PSHSBulletin

A Publication of the Public Safety and Homeland Security Bureau

August 2011

CSRIC Recommendations Impacting Security and Reliability of Communications Technology

A new generation of technology has come of age, shaped by a generation who has grown up with personal computers, cell phones and the Internet. The Internet has benefited these consumers as the means to handle all of their personal affairs from banking to shopping, social networking, and scheduling appointments; however, cyber thieves are cashing in on consumers' growing reliance on the Internet and exploiting their personal information.

One of the remedies to minimize computer attacks is best practices recommended by Communications Security, Reliability and Interoperability Council (CSRIC). Best practices are methods that have consistently shown results, often superior to those achieved with other means, and that are used as a benchmark. Over the next two years, the Council will examine the next generation of technology issues – alerting, next generation 9-1-1 and network security.

CSRIC is the primary public-private forum for the development of best practices and other recommendations to the Commission in a number of areas regarding public safety. The Council was established at the direction of the Chairman of the Federal Communications Commission (FCC) in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App. 2.

Council members (see CSRIC Members on page 3) represent a balance of expertise and viewpoints from senior officials who have knowledge from legacy and broadband communications to Internet security. These experts will explore the usage of current and next generations of technology through its working groups (WGs). CSRIC is charted for two years from March 19, 2011 to March 18, 2013. Within those years, the Council will meet approximately each calendar quarter at FCC headquarters, and WGs will submit reports and recommendations. The working groups do the bulk of their work in between CSRIC meetings, mostly by conference call. Public Safety and Homeland Security Bureau staff will act as liaisons for each of the working groups.

As the next generation of Internet-savvy users shaped technology, dramatic events also influenced the use of technology software – most notably, the 9/11 terrorist attacks. People now want their mobile devices to warn them of immanent dangers and threats. Text messaging, instant messaging, and e-mail keep them in constant contact with friends, and they expect to be alerted during a disaster using the same technologies they have grown accustomed to in their social circles.

Alerting Issues

Next Generation Alerting

The CSRIC will explore the technical next generation alerting issues surrounding the following:

- Review alerting architectures: Integrated Public Alert and Warning System; the Personal Localized Alerting Network (PLAN); Authority to Citizen Alert.

- Examine different communications distribution platforms: Internet, Satellite, and DTV Datacast. These platforms have shared architectures and examine its usage for alert delivery.

- Explore social networking sites like Facebook, MySpace and MyYearbook. These sites have become tools to broadcast disaster information and send warnings.

Legacy Broadcast Alerting Issues

As the industry migrates from legacy broadcast alerting platforms to Common Alerting Protocol-based platforms, there is a need for common deployment plans and best practices to help ease the transition. The challenge is to keep the legacy application running while converting it to newer, more efficient code that makes use of new technology.

9-1-1 issues

NG 9-1-1

- Explore issues related to NG911 network architecture, particularly issues related to NENA's i3 standard.

- Develop recommendations on how carriers and PSAPs should handle the partial geographic deployment of IP-based NG911 systems.

E9-1-1 Location Accuracy

Outdoor Location Accuracy: Address questions referred to CSRIC in PS Docket No. 07-114, "Wireless E911 Location Accuracy Requirements, " and develop approaches to outdoor location accuracy testing criteria, procedures, and timeframes that are reasonable and cost-effective, considering alternatives to current OET Bulletin 71.

Indoor Location Accuracy: Transmission and reception can be fickle due to different types of indoor structures, e.g., the fraction of calls placed from concrete-and-steel vs. woodframe construction, or the displacement within the building (e.g., near windows vs. deep inside the structure).

Leveraging Commercial Location-Based Services:
Explore and make recommendations on methodologies for leveraging commercial location-based services for 9-1-1 location determination.

continued ▶

CSRIC Recommendations Impacting Security and Reliability of Communications Technology, cont'd.

Provide recommendations on the feasibility or appropriateness for the Commission to adopt operational benchmarks that will allow consumers to evaluate carriers' ability to provide accurate location information.

E9-1-1 Best Practices

Review the existing set of CSRIC 9-1-1 best practices and recommend ways to improve them, accounting for the passage of time, technology changes, and operational factors.

