GENERAL DYNAMICS C4 SYSTEMS

General Dynamics Recommendations to the Technical Advisory Board for First Responder Interoperability

May 1, 2012

Copyright © 2012, General Dynamics C4 Systems

Contents

1 Executive Summary 1
2 Background 1
3 Specific Recommendations 2
3.1 Recommendation 1 – Converged LMR/LTE User Equipment 2
3.2 Recommendation 2 – Mesh Networks/MANETs 5
3.3 Recommendation 3 – Advanced security features 7
3.4 Recommendation 4 – Early demonstrations 9
3.5 Recommendation 5 – Open, accessible acquisition strategy 9
4 General Dynamics Programs and Capabilities Relevant to Public Safety Communications 10
4.1 Department of Homeland Security/US Coast Guard: Rescue 21 10
4.2 Department of Justice: Integrated Wireless Network 11
4.3 Department of Homeland Security/US Secret Service: TacCom (Tactical Communications) 12
4.4 Pathmaker™ Technology 13
4.5 Network Deployment Capability 15
5 Conclusion 15

1 Executive Summary

The U.S. Federal Communications Commission recently solicited comments "from interested parties desiring to contribute materials for the Interoperability Board to consider in developing its recommendations" relevant to the National Public Safety Broadband Wireless Network (DA 12-474, March 26, 2012). General Dynamics C4 Systems, a market leader in communications networks, is submitting five recommendations to the Interoperability Board. These recommendations are:

(1) Include standards for converged LMR/LTE User Equipment;
(2) Include standards to support mesh networks;
(3) Include advanced security features;
(4) Conduct early demonstrations; and
(5) Maintain an open, accessible acquisition strategy.

2 Background

Title VI of the Middle Class Tax Relief and Job Creation Act of 2012 (Public Law 112-96, "the 2012 Act") mandates various actions including the establishment of a Technical Advisory Board for First Responder Interoperability ("the Interoperability Board"). Per Section 6203 of the 2012 Act, the Interoperability Board will develop recommended minimum technical requirements to ensure a nationwide level of interoperability for the nationwide public safety broadband network, and submit these recommendations to the Federal Communications Commission (FCC). These recommendations will have a significant impact on the development of a future single, national, interoperable public safety broadband wireless network. The Interoperability Board's recommendations will also impact the ability of private sector entities to conduct business in the public safety communications market.

In the interests of fostering development of a successful broadband wireless network for the public safety community, and maintaining continued free and open competition in this market, General Dynamics C4 Systems ("GDC4S") is respectfully submitting recommendations to the Interoperability Board. GDC4S is qualified to comment because it has a large established market position in the wireless broadband market, with business interests spanning communications networks in the commercial and government (including public safety and military) markets. See Section 4.

GDC4S recognizes the public safety community is experiencing a generational shift in technology that will revolutionize the way it communicates. 4G (Fourth Generation) broadband wireless technology has emerged as a commercially viable capability. 4G offers mobile data rates that will enable deployment of a new generation of mission critical data and multimedia applications. These applications improve the ability of public safety personnel to perform their diverse missions. The public safety community seeks to leverage these latest developments in commercially available wireless technology, but without sacrificing heritage LMR (Land Mobile Radio)-unique capabilities that are not yet implemented in broadband technology. Although heritage LMR technology has limited data capabilities, non-standardized stand-alone proprietary systems in the thousands, and non-contiguous, inefficient spectrum assignments, it nonetheless enjoys a large installed base. An extended transition period is therefore likely.

GDC4S is committed to support this transition, which will occur over the next five to ten years. Over the coming decade, the public safety community will reap the benefits of technology progress that is driven by private investment for the much larger commercial markets. The prudent selection of commercial LTE (Long Term Evolution) as the 4G wireless access technology for public safety allows the community to leverage commercial investment, and finally achieve nationwide interoperable communications governed by a globally accepted industry standard with an unlimited applications horizon. However, maximum leverage from commercial investment will most likely ensue only when economies of scale operate and market competition flourishes. We respectfully submit our views on preserving this efficient, competitive environment for consideration by the Interoperability Board.

3 Specific Recommendations

GDC4S' five specific recommendations are listed here in summary form:

Recommendation 1 – Include features and interoperability standards to support development of a converged LMR/LTE User Equipment terminal that supports public safety applications.

Recommendation 2 – Include Mesh Network/MANET capability and interoperability standards in the solution architecture for public safety.

Recommendation 3 – Include advanced security features and interoperability standards in Public Safety interoperability standards.

Recommendation 4 – Advocate early demonstrations in a public-private context.

Recommendation 5 – Maintain an open, accessible acquisition strategy.

3.1 Recommendation 1 – Converged LMR/LTE User Equipment

GDC4S recommends the Interoperability Board include features and interoperability standards to support development of a converged LMR/LTE User Equipment terminal that supports public safety applications. These standards should facilitate convergence, in a single device, of today's LMR capabilities with broadband-based voice, video, and data. Convergence will create a more integrated, convenient, and capable family of User Equipment terminals for the public safety community.

To meet the unique needs of the public safety community, GDC4S believes that the integration of P25-standard and 4G broadband wireless functionality into a single multimode device is inevitable (Figure 1). P25 is the primary U.S. standard for the LMR technology. In the longer term, public safety-specific capabilities and commercial device technologies will converge as both transition to 4G LTE systems. With proper engineering, multimode devices will provide a viable commercial business case for manufacturers.

