Before the
Federal Communications Commission
Washington DC 20554

In the Matter of	)	
	)	
Recommendations of the Independent Panel	)	EB Docket No. 06-119
Reviewing the Impact of Hurricane Katrina on	)	
Communications Networks	)	

COMMENTS OF CISCO SYSTEMS, INC.

Mary L. Brown
Senior Telecommunications Policy Counsel
1300 Pennsylvania Ave. NW Suite 250
Washington, D.C. 20004
(202) 354-2923

Summary

In Cisco's view, policy makers and public safety officials alike should be attuned to the value that IP technologies bring to first responder and emergency communications. Failure to understand how standards-based IP technology can be utilized will result in policies that could incorrectly place to great a weight on proprietary solutions. The Commission should inform itself about new, more resilient and robust technologies that can be placed in the service of emergency response and disaster relief, and encourage network decision-makers to take advantage of those technologies where possible. Cisco's comments provide three examples: an IP-based E911 deployment in the state of Indiana, IP-based interoperability for first responders, and an IP-based Emergency Response Network that can be "parachuted in" to serve emergency personnel when existing network is non-operational. Cisco urges the Commission to continue to inform itself about how cutting-edge technology can be used to provide communications in emergencies, and to adopt policies that allow for, if not encourage, its use.

Second, proposals for a credentialing system for service provider employees are useful, but not sufficient. Cisco's experience in supporting our customers during the Katrina disaster demonstrates that vendors' and manufacturers' employees must be included in any credentialing process that would facilitate entry into affected areas post-disaster.

Table of Contents

I. Introduction and Background **1**

II. Discussion **3**

A. Champion Use of New IP-based Technologies Where Possible **3**

1. IN911 – E911 services in Indiana **4**

2. IP is solving the first responder interoperability problem **7**

3. Emergency Response Networks **12**

B. Credentialing proposal should be expanded to include vendor participation **14**

III. Conclusion **16**

Before the
Federal Communications Commission
Washington DC 20554

In the Matter of	)	
	)	
Recommendations of the Independent Panel	)	EB Docket No. 06-119
Reviewing the Impact of Hurricane Katrina on	)	
Communications Networks	)	

COMMENTS OF CISCO SYSTEMS, INC.

I. Introduction and Background

Cisco Systems, Inc. ("Cisco") hereby respectfully submits comments in response to the above-captioned Notice of Proposed Rule Making ("Notice").[1] Cisco is the worldwide leader in IP-based networking solutions for the Internet and is also a leading manufacturer of equipment for unlicensed wireless services.[2] Cisco equipment is widely used in emergency responder networks, and, over the past few years, Cisco has introduced products specifically targeted to the emergency responder community. Cisco employees and Cisco technology have been employed in all the world's recent disasters, from Hurricane Katrina to the Asian tsunami. We welcome the opportunity to comment on the excellent work of the Independent Panel and its recommendations to the Federal Communications Commission for improving how communications networks perform in major disasters.

---

[1] *Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks*, EB Docket No. 06-119, Notice of Proposed Rulemaking, released June 19, 2006 (hereinafter "Notice").

[2] As a legal matter, the use of the bands that do not require individual authorization is licensed by rule, rather then unlicensed. However, for sake of convention we will use the term "unlicensed" in this comment.

In Cisco's view, the report completed by the Independent Panel, and now the work to be done by the Commission itself in evaluating the Panel's recommendations, is extremely valuable. The Independent Panel's report contains strong proposals that will be helpful in future emergencies. As the expert communications agency within our system of national government, the Commission can and should extend the work it has already done in the area of network reliability by assisting networks in getting ready for natural or man-made disasters that disable existing networks, assisting in recovery, helping to ensure the flow of emergency communications to and between first responders, as well as in fostering emergency alert systems to alert the public to important information about the disaster.

Cisco's comments focus on two topics that did not appear in the Independent Panel's report that deserve greater emphasis as the Commission considers its role in future emergencies: (1) the flexibility and resiliency of IP-based technology and networks; and (2) inclusion of manufacturer and vendor employees in emergency credentialing.