Network Security Issues

An entire industry – cyber security – has been created to develop online software protection, as well as public and private agencies having to revamp their policy to combat cyber theft. The next generation of cyber-savvy consumers expects technology to take its place in a world where the only constant is rapid change.

These expectations of new technology have made current users uniquely aware of its advantages. They use cyber-tools to make it easier for them to make new friends and connect with family, but they expect their network to protect their computer system from unwanted intrusions. The Council will examine network security issues and make recommendations to improve the following areas:

Network Security Best Practices

Issues to be examined include:

- Explore the usage of Domain Name System (DNS) and routing system of the Internet during the period leading up to the successful global implementation of DNSSEC (DNS Security Extensions) and Secure BGP (Border Gateway Protocol) extensions.

- Review the possible vulnerabilities within the interfacing of those areas and recommend best practices to better secure these critical functions of the Internet during the interval of time preceding deployment of more robust, secure protocol extensions.

DNSSEC Implementation Practices for ISPs

Issues to be examined include:

- Best practices for deploying and managing the DNSSEC by Internet service providers (ISPs).
- Proper metrics and measurements that allow for evaluation of the effectiveness of DNSSEC deployment by ISPs.
- Availability of a zone, verification of received data, and validation of verified data.
- Methods for the ISP community to deploy DNSSEC.

Secure BGP Deployment

The Border Gateway Protocol (BGP) controls inter-domain routing on the globally routable Internet. BGP relies on trust among operators of gateway routers to ensure the integrity of the Internet routing infrastructure. Over the years, this trust has been compromised on a number of occasions, revealing fundamental weaknesses to this critical Internet utility.

- Recommend the framework for an industry agreement regarding the adoption of secure routing procedures and protocols based on existing work in industry and research. The framework will include specific technical procedures and protocols. The framework will be proposed in a way suitable for opt-in by large Internet Service Providers (ISP) to create incentives for a wider scale ISP deployment of secure BGP protocols and practices in a market-driven, cost-effective manner.

Botnet Remediation

This working group will address the following:

- Review the efforts undertaken within the international community and among domestic stakeholder groups, such as the Australian Internet Industry Code of Practice [1], relevant Internet Engineering Task Force, Requests for Comments, and the work of the Messaging Anti-Abuse Working Group for applicability to U.S. ISPs.

- Propose a set of agreed-upon voluntary practices that would constitute the framework for an opt-in implementation model for ISPs. The Working Group will propose a method for ISPs to express their intent to op-into the framework proposed by the WG.

- Identify potential ISP implementation obstacles to the newly drafted ISP Botnet Remediation Business Practices and identify steps the FCC can take that may help overcome them.

- Identify performance metrics to evaluate the effectiveness of the ISP Botnet Remediation Business Practices at curbing the spread of botnet infections.

In summary, alerting, next generation 9-1-1 and network security have in common one element – to protect consumers. These issues, if left on their own, will exacerbate and increase in intensity as the telecommunications sector struggles to keep up with the ever growing threats posed by computer hackers and cyber criminals. The Council recognizes the potential consequences of these cyber issues and will bring together the right mix of public and private sector experts and thought leaders to holistically review the cybersecurity challenges faced by U.S. telecommunications consumers, and recommend solutions that will improve the security and reliability posture of the telecommunications sector.

[1] *See, for example, "Let the Market Drive Deployment: A Strategy for Transitioning to BGP Security," Gill, Schapira, Goldberg.*

continued ▶

CSRIC Recommendations Impacting Security and Reliability of Communications Technology, cont'd.