Multimode devices will support the unique mission critical needs of the public safety community and provide desirable high speed data capabilities and access to broadband applications. These devices will require the infrastructure to support mobility and handover as the multimode user moves across coverage areas with differing Radio Access Technologies (RAT), for example LMR-to-4G mobility. The 3rd Generation Partnership Project (3GPP) Release 8 specifications define the LTE architecture and already include the specific interfaces that are required to support intermodal roaming, including roaming to CDMA (Code Division Multiple Access) and GSM (Global System for Mobile Communications) networks. However, standards to support roaming between LMR and 4G technologies await definition.

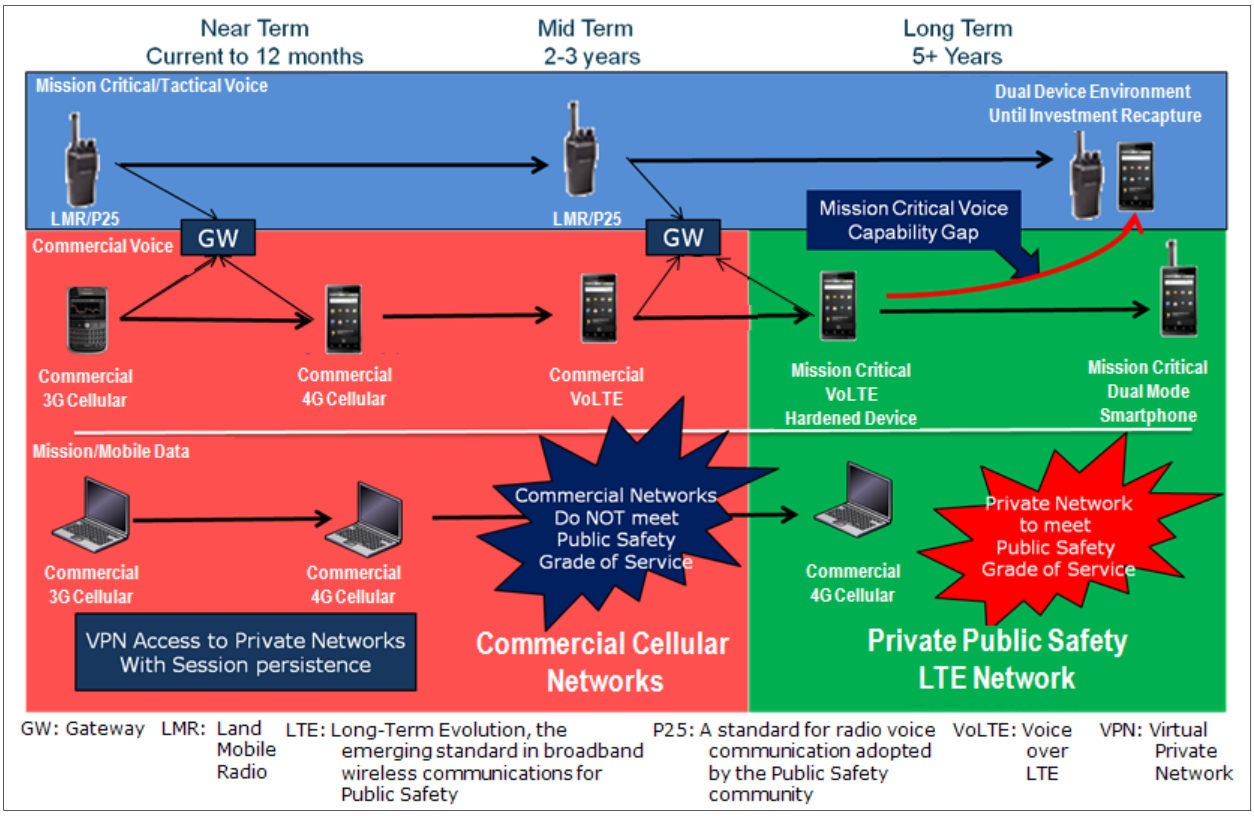


Figure 1. Transition to multimode devices supporting mission critical voice and broadband applications.

Native 4G multimode devices will eventually support a new LMR mode which provides true public safety-grade capabilities. These two technologies will be integrated seamlessly together in Network Level Gateways, which will provide seamless interworking between legacy LMR systems and the new 4G systems. Obsolescence will be minimized through the use of commercial platforms which support multiple modes of operation, and through use of technologies such as soft radios as enablers for LMR capabilities.

While new public safety grade multimode devices and interoperability standards are being developed, GDC4S anticipates that Federal, state, and local subscribers who have commercial mobile broadband devices will use PTT/VoIP (Push-to-Talk Voice over Internet Protocol) technology, such as Twisted Pair's Mobile Communicator product, to interoperate with their legacy deployed P25 LMR systems through the use of Network Packet Gateways. The new

gateways are superior to currently deployed Radio Gateways because Network Gateways are more scalable, more flexible, more capable of passing caller information between networks, support more levels of prioritization, and have better audio quality.