First, IP technologies have already proved to be the most resilient in disasters. Simply put, IP networks demonstrate better survivability, and, when existing networks are rendered unusable, IP networks can more readily be built to provide critical replacement service. Cisco's comments provide three examples: an IP-based E911 deployment in the state of Indiana, IP-based interoperability for first responders, and an IP-based Emergency Response Network that can be "parachuted in" to serve emergency personnel when existing network is non-operational. Cisco urges the Commission to continue to inform itself about how cutting-edge technology can be used to provide

communications in emergencies, and to adopt policies that allow for, if not encourage, its use.

Second, proposals for a credentialing system for service provider employees are useful, but not sufficient. Cisco's experience in supporting our customers during the Katrina disaster demonstrates that vendors' and manufacturers' employees must be included in any credentialing process that would facilitate entry into affected areas post-disaster.

II. Discussion

A. Champion Use of New IP-based Technologies Where Possible

The Commission's activities in the area of network reliability have correctly focused on the service providers and the availability and reliability of existing communications networks. The Independent Panel report extends that concept by asking a series of questions about pre-positioning equipment that would assist service providers in the event of outages, as well as questions about pro-actively establishing a "Readiness Checklist" for networks to include business continuity plans and training. These are laudable ideas. However, the Commission should not stop there. It should inform itself about new, more resilient and robust technologies that can be placed in the service of emergency response and disaster relief, and encourage network decision-makers to take advantage of those technologies where possible. The Commission should also encourage policy-makers throughout the federal government to ensure that federal policies do not inhibit the use of new technologies.

There are three examples of IP-based technologies that we highlight for the Commission's attention. The first is a re-design of the State of Indiana's E911 system, which has been transformed to an IP-based system that will enable statewide transferability of 911 calls and ensures back up and redundancy even if a portion of the network becomes unavailable. The second example is a multi-jurisdictional deployment of Cisco's IP-based interoperability technology. Finally, we discuss a new managed service jointly developed by Cisco and IBM that enables a customer, public or private, to immediately deploy a wireless network when its communications network is rendered inoperable.

1. IN911 – E911 services in Indiana

The Notice summarizes the key recommendations that the Independent Panel made with respect to 911, E911 and Public Safety Access Points. Among the Panel's ideas are to create diverse interoffice transport for 911 circuits, employ dual selective routers, and establish back-up PSAPs. These recommendations align well with existing 911, E911 and PSAP network architectures, in which service providers must trunk 911 traffic to selective routers managed by wireline providers. What the Independent Panel's report fails to do, however, is to discuss alternative network architectures for delivering 911 and E911 services. This section discusses one prominent example from the State of Indiana.

The State of Indiana is midstream in embarking on a new model for 911 and E911. When complete, Indiana will have a state-of-the-art, managed IP-based system that will provide better functionality to PSAPs in terms of call set up time and information about

the calls, better performance for anyone seeking to reach 911 assistance in Indiana, and will cost Indiana taxpayers less money.

Indiana began this process with a conventional service provider network architecture, and a focus on the high cost of connecting wireless carriers to that architecture for wireless E911 services. In sum, each wireless carrier operating in the state needed to trunk to each selective router. That trunking cost was contributing to high end user fees. A state-appointed oversight board, run by Indiana Treasurer Tim Berry, decided to ask industry if there was a better way to deploy E911. The board ultimately accepted a proposal from INdigital Telecom, a consortium of rural and competitive local exchange carriers operating in Indiana, to revamp Indiana's entire 911 infrastructure in two phases. (Cisco Systems is a vendor to INdigital on this project.)

In the first phase, known as "Project Crossroads," INdigital added two new selective routers to the state, and used those routers to aggregate 911/E911 traffic from the state's wireless carriers. Wireless carriers were no longer required to connect to each local exchange carrier selective router. Instead, wireless carriers trunked E911 traffic to INdigital, which aggregated wireless traffic and ran redundant trunks from its two selective routers to local exchange carrier facilities. With fewer trunks to run, statewide costs to support E911 dropped. In addition, this phase of the project allowed for SS7 signaling between the wireless carriers and INdigital, and allowed for centralized accounting and trouble reporting. This phase of the Indiana transformation is largely complete.

