop and implement, as appropriate, travel security awareness training and briefings before traveling internationally.	Important	
7-7-5092	Network Operators, Service Providers 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.	Important	
7-7-5099	Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider keeping centralized trash collection outside the building to reduce the potential for fire and access to the building. Dumpsters should be located away from the buildings where feasible.	Important	
7-7-5100	Network Operators, Service Providers and Equipment Suppliers should interact as needed with federal, state, and local agencies to identify and address potential adverse security impacts of new laws and regulations (e.g., exposing vulnerability information, required security measures, fire codes).	Important	
7-7-5105	Network Operators and Equipment Suppliers should consider the security implications of equipment movement both domestically and internationally, including movement across borders and through ports of entry.	Important	
7-6-5106	Equipment Suppliers should consider participating in and complying with an industry organization that develops standards in their security, logistics and transportation practices.	Important	
7-7-5114	Network Operators, Service Providers, Equipment Suppliers and Property Managers should establish, implement and enforce mailroom and delivery procedures that recognize changes in threat conditions.	Important	

Physical Security Committee

Best Practice Number	Best Practice Description	Final Priority	Notes
7-7-5115	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.	Important	
7-7-5120	Network Operators, Service Providers, Equipment Suppliers and Property Managers should evaluate the potential benefits and security implications when making decisions about building and facility signage, both internally and externally.	Important	
7-7-5129	Network Operators and Service Providers who are required by the government to file outage reports for major network outages should ensure that such reports do not unnecessarily contain information that discloses specific network vulnerabilities, in order to prevent such information from being unnecessarily available in public access.	Important	
7-7-5130	Network Operators, Service Providers and Equipment Suppliers and the Government should conduct public and media relations in such a way as to avoid disclosing specific network or equipment vulnerabilities that could be exercised by a terrorist.	Important	
7-6-5132	Network Operators should identify primary and alternate transportation (e.g., air, rail, highway, boat) for emergency mobile trailers and other equipment and personnel.	Important	
7-7-5134	Network Operators, Service Providers and Equipment Suppliers should consider establishing a policy to manage the risks associated with key personnel traveling together.	Important	
7-7-5141	Network Operators, Service Providers and Equipment Suppliers should consider restricting, supervising, and/or prohibiting tours of critical network facilities, systems and operations.	Important	
7-7-5151	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.	Important	
7-7-5152	Network Operators, Service Providers and Equipment Suppliers should consider performing targeted sweeps of critical infrastructures and network operations centers for listening devices when suspicion warrants.	Important	
7-7-5153	Network Operators, Service Providers 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.	Important	
7-7-5158	Network Operators, Service Providers and Equipment Suppliers should consider unannounced internal security audits at random intervals to enforce compliance with company security policies.	Important	
7-7-5163	Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider establishing procedures for video equipment and recording, where utilized (e.g., storage, accurate time/date stamping and regular operational performance checks).	Important	
7-7-5166	Equipment Suppliers should, wherever feasible, isolate R&D and software manufacturing of Network Elements from general office systems to prevent unauthorized access.	Important	

Physical Security Committee

Best Practice Number	Best Practice Description	Final Priority	Notes
7-7-5167	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.	Important	
7-6-5168	Equipment Suppliers should periodically review personnel background information and assess changes in personnel, departmental, or corporate environment as they affect the security posture of R&D and manufacturing areas and processes.	Important	
7-6-5169	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).	Important	
7-7-5175	Network Operators, Service Providers and Equipment Suppliers should establish a proprietary information protection policy to protect proprietary information in their possession belonging to the company, business partners and customers from inadvertent, improper or unlawful disclosure. The policy should establish procedures for the classification and marking of information; storage, handling, transfer and transmission of information as well as the destruction of information.	Important	
7-6-5185	Network Operators, Service Providers, Equipment Suppliers and Property Managers should ensure the inclusion of fire stair returns in their physical security designs. Further, they should ensure that there are no fire tower or stair re-entries into areas of critical infrastructure, where permitted by code.	Important	
7-7-5188	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 NRIC Best Practices and in coordination with the existing security programs for the building.	Important	
7-7-5192	Network Operators and Service Providers tenants of a telecom hotel should provide a current list of all persons authorized for access to the Property Manager, provide periodic updates to this list, and provide instructions for exceptions (e.g., emergency restoration personnel).	Important	
7-7-5216	Network Operators, Service Providers and Property Managers should consider providing secure pre-constructed exterior wall pathways for mobile generator connections or tap box connections.	Important	
7-7-5234	Network Operators, Service Providers and Property Managers should provide or arrange for security to protect temporary equipment placements and staging areas for critical infrastructure equipment in a disaster area.	Important	
7-6-5254	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.	Important	
7-6-5255	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.	Important	