The current level of public safety interoperability maturity supports narrowband public safety Radio Access Technologies, such as P25 LMR. Specifically, both P25 trunked and conventional systems can be supported in a single device. Interoperability between systems is typically supported via an interoperability Radio Gateway within the infrastructure. These Gateways allow diverse single-mode devices to communicate. Virtual radio software can be installed on smartphone devices to enable smartphone users to communicate with LMR radio users via Network Level Gateways. Today, several equipment vendors are considering development of multimode devices that support LMR and other RATs, such as LTE, CDMA, and GSM. This includes multimode radios supporting P25 and a wireless broadband interface in a single device.

There is currently no standards activity associated with mobility and handover between LTE (or other cellular Radio Access Networks) and P25 networks. This may be a productive area of inquiry for the Interoperability Board as it develops its standards recommendations.

While these standards are being developed, the same devices commercially available for LTE will soon support public safety in addition to their existing broadband capabilities. These devices will initially be data-only devices (for example, USB sticks), with smart phone devices following in the 2013-2014 timeframe. For example, PSCR (the Public Safety Communications Research program under the U.S. Department of Commerce) is working with public safety practitioners to identify specific devices and categories of devices that can help them achieve the fundamental level of interoperability they need.

GDC4S maintains business relationships with the major LTE public safety vendors. While each vendor's device roadmap is unique, our interpretation of the most likely timeframe and feature set for support of single/multimode LTE public safety devices is shown in Figure 2. The roadmaps for these commercial devices include support for multimode RATs.

Device	Timeframe	Features
USB dongle data adaptor	Available now	Public Safety only (Commercial trials underway)
In-vehicle modem	Available now	PS with 2G/3G roaming support, Wi-Fi
Rugged Handheld	Within one year	PS with 2G/3G roaming support, commercial telephony (CDMA/GSM), Wi-Fi, Bluetooth
Fixed Device	Within two years	PS with 2G/3G roaming support, Wi-Fi

Figure 2. Maturity timeline for public safety User Equipment.

Operating modes for integrated LMR/broadband devices must, at a minimum, support existing LMR services as defined in P25 standards. The use of broadband opens up the possibility for many new services, such as video-based calls, location based services and file sharing. Some services would use a "legacy mode" if not supported on existing devices. For example, a public safety video group call would transmit only the audio portion of the bearer to a legacy user device that is incapable of rendering video.

3.2 Recommendation 2 – Mesh Networks/MANETs

GDC4S recommends the Interoperability Board include Mesh Network/MANET capability and interoperability standards in the solution architecture for public safety. Standards that enable Mesh Network/MANET technology to join the fabric of the emerging national public safety network will enhance its utility and operability. Mesh Networks/MANETs can provide a key gapfiller capability in remote areas. During the decadal transition to denser national network coverage for public safety, this capability will enable better communications for public safety applications ranging from border security to maritime surveillance.

In August 2010, the DOJ (U.S. Department of Justice) COPS (Community Oriented Policing Services) office held the National Forum on Public Safety Broadband Needs. One of the COPS themes was resiliency, defined as:

> "the ability of operable systems to recover from mishap, change, misfortune, or variation in mission or operating requirements. Encompassing the technical aspects as well as the end-user information exchange aspects of interoperable communications, resiliency insures that the interoperability of communications systems is not affected by known or unknown circumstances of change. Resiliency also refers to the ability of the system to evolve and advance as new technologies or capabilities are developed. Furthermore, resiliency is a reflection of the flexibility of the system to respond to changes in operational requirements or implementation strategies and technologies."

The Forum report further highlighted three technology concepts essential to ensure resiliency in an emergency:

> (1) Self-organizing. Self-organizing networks dynamically manage their own configuration by automatically making changes to ensure messages reach their destinations.
> (2) Meshing (ad-hoc device-to-device communication). A type of networking where each node must not only capture and disseminate its own data, but also serve as a relay for other sensor nodes, that is, it must collaborate to propagate the data in the network.
> (3) Adaptability. The ability of the network and/or device to modify/change behavior based upon external conditions.

Wireless mesh networking refers to wireless networks that allow traffic to traverse a network through multiple hops across wireless relay devices, or nodes. Mesh networks provide the following benefits:

- allow a network to be set up and/or extended quickly and easily without running cables between the nodes, reducing deployment cost and time;
- provide better fault-tolerance if there are multiple paths between nodes, so if a node or path becomes unavailable, an alternate path can be used;
- support mobile nodes in applications such as vehicle networking where running cable is impractical;
- support dynamic network environments between vehicle convoys or groups of dismounted personnel where nodes may regularly join or leave the network and the connectivity between nodes may change frequently; and
- provide better in-building support where mesh nodes within buildings can relay communications to the main radio systems outside of the building.

In short, a “mesh” network can be described as self-forming (the network forms with little or no user intervention), self-healing (the network can route around a failed node), and path optimizing (the network uses the optimal path between any nodes.)

Mesh capabilities are necessary for many outdoor and tactical wireless solutions because these deployments often contain mobile nodes that can leave and rejoin the network as they travel from one location to another. In a dynamic network environment where nodes are mobile or temporary, a mesh solution ensures a level of fault-tolerance since network paths can be re-calculated on the fly as the network changes. Mobile mesh networks are enclave networks and/or semi-detached networks connected to the outside world with a slower satellite link. Multicast can constitute a significant percentage (approximately 80 percent) of mobile mesh traffic, driven by video applications. In mobile environments, mesh points are attached to individuals and vehicles. In mobile networks, a mix of radio technologies is typically employed to meet the challenging performance needs of these networks. Finally, mobile mesh networks must meet significant security requirements.