Next, Indiana will turn to the next phase of the project, dubbed "IN911", which will transform the transport between INdigital's selective routers to an IP-based transport

network that rides self-healing SONET rings throughout the state. INdigital, in its project description for this phase of the project, notes that:

> "Inherent characteristics of the Internet Protocol (IP) permit the design of mesh networks that are highly reliable and survivable. The design of the Internet Protocol itself was motivated in part by mathematical studies of command and control requirements and solutions for the battlefield, among other considerations….
>
> "IP networks can economically be built in a mesh topology with multiple interconnection points rather than in the hub and spoke models common to local telephone industry practice today. Failure or damage to a transport link in the mesh does not render the remaining elements of the mesh inoperable. In fact, the network can sustain multiple failures, often with minimal impact. Failures in a well-designed mesh network with automatic reroute capability typically cause reductions in available bandwidth, rather than complete loss of connectivity."[3]

In addition to providing improved network resiliency, the benefits of the IP911 phase of the project are many, but include statewide 911 call transferability, dynamic bandwidth allocation in support of voice, and use of the network to transport data traffic when bandwidth is not required for E911 calls, and close monitoring and trouble resolution of the E911 network itself. Cost savings generated from the IP-based approach can be re-directed toward improving PSAP networks. It is noteworthy that, in Indiana's system, PSAPs are not being required to convert to IP in the PSAP operation itself,

---

3 An Improved Wireless E9-1-1 Voice and Data Delivery Network, INdigital Telecom, Project Description. Further information project, including an online version of the project description, can be found at https://www.in911.net

although the all-IP transmission network will lay a foundation for improved E911 functionality should the PSAP choose to become IP-based. Among the future improvements being considered by INdigital and the State of Indiana are a standardized visual tool that would map the caller's location for the PSAP and permit interoperability with other emergency services, such as OnStar's subscription service.

Indiana's solution to improving E911 delivery, at a lower cost, depends upon the use of new IP-based technologies. As Indiana has discovered, IP is more flexible and resilient than older the telecommunications network topologies and technologies. The Commission should actively encourage reform efforts like the one in Indiana that will lay the groundwork not just for a more resilient network, but improved E911 service.

2. IP is solving the first responder interoperability problem

The FCC Notice seeks comment on what it should do to advance interoperability, such as ensuring the expeditious transformation of the 700 MHz band from broadcast television use to its new purpose in support of public safety and commercial wireless broadband technology.[4] Ensuring that the digital television transition remains on track is extremely important to enabling key public safety spectrum to become available in support of the new "Project 25" standards-based radios. Cisco was disappointed, however, that none of the Independent Panel's recommendations for public safety interoperability included any reference to IP-based interoperability solutions.[5] Our public policy message to the FCC, and all federal policy-makers, is this: whenever you are thinking about the public safety interoperability problem and solutions to it, you should

[4] Notice at 6.

[5] Independent Panel Report at 38-39.

be considering all technologies that address interoperability, such as IP-based interoperability, and not restrict your field of view to the radio-based solutions that have been the subject of historical discussion. Interoperability policy must be technology neutral.

Last fall, Cisco announced an IP-based interoperability solution that solved the most immediate problem facing first responders – each agency, even within a single jurisdiction, relied on incompatible proprietary radio networks that operate on different frequencies. Cisco's solution uses the power of IP to allow any-to-any voice interoperability, including existing public safety radio technologies. In sum, first responder agencies can use existing radio systems to interoperate today with any other agency when using this IP-based system.

IP-based interoperability of the type that Cisco operates is not a "gateway" solution. "Gateways" are simply devices that perform the basic function of transferring a communications flow into IP. Gateways have been available in the market for a number of years, and have facilitated the migration of emergency call centers to IP-based platforms. But this should not be confused with the robust interoperability product that Cisco offers in the marketplace today. While the Cisco solution – IP Interoperability and Collaboration System (IPICS)– uses gateways to transform radio-originated voice into IP that is only the beginning of a much more comprehensive solution to enable interoperability. IPICS includes both a server and other software to enable emergency managers to create talk groups to address emergency conditions. Among the key benefits of the system:

- Traffic is "mixed" from different radio networks at the network edge – traffic does not have to be transported to an emergency command center, creating a single point of failure.
- The command center can choose to add any voice connection to the talk group – from the mayor on his/her cellphone to the police chief on his/her VoIP phone. IPICS software allows these types of devices, even including laptops, to be used as "push-to-talk" devices when communicating via IPICS. In this way, a user can be connected to the talk group from anywhere in the world.
- The system is secure and utilizes the first responder's network, not the public Internet.
- The system does not consume additional radio resources, as repeater-type technologies do.
- The system is easily scalable, and in its basic configuration, allows multiple incidents to be managed simultaneously. The system can also be partitioned, so that multiple agencies can administer their own interoperability tool.
- Incident commanders can give permission for participants to talk, or require participants engage in listen-only mode.
- Audit trails on each activity are created.
- The system has built-in intelligence to allow the formation of pre-specified talk groups in response to certain types of incidents, or allows emergency command centers to form talk groups on the fly, as circumstances permit.

Cisco is already adding new capabilities to IPICS. Graphic user interfaces on the command screen, such as maps that show geographic location of radio resources, integration of sensor technology, other data, and fully interoperable video, are all part of the evolution of this technology.

Arguably, the most important feature of IPICS, however, is what it does not do – it does not require users to purchase new radio systems. Existing radio systems can continue to be used as long as there is useful life in them. That means interoperability can be provisioned today, with existing radio systems. And as new radio systems are deployed, those can be added to IPICS as well. Significantly, IP-based solutions like IPICS are inexpensive relative to the cost of new radio networks.

Finally, in comparing current and future interoperability functionality of IP-based systems, like IPICS, to radio-based interoperability, radio-based interoperability in one important sense delivers less. A radio-based solution will only allow communication between those with interoperable radios. Other than first responders, it is unlikely that other organizations (such as the National Guard or military units) will have the same radio technology equipped to work on the 700 MHz bands as public safety. And even in the case of first responders, it will take years (current Department of Homeland Security estimates are on the order of 20 years) to equip first responders with 700 MHz radios, even assuming money can be found to do so. While Cisco strongly believes in, and supports, standards-based first responder radio systems, Cisco more fundamentally believes that an IP-based interoperability solution is the preferred foundation for robust interoperability for voice, data and video in the 21st century.

Recently, the Cisco solution has been part of a multi-jurisdictional test of IP-based interoperability in Danville, Virginia, located on the border with North Carolina. Prior to the start of this project, no interoperability capabilities existed between public safety entities, local and state jurisdictions, and entities on either side of the Virginia and North Carolina state lines. The following is an excerpt of a summary of the project prepared by local officials for Virginia state interoperability review:[6]

> In the fall of 2005, Cisco Systems, Inc. and the City of Danville began discussing the possibility of testing a product that addressed the problem of radio interoperability. Cisco Systems had developed an integrated radio solution, which had been tested within smaller single agency venues. Looking for a multi-agency environment for expanded testing, Cisco entered into an agreement with the City of Danville to test their product in

[6] City of Danville, submission to the Virginia State Interoperability Executive Council.

a multi-jurisdictional pilot project that would address radio interoperability via an IP network.

The tentative project name is the "Piedmont Regional Voice over IP Pilot Project." The project involves a collaborative effort between Cisco Systems, Inc., Sprint/Nextel, National Institute of Justice, CommTech Program, and a multi-agency consortium that includes the City of Danville, VA; Pittsylvania County, VA; Caswell County, N.C.; the Virginia State Police; and the North Carolina State Highway Patrol. Virginia Tech University is a non-participant observer assessing the project to study the future applicability of the technology.

The proposed system is designed to provide connectivity between disparate communication systems where none previously existed. The system does not extend existing networks, but simply allows on-demand connectivity between available resources during emergency or routine situations. The initial system deployment will provide unified voice interoperability using any voice enabled device, but subsequent versions will include data and video integration.

The implementation schedule has been defined in a three-phase approached. Phase I seeks to address the issue of operability within the City of Danville. Participants include public safety (police, fire, and EMS) and the Emergency Operations Center (EOC). Also included are the departments of utilities (water, gas, & electric) and public works. Phase II will initially incorporates the law enforcement and emergency services entities from the Counties of Pittsylvania, VA and Caswell, N.C. Phase III will expand the project to incorporate the two adjoining state police agencies; the Virginia State Police and the North Carolina State Highway Patrol….