Physical Security Committee

Best Practice Number	Best Practice Description	Final Priority	Notes
7-7-5256	Network Operators, Service Providers and Equipment Suppliers should monitor temporary connections of network test equipment that are established for restoration to prevent access by unauthorized personnel.	Important	
7-6-5265	Network Operators', Service Providers', Equipment Suppliers' and Property Managers' senior management should actively support compliance with established corporate security policies and procedures.	Important	
7-7-5269	Network Operators, Service Providers, Equipment Suppliers and Property Managers should incorporate various types of diversionary tactics into exercises to assess the security response.	Important	
7-7-5280	Network Operators, Service Providers and Equipment Suppliers should instruct security personnel to confirm the authenticity of directions to supersede existing security processes or procedures.	Important	
7-6-5179	Network Operators, Service Providers and Equipment Suppliers should establish policies and procedures that mitigate workplace violence.	Important	

ATTACHMENT 2 – NRSC MODIFIED & PROPOSED BEST PRACTICES

Network Reliability Steering Committee Modified & Proposed Best Practices			
Number	Modified ¹ or New ²	Wording	CSRIC WG 6 Recommendation (Approve/Reject)
7-P-0472	Modified	Network Operators and Equipment Suppliers should consider connector choices and color coding to prevent inappropriate combinations of RF cables.	Approve
7-P-0590	Modified	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.	Approve
7-P-0599	Modified	Crisis event simulation: Network Operators and Service Providers should conduct exercises periodically to test a network's operational readiness for various types of events (e.g., hurricane, flood, nuclear, biological, and chemical) , through planned, simulated exercises. The exercise should be as authentic as practical. Scripts should be prepared in advance and team members should play their roles as realistically as possible.	Approve
7-P-0674	Modified	Smart power systems: Network Operators, Service Providers and Property Managers should initiate or continue a modernization program to ensure that outdated power equipment is phased out of plant. They should consider the capabilities of smart controllers, local and remote monitoring and control, and alarm systems when updating their power equipment. Power monitors and smart controllers should be integrated into engineering and operational strategies.	Approve
7-P-0731	Modified	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 .	Approve
7-P-0755	Modified	Network Operators, Service Providers and Property Managers should document and communicate their installation and maintenance guidelines (e.g., MOP) and the expectation of compliance by all involved parties.	Approve
7-P-0782	New	Network Operators and Service Providers should detect DS3 simplex events and restore the duplex protective path expeditiously by executing appropriate incident response and escalation processes.	Approve
7-P-0783	New	Cable Management: Network Operators and Service Providers should consider including spare fiber connectors and their locations in asset	Reject

Formatted: Font: 10 pt, Bold

Formatted: Font: 10 pt, Bold

Formatted Table

Formatted: Font: 10 pt

¹ "Modified" means existing Network Reliability & Interoperability Council (NRIC) Best Practice that was modified by the NRSC

² "New" means a Best Practice created by the NRSC

ATTACHMENT 2 – NRSC MODIFIED & PROPOSED BEST PRACTICES

Network Reliability Steering Committee Modified & Proposed Best Practices			
Number	Modified ¹ or New ²	Wording	CSRIC WG 6 Recommendation (Approve/Reject)
		inventory systems.	
7-P-0784	New	Cable Management: Network Operators and Service Providers 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).	Approve
7-P-0785	New	Network Operation Center (NOC) Communications Remote Access: Network Operators and Service Providers should consider secured remote access to critical network management systems for network management personnel working from distributed locations (e.g., back-up facility, home) in the event of a situation where the NOC cannot be staffed (e.g., pandemic).	Approve
7-P-0786	New	Remote Access for Technical Support: Network Operators and Service Providers should consider allowing equipment suppliers or 3rd party service providers remote secured access to vital hardware components.	Approve
7-P-0787	New	Back-Up Power Fuel Supply: Network Operators, Service Providers, and Property Managers should consider the use of fixed alternate fuel generators (e.g., natural gas) connected to public utility supplies to reduce the strain on refueling.	Approve
7-P-0789	New	Travel Guidelines: Network Operators, Service Providers, and Equipment Suppliers should consider modifying travel guidelines/policies for use during a pandemic or other crisis situations.	Approve
7-P-0790	New	Personal Protective Equipment: Network Operators, Service Providers, and Equipment Suppliers should consider providing personal protective equipment barriers to infection (e.g., masks, disposable gloves, and sanitizers) in locations where multiple employees are located.	Approve
7-P-0791	New	Personal Protective Equipment Training: Network Operators, Service Providers, and Equipment Suppliers should consider providing personnel training in the use of personal protective equipment specific to a pandemic or other crisis situations and the employee's particular job.	Approve
7-P-0792	New	Attendance Guidelines: Network Operators, Service Providers, and Equipment Suppliers should consider modifying attendance guidelines during a pandemic, or other crisis situations.	Approve
7-P-0793	New	Telecommuting: Network Operators, Service Providers, and Equipment Suppliers should, as part of business continuity planning, identify employees that can perform their tasks from	Approve