Using radio frequency technologies in conjunction with mesh networking creates a networking paradigm that provides greater coverage, throughput, and mobility. Wireless mesh networking also allows for faster deployment and more flexibility for nodes to join, leave or create their own networks.

A MANET (Mobile Ad hoc NETwork) is a self-configuring infrastructure-less network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each forwards traffic unrelated to its own use, acting as a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a type of wireless ad hoc network that usually has a routable networking environment on top of an ad hoc network.

This paradigm is particularly well-suited for mobile environments such as emergency response where network nodes need to be quickly deployed and highly mobile. To be effective, the network must support situational awareness and command and control applications which often include the transmission of sensitive data, video surveillance, mapping overlays and VoIP (Voice over Internet Protocol). When combined with appropriate security, wireless mesh networking is the best way to provide the requisite coverage, flexibility, and throughput for these applications.

The suitability of these solutions for outdoor, indoor, mobile, and tactical environments is characterized by these attributes:

- Performance – throughput and latency
- Scalability – performance independent of the number of nodes
- Mobility – movement of nodes
- Security – appropriate security protocols and certifications
- Media Independence – accommodate heterogeneous wireless infrastructures

These attributes support public safety applications such as emergency response, border security, vehicle-based networks, deployed operations/event management, unmanned sensors, and maritime domain awareness.

While MANET/mesh network technologies are mature, today there is a paucity of standards and many implementations remain vendor-specific. The Interoperability Board may wish to consider development of standards for the listed attributes as they relate to MANET/mesh networks for public safety.

3.3 Recommendation 3 – Advanced security features

GDC4S recommends inclusion of advanced security features and development of interoperability standards that embrace a comprehensive approach to security for the network and its users. Security standards should leverage recent advanced in the national cybersecurity domain, including enterprise-level security management and secure mobility.

Security in national networks such as the National Public Safety Wireless Broadband Network cannot be implemented piecemeal. Implementing a truly secure capability requires a system-wide perspective and understanding of the interdependencies of the components, as well as their individual vulnerabilities. The security approach must address all the elements within the system: users; endpoints (handhelds, laptops, desktops, and servers); networking and infrastructure equipment (firewalls, routers, switches, and encryptors); as well as the critical and sensitive information on the network. Both data in motion and data at rest must be protected. One general model (discussed by the panelists at the Interoperability Board workshop held on April 23, 2012 at the FCC) maintains that networking and infrastructure equipment that will support the future National Public Safety Wireless Broadband Network is roughly analogous to that existing today. Therefore, according to the panelists, models for today's security and cybersecurity environments for network and infrastructure provide adequate models for the near- to medium-term future, but additional focus is needed on the endpoint User Equipment.

GDC4S recommends to the Interoperability Board that standard models such as ESM (Enterprise Security Management) should be examined for enterprise-level use in the future national network. A recent presentation by a U.S. Intelligence Community Information Assurance leader characterized Enterprise Security Management functions as divided into three major classes:

(1) Identity Management – consisting of issuing identities, managing identity credentials, authenticating those credentials, and managing identity attributes;
(2) Authorization Management – consisting of managing digital policies, managing privileges, and managing Information Assurance "metadata" or data describing data; and
(3) Provisioning Management – consisting of managing cryptologic keys, configurations, and auditing.

ESM is viewed as a stable framework for addressing network security. As a result of the national focus on cybersecurity, ESM already has a development and research community focused on securing networks. The ESM model, recently advocated by elements of the U.S. Intelligence Community, has broader applicability for enterprise-wide networks including for public safety.

In the public safety context, ESM approaches can be used to implement public safety-specific access control for all human, machine, and data entities in the system. Constraints imposed by operational factors (e.g. Law Enforcement Sensitive databases), legal regimes (e.g. personal health records), or National Security categories (e.g. traveler watch lists) will probably engender a dynamic multi-level security regime for the National Public Safety Wireless Broadband Network. In these regimes, human, machine, and data entities are assigned security enclave privileges where there is "need to share," but denied access where there is "need to protect." Again, standards developed in the US Intelligence Community, which includes DHS (the U.S. Department of Homeland Security) and DOJ, could serve as a model for consideration by the Interoperability Board.

Figure 3 summarizes the capabilities and technologies we view as essential for securing the National Public Safety Wireless Broadband Network:

Capability	Description
Identity & Access Management	• Strong identity solutions for human users and devices • Network access control solutions based on device configuration and health • Data access control based on need and user privileges • Trusted computing for endpoint integrity
Multi-Level Security Solutions	Allow for sharing among different organizations/compartments, etc, based on mission need and policy
Transactional Audit	Allow visibility and insight into what devices are on the network, their status and what data is being shared
Situational Awareness using Visualization/Collaboration	Situational awareness of network security posture, asset management and logistics planning

Figure 3. Essential capabilities for advanced security in future national networks.