Goals:

1. *Plan with Information Sharing – Voice, Video, Data and Radio*
2. *Connecting PSAP's*
3. *Clear migration plan*
4. *Strong governance*
5. *Remote Dispatch Monitoring*
6. *Investment protection*
7. *Off the shelf technology*
8. *More effective service to the public through direct communication*
9. *Equality in resource command and control*
10. *Reduced delay and distortion of information*
11. *More timely and accurate transfer of information*
12. *Partnerships…with regional and state agencies, Industry partners*
13. *Economic Development*
14. *Business Continuity*

> For the first time ever, we are utilizing IP protocols to communicate via radio to cell phones and PC devises. We have the capacity to remotely monitor emergency communication traffic…from anywhere in the world where an IP connection exists.

More information on this project will be available later this year, as participants continue to assess both the technology and the governance issues presented by a comprehensive interoperability platform.

IP interoperability solutions are a reality. While the Commission should be actively supporting the transition to new 700 MHz radio systems, through its administration of the digital television transition, it should not ignore the powerful new IP-based tools available to first responders now, and the role in which these systems will play even as 700 MHz radio systems become available. The Commission has an important policy voice in Washington, and can help educate others about how IP-based technologies can perform to solve problems that were previously defined as "spectrum"-based.

3. Emergency Response Networks

A significant part of the Independent Panel's work focused on what to do when entire networks became unavailable as a result of the damage done by Hurricane Katrina. The Panel recommended that the FCC pro-actively work with industry to pre-position equipment, to develop plans for future events of similar magnitude, and to conduct training exercises in an effort to get networks functioning again. These are useful ideas that warrant serious consideration by the FCC and industry. Pre-positioning equipment could be beneficial, provided the intellectual and human capital remains in the area post-disaster, and provided the equipment is sufficiently out of harm's way (geographically

removed or in a hardened site) in order to survive the disaster. Should the Commission adopt the Panel's suggestions, the Commission should also be aware of a capabilities being developed within the technology sector to instantly create networks where there none have survived, especially in circumstances where the provider has lost access to its own network personnel.

IBM and Cisco are partnering in one such effort to produce a scalable managed service, known as "Emergency Response Networks," that provides public or private customers with a replacement network to serve in times of emergency. At present, the wireless technology in use consists of unlicensed WiMax point-to-point links, unlicensed 802.11 Outdoor Access Points and/or mesh architecture, and satellite backhaul acquired from a service provider or other source. In the IBM/Cisco model, the current replacement network has the capability, depending on local topology, to reach a maximum of 350 square miles, and to serve 250 users.[7] Networks with less geographic reach, and supporting fewer users, are also available. Users will communicate using 802.11 compatible devices, such as 802.11 phones or laptops, as well as VoIP phones wired to the system located at the installation. Because this is a managed service, IBM and Cisco will over time be introducing new technology in support of the capability that the user has purchased, and we expect the set of capabilities that we offer will adjust over time in response to user demand.

The equipment that supports these emergency networks is contained in vehicles, and the support for the networks, vehicles, and the personnel to initiate them is entirely self-contained. For example, technicians running the networks are equipped with

[7] Capacity is a function of scalable IP equipment on board the mobile units, and can be expanded.

everything they need for the duration of the emergency and do not require further assistance (e.g., fuel, food, water) from local, state or federal authorities. And, because the system includes IPICS at the core, as other networks come on line, they can be interoperated with the Emergency Response Network. For first responders and emergency relief agencies, as well as critical infrastructure businesses, this enables continuous command and control in the immediate aftermath of a disaster, until the entity's usual network is back on line.

Cisco offers these examples of how IP technologies are transforming public safety and emergency response because it is important for the Commission to understand, as it embarks upon a more aggressive role in this arena, that IP-based technology has the capability to improve emergency response and disaster relief. The Commission should consider whether the policies it is promoting and the work it is doing are including and encouraging these new technology solutions to be deployed.

B. Credentialing proposal should be expanded to include vendor participation

The Notice discusses the Independent Panel's recommendation that the Commission encourage the development of credentialing requirements and procedures to facilitate network repairs.[8] The Panel recommends that the Commission take whatever actions are open to it to enable the designation of service provider employees and contract employees as "emergency responders" under the Stafford Act.

