COMMERCIALIZATION OFFICE - PILOT OPERATIONAL REQUIREMENTS DOCUMENT

National Emergency Response Interoperability Framework and Resilient Communication System of Systems

February 2009

Point of Contact:

Mark Protacio
DHS S&T Commercialization Office
SETA Support
Mark.Protacio@associates.dhs.gov

Contents

1. General Description of Operational Capability for a National Emergency Response Interoperability Framework and Resilient Communication System of Systems

1.1. Capability Gap

Interoperability and compatibility of First Responder communication systems is a mandate of the National Incident Management System (NIMS). However, as of 2009, the only interoperability systems widely in use are expensive and complicated proprietary voice-over-radio systems. These aptly described “patchwork” interoperability systems are unable to scale without additional, costly equipment coupled with costly on-site support provided by highly trained technicians. This current mode of operations is not feasible in the critical first minutes and hours of an incident response.

The vast majority of emergency responders are limited in their ability to communicate and collaborate with each other. They are unable to communicate with command, support teams and other responding organizations present at an incident scene. In 2008, almost 7 years after the tragic lessons learned by 9/11, the majority of emergency response organizations (ERO) do not have the basic capability for any of their team members to establish communications at an incident site. They may have to wait hours for large trucks and/or trailers with very expensive[1] and complicated communications equipment delivered to the site. In the case of a catastrophic incident causing a scorched earth[2] environment, it may take days to get the necessary equipment and communication support personnel to the incident site.

It is not only the complexity and cost of existing systems that inhibit NIMS compliance; most systems often render previous technology investments obsolete or require a need for costly upgrades to legacy systems proving impractical or unaffordable. A system is required that creates a communications framework enabling the ability to allow not only interoperability of disparate systems, but also the ability to interconnect legacy systems and new systems.

Another major capability gap exists in providing an affordable solution for the interoperability and interconnection of communication systems that support IPv4 routing with those systems that answer the Department of Defense mandate for IPv6 compliance. The cost of phasing out an IPv4 system (which is prevalent in the vast majority of state and local ERO’s, Non-Government Organizations and private sector security) is not realistic from a budgetary feasibility prospective and would take years to accomplish.

Yet, closing this gap is mandatory. The NIMS mandate for interoperability is unattainable without a cost-effective, easy-to-implement system that provides a framework for the interoperability of data and video between responders and EROs. Data is as critical as voice communications within an incident site. If noise levels inhibit voice communications or silent communications are necessary, instant messaging is an effective tool. Video from an inexpensive webcam on a first responder’s laptop may make a critical difference by providing a visual assessment to the ERO. Maps and other files needed at the incident site must get to the response team without the need to deliver files physically via courier, currently the most widely-used solution[3].

Existing interoperable voice, data and video communications require fixed private networks or access to the Internet via a virtual private network (VPN) requiring authentication servers and server-based network management systems. This requirement for access to remote servers creates an insurmountable capability gap for interoperable communications among responders in the hours or days they must wait for communications trucks and/or trailers to arrive at the incident

scene. This operational requirement document (ORD) requires a system that provides peer-to-peer interoperability between responders and EROs without the requirement for remote servers or dedicated networks. The requirement is for secure peer-to-peer communication between any responder using any type of voice, video or data communication device and any other responder or ERO without requiring the receiving communication to be of similar device type or dedicated network. Responders at an incident site must be able to establish incident area peer-to-peer communications within minutes of responding and interoperate with EROs both at the incident site and/or remotely across readily available disparate communications networks without the need for third-party services or servers.

Even more problematic is the fact that most EROs still depend on vulnerable radio or cellular infrastructure to support expensive communication and command vehicles. Network failures caused by destruction of critical infrastructure, such as radio towers, landlines and network control centers represent a major challenge for both the public and private sectors. If they do have systems, the majority is not portable enough for easy transport to the incident scene by a first responder; or is so complicated, extensive training is required to operate the system. Very few EROs currently have portable systems whose capabilities allow a responder to establish interoperable voice, data and video communications at the incident site without technical support in ten to twenty minutes. All EROs require this capability.

The aftermath of the 2004-2005 hurricane season, which resulted in catastrophic damage across the Gulf States, is the ultimate example of not possessing the capability in discussion. Vast areas realized devastating damage to their communications infrastructure. There was no communications resiliency. The available response recovery solutions were inadequate or failed altogether, leaving many areas where lives were at risk without communications for days.

Many critical infrastructure facilities of importance to the security of the region did not have effective communications for weeks.[4] Belle Chase Naval Air Station, critical for the staging of over 30,000-rescue operations south of New Orleans, did not have reliable voice communications for nearly 96 hours after the landfall of Hurricane Katrina. With a system that meets the requirements of this ORD, the Coast Guard Rescue Operations in New Orleans would have had telephone capability and data communications within 10 to 20 minutes of beginning the emergency response. This communication could have been established by anyone at the staging area regardless of whether they had training in deploying communication networks or not.

Almost all communication systems in 2009 still require some type of fixed infrastructure in order to function and the presence of qualified technicians or engineers is required. Yet many disaster situations result in no useable infrastructure to support either local area or wide area communications.

> According to an Associated Press report in 2005, “Downed telephone lines and damaged cellular towers left emergency crews confused and isolated in the aftermath of Hurricane Katrina.” The report, quoting experts, said communications systems eroded as the waters rose and only became worse.
>
> “We had no way to communicate except by line of sight. Our radios were not operable, most landlines and cell phones were useless and our communications centers were under water. When help arrived, we could not communicate with them either." Juliette Saussy, Director of Emergency Medical Service of New Orleans, told regulators.
>
> “Some three million telephone lines were knocked out as the violent storm hit the Gulf Coast on August 29, 2005. At least thirty-eight 911-call centers went down, and more than 1,000 cellular towers were out of service. As many as 20,000 calls failed to go

through the day after the storm, and about 100 TV and radio stations were knocked off the air…" FCC Chairman, Kevin Martin commented.

There must be a framework for enabling communications, interoperability and collaboration that is affordable. The biggest gap in 2009 is that existing solutions are too expensive for most EROs and funding for staffing communication technicians to operate these solutions reduces the ability of most EROs to equip and staff for other vital capabilities necessary for mission effectiveness. This ORD requires, not only that the technology-based solution works, but that it is affordable.

The local incidents, as well as the wide area natural disasters within the past seven years clearly identify the capability gap to enable First Responders to communicate, interoperate and collaborate with each other, their command and their support teams or with other organizations present at an incident scene within minutes of arriving at an incident site. This ORD provides the system requirements to close this vital gap saving lives and increasing security.

1.2. Overall Mission Area Description

A first emergency response provider (FERP) by definition is any professional who first arrives at an incident site to provide emergency medical services, security, law enforcement, assessment of the scope of the incident and recommend and coordinate an extended response, if required. The mission area covered by this ORD is to outline the capabilities needed to enable FERPs to communicate and collaborate with each other, their command and interoperate with mutual aid, support teams and other responding organizations within minutes of arriving at an incident site. This ORD will also address the capabilities needed to provide interoperable voice and data systems to command in control of the incident; dynamically managing the incident as the response grows and scaling communications as required; increasing collaboration and extending the chain of command across jurisdictions. Finally, this ORD will identify the requirements of the proposed system capabilities and provide a communications framework for the creation of a dynamic, interoperable system of systems.

1.3. The Description of Resilient Portable Communications Responder Kits that Create a System of Systems.

The primary system solution that closes the capability gap described above and accomplishes the mission of this ORD is a system of systems (SoS). The SoS must meet three primary requirements. First, the SoS must be dynamic, enabling interoperability between any combinations of different communication device types; converge any type or number of disparate networks on-demand at any incident site. The SoS also fosters dynamic communications with EROs, elected officials whose districts are affected by the incident, supporting emergency operations centers (EOCs), medical facilities, military bases, etc. and private sector security involved in the area of the event. There can not be any operational restrictions on the number of, or combination of, systems available to support the incident response. The requirement is that the EROs and FERPs use the same software-based framework that is freely distributable at the incident site and can be loaded on or accessed by any device in minutes.

In order to create a dynamically interoperable SoS, the SoS must be based on software that converges network protocol types and provides network presence awareness. The SoS is required to enable data interoperability among any combinations of ad hoc, terrestrial data, telephony or satellite networks that are immediately available to FERPs or will be introduced to the SoS by other FERPs or EROs as the response develops.