COMMUNICATIONS SECURITY, RELIABILITY & INTEROPERABILITY COUNCIL MEMBERS

CHAIR: Glen F. Post III, CenturyLink

MEMBERS:

- Dr. Edward Amoroso, AT&T
- Robert Azzi, Sprint Nextel Corp.
- Donna Bethea-Murphy, Iridium Satellite LLC
- Bill Buchholtz, Texas 9-1-1 Alliance
- Uma Chandrashekhar, Telecommunications Industry Association
- Lynn Claudy, National Association of Broadcasters
- Doug Davis, Hypercube Telecom, LLC
- Timothy Defoggi, Indian Health Service, U.S. Department of Health and Human Services
- Jack Doane, National Association of State Chief Information Officers
- Donna F. Dodson, National Institute of Standards and Technology
- Craig Donaldson, Intrado
- Dr. Brian K. Done, Office of Cybersecurity and Communications, U.S. Department of Homeland Security
- Dr. Stuart Elby, Verizon Communications
- Andy Ellis, Akamai Technologies
- Chris Fischer, North East King County (WA) Regional Public Safety Communication Agency
- Laurie Flaherty, National Highway Transportation Safety Administration, U.S. Department of Transportation
- Dr. Brian Fontes, National Emergency Number Association
- James Fowler, NYC Department of Information Technology and Telecommunications
- Barry Lee Greene, Internet Systems Consortium
- Brenton Greene, Telcordia Technologies
- Thomas Hanson, Charlottesville (VA) Regional Emergency Communications Center
- Hon. Maureen Harris, National Association of Regulatory Utility Commissioners
- Jennifer Hightower, Cox Communications
- Christian Hillabrant, T-Mobile USA
- Christopher Homer, DIRECTV
- Brett E. Jenkins, ION Media Networks
- Rodney Joffe, NeuStar, Inc.
- Brett Kilbourne, Utilities Telecommunications Council
- Elisa Kim, 9-1-1 for Kids
- Stephen Malphrus, Federal Reserve Board of Governors
- Danny McPherson, Verisign
- Susan Miller, Alliance for Telecommunications Industry Solutions
- Brian Oliger, WTOP Radio, Washington, D.C.
- Michael O'Reirdan, Messaging Anti-Abuse Working Group
- Alan Paller, The SANS Institute
- Damon Penn, Federal Emergency Management Agency, U.S. Department of Homeland Security
- Jacqueline Randall, State of Washington E911 Program Office
- Rod Rasmussen, Internet Identity
- José Luis Rodriguez, Hispanic Information and Telecommunications Network
- Robert Ross, CBS Broadcasting, Inc.
- William Sagel, Major County Sheriffs Association
- Stephen Schmidt, Amazon Web Services
- Richard Shockey, SIP Forum
- Bill Smith, PayPal
- Dr. Dorothy A. Spears-Dean, Virginia Information Technologies Agency
- Craig Spiezle, Online Trust Alliance
- Maurice Tosé, TeleCommunication Systems, Inc.
- Daniel A. Traynor, Tennessee Valley Authority
- Dr. Christian Vogler, Rehabilitation Engineering Research Center on Telecommunications Access
- John P. Wick, Jr., Syniverse Technologies
- Stephen J. Wisely, APCO International
- Karen Wong, California Technology Agency

STATEMENT FROM FCC CHAIRMAN JULIUS GENACHOWSKI ON RESPONSE AND RECOVERY EFFORTS POST-HURRICANE IRENE

August 28, 2011, Washington, D.C. – The FCC issues the following statement from FCC Chairman Julius Genachowski regarding the Commission's efforts following Hurricane Irene:

"I want to begin by offering my deepest condolences to those who lost loved ones as a result of Hurricane Irene. While we hope that the worst has passed, we continue to remain vigilant in our evaluation and response to the situation as it evolves. Working with FEMA, our other federal and statement partners, and communications service providers, we're focused on ensuring that people can communicate with each other and with first responders during this difficult time. Communications networks are of course essential for public safety and for the functioning of our economy.

"As Hurricane Irene gets downgraded to a tropical storm, the FCC continues to evaluate the damage from the areas affected in its aftermath. Based on reports to date, there have been some wireline and wireless outages. The good news, based on these initial reports, is that there hasn't been major damage to our communications infrastructure, except for damage along coastal regions hit hard by the storm.

"We are pleased that current reports indicate no 9-1-1 center is without service, and we have received no reports of public safety communications outages. Overall, broadcast and radio are largely unaffected, though in North Carolina a significant number of cable customers are out of service.