Formatted: Font: 10 pt, Bold

Formatted: Font: 10 pt, Bold

Formatted: Font: 10 pt, Font color: Red

Formatted: Font: 10 pt

Formatted: Font: 10 pt, Bold, Font color: Red

Formatted: Font: 10 pt, Font color: Red

Formatted: Font: 10 pt, Bold

Formatted: Font: 10 pt

ATTACHMENT 2 – NRSC MODIFIED & PROPOSED BEST PRACTICES

Network Reliability Steering Committee Modified & Proposed Best Practices			
Number	Modified¹ or New²	Wording	CSRIC WG 6 Recommendation (Approve/Reject)
		<u>alternate locations and consider provisions for enabling them to do so.</u>	
7-P-0794	New	Telecommuting Infrastructure: <u>Network Operators, Service Providers, and Equipment Suppliers should plan for elevated utilization of remote access capabilities by employees during a pandemic, or other crisis situations.</u>	Approve
7-P-0795	New	Virtual Collaboration: <u>Network Operators, Service Providers, and Equipment Suppliers should plan for elevated utilization of virtual collaboration and remote meetings during pandemics or other crisis situations.</u>	Approve
7-P-0796	New	Deferral of Operations Activities: <u>Network Operators, Service Providers, and Equipment Suppliers should consider developing guidelines for the deferral of specific maintenance or provisioning activities during certain situations (e.g., pandemic, holiday, National Special Security Event).</u>	Approve
7-P-0797	New	Workforce Augmentation: <u>Network Operators, Service Providers, and Equipment Suppliers should consider creating a workforce augmentation plan prior to a pandemic or other crisis situation.</u>	Approve
7-P-0798	New	Transportation and Delivery Delay Contingencies: <u>Network Operators, Service Providers, and Equipment Suppliers should consider 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).</u>	Approve
7-P-0799	New	Cell Site & Remote Location Power Backup: <u>Service Providers, Network Operators and Property Managers should periodically evaluate the need for and feasibility of providing back up power at cell sites and remote locations taking into consideration the criticality of the site or location, as well as local zoning laws, statutes, and contractual obligations.</u>	Approve