The second primary requirement that must be in place to meet the mission of this ORD is human portable resilient communication systems that can provide connectivity to the interoperability framework. These systems will be in a kit form that has everything a FERP needs, to be hand-carried to the incident site, transported by car, helicopter or small watercraft. The kit must be able

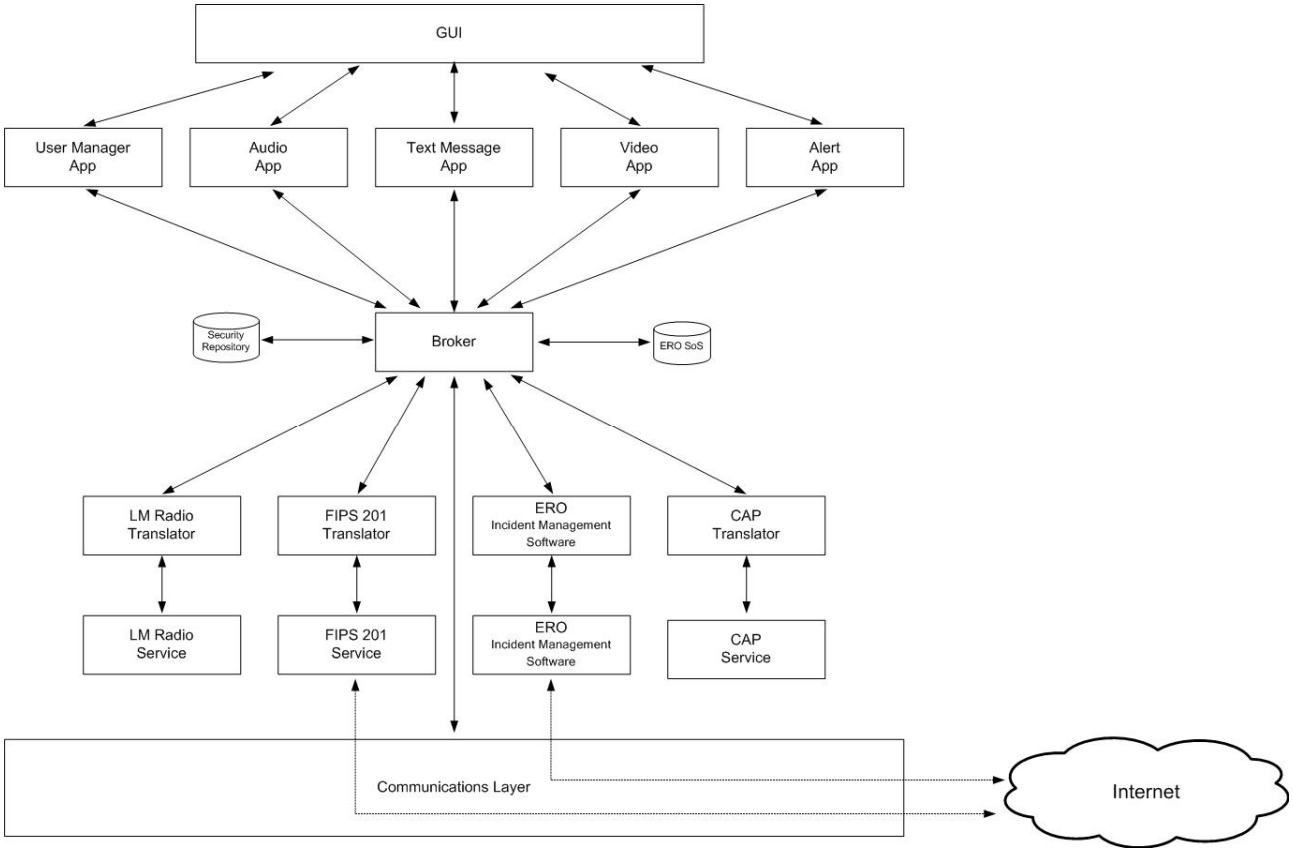
to provide voice, video and data communication peer-to-peer among FERPs at the incident site as well as capability across any available network. If normal network infrastructure is unavailable, the kit will contain a broadband satellite system to insure connectivity beyond the incident site. The resilient portable communications kit (RPCK) will be easy to setup and become operable within 10 to 20 minutes by any FERP. The kit will require no technical support to setup. The RPCK shall seamlessly participate in an expanding system of systems. The kit will be available in multiple form factors providing EROs the flexibility to have kits carried by hand in cases, mounted in vehicles, installed in mobile EOCs or any other type of response apparatus. If an ERO needs to support large-scale recovery operations, the RPCK will be modifiable to meet the requirement of the ERO.

The communication capabilities of the RPCK require:

- the ability to operate via both AC and DC power without requiring filtering. It will directly connect with any 12-volt battery, vehicle cigarette lighter adaptor, generator, tactical solar array or tactical fuel cell.
- a full featured VoIP PBX with at least five handsets (wired or wireless) with the ability to scale the support of VoIP handsets for every FERP at the incident site.
- wired Ethernet connectivity for a minimum of four external devices.
- wireless access to the network for any 802.11-enabled COTS computer at the incident site. The system's wireless coverage will be scalable simply by deploying software definable wireless routers operating on AC or DC power deployable by the FERP.
- network management software converging data, telephony and video protocols while interconnecting seamlessly and without configuration with IPv4 and/or IPv6 networks and devices.
- IPv6 and IPv4 network routing with a software firewall as well as allowing external firewalls and VPNs to be used if required.
- simple operating instructions with color-coded connections allowing any FERP to deploy the network without prior exposure or training to the RPCK.
- the capability to add IP-based devices and peripherals as needed to support an extended response or recovery operation.
- the ability to interconnect with any land mobile radio network (LMR) or cellular "push to talk" (CPT) phone patchwork interoperability system, enabling LMR or CPT devices to interoperate with any other type of device on the SoS, such as a laptop computer. This ability allows EROs utilizing IP-based devices (laptop, PDA, desktop computer, etc.) to have voice communications with LMR or CPT devices
- interoperability support with cellular systems.

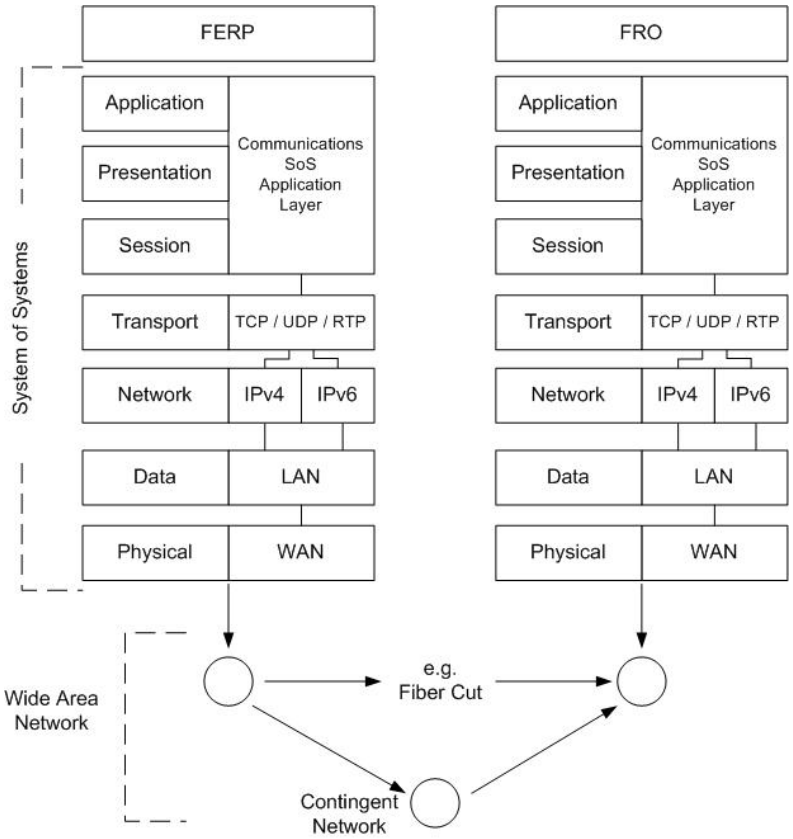
The third primary requirement is the kit must be affordable and scalable. The SoS will fail if the FERP does not carry resilient communications to the incident. EROs will need multiple RPCKs. If the kits are too expensive they will not be available where they are needed most as an integral part of any FERP's support equipment. The RPCK should be affordable to rapidly fund the distribution of enough kits across the United States, enabling the deployment of a resilient SoS, which in turn creates a national communication resiliency network (NCRN). Even if parts, or all of the national power and communications infrastructure are compromised or destroyed, the NCRN would survive.

The following diagram details the architecture needed to create the framework of a SoS:



The kits are required to interconnect with any available IPv4 or IPv6 data network that the FERP has authorization to use; providing Wide Area Network (WAN) connectivity without requiring any configuration or modifications by an FERP. By enabling the IPv6 capability, the system provides the ERO the ability to create secure collaboration with supporting agencies anywhere in the world, on-demand. The following diagram details the capability of creating secure peer-to-peer collaboration on-demand without the need of a server.

The following diagram is the position of components on the open systems interconnection (OSI) stack necessary to support interoperability:



The contingent network in the diagram above is any available WAN connection. If a WAN connection is not available at the incident site, the RPCK will include a small broadband satellite system, with active service.

1.4. Supporting Analysis

These requirements have been verified through interviews with DHS and first responder personnel throughout the United States.

1.5. Mission the Proposed System Shall Accomplish

Homeland Security Presidential Directive 5 (HSPD-5) mandated the National Incident Management System (NIMS) calls for the creation of a system that enables:

> "Federal, state and local governments to work effectively and efficiently together to prepare for, respond to and recover from domestic incidents, regardless of cause, size or complexity. To provide for interoperability and compatibility among Federal, state and local capabilities, the NIMS will include a core set of concepts, principles, terminology, and technologies covering the incident command system, multiagency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications; and certification; and the collection, tracking and reporting of information and incident resources." HSPD-5 (February 2003)

The proposed SoS and RPCK would enable the accomplishment of this directive. If FERPs and EROs cannot communicate, they fail. The proposed system creates the communication resiliency necessary for an "interoperable and compatible response" to an incident.