Turning from enterprise-level to endpoint-level security, the Interoperability Board should consider and rapidly arrive at a functional definition and standards for security "good enough" for use by the public safety community. Based on prior GDC4S-funded studies, functionality for "good enough" should include at a minimum:

- User authentication before application launch;
- Endpoint authentication before use (whether application-to-application or application-to-server);
- Confidentiality and integrity for data at rest and data in motion;
- Support for unprotected data storage and messaging within a security or physical enclave; and
- Security functions operate even lacking network connectivity.

For the endpoint security solution (chiefly User Equipment), industry is developing security architectures for MDM (Mobile Device Management) regimes at various levels from the application to the enterprise. There are several paths that the Interoperability Board may wish

explore. For example, in the Android context there are security models under consideration at four levels:

(1) Securing the application;
(2) Securing the operating system (using hypervisor or Trusted Root technology);
(3) Securing the enterprise for Sensitive but Unclassified information; and
(4) Securing the enterprise for classified information.

Depending on sensitivity, at a less rigorous security level, MDM functions might include: remote wipe (total and selective), remote lock, report audit information, report software configuration, detect "jail broken" and "rooted" devices, remote password management/reset, and over-the-air software updates. More rigorous security might include: tamper-resistant reporting of integrity status (attestation), strongly authenticated over-the-air software updates and rekey, dynamic policy updates, remote device reconfiguration, Information Assurance compliance via SCAP (Security Content Automation Protocol) reporting, and multiple virtual machine/multi level security capability. Standardization of these security levels of services should be considered by the Interoperability Board.

3.4 Recommendation 4 – Early demonstrations

GDC4S recommends an incremental approach to development of the emerging National Public Safety Wireless Broadband Network, including prototyping, pilots, user involvement, early demonstrations, and public-private partnerships.

GDC4S advocates that the Interoperability Board urge the Commission and FirstNet to include early demonstrations and pilots in the buildout of the future national network. As panelist Patrik Ringqvist opined to the Interoperability Board during the April 23, 2012 workshop at the FCC, standards alone do not guarantee success. Ringqvist further noted that a development approach based on planning, incremental testing, learning, and feedback is also a key enabler of success. We encourage the Interoperability Board to consider approaches to standards that support implementation based on early laboratory and fielded demonstrations, partnerships between industry and the public sector, incremental testing, rapid development and prototyping cycles ("spins") and interagency involvement with public safety-centric agencies such as DHS and DOJ, and regional, state, local, and tribal first responders. For example, we note emerging plans in some Federal agencies for broadband wireless demonstrators and the existence of several Government programs of record (see Sections 4.1 – 4.3 below for examples) which could provide the Government with a potential contractual framework for early experiments to begin incremental progress on the national network.

3.5 Recommendation 5 – Open, accessible acquisition strategy

The charter of the Interoperability Board under the 2012 Act – to recommend standards for the implementation of the National Public Safety Wireless Broadband Network – is rooted in the realization that many vendors, manufacturers, integrators, and public agencies will be partners in building the network. The recognized need for standards is an acknowledgement that a monolithic development cannot provide the public safety community with the competition, innovation, and resultant cost savings it needs to thrive. Therefore, we urge the Interoperability

Board to recommend a set of standards that engenders modularity, allows for regional and local spans of control, eases integration at all levels and of all necessary capabilities (including security), fosters service provision competition as a business model, and includes open architectures to allow for innovation and continued access to markets by all. An open, accessible acquisition strategy will facilitate innovation.

4 General Dynamics Programs and Capabilities Relevant to Public Safety Communications

4.1 Department of Homeland Security/US Coast Guard: Rescue 21

Rescue 21 (Figure 4) is relevant as an example of a national-scale buildout by GDC4S in support of a key public safety mission. Rescue 21 is the United States Coast Guard's advanced command, control and communications system. Created to improve the ability to assist mariners in distress and save lives and property at sea, the system is currently being installed in stages across the United States.

Figure 4. Rescue 21 – a large-scale national public safety communications program.

Almost at completion as of this writing, this vital system provides an updated, leading-edge Very High Frequency – Frequency Modulated communications system, replacing the National Distress Response System installed and deployed during the 1970s. Rescue 21 covers coastline, navigable rivers and waterways in the continental United States, Alaska, Hawaii, Guam and Puerto Rico. By replacing outdated legacy technology with a fully integrated system, Rescue 21 provides the Coast Guard with upgraded tools and technology to protect the nation's coasts and

rescue mariners at sea. By harnessing global positioning and cutting-edge communications technology, Rescue 21 enables the Coast Guard to perform all missions with greater agility and efficiency. The new system will close 88 known coverage gaps in coastal areas of the United States, enhancing the safety of life at sea. The system's expanded system frequency capacity enables greater coordination with DHS, as well as other Federal, state, and local agencies and first responders.

Rescue 21 replaces a wide range of aging, obsolete radio communications equipment to include: consoles at Coast Guard Sectors and Stations, remote transceiver sites (antenna towers), as well as the network connecting them to the facilities above. GDC4S is the contractor to replace the Coast Guard's outdated system in the contiguous 48 States and Hawaii. (The Coast Guard assumed the role of system integrator for deployment to sectors in Alaska.) Rescue 21 revolutionizes how the Coast Guard uses command, control, and communications for all missions within the coastal zone. The system incorporates direction-finding equipment to improve locating mariners in distress, improves interoperability among federal, state, and local agencies, enhances clarity of distress calls, allows simultaneous channel monitoring, upgrades the playback and recording feature of distress calls, reduces coverage gaps for coastal communications and along navigable rivers and waterways, supports Digital Selective Calling for registered users, and provides portable towers for restoration of communications during emergencies or natural disasters. The Rescue 21 service area covers more than 40,000 miles of coastline.