Formatted: Font: 10 pt, Bold

Formatted: Font: 10 pt, Bold

Formatted: Font: 10 pt

ATTACHMENT 3 – EDUCATIONAL AWARENESS BENCHMARK SURVEY TABLES

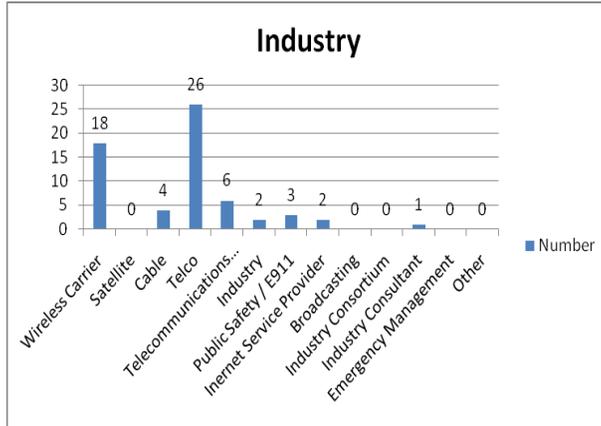


TABLE 1: INDUSTRY REPRESENTATION

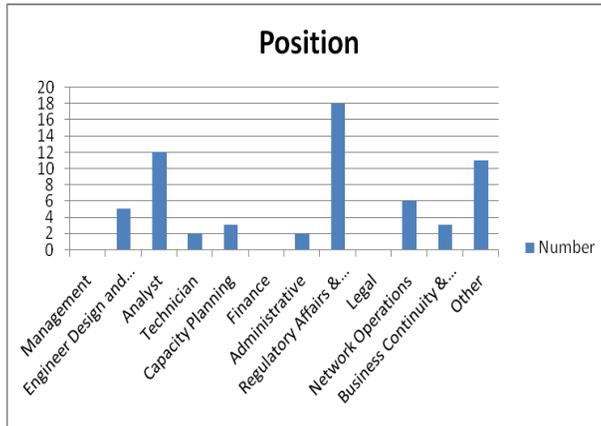


TABLE 2: REPORTING ORGANIZATION

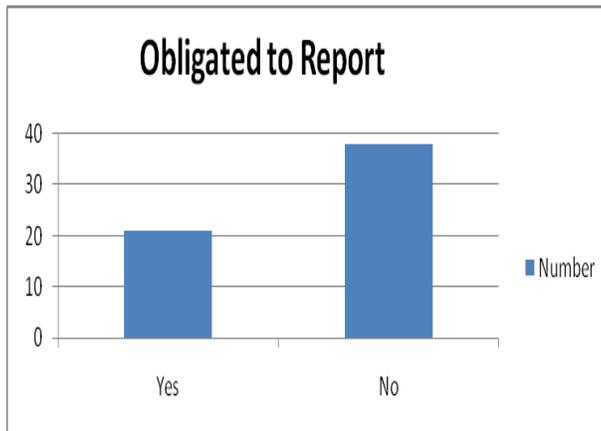


TABLE 3: FCC OUTAGE REPORTING OBLIGATION

ATTACHMENT 3 – EDUCATIONAL AWARENESS BENCHMARK SURVEY TABLES

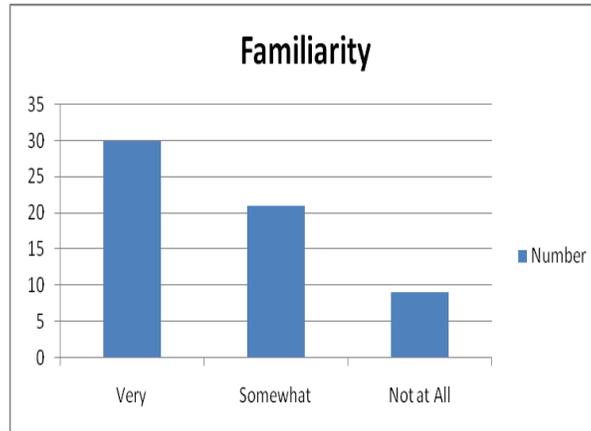


TABLE 4: FAMILIARITY WITH BEST PRACTICE WEBSITE(S)