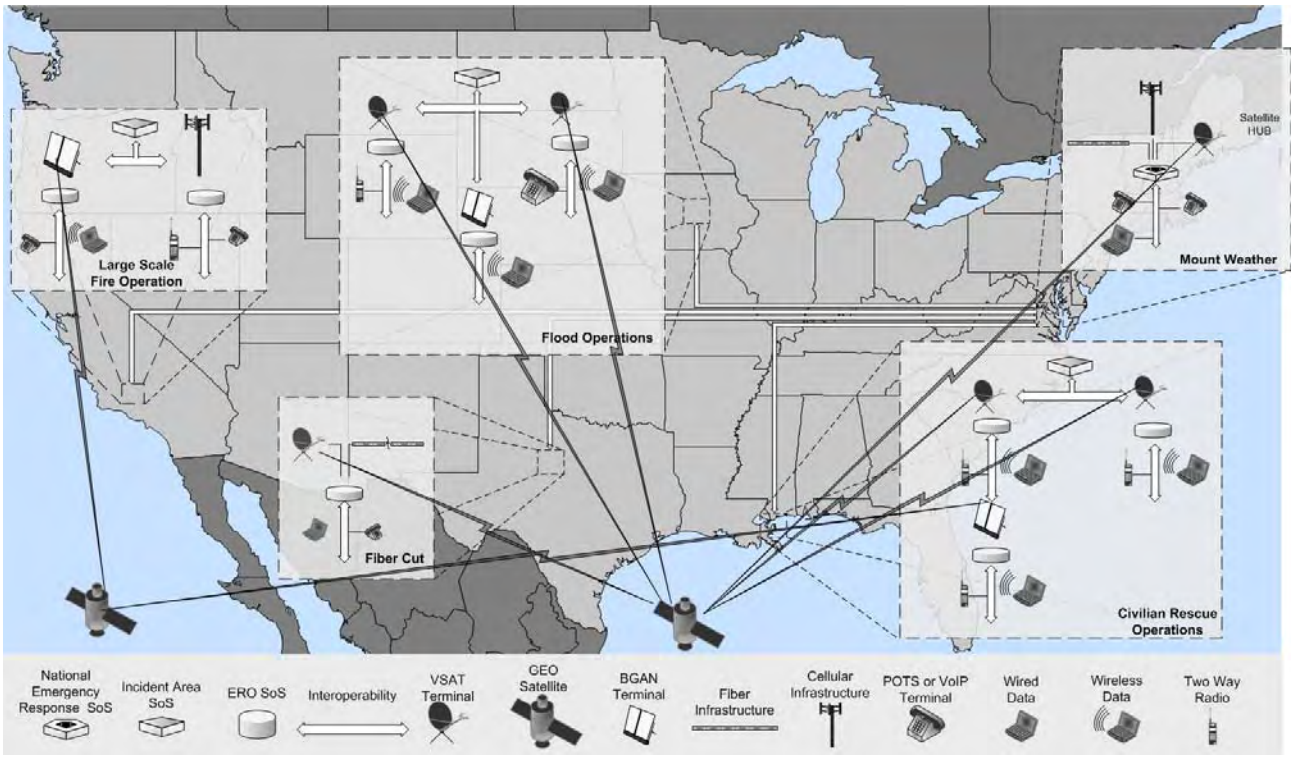
Specifically the proposed system shall accomplish this mission by:

- providing a communication framework that creates dynamically interoperable communications on-demand.
- providing any FERP with the capability to communicate at an incident site with other responders and with anyone else who has data or telephony capability anywhere in the country with what the FERP brings to the incident site with no need for additional equipment.
- enabling any responder, even if it is the first time the FERP has used the kit, to set up the system within 10 to 20 minutes.
- interoperating with other systems, creating a system of systems for voice, data and video interoperability.
- providing the ability to log communications among FERPs for reporting purposes.
- interconnecting command systems in a multi-agency response across disparate networks on-demand.
- creating visibility among responders to know what resources are available and coordinate the use of those resources.
- enabling the creation of "ad hoc" incident site, area, regional and national communication networks as needed within minutes.
- providing peer-to-peer communications that enable instant alerts, warnings and advisories that can be viewed and responded from anywhere in the country.

1.6. Operational and Support Concept

1.6.1. Concept of Operations

The RPCK and a SoS framework shall establish communications anywhere and anytime without any other support. These systems will be a part of the FERP team's basic response tools. The system creates a system of systems with other systems and will interoperate with any other IP-based network. If FERP vehicles in every locality in the country carried the RPCK /SoS system or used the software that provides the system capabilities for legacy systems, in effect, the NCRN is created that provides communication capability even in the aftermath of a large scale infrastructure disaster. The diagram below illustrates the NCRN.



The NCRN shall be available to as many FERPs and EROs as possible on a 24/7 basis. The system creates the communication resiliency and provides the capabilities to accomplish the mission only if the SoS is available to the FERP teams and their commanders. Every EOC, fire station, police station, hospital emergency room, private security force at critical infrastructure sites could have a RPCK in order to create a system of systems on-demand. In addition, key response vehicles, apparatus and command vehicles could also have systems in order to be apart of the system of systems. Finally, civilian and political leaders who are integral to the NIMS could also travel with the RPCK to guarantee their availability to collaborate by having personal communication resiliency.

Sites and agencies not affected by the loss of communication capabilities, but who still need to be a part of the SoS can simply do so by running the proposed system software on their existing systems. This ability to run SoS software on any network from any location will provide the capability of a virtual on-demand NCRN, resilient by design. The SoS communication framework is agnostic of device type or network type. The SoS system framework simply requires a MAC or IP address within an IPv4 or IPv6 network.

Despite the fact that billions of dollars have been spent on interoperability since the NIMS mandate, there is no real capability for interoperability of voice, video and data that can be used on

a local, state, regional and national basis immediately following an incident. The proposed RPCK/SoS shall provide that capability for far less than the cost of alternative systems that do not have the capability of meeting the mandate. Meeting this requirement has the potential to save hundreds of millions of taxpayer dollars while also being rolled out nationally in less than three years.

1.6.2. Support Concept

The core concept of the SoS deals in providing connectivity when and where it is needed. A staff of network convergence engineers could support the system around the clock. A support engineer shall have the ability to troubleshoot problems in real-time. Because one of the major requirements of this ORD is that hardware components be minimized when possible by providing network functionality with software, a support engineer shall run remote diagnostics on any supported system.

Software updates shall be available to all systems in a planned and coordinated manner. Because the SoS is a peer-to-peer framework, updates shall automatically be logged to the support database with an acknowledgement of a successful update. If updates are required at the incident site, a support engineer would have the ability to remotely update the RPCK at the incident.

If there are hardware failures with the RPCK, replacement systems and parts can be staged at regional logistic depots which would guarantee a maximum delivery time of eight hours to the ERO. Spare parts should be included with each RPCK for repairs that can be made by the FERP.

Live interactive webinars can be held daily on a regional basis allowing any FERP to not only receive training, but also ask for advice and share ideas with other FERPs. These webinars will be coordinated and monitored by a national support staff. Because every RPCK would provide peer-to-peer video capability, enhanced support would be provided to any FERP when needed.

2. Threat

If FERPs and EROs cannot communicate, they cannot respond effectively. Lives have been lost because communications systems were not resilient or could not interoperate with other systems at the incident. Rescue operations can not be coordinated or assets requested or deployed because valuable time is lost without critical communications capability.

On a local level incident response, too many missions are compromised because some EROs cannot afford easy-to-use resilient communication systems. The systems sold to them are too expensive and require costly support. Complex systems requiring this type of support take resources away from other critical areas.

In most cases, as communications systems funding becomes available, EROs do not possess the knowledge or experience to adequately obtain a system that addresses all the communication risks they will face in a disaster. There are no current standards published that give them guidance on possible solutions that will meet the demands necessary to implement this ORD. Instead, to a large extent they rely on existing relationships with vendors, who quite often are not skilled or adept in disaster recovery communications. Also, companies whose business model relies on proprietary technology that does not allow other manufacturers' products to integrate creates obvious issues for the mission of this ORD. Additionally, EROs find that what they get is not what they thought they were buying. There are dozens of anecdotal stories of EROs spending millions to deploy systems that do not accomplish the intended mission and when they voice their dissatisfaction, they are often informed they will need to spend millions more to actually get the system to do what they need, if in fact the system can do what they need.

On a state and regional level where interoperability exists, only certain types of radio systems have this ability. These systems depend on an infrastructure with little or no resiliency. Major budget dollars spent on incident management software and services by EROs to manage incidents on a regional or state basis will not work well if they do not have connectivity to the Internet. Alert and warning systems have become a major business since the Virginia Tech tragedy, but they all depend on networks that provide little or no resiliency. If power fails, campus communications fail. You cannot send a SMS alert and have any guarantee the message was received if you are depending on a highly vulnerable cellular network for example. If one sends an emergency email, there is no way to guarantee that the multiple e-mail servers required for the delivery of the email will be available and able to deliver the increased amounts of email generated due to an event. Not only are many EROs creating plans that will fail without resilient and an interoperable communication framework, they are spending hundreds of millions of dollars building a false sense of readiness.

There is currently no interoperable resilient national communication solution across federal, state and local EROs. Solutions that will take decades, costing billions of dollars and do not provide resilient interoperability and can become a major threat to homeland security. A response to a pandemic, major terrorist strike at key infrastructure, a cyber attack on telecommunication centers, super regional earthquakes and catastrophic oil shortages planned to cripple the US economy or any other scenario with national impact could fail because current communications infrastructure will be compromised or worse yet, destroyed. Without proper communications, EROs are “blind, deaf and mute” to any coordinated national response. There is currently no capability to create a national “ad hoc” communications network for a coordinated national response. This inability makes NIMS vulnerable to failing on a catastrophic level.