4.2 Department of Justice: Integrated Wireless Network

IWN (Integrated Wireless Network, Figure 5) is relevant as an example of an advanced LMR system that incorporates features desirable for future public safety communications architectures. IWN provides valuable lessons learned for future LMR/LTE convergence. IWN was designed to replace aging and increasingly unreliable LMR systems that were in place at DOJ. IWN consolidates the multiple communications systems into a single P25 standard-based system available to all Federal law enforcement, and is extensible for non-Federal users. IWN provides real-time interoperability for all agents across agencies on the system, ending the practice of physically exchanging radios during joint operations.

GDC4S is the IWN system integrator designing a shared system to consolidate existing diverse networks. The DOJ regionalization strategy for IWN segments divided the country into six geographic regions. DOJ accepted the NCR (National Capital Region) IWN system in 2011. As of this writing, an expanded NCR demonstration is in progress. The NCR system comprises 15 radio sites (a threefold savings), 2 switching sites, 44 agency dispatch centers, and 1 System Operations Center. More than 7000 mobile and portable radios are supported for users from the Federal Bureau of Investigation; the U.S. Drug Enforcement Agency; the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives; the U.S. Treasury; the U.S. Marshals; and the U.S. Park Police. Additional agencies such as DHS components or state, local and tribal entities can easily be added to IWN at any time.

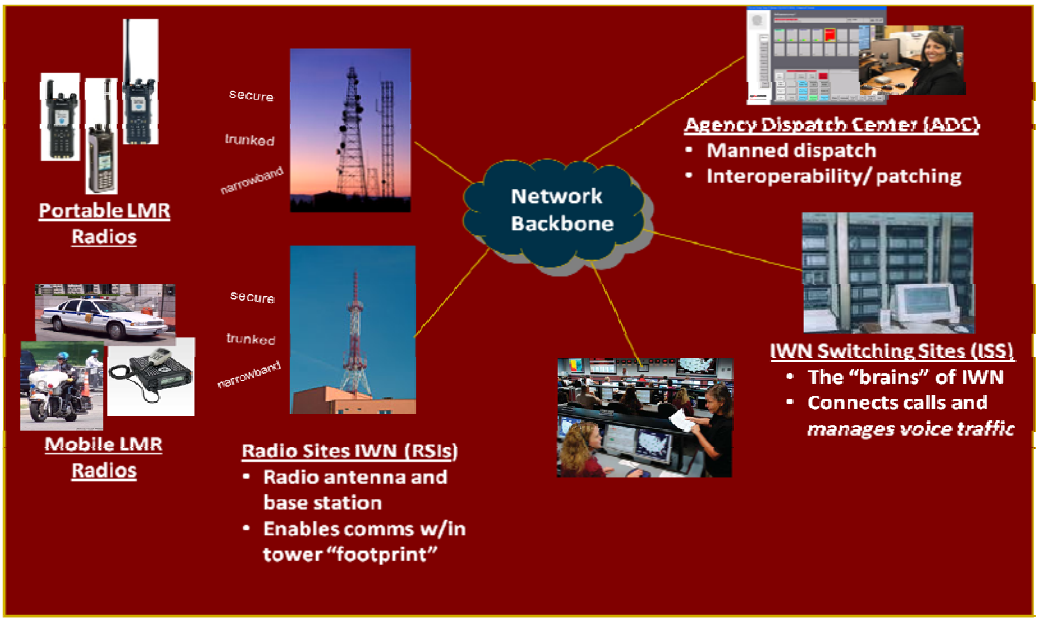


Figure 5. IWN – a transitional LMR program.

The fivefold solution objectives of IWN are directly relevant to future work in public safety communications for the national network:

(1) Security – AES (Advanced Encryption System) encryption provides secure voice traffic for agents, a major upgrade from current outdated encryption standard.
(2) Reliability – State-of-the-art trunked LMR hardware and network performance management provide agents with greater than 99 percent system availability.
(3) Efficiency – The narrowbanded system uses 50 percent less radio spectrum and consolidates agencies onto a single, shared VHF network that preserves agency operational autonomy.
(4) Productivity – User-friendly features (e.g., over-the-air-rekey; roaming) allow agents to focus on mission duties, rather than managing their radios.
(5) Interoperability – Use of open standards (P25) and Internet Protocol enables a multi-vendor environment that is upgradeable to data applications/smart phones.