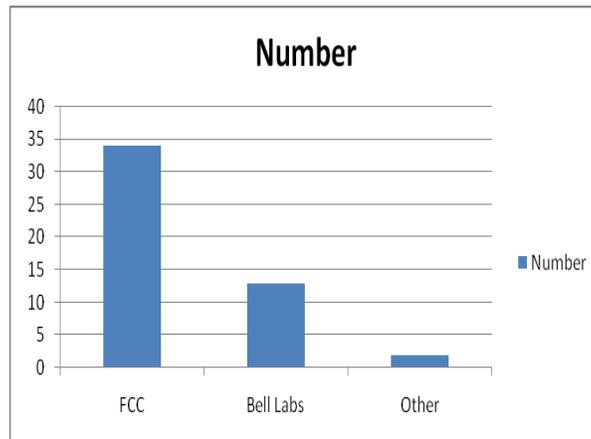


TABLE 5: BEST PRACTICE WEBSITE MOST FREQUENTLY VISITED

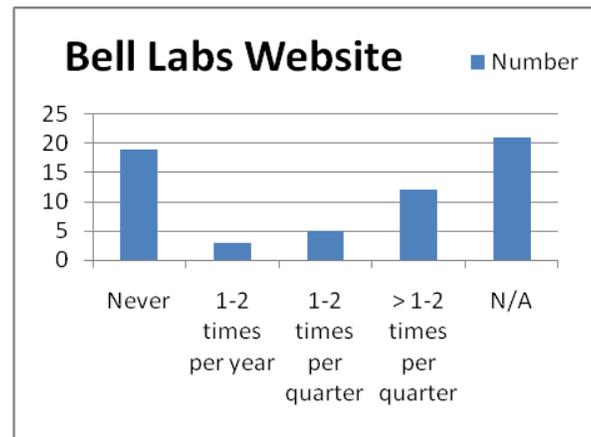


TABLE 6: BELL LABS WEBSITE - HOW OFTEN VISITED

ATTACHMENT 3 – EDUCATIONAL AWARENESS BENCHMARK SURVEY TABLES

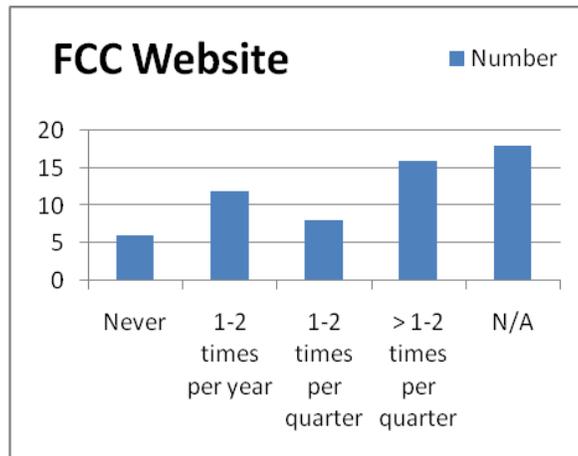


TABLE 7: FCC WEBSITE - HOW OFTEN VISITED

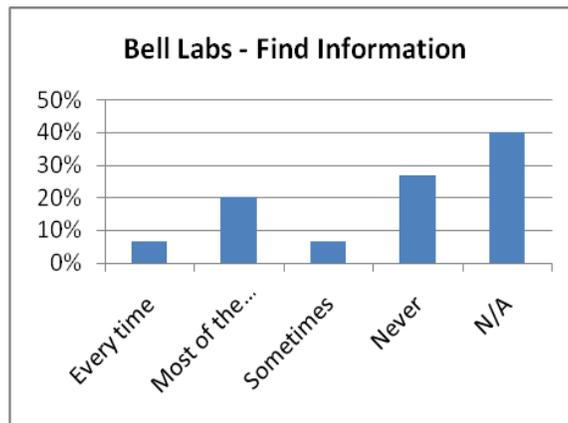


TABLE 8: BELL LABS WEBSITE - ABILITY TO FIND INFORMATION

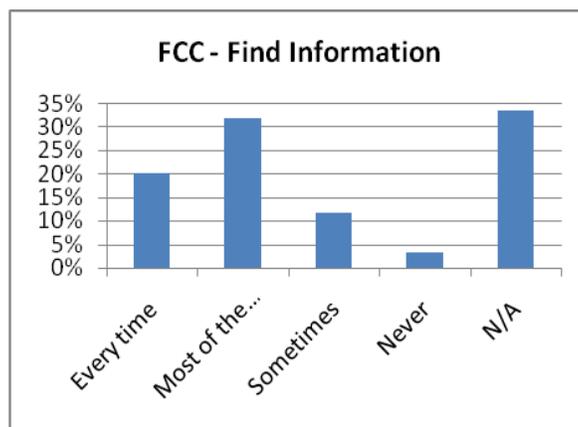


TABLE 9: FCC WEBSITE - ABILITY TO FIND INFORMATION

ATTACHMENT 3 – EDUCATIONAL AWARENESS BENCHMARK SURVEY TABLES