Finally one of, the greatest threats is ignoring the plurality of our system of government. Incident response always starts at the local level therefore, expenditures must happen at the local level. It is impractical to implement a federally mandated one-size-fits-all system. William Waugh points out this in his paper “*Terrorism, Homeland Security and the National Emergency Management Network*”:

> “On September 11, 2001, officials and agencies that are part of the national emergency management system orchestrated the responses to the collapse of the World Trade Center towers and the fires at the Pentagon. The efforts of local, state, and federal emergency agencies were augmented by nonprofit organizations, private firms, and organized and unorganized volunteers. The system reacted much as it would have for a major earthquake or similar disaster. In the rush to create federal and state offices to deal with the threat of terrorism and, ultimately, to create a Department of Homeland Security, the very foundation of the nation's capacity to deal with large-scale disasters has been largely ignored. Although the human and material resources that the emergency management network provides may again be critical in a terrorist-spawned catastrophe, the new Homeland Security system may not be capable of utilizing those resources effectively. The values of transparency, cooperation, and collaboration that have come to characterize emergency management over the past decade seem to be supplanted in the new command-and-control-oriented Homeland Security system. If that occurs, when the resources of the national emergency management system are needed most, the capacity to utilize the system may be severely damaged and cultural interoperability will be a serious problem.”

Avoiding this problem lies in a communication system that is based on the concepts of the type of SoS called for by this ORD. All of the efforts of the National Emergency Management Network (NEMN) is wasted without a NCRN. Ham radios alone will not coordinate the management of a national response effort. EROs and FERPs require resilient voice and data communication capability that will interoperate with other EROs and FERPs.

3. Existing System Shortfalls

Why do current systems fall short of providing the capability to meet the NIMS requirements?

> "To provide for interoperability and compatibility among Federal, state and local capabilities, the NIMS will include a core set of concepts, principles, terminology, and technologies covering the incident command system, multi-agency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications; and certification; and the collection, tracking and reporting of information and incident resources."

Specifically, current systems fall short in these major areas:

- Most systems are not resilient. Systems that depend on a fixed infrastructure, dedicated networks and proprietary technology are not reliable in a response to a major disaster or infrastructure failure. Most systems take days if not weeks to restore when they fail. Without communications, NIMS' plans will fail.

- The requirements published for NIMS compliance by EROs lack a communications framework that simplifies the process of implementing a system that meets the requirement for interoperability and compatibility. Most EROs lack the technical resources to filter through the plethora of available systems. In many cases, communications specialists who are making these decisions are only experienced in analog radio systems or telephony and are being forced to make IP networking decisions in which their lack of knowledge leads them to spend their budget on systems that only provide part of the capability they need. EROs need options that work within a communications framework that will guarantee interoperability and compatibility with any agency or ERO.

- Systems are too expensive. The ERO buys a system that is limited by budget or grant potentials. Many have what they can afford, not what they need. Every ERO and FERP need full resilient communications capability.

- Systems are too complicated. For example, one major provider of systems that any ERO would deem reliable is selling a solution that requires several certified technicians to operate. The ERO may have a powerful system that may in fact cost more in five years to operate than it cost to purchase. A FERP will not have the needed communication capability if the technician can not get to the incident scene. This could take hours in most cases and in the case of a major disaster, days.

- Many systems rely on proprietary technology that can only integrate with like devices. The major providers of communication systems provide systems based on proprietary technology that drives up the price for the ERO to not only acquire and support, but also makes it difficult and expensive to interoperate with other EROs. In some scenarios, voice, video and data interoperability between different proprietary systems is not feasible.

- Many systems will fail to provide resilient communication because they are so cumbersome they require dedicated power and transportation, rendering them useless to the FERP in the first critical minutes of a response. Semi-trailers cannot easily travel over roads blocked by fallen trees and downed power lines. Due to the flooding, responding to Hurricane Katrina meant having to fly systems and technicians in by helicopter or small planes, taking days to provide communication capabilities for rescue

operations. If the systems are simple to use and FERP-portable, they could and should go to the incident site with the FERP.

- Since there is no practical framework to create a system of systems today, even the grant process for funding systems is slowed down. Without a framework, it is a daunting challenge for a multi-agency grant process to verify what is being bought by the ERO is necessary and will meet the mission requirements. With a SoS, it becomes feasible to require systems be compliant with the framework, making purchasing decisions and grant processes easier.

- Most EROs have system networks that are IPv4 and not IPv6 compliant. The majority of FERPs would not even notice the difference, but a system that is not IPv6 compliant is more difficult to secure in trying to support interoperability. These security concerns by themselves can cause any mutual response to fall short of the requirement for interoperability and compatibility.

- Current systems also fall short because, due to a lack of an interoperability framework supporting systems being apart of a system of systems, it is problematic, if not impossible to allow EROs not only to interoperate with other EROs and FEMA, but National Guard, military and private sector security as well. Without a communications framework supporting communications across organizations, a mutual-aid response will likely fall short on what is needed for an effective response and rapid recovery.

4. Capabilities Required

4.1. Operational Performance Parameters

The SoS and RPCK shall meet the NIMS mandate. To do so, the RPCK, at a minimum must be able to:

- Converge multiple protocols and networks to provide interconnectivity to any IPv4 or IPv6 network or optimally a system that will interconnect to IPv4 and IPv6 networks wired or wireless, and terrestrial or satellite (O/T)
- Support IPv6 connectivity and be capable of routing to an IPv4 LAN. (O/T)
- Run two or more RPCKs at the same incident site (T) to run two or more RPCKs at multiple sites across a large area and support collaboration of every RPCK or IP network being used in the response. (O)
- Operate on either AC or DC power (T), directly connect to any 12-volt battery, vehicle cigarette lighter, generator, tactical solar array or tactical fuel cell. (O)
- Support interoperable voice, video and data applications at the incident site (T), the ability to support secure interoperable voice, video and data from the incident site with any other location in the country (O).
- Provide two form factors, one portable and one that can be mounted in a mobile transport in less than one hour (T), multiple form factors enabling the ability to put a RPCK anywhere. (O)
- Be carried by a FERP to an incident on foot, by small watercraft, car/SUV, helicopter/ small plane (T) or the RPCK is small enough to fit in a bag or case that the FERP is using to carry other gear into the incident (O).
- Mount in fire apparatus or emergency response vehicle (T) or, small enough to fit in any ERO network rack or any mode of transportation available in the response. (O)
- Setup in 20 minutes by the FERP (T) in less than ten minutes. (O)
- Require no more than six steps to setup (T) no more than three steps to setup. (O)
- Provide VoIP calling anywhere in the United States (T) anywhere in the world. (O)

- Provide a software VoIP PBX that supports at least three phone calls at one time using a single toll-free DID (T) or able to support thirty phone calls at one time using a single toll-free DID. (O)
- Support extension-to-extension dialing over the incident area (T) or support extension dialing across a WAN. (O)
- Create a LAN for the incident site (T) or create a “no setup required” LAN for the incident site with software providing secure IPv4 and IPv6 routing and the ability to support organizational security requirements. (O)
- Interconnect with any available network providing Internet connectivity (T) or the ability to connect to multiple networks and rollover to a backup network when the primary fails or load balance between the two. (O)
- Provide 10mb network connectivity between users on the LAN (T) or 54mb network connectivity between users on the LAN. (O)
- Support interoperable peer-to-peer networking (T) support peer-to-peer video, audio and data connectivity. (O)
- Provide a minimum 400mw 802.11 a/b/g wireless access point that can support non-line-of-sight wireless access to the incident LAN from up to 100 yards (T) or a minimum 400mw 802.11 a/b/g wireless access point that can support the same access from up to one mile. (O)
- Support up to at least twenty-five users on the network at one time (T) or support up at least to one hundred users on the network at one time per RPCK. (O)
- Provide one VoIP handset (T) or five VoIP handsets with the option of adding up to at least twenty-five handsets per RPCK. (O)
- Support any IP-over-satellite network access (T) or have the ability to provide satellite service for the RPCK without having to increase the size of the RPCK. (O)
- Provide complete instructions for setup and trouble shooting (T) or complete color-coded instructions with pictures that a FERP with an elementary education can setup. (O)
- Be affordable enough to purchase and maintain (T) or affordable enough for the ERO to have RPCKs at all supporting sites with enough RPCKs to support every FERP responding to the incident. (O)

The SoS at a minimum must:

- Create a system of systems at an incident site simple enough for a FERP to setup in 10 to 20 minutes or optimally extend the system of systems to any system in the country, if the system has access to the Internet or mutually accessible dedicated network. Nothing more should be required other than entering the location code of the SoS.
- Create a communications framework for interconnecting disparate local area data networks, video networks and radio networks and enable automatic interoperability between all interconnected networks at the incident site or optimally securely interconnect disparate networks anywhere in the country creating a WAN on-demand.
- Support the interoperability of peer-to-peer communications of voice, video and data or optimally support peer-to-peer and one-to-many and many-to-many connectivity of all users within the SoS.
- Provide a framework for collaboration or optimally a framework for collaboration that can provide application functionality by writing an XML document.
- Support presence management and optimally will include a self aware application that several times a minute updates the SoS user list enabling dynamic collaboration and peer-to-peer communication.
- Support multiple applications or optimally multiple applications and services, including multiple security services.