4.3 Department of Homeland Security/US Secret Service: TacCom (Tactical Communications)

TacCom is an example of a GDC4S IDIQ (Indefinite Delivery/Indefinite Quantity) contract for flexibly and responsibly provisioning public safety communications. TacCom is relevant because it is a model of a comprehensive acquisition and contract structure for network buildout on a large scale for public safety agencies. TacCom is a DHS multiple-award contract vehicle. The new contract (awardees were notified in March 2012) has a potential of $3 billion for all awardees. Generally, TacCom will provide tactical communications equipment to support mission critical public safety communications for DHS and its components. The specific purpose of the contract is "to support the Department of Homeland Security's purchase of a full array of tactical communications (TacCom) commodity products, infrastructure and services. DHS seeks

to establish a multi-vendor approach to implementing fully interoperable solutions to support mission critical, Public Safety communications." Some of the technical categories include portable/mobile radios, control/base stations, software, upgrades, repeaters, routers, comparator systems, engineering, design, installations, maintenance, frequency managers, spectrum managers, and test equipment/tools. TacCom workscope is awarded in five categories: Subscriber Base, Infrastructure, Infrastructure Services, Operations and Maintenance Services, and Test Equipment. GDC4S was selected for eligibility in all five categories.

The intent of TacCom is "to leverage the Government's buying power to receive high volume discounts and the lowest price possible." Besides the applicability of fiscal probity to acquisitions by FirstNet, additional TacCom acquisition objectives are congruent with those for public safety under the 2012 Act. Multi-vendor interoperability, technical neutrality, and competitive acquisition will all afford valuable lessons learned for the National Public Safety Broadband Wireless Network buildout. A diverse DHS Integrated Project Team supported the Executive Agent for this acquisition, the U.S. Secret Service. The team included Customs and Border Protection, Federal Emergency Management Agency, the Federal Law Enforcement Training Center, the Federal Protective Service, U.S. Immigration and Customs Enforcement, the National Protection and Programs Directorate, the Science and Technology Directorate, the Transportation Security Administration, and the U.S. Coast Guard. Further, TacCom ordering is open to DHS partner agencies and their subordinate components, including the White House Communications Agency, and the Departments of State, Justice, and Interior. This diversity of interests will provide a reasonably broad and representative test bed for applications provisioning for the federal public safety community. As a potential provisioner under FirstNet acquisition, GDC4S will apply lessons learned under TacCom to the future buildout and provisioning in broadband. Further, GDC4S' ability to respond rapidly (response cycles of 7 – 21 days' duration are common) to IDIQ Task Order Requests for Proposal will allow FirstNet to acquire goods and services without long delays, bringing the national network that much closer.

4.4 Pathmaker™ Technology

Pathmaker™ is an example of GDC4S manufacturing and technology innovation that is directly relevant for public safety users in communications-disadvantaged areas. Pathmaker network radios (Figure 6) provide dynamic wireless, mobile, multi-hop, ad hoc networking communications without reliance on network infrastructure. Pathmaker radio users become their own network, which makes the radios ideal for use in remote locations where no infrastructure exists or where the infrastructure has been destroyed or overloaded. Pathmaker operates with existing radio systems to extend coverage.

Where legacy network infrastructure exists, the Pathmaker Network Radio System can take advantage of those networks by providing gateways, thereby increasing the network's footprint and reach. With a capacity of 32 radio users per network, users can form traditional squad communications groups, or extend range and coverage by connecting to multiple networks. Users can communicate privately (one-to-one), as a group (one-to-many), and have multiple private and group sessions. This capability corresponds to "Direct Mode" operations commonly employed in by first responders.

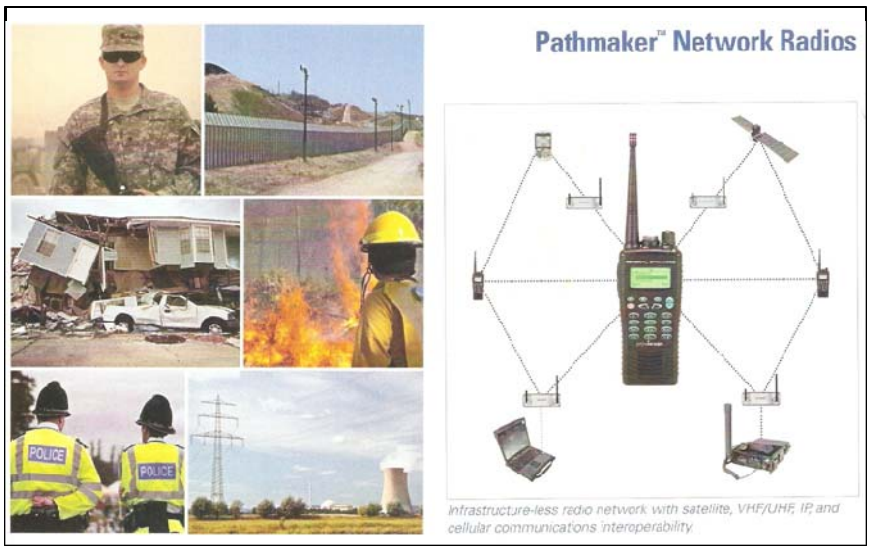


Figure 6. Pathmaker – technology development and production-scale manufacturing.