Cisco agrees that such steps would help ensure that key workers could access communications networks quickly in times of emergency. However, the proposal does

[8] Notice at 5.

not go far enough. Manufacturers, system integrators and other vendors also have key workers who need to be deployed to geographic areas hit by emergencies, and these workers need to be eligible for the credentialing process as well. In Hurricane Katrina, Cisco deployed hundreds of workers in the hardest-hit portions of the Gulf region in support of service provider customers, critical infrastructure customers, and non-governmental organizations assisting with disaster relief. A partial list of the in-region Cisco activities during Katrina would include the following:

- When Mississippi National Guard troops were relocated to Camp Shelby, Cisco provided equipment and technical expertise to secure their temporary network and established communications with the National Guard Bureau in D.C.
- For the Texas National Guard, Cisco established communications for deployed troops in New Orleans, Houston Astrodome and Camp Beauregard, LA.
- Provided IP phones and other technology in support of a voice network for South Carolina National Guard troops deployed in New Orleans.
- Supplied routers to the California National Guard in support of troops deployed in New Orleans. In addition, the California Guard has a tactical communication vehicle that is outfitted with a satellite link, a Cisco 3825 router and Cisco IP Communications. The Guard uses the satellite link, Cisco VPN and IP Communications to register the IP Phones with their Sacramento-based Call Manager to get communication and dial tone in California.
- Responded to numerous requests from state and local governments to rebuild networks, deploy communications systems and establish call centers.
- When the Louisiana Department of Public Safety lost voice communication, used Cisco IP technology at the Department's location in Baton Rouge to establish VoIP communications using a working data circuit. Installed IP phones in New Orleans, Houma, Convington, and Baton Rouge State Trooper offices, Jefferson Parish Sheriff Office.
- Re-established voice service for the City of New Orleans at City Hall using both wireless and wired IP phones.
- Installed routers, switches, and a firewall to allow administrators of the Louisiana State University Health Sciences Center to connect from their temporary offices in Shreveport and Baton Rouge with the hospital in New Orleans.
- Expanded the capacity and assisted in supporting the call center operations (staffing and technical support) for the Louisiana Office of Telecommunications Management, which maintains the Louisiana Wide Area Network, a network service that provides state agencies with hardware, software, and support.
- Deployed mobile communications kits to the American Red Cross, the South Carolina National Guard, Unisys Group (on behalf of the City of New Orleans),

Mississippi State Highway Patrol, and to Perlington, Mississippi at the Charles B. Murphy Elementary School and Library. The school served as the only point of distribution for relief services in the area. Perlington is a rural community close to the Gulf of Mexico in southern Hanover County and was one of the hardest hit communities in Mississippi.

Cisco is not alone among vendors, manufacturers, and systems integrators in supporting customers in emergency situations. Employees from the technology sector were critical to restoring key communications to enable the restoration of order and the delivery of relief services. Cisco employees supported service provider customers, governmental agencies, critical infrastructure customers, and non-governmental organizations throughout the crisis. Should the Commission proceed with the proposal before it to cause certain communications workers to be included as emergency responders under the Stafford Act, or take action to allow these workers to be credentialed, workers in the technology sector must also be eligible for such designation and/or credentials.

III. Conclusion

Cisco commends the Commission for initiating a thorough review of the industry's response to the Hurricane Katrina disaster, and for asking the right questions about how the Commission itself could facilitate restoration of communications networks in future disasters. In the Commission activity that will flow from this important docket, it is Cisco's hope that the Commission will seek out and learn about ways in which IP-based technology can be leveraged in support of 911, interoperability, emergency networks, and disaster recovery. These are important new tools that we believe will prove to be invaluable to government and private industry in the future. In addition, it is important for the Commission to recognize the critical role that vendors, manufacturers

and systems integrators play in disaster relief, and to include those workers in any "emergency responder" designation and/or credentialing program.

Respectfully submitted,

CISCO SYSTEMS, INC.

Mary L. Brown
Senior Telecommunications Policy Counsel
1300 Pennsylvania Ave. NW Suite 250
Washington, D.C. 20004
(202) 354-2923

August 7, 2006