- Operate at level 4 of the IP communication layer and optimally as much functionality as possible should operate at layer 5, 6 and 7.
- Support the Federal efforts to provide extended alerting:
    - Commercial Mobile Alert System (CMAS)
    - Common Alerting Protocol (CAP)
    - existing broadcast alert services.
- Provide a mechanism for Trusted Identity Management:
    - National Incident Management System (NIMS) requirements (SP 800-73, SP 800-78, SP 800-79, IR 6887)
    - Homeland Security Presidential Directive 12 (HSPD-12) and Federal Information Processing Standard (FIPS) 201 compliance and support.
    - First Responder Identification Credential (FRAC) support
    - Public Law 110-53 compliance .

4.2. Key Performance Parameters (KPPs)

The key performance parameters for the SoS and the RPCK are:

- Resiliency - Interoperable communications must be able to establish voice and data communications within 15 minutes from the time of arrival at the incident site. The system must provide required communications capability even if all communications infrastructure is compromised or destroyed. Redundant communication must be provided with the RPCK. If the VoIP services are not working, the FERP should be able to have peer-to-peer voice capability with anyone on the SoS. If conditions are not favorable for audio communications, the FERP should be able to send private and public instant messages or alerts and advisories using the SoS software.

- Accessibility - Communications must be established by a FERP without the need for technical support. No configuration of the software should be required to setup the RPCK. The system will be connected to the best available network and connected to an AC or DC power with phone and Internet services available to all FERPs.

- Portability – The FERP shall have a portable solution they can literally carry with them to the incident to assure they will have communications capability immediately upon arrival. RPCKs must be man portable and operate independent of large vehicles and/or trailers.

- Interoperability - The SoS provides full interoperable voice, video and data communications among FERPS and supporting agencies and EROs regardless of communication device types. The interoperability shall be dynamic. Dynamic interoperability is defined as the ability to connect any user across any network and have the ability to connect any IP communication device with any other IP communication device. The interoperability shall be at level 4 or 5 of the communication layer enabling the SoS to connect any network and run on any IP device. The SoS should also enable interoperability between interoperable radio and telephone switching systems and any data user of the SoS.

- Expandability - The SoS shall not have any limitation on the number of users it can support. The number of interconnected networks cannot be limited. The RPCK must be scalable either by linking multiple RPCKs together or by running the SoS on a larger Resilient Communication Command System (RCCS). A RCCS should support hundreds of users exactly as a RPCK supports dozens of users. The RCCS must also be tactical and transportable, but the need for greater scalability may limit the method of transportation with an SUV or pick-up truck. The RCCS should not only offer the same features and functionality as a RPCK, but also be as easy to setup and be available in a kit form. Because of the greater processing power of a RCCS, the area of coverage shall increase, providing greater flexibility.

- Visibility - The SoS must be able to allow span of control and mutual assessment and collaboration at and beyond the incident area site. The software interface must support a span of control over the users allowing for grouping users into manageable groups and sub-groups without compromising security. The ability to group should be as simple as entering a code that will direct the user to their group, while allowing incident command the ability to see all resources. Peer-to-peer voice, video and data communication must allow users on demand the ability to have private one-on-one communication or private group conversations, while at the same time having incident wide communications.

- Transparency - The SoS must not only enable the interoperability of voice, video and data communications, but it must also interconnect and support other systems and networks providing alert, warnings and advisories. The SoS software shall enable alerts and advisories between any FERP or ERO without needing anything but the SoS software. The alerts and advisory capability will expand to provide public advisories.

- Flexibility - The RPCK must provide a full featured software PBX that is configurable from an easy-to-use GUI interface providing QoS and options to meet the ERO and FERP requirements. The PBX should provide a toll-free DID and support hundreds of extensions if needed. The PBX will have defined calling features available for configuration by the ERO. The RPCK must support as many simultaneous calls as the backhaul will allow. The SoS should also support both IPv4 and IPv6 networking and the RPCK should provide IPv6 capability to EROs who only have IPv4 capability.

- Usability - The RPCK and SoS must work with both AC or DC power, be network agnostic and able to work in any type of weather or climate that the FERP is operating in. The RPCK should require no special environmental conditions. The RPCK must converge the network protocols involved in providing voice, video and data so that network configurations are automatically provided to the user. The FERP should be able to connect color-coded cable, power the system up and have full communication capability.

- Adaptability - The SoS communication framework must be built using XML to allow for the rapid implementation of services and development or integration of applications used for collaboration. The FERP must be able to create a system of systems, enabling scalability, interconnectivity and rapid data convergence among all responders in just minutes, for all responding mutual aid agencies, remote support and chain of command. This capability will not require dedicated technical resources to maintain. The SoS and RPCK must function in any environment without need of other systems if they are not available, but seamlessly interconnect to those systems without requiring the FERP to do anything. The RPCK will turn any vehicle into a forward command post for areas that have been cut-off or are a HAZMET site. The system will go anywhere in the United States and work without modifications or additional configurations.

- Affordability - The SoS shall be affordable to the ERO. The software enabling peer-to-peer interoperability will be freely distributed with the ERO only paying for the delivery medium. The cost of the communications framework software should decrease with the number of groups within the ERO's span of control and should be available as a software service if the ERO has limited technical resources for organizational installation and system administration. The RPCK must be COTS compliant and provide volume-pricing incentives.

4.3 System Performance.

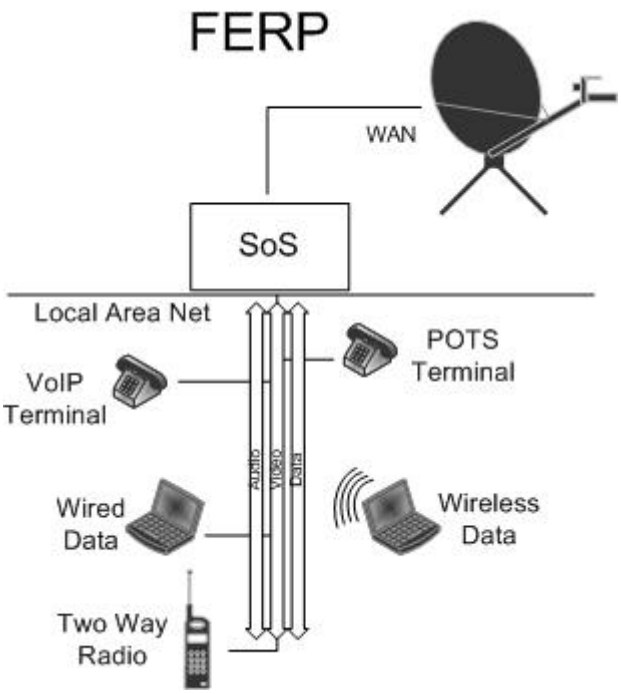
There are many types of disasters in the United States, but the most common emergencies are:

Dam Failure	Hurricane	Tornado
Earthquake	Landslide	Tsunami
Fire or Wildfire	Nuclear Power Plant Emergency	Volcano
Flood	Pandemics	Winter Storm
Hazardous Material	Terrorism	
Heat	Thunderstorm	

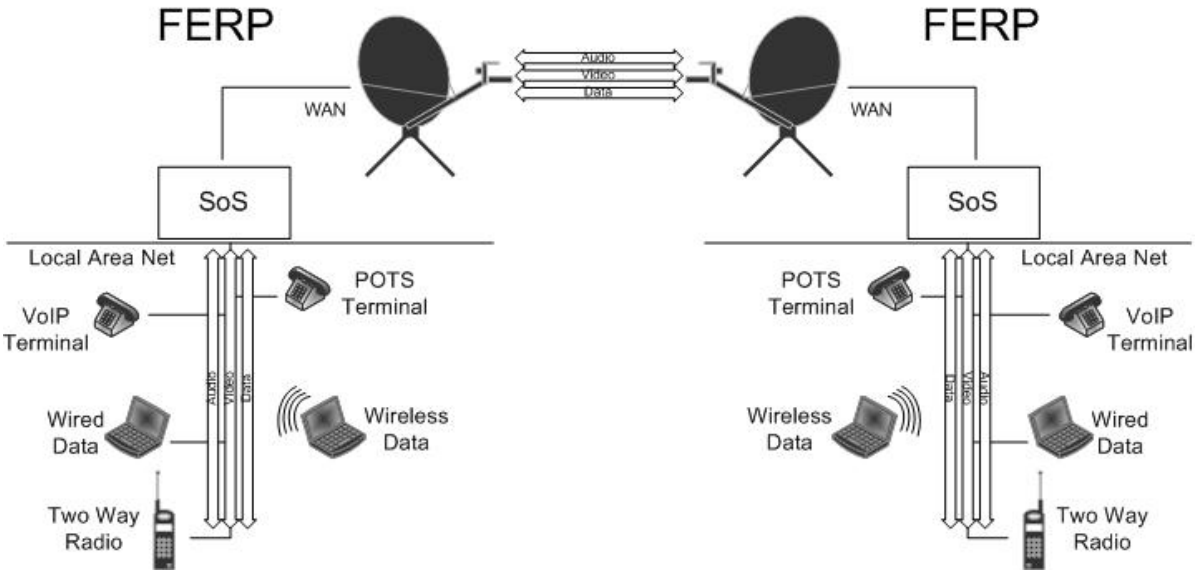
4.3.1 Mission Scenarios

Preparation and/or planning for these scenarios are paramount to enable recovery. The first and foremost consideration must be the lives of any potential victims or personnel within the immediate area of the incident site. Secondly, no situation, no matter how small, should ever be viewed in any other term than worse case scenario. If emergency responders are prepared for the worst possible situation, they inevitably will increase their odds for success. Those who fail to plan and fail to prepare are our greatest liabilities.