"The FCC remains on active watch around-the-clock to assess and respond to outages where necessary. We currently have four Roll Call teams deployed to conduct post event scans of the radio signal environment. I have also spoken directly to the CEOs of wireless, teclo and cable companies, and we are working to ensure continuation of service, and that service is restored quickly where needed.

"In the hours and days ahead, the hurricane's impact is not over. The FCC will remain vigilant as we address continued outages from flooding and commercial power outages. During this time we have activated our 24-7 response capabilities and have resources deployed in the field and monitor and respond, as appropriate, to outages.

"We also continue to work with our federal and state partners on key steps to ensure that our emergency communications systems meet the needs of Americans in the 21st century – including getting an interoperable mobile broadband public safety network funded and built; launching PLAN nationwide, a new mobile alerting system which would provide a "fast-track" for emergency alerts around network congestion; and accelerating the move to Next Gen 911 so that people can send text, video or photos to 9-1-1 in times of emergency.

"I want to thank Ret. Admiral Barnett and the staff of the Public Safety Bureau and throughout the FCC who have been working to anticipate, and now respond, to this hurricane. I've seen first-hand, including this morning at the FCC Ops Center, the dedication and commitment of FCC staff, and we owe them our thanks for their ongoing service."

FCC: TIPS FOR HOW TO COMMUNICATE DURING AN EMERGENCY

1) Limit non-emergency phone calls. This will minimize network congestion, free up "space" on the network for emergency communications and conserve battery power if you are using a wireless phone;

2) Keep all phone calls brief. If you need to use a phone, try to use it only to convey vital information to emergency personnel and/or family;

3) For non-emergency calls, try text messaging, also known as short messaging service (SMS) when using your wireless phone. In many cases text messages will go through when your call may not. It will also help free up more "space" for emergency communications on the telephone network;

4) If possible try a variety of communications services if you are unsuccessful in getting through with one. For example, if you are unsuccessful in getting through on your wireless phone, try a messaging capability like text messaging or email. Alternatively, try a landline phone if one is available. This will help spread the communications demand over multiple networks and should reduce overall congestion;

5) Wait 10 seconds before redialing a call. On many wireless handsets, to re-dial a number, you simply push "send" after you've ended a call to redial the previous number. If you do this too quickly, the data from the handset to the cell sites do not have enough time to clear before you've resent the same data. This contributes to a clogged network;

6) Have charged batteries and car-charger adapters available for backup power for your wireless phone;

7) Maintain a list of emergency phone numbers in your phone;

8) If in your vehicle, try to place calls while your vehicle is stationary; Have a family communications plan in place.

9) Designate someone out of the area as a central contact, and make certain all family members know who to contact if they become separated;

10) If you have Call Forwarding on your home number, forward your home number to your wireless number in the event of an evacuation. That way you will get incoming calls from your landline phone;

11) After the storm has passed, if you lose power in your home, try using your car to charge cell phones or listen to news alerts on the car radio. But be careful – don't try to reach your car if it is not safe to do so, and remain vigilant about carbon monoxide emissions from your car if it is a closed space, such as a garage.

12) Tune-in to broadcast and radio news for important news alerts.

13) If you have an emergency, call 9-1-1 immediately. But if it's not an emergency, use other options.

For More Information

More information on emergency communications during Hurricane Irene from the FCC can be found at www.fcc.gov. Residents can also find more information at www.ready.gov, http://www.redcross.org/en/irene

Upcoming Events

- September 1 - 30, 2011 - FCC Technology Demo, FCC Headquarters, Washington, DC
- September 8, 2011 - Network Reliability Workshop, FCC Headquarters, Washington, DC
- September 22, 2011 - Open Commission Meeting, FCC Headquarters, Washington, DC
- September 23, 2011 - CSRIC Meeting, FCC Headquarters, Washington, DC

For more information about the Public Safety and Homeland Security Bureau,
visit our webpage at http://www.fcc.gov/public-safety-homeland-security-bureau or email us at pshsbinfo@fcc.gov.

Questions or Comments? Email your questions or comments concerning the content of this bulletin to Kim Anderson (kim.anderson@fcc.gov).