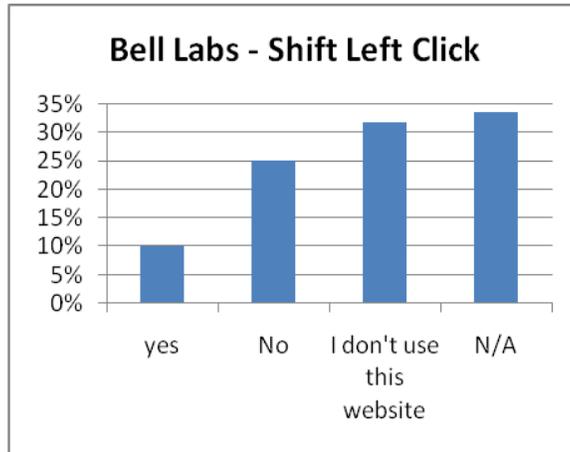


TABLE 10: BELL LABS WEBSITE - AWARENESS OF "SHIFT AND LEFT CLICK" FUNCTION

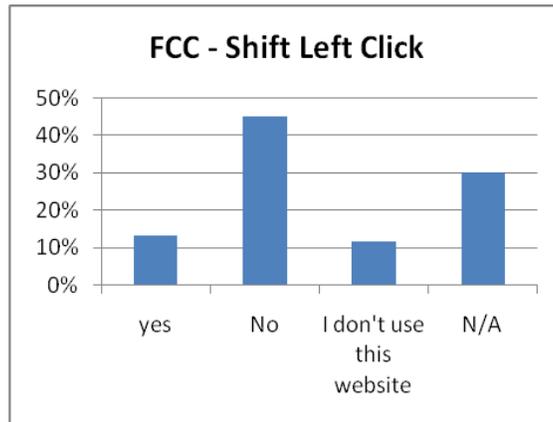


TABLE 11: FCC WEBSITE - AWARENESS OF "SHIFT AND LEFT CLICK" FUNCTION

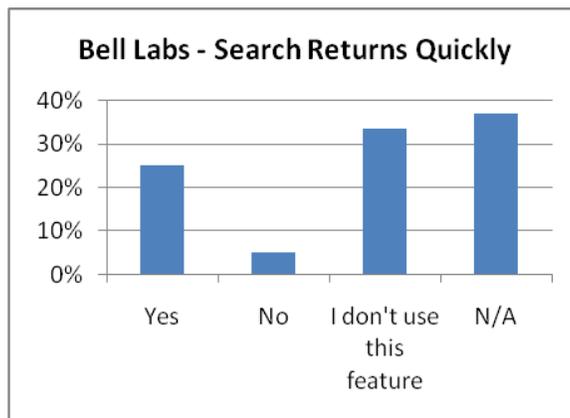


TABLE 12: BELL LABS WEBSITE - SEARCH FUNCTIONALITY RETURNS QUICKLY

ATTACHMENT 3 – EDUCATIONAL AWARENESS BENCHMARK SURVEY TABLES

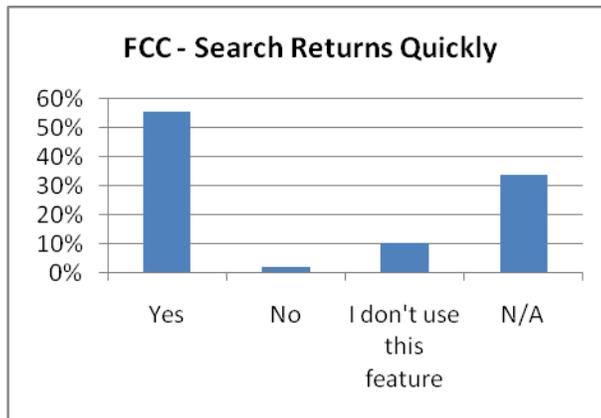


TABLE 13: FCC WEBSITE - SEARCH FUNCTIONALITY RETURNS QUICKLY

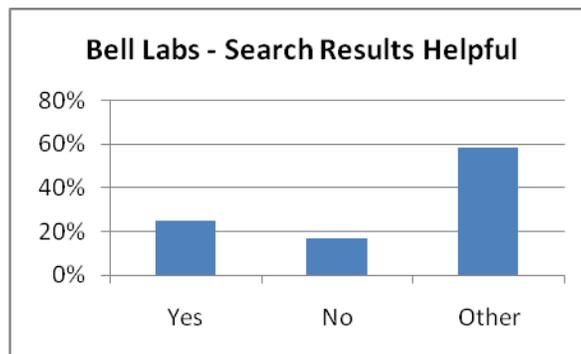


TABLE 14: BELL LABS WEBSITE - HELPFULNESS OF SEARCH FUNCTIONALITY