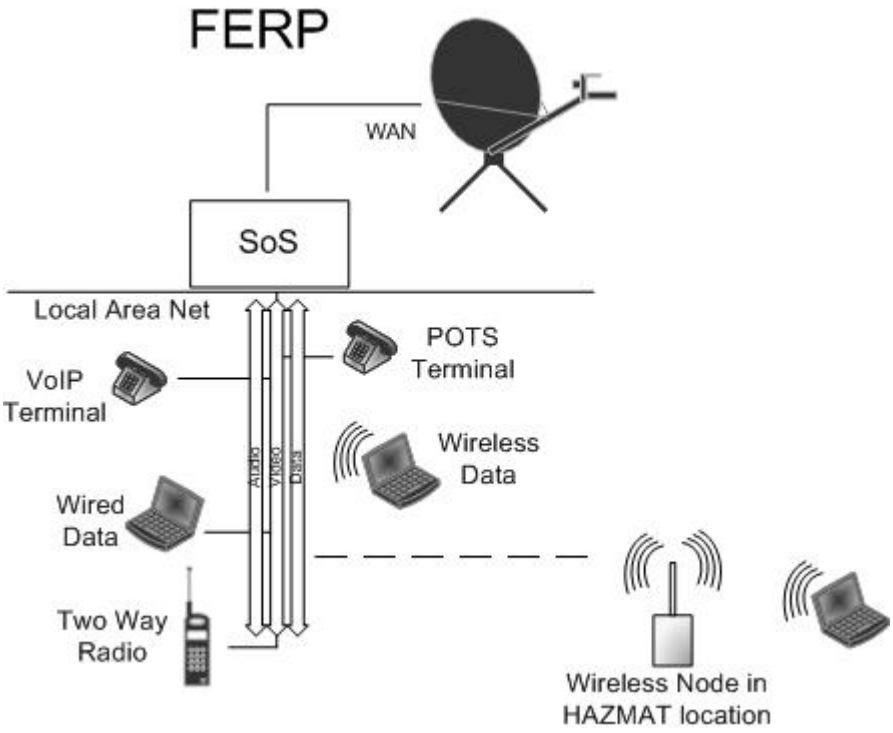
The most frightening and destructive forces of nature (e.g. hurricane, tornado, earthquake, tsunami, wild fires, or flooding) strike suddenly, violently, and many times in the event of an earthquake or tornado they occur without warning. If an earthquake or tornado occurs in a populated area, it may cause many deaths, injuries, and extensive property damage. There are no guarantees for safety following a disaster, identifying potential hazards ahead of time and advance planning can save lives and significantly reduce injuries and property damage. In the event of a disaster, EROs are required to do an assessment of the damage prior to allowing safety personnel and restoration groups into the incident area. Most likely, this would require communications in a scorched earth environment. FERPs would be required to setup and deploy the SoS in the disaster region and communicate to other reporting agencies to coordinate relief and aid.



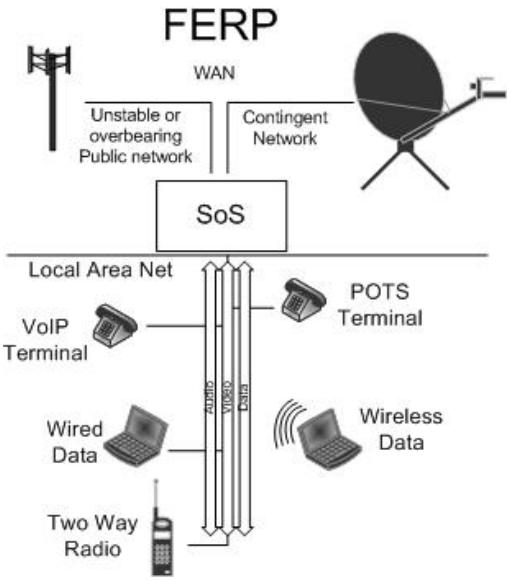
In the event of a Man-Made Disaster (e.g. Terrorist or Enemy-Nation Attack) the ERO would require a number of FERP teams to respond and report. There is now a requirement to have interoperability with these team members to include establishing two-way radio communications, data transmissions to and from multiple agencies as well as establishing an Incident Area Command Center (IACC) with full voice telephony communications mandated. If the immediate responsibility of the ERO is to assess the damages by physically entering the disaster area providing an assessment to the IACC in order to organize and manage the critical next steps of the rescue, video transmission may be required to ascertain the damages and environmental impact.



In all cases of the aforementioned disasters, all EROs need to asses the damage within the incident area, establishing communication to and from the incident site, enabling them to relay information of assessments to decision making authorities to enable them to conclude on the critical decisions for recovery. This would require that the ERO have minimal setup steps in deploying communications since the focus must be the disaster site itself. The SoS must be able to quickly deploy in different scenarios and adapt to different topologies of networks and environments seamlessly:



Within 10 to 20 minutes of the FERPs' arrival at the incident area, IACC should be able to move into rescue operations. The system must now move to providing LAN and WAN capability, allowing responding personnel and agencies the ability to interoperate immediately:



Not all responses are for emergency operations, some exceptions are large-scale events (e.g. National Conventions, Super Bowl, National Sports Events, Concerts, Demonstrations or Political Rallies). These types of events can often cripple existing communication layers with an influx of traffic generated at the event site. The ERO must have the ability to over come these obstacles easily and seamlessly. The FERP must have the ability to support two-way communications as well as telephony communications. In addition, the FERP must have the ability to send video data to and from the event site. Typically, in these types of situations, FERP members often work with civilian security and/or corporate personnel where interoperability is just a word in the dictionary. Many agencies are responsible for security at large scale events where tens of thousands of people attend. In many cases, multiple agencies, public and private are "working" the event in some manner. All require a system that establishes a LAN and WAN for all to utilize quickly and easily. In addition, this system must be able to utilize any current network infrastructure or establish its own infrastructure immediately.

Other concepts of operations are also acceptable that are not explicitly discussed here.

4.3.2 System Performance Parameters

Key Performance Parameters (KPPs) for the RPCKs

- Resilient communication established within 10 to 20 minutes.
- No technical support is required for any FERP to set up system.
- Portability: the common form factor should weigh less than 40lbs and be small enough to be carried on commercial airplane and stored in an overhead compartment.
- Equivalent functionality in different form factors.
- Very low power consumption, target 30 watts typical.
- Complies with Part 15 of FCC Rules.
- Extended-temperature operation up to +54°C (130°F) or down to -34°C (-30°F).
- The enclosure must meet or exceed:
    - FED-STD-101C, Method 5007.1, Paragraph 6.3, Procedure A, Level A Tests are superseded and concurrent with ASTM B 4169, DC-18, Assurance Level I, Schedule A.
    - MIL-STD-810F, method 506.4, Procedure II of 4.1.2. FED-STD-101C Method 5009.1, Sec 6.7.1Tests are superseded and concurrent with ASTM B 4169, DC-18, Assurance Level I, Schedule H.
    - ATA 300, Category I, "General Requirements for Category I and II Reusable Containers".
    - Resilient to salt water spray: MIL-STD 810E Method 509.3.
    - Immersion MIL-STD-810F, method 512.4.
    - Qualified to MIL-STD-810 environmental standards.
    - Qualified to MIL-STD 810E Method 516.4. High shock/vibration exist.
    - Qualified to meet Ingress protection (IP67) while in use.
- Consist of at least 2-port WAN connections with fail over and load balancing.
- Provide an easy-to-use administration control GUI or HMI.
- Consist of at least a 4-port Fast Ethernet switch.

- Support auto-MDI-MDIX network installations, along with support for auto-crossover, auto-polarity, auto-negotiation, and bridge loop prevention.
- Allow for computing devices to be networked together using 10BaseT or 100BaseTX LAN connections.
- Field programmable, port-based VLAN functionality.
- Allow any combination of LAN ports to be connected together in subnets for use in a small secure or non-secure network.
- IEEE 802.3 and IEEE 802.3u compliant.
- Fully independent media access controllers (MACs).
- Embedded frame buffer memory.
- High-speed address look-up engine.
- Qualified to MIL-STD-810 environmental standards.
- Equipped with system status, warning and error indicators.
- Network cable complies with Category 6 standards, providing performance of up to 250 MHz.
- IEEE 802.11a/b/g/n standards (2412-2462MHz) (FCC), (5475-5725MHz) (CE), (5745-5825MHz) (FCC).
- Encryption standard must compile with 802.11i with AES-CCM & TKIP Encryption, 802.1x, 64/128/152bit WEP.
- Wireless data transfer speed up to target of 300Mbps.
- Wireless nodes peer-to-peer exceed a target of 1 km in range in line of sight environments.
- Port forwarding / tunneling allowing an external user to reach a port on a private IP address (inside the LAN) from the outside WAN connection.
- Administration of the system must support hypertext transfer protocol over secure socket layer (HTTPS) and an additional encryption/authentication layer between the HTTP and TCP.
- VoIP wired terminals support multi-line usage with up to 11 line indicators (expandable to 100 lines).
- VoIP wired terminals must support dual 10/100Mbps Ethernet ports.
- VoIP wired terminals must support basic enterprise call features (e.g. caller ID display or block, call waiting, hold, mute, speaker, transfer (blind or attended), forward, and 3-way conferencing.
- Interconnection of radio-over-IP (RoIP) interfaces allowing LMR radio to broadcast over SIP network.
- Connection of analog telephones or POTS terminals.
- Call types required in the RPCK or RCCS PBX.
- Activity Detection - Activity detect call feature, which provides an integrated voice terminal user a visual indication of voice activity of a particular terminal.
- Alternates / Fail-over Trunk - Automatic trunking fail-over if a primary voice trunk is determined busy, the system will switch to the next available trunk, this operation must be seamless to the terminal.
- Announcement on Hold (AoH) - Allow callers to listen to a recorded announcement\s to callers on hold or to a predefined extension. The system shall allow for one or more audio channels to be programmed to distribute audio information that is pertinent to the operation.
- Assigned Access - It shall be possible for selected dial terminals to have an assigned access (by class of service) to any combination of the following: individual nets, public address systems, radio trunks, and PSTN connections. Terminals assigned such access shall be able to obtain the desired connection by keying the appropriate number from the Address Numbering Plan, and terminals that attempt to complete a call to a destination to which access has not been assigned will receive an unavailable tone.

- Automated Attendant (AA) - The PBX shall allow callers to be automatically transferred to a user's extension without the intervention of a live receptionist. (e.g. select 1 for EOC, 2 for Field Director)
- Blacklists - The PBX must have the capability of using a list of persons or organizations that have incurred disapproval or suspicion and therefore the call is rejected by the system.
- Call Details - The PBX shall make record and a log of all calls made including:
    - Source number, destination number, call duration, date, and time.
- Call Forward - The PBX shall support a telephone call forward capability, for:
    - The user of a particular extension can chose to automatically forward calls to another desired extension or phone if their extension is busy.
    - The user of a particular extension can chose to automatically forward calls to another extension if not answered after a defined number of rings.
- Call Groups - The PBX shall support a telephone call groups' capability, for:
    - Rotary hunting (where an incoming call is automatically rerouted to another terminal in a call group if the first terminal is busy, unavailable, or is not answered during the ring time out period.
    - Call pickup within a call group (where any terminal in a call group can pick up a ringing call to a group member, by dialing a designated call pickup number).
- Call Monitoring - A call monitor capability shall be supported to allow supervisors or trusted users to listen or tap into an active call with out alerting the other parties of the monitoring.
- Call Queuing - Allows multiple calls to be placed in a queue and answered by the next available call group or extension.
- Call Recording - The PBX shall support recording audio of a phone conversation for later playback or retrieval.
- Call Transfer, Hold - Once a call is connected, it shall be possible to place the call on "Hold" "Transfer" by pressing the feature code.
- The PBX must have the ability to blind transfer a call to another extension without the need to wait for the other extension to pick up.
- The PBX must have the ability to transfer a call to another extension without the need for the other extension to pick up before the call is transferred.
- The PBX must allow a call to be placed on hold. A call hold capability shall be available to all PBX subscribers who are involved in a two party call.

- Caller ID:
    - The specific terminals will display the caller's phone number on the phones screen.
    - Remote phone must send caller's ID.
    - The specific terminal will display the phone number of a second caller whilst talking to the first caller.
    - The PBX must have the ability for an administrator to change or correct the outgoing caller ID information.
- Conference Bridging - It shall be possible to host a conference bridge or room that multiple parties at multiple locations using different phone types can access. All conference bridges will have the ability to be password protected by the administrator choice. (e.g. conference calls on a local extension, remote fixed line, mobile and VoIP connection all in one conference.)
- Extensions Numbering - The PBX shall have a true flexible numbering plan feature, whereby any number from "0" to "9999" may be assigned to stations or feature codes.
- Hot-line Trunk - The PBX shall have the ability to assign designated trunks to ring designated extensions.

- Interactive Directory Listing (IDL) - IDL allows the inbound callers to lookup a person's extension by their name.
- Paging - All terminals will have the ability to 'dial direct' to an overhead speaker and or capable terminal that can be grouped or zoned for announcement or an alert to be made.
- Protocol Conversion - This allows the interconnection of disparate phone networks: (e.g. connect a Telstra call to a VoIP call.)
- Standard protocols supported include: TDM, SIP, H.323, LAX, SCCP.
- Radio Device Connection:
    - The PBX must allow the interconnection of analog terminals (e.g. Two Way Radio, Land Mobile Radio, and other like devices)
- Remote Call Pickup - This allows a call to be picked up at a remote terminal location.
- Remote Office Support - Ability to connect phones located in a remote office to the office system as local extensions.
- Speed Dialing - Speed dial numbers shall be programmable at both the local level (speed dialing numbers that are applied to a unique terminal) and at the global level (speed dialing numbers that are applied to all terminals). Each local level speed calling list is unique to a specific terminal while the global level is available to all configured terminals.
- Three-Way Calling - Connect three people into a mini conference call.
- Voice-Mail - The PBX must have the ability to record a message from a caller when you are away from your desk. This includes ability to deliver the voice-mail message via email as well as the standard flashing light on your terminal (this feature is terminal specific).
- Satellite services when they are needed.

Key Performance Parameters (KPPs) for Satellite Services for the RPCK

- VSAT data terminal shall have the capability for Star and SCPC configurations.
- VSAT data terminal shall support at least 4 public IP addresses.
- VSAT data terminal shall support an 8 Port 10/100 Ethernet Switch.
- VSAT data terminal shall support Ku-band.
- VSAT data terminal shall support auto antenna acquisition with one button push operation.
- VSAT data terminal shall support TCP/IP throughput of transmit of 18 Mbps and receive 4.2 Mbps.
- BGAN data terminal shall support TCP/IP throughput of transmit of 464 kbps and receive 448 kbps.
- BGAN data terminal shall support audible tone signal strength for manual acquisition.
- BGAN data terminal must meet IP-54 rating (dust and spray proof in all directions).

Key Performance Parameters (KPPs) for SoS Framework and Software

- Provide for modular system development and composition.
- Provide a method for brokering transactions amongst the composed subsystems.
- Provide translators that act as proxies for services, translating requests/responses into and out of a common, shared format (our XML-based language).
- Provide a method for definition of composition of services.
- Provide for communications among/between asymmetric clients.
- Respond to other well-known communications protocols for discrete info (including, for example, Jabber et al)
- Be able to render audio and video supplied in various formats.
- Be able to capture audio and video in some number of oft-supported formats.
- Provide a method for publishing availability/capabilities to other possible clients.

- Provide for authentication of credentials and access to identity information.
- Provide for transport of content in cases where peer-to-peer is not possible due to underlying network configuration.
- Provide for ad hoc network creation where indicated.
- Provide for store and forward of data where required (in, for example, cases where a client is not available at the time of original sending).
- Provide a method of finding clients with known characteristics.
- Provide a method for decoupling content itself from the method for transporting said content to other clients.
- Provide for data transport.
- Provide for control/throttling of data transfer (particularly streamed data transfer) to ensure the viability of the local network as a whole.
- Support the Federal efforts to provide extended alerting:
    - Commercial Mobile Alert System (CMAS).
    - Common Alerting Protocol (CAP).
    - Existing broadcast alert services.
- Provide a mechanism for Trusted Identity Management.
    - National Incident Management System (NIMS) requirements (SP 800-73, SP 800-78, SP 800-79, IR 6887).
    - Homeland Security Presidential Directive 12 (HSPD-12) and Federal Information Processing Standard (FIPS) 201 compliance and support.
    - First Responder Identification Credential (FRAC) support.
        - Public Law 110-53 compliance.

4.3.3 Interoperability

Interoperability provided by software that creates a communication framework enables any IP device or system to create a system of systems allowing interconnectivity between any IPv4 or IPv6 user device and multiple IPv4 or IPv6 networks. Any FERP can communicate using voice, video or share data with any other FERP; limited only by the capability of their device (i.e. a LMR would be limited to voice communications only, for example). The FERP can communicate with their ERO and can collaborate with other agencies and FROs, National Guard, military response teams or private sector security that may be responding to the incident. If responding organizations do not have the software prior to the incident, the SoS software that is included with every RPCK can be freely distributed from any FERP to anyone who needs it. This allows interoperability to be dynamic, changing to meet the communication needs as the response grows and evolves.
The only requirement for interoperability is that the FERPs terminal or device has an IP or MAC address. If the use of analog devices are part of the EROs response plan the analog network can be given an IP or MAC address by connecting one of the analog terminals using the analog network be connected to a patchwork interoperability switch that in turn is a part of the SoS.

4.3.4 Human Interface Requirements

Based on the type of communications framework required by this ORD, the strength of a system of systems, is based on software that will run on any operating system, which will run on an IPv4 or IPv6 networks. There are no special human interface requirements other than knowing how to use a common phone, a LMR or computer. If the FERP can access and use day-to-day computer applications used by the ERO, then they should be able to run the SoS software. It is, in fact easier than sending an email. The FERP can use devices and terminals they already use.

Since the RPCK standard form factor will weigh less than 40lbs, any FERP can hand carry the kit, if necessary. The SoS and RPCK should require no specialized personnel at the incident site. Any FERP should be able to set up a RPCK within 10 to 20 minutes even if they have no experience or

training. No matter how well designed the system is, systems can require support due to user, hardware or software malfunction. If for any reason support should be required due to equipment failure, the user must be able to use the troubleshooting guide included with the system. Around-the-clock telephone and online support shall be available from the RPCK provider. The human interface requirement for this system assumes that the FERP to be able to read simple instructions.