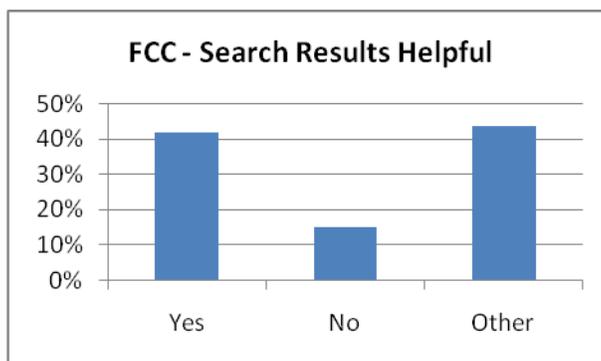


TABLE 15: FCC WEBSITE - HELPFULNESS OF SEARCH FUNCTIONALITY

ATTACHMENT 3 – EDUCATIONAL AWARENESS BENCHMARK SURVEY TABLES

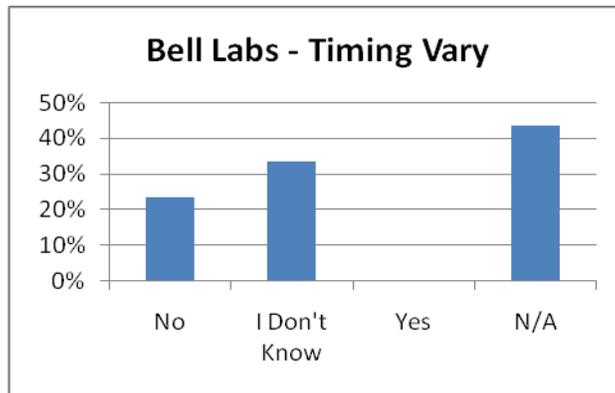


TABLE 16: BELL LABS WEBSITE – TIME VARIANCE FOR DATA RETREIVAL

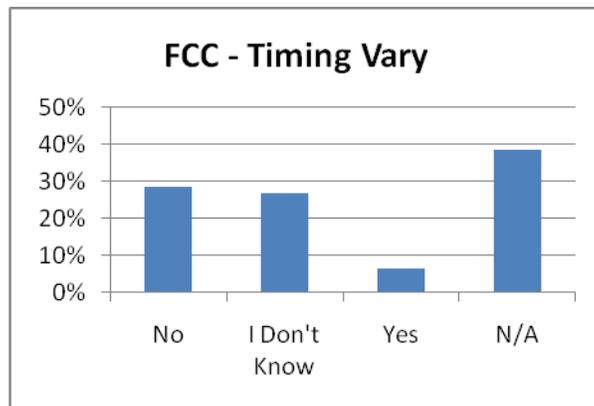


TABLE 17: FCC WEBSITE - TIME VARIANCE FOR DATA RETREIVAL

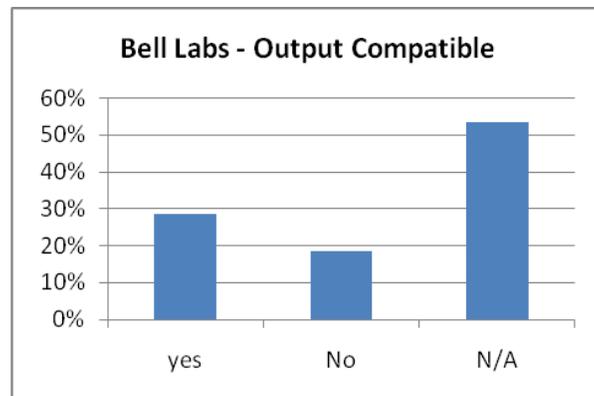


TABLE 18: BELL LABS WEBSITE - OUTPUT FILE COMPATIBILITY

ATTACHMENT 3 – EDUCATIONAL AWARENESS BENCHMARK SURVEY TABLES

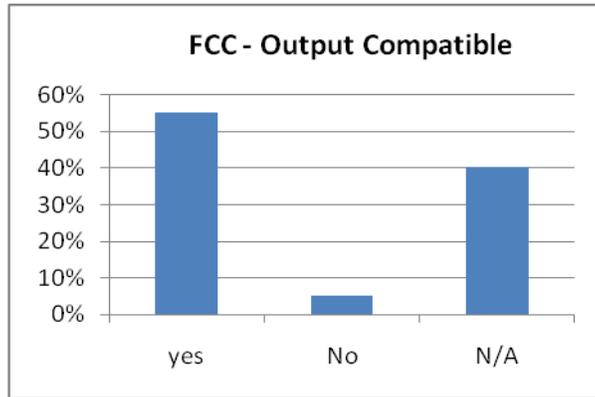


TABLE 19: FCC WEBSITE - OUTPUT FILE COMPATIBILITY