4.3.5 Logistics and Readiness

The SoS will be available and utilized constantly by EROs. It can provide inter-agency interoperability on a daily basis and be in operation when an incident occurs. As the FERP arrives at the incident site, interoperability and collaboration are immediately available just by the FERP turning on the devices they are using as the FERP connects automatically to the SoS.

In order to facilitate interoperability with EROs and FERPs that do not have the SoS software, the software shall be available to every FERP on a USB thumb-drive that can be used to freely install on any computer required to join the SoS. The installation software should also be available to load on ERO servers so that the software can be freely downloaded if necessary. The SoS software should also be downloadable from approved websites with proper security clearance. Installation of the software shall be quick, simple and intuitive. No training should be necessary for any FERP to install the software and connect to the SoS.

If the device is only able to run on an IPv4 network, free VPN software must be available for installation. Installing and using the VPN should require no configuration. If a VPN is needed, it should be as simple as clicking on “install VPN” and the VPN must automatically install, configure and connect the FERP to the SoS via the VPN.

If software updates are released for the SoS or RPCK, a release method of free upgrading will be implemented by a vendor.

At least one RPCK should be available to every ERO in the country. Because a requirement for the RPCK is that it be a self-contained kit, distribution of new kits, additional kits, accessories such as additional VoIP handsets, cameras, headsets, cables, satellite systems may be managed under a contract with a national technology logistics company. Logistics must be handled by an organization, which specializes in delivering network technology efficiently to the public/private sector. Efficient distribution and parts should be stored in strategically located sites in order to guarantee delivery to the ERO in less than eight hours. An efficient inventory method should be used to avoid using potential public funds to stockpile systems. A purchasing system should be instituted to guarantee EROs the ability, once a state of emergency is declared, to order additional systems, parts and accessories immediately.

4.3.6 Other System Characteristics

The SoS and RPCK shall be simple to use and affordable. VoIP services will be provided with a flat rate annual contract for unlimited calls. Every RPCK will have an available satellite option for resiliency, the cost of constant satellite services will be affordable. Flat rate contracts with providers for on-demand satellite service when the RPCK is deployed are required. Every system should always be on and able to support a phone call to the national support center requesting that additional bandwidth be provided for the duration of the incident.

5. System Support

5.1 Maintenance

A maintenance agreement should be available on every SoS system and RPCK.

The SoS will operate 24/7, if issues arise, users can contact a 24/7 support desk. If updates to the SoS software are needed, the update will be sent directly to the user by the support desk and will also be downloadable from a support website.

The RPCK must be used regularly in everyday operations or be required to be tested at least twice a month to be confident that there are no problems with a kit's performance. The day-and-night support center must have the ability to run remote diagnostics on any kit and if possible repair the system remotely. If a kit has a component failure that cannot be immediately fixed at the users' location with the assistance of the support desk, a loaner will be shipped to the ERO immediately. The ERO will ship the "down" system to the repair depot. Under a support maintenance agreement, a loaner system is provided at no charge until their repair kit is returned and tested by the ERO. A ratio of loaners available to kits in service will be at least 1 to 25.

5.2 Supply

The installation software will also be available on ERO servers so that the software can be downloaded from the ERO server, if necessary. The SoS software should also be downloadable from approved, secure websites with proper authorization. Installation of the software must be quick, simple and intuitive. No training should be necessary for any FERP to install the software and connect to the SoS.

Because a requirement of the RPCK is "self-containment," distribution of new kits, additional kits, or loaner kits should be available if a RPCK fails. Accessories such as additional VoIP handsets, cameras, headsets, cables, satellite systems should be managed under a contract with a national technology logistics company that specializes in delivering network technology efficiently to the private/public sector. Efficient distribution requires parts be stored in strategically located depots in order to guarantee delivery to the ERO in less than 8 hours. An efficient inventory method is required to avoid using public funds to stockpile systems. An easy-to-use purchasing system is required to guarantee EROs the ability, once a state of emergency is declared, to order additional systems, parts and accessories immediately.

5.3 Support Equipment

The RPCK will include any equipment necessary for testing and the system must be available to be tested remotely by support, if needed. The remote diagnostics will require nothing more than a given customer's approval.

5.4 Training

The SoS and RPCK will be simple enough that user training is not required. However, in order to maximize the power of the SoS and to fully understand what the RPCK is capable of, webinars will be held everyday on a regional basis covering topics that will improve the effective use of the SoS and RPCK. An online group forum will be available for FERPs to share ideas and ask questions of other FERPs. This service will be a feature of the SoS software.

5.5 Transportation and Facilities

The SoS is software and does not require transportation or storage. The RPCK by design must be small enough to store in the trunk of a car or in a closet in the FERPs office or duty station. It will be able to be stored anywhere with a temperature between -10°C and +50°C. The RPCK will require no special transportation; however, it must be available in a form factor that can be mounted in any vehicle, making that vehicle a mobile resilient communication center. It also will be able to be used anywhere at anytime without any special installation being required and easily be transportable as carry-on luggage on any commercial airline.

6. Force Structure

Many homeland security applications rely on resilient communications; there can be no SoS without communications systems to connect to. In order to implement a national SoS providing national interoperability, enough RPCKs must be distributed across the country to provide resilient communication in enough locations to generate a national emergency communication network. It would take 200,000 RPCKs to provide at least one system to each of the following:

Potential system users	Approximate Number
Law enforcement agencies in the United States	**17,000**
Fire departments in the United States	**30,000**
Incorporated cities in the United States	**80,000**
Counties and or Parish Governments in the United States	**3,000**
School Districts and Colleges in the United States	**20,000**
Emergency Operation Centers in the United States	**15,000**
Ports of entry in the United States	**240**
Critical Infrastructure and Key Assets in the United States	**33,000**
Hospitals in the United States	**5,500**

These numbers do not reflect the number of court houses, the number of jails and/or prisons, total number of government facilities (approximately 500,000 buildings) or of High Schools, Middle Schools or Elementary Schools in the United States. The figures above also do not reflect the number of substations and offices within a particular category. If a RPCK was distributed for example to each of the approximately 53,000 fire stations alone in the United States, the infrastructure for a national resilient communications network would be in place.

7. Schedule

The SoS could be rolled out in phases. Year one should establish SoS groups in the most vital areas creating a national framework of senior FERPs, EROs and supporting agencies with a nation-wide roll-out completed in less than three years.

8. System Affordability

The total price for core components to meet the mission described in the ORD shall be less than $20,000 (in high volume production).

9. References

Note: In this document, the terms "product" and "system" are synonymous. The word "system" is used to refer to either.

1. The word expensive as it relates to emergency response communications not only means the acquisition costs of expensive hardware and software, but the costs of ongoing maintenance, training and support costs that many times exceed the cost of the actual hardware and software.

2. The term "scorched earth" here means an incident scene where normal communication infrastructure needed for voice, data and/or video communication has been severely compromised, destroyed or does not exist.

3. Stennis Space Center was without communication infrastructure for over 2 weeks after Hurricane Katrina made land fall.

4. This is an example of what is meant by “pony express." In responding to the disaster created by Hurricane Charley in August of 2004, 17 FROs responding to provide mutual aid to a devastated Hardee County Florida, for days had to rely on passing notes between command posts and having responders drive 45 miles to relay communications to areas not affected by the destruction of the communication infrastructure in southwestern and central Florida.

10. Glossary

Resilient	Recovering readily from injury, adversity, or the like while returning to the original form.
System of Systems	A collection of task-oriented or dedicated systems that pool their resources and capabilities together to obtain a new, more complex, “meta-system” which offers more functionality and performance than simply the sum of the constituent systems.
Dynamic Interoperability	A property referring to the ability of diverse systems and organizations to work together (inter-operate) characterized by continuous change, activity, or progress.
IPv4	Internet Protocol version 4 (IPv4) is the fourth iteration of the Internet Protocol (IP) and it is the first version of the protocol to be widely deployed. IPv4 is the dominant network layer protocol on the Internet and apart from IPv6 it is the only standard internetwork-layer protocol used on the Internet. IPv4 is a data-oriented protocol to be used on a packet switched internetwork (e.g., Ethernet). It is a best effort protocol in that it does not guarantee delivery. It does not make any guarantees on the correctness of the data; this may result in duplicated packets or packets delivered out of order. These aspects are addressed by an upper layer protocol (e.g., TCP and partly by UDP).
IPv6	Internet Protocol version 6 (IPv6) is a network layer for packet-switched internetworks. It is designated as the successor of IPv4, the current version of the Internet Protocol, for general use on the Internet. The main change brought by IPv6 is a much larger address space that allows greater flexibility in assigning addresses. The large number of addresses allows a hierarchical allocation of addresses that make routing and renumbering simpler. With IPv4, complex CIDR techniques were developed to make the best possible use of a restricted address space. Renumbering, when changing

	providers, can be a major effort with IPv4. With IPv6, however, renumbering becomes largely automatic, because the host identifiers are decoupled from the network provider identifier.
COTS	Commercial-off-the-shelf
ERO	Emergency response organization
FERP	First emergency response provider
RPCK	Resilient portable communications kit
RCCS	Resilient communication command system
NCRN	National communication resiliency network
GUI	Graphical user interface
QoS	Quality of service
IACC	Incident area command center
OSI	Open systems interconnection