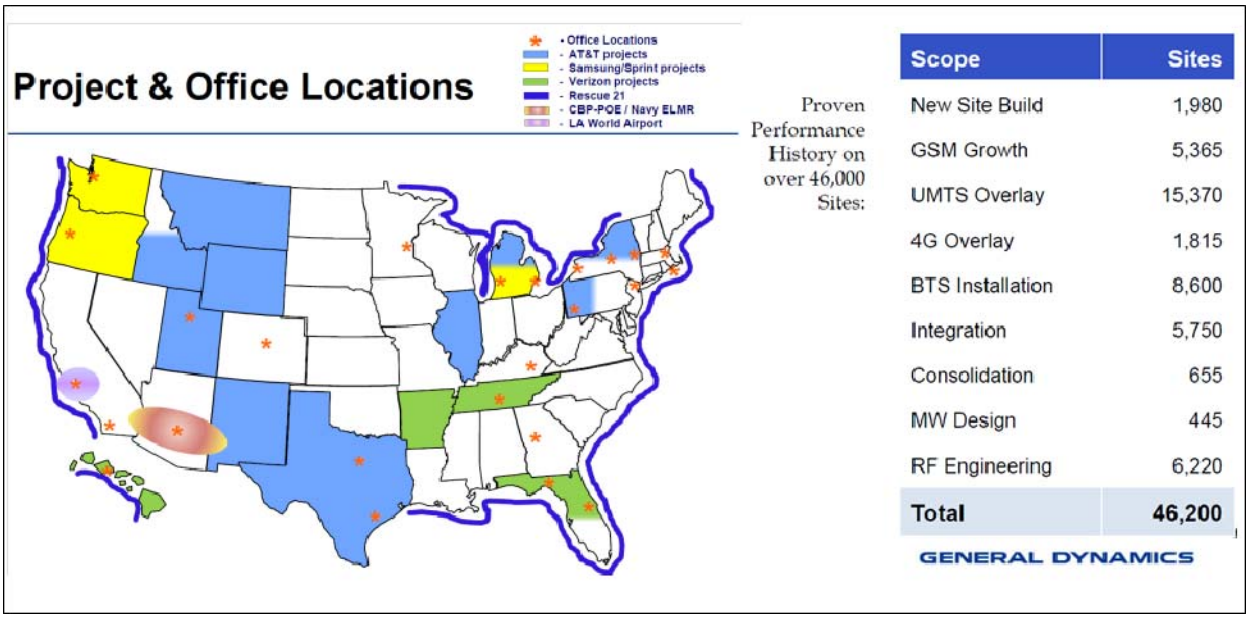
Pathmaker radios are built for critical missions in challenging conditions and provide

- Superior grade voice, data, and video communications, including multiple simultaneous voice and data sessions and unicast, broadcast, and unicast modes
- Text messaging
- Preemption for voice (4 levels) and data (8 levels)
- Multiple sub-networks (groups), with up to 32 radios per group
- Automatically adaptive number of hops (up to 8) according to user position and mobility
- Dynamic allocation up to 32 registered users per channel
- Position location information to track radio users' locations
- Light weight, low power use with 18 hours of battery life
- Network management software for radio configuration, radio elimination (in case of loss or compromise), prioritization changes, and over-the-air programming
- Network gateway options for communication with other networks and/or systems (CDMA/GSM, Tetra/P25,VHF/UHF, Internet Protocol, satellite, and public switched telephony)
- Optional 256-bit Advanced Encryption Standard for security

Today, versatile Pathmaker radios are ideal for missions such as: military or paramilitary; first responders and disaster relief; law enforcement, border patrol, and drug interdiction; Forest Service and National Parks and Monuments; and commercial and private industry. In the context of the National Public Safety Wireless Broadband Network, Pathmaker could represent an experimental, transitional, or operational interim gapfiller capability for areas disadvantaged with respect to radio infrastructure access. For example, Pathmaker radios could be modified for technical and operational compatibility with the emerging Interoperability Board/FirstNet standards developed under the 2012 Act. The current capability of Pathmaker to operate with existing radio systems to extend coverage makes this a potentially fruitful technology excursion.

4.5 Network Deployment Capability

Under the leadership of General Dynamics' Wireless Services business unit, the technical and operational skill base and expertise in wireless network deployment has matured and grown since General Dynamics Corporation acquired GTE Government Systems in 1999. As a prime contractor and in partnership with wireless carriers (Verizon, AT&T, Sprint) and peer integrators (Northrop Grumman, MACOM), General Dynamics is a key performer on commercial and public safety programs alike. For commercial wireless programs, General Dynamics provides turn-key site construction, radio engineering, equipment and power upgrades, and backhaul design/builds for national commercial providers. In the public safety market, General Dynamics provides general contracting, site acquisition, site construction, site integration, site design and layout, shelter integration, construction management, radio site design, material procurement/logistics, and installation and test. Example projects are National Capital Region Land Mobile Radio, State of New York Wireless Network, Oregon Wireless Interoperable Network, U.S. Coast Guard's Rescue 21 (section 4.1), DOJ's Integrated Wireless Network (section 4.2), Los Angeles Airport Response Command Center, and DHS's Customs and Border Protection Port-of-Entry (CBP-POE) Wireless Vehicle Identification System. Figure 7 depicts the reach and scope of General Dynamics performance on over 46,000 sites nationwide, including UMTS (Universal Mobile Telecommunications System), BTS (Base Transceiver Stations), and MW (microwave) provision.



Scope	Sites
New Site Build	1,980
GSM Growth	5,365
UMTS Overlay	15,370
4G Overlay	1,815
BTS Installation	8,600
Integration	5,750
Consolidation	655
MW Design	445
RF Engineering	6,220
Total	**46,200**

Figure 7. General Dynamics – a legacy and a future in wireless infrastructure buildout.

5 Conclusion

The nation is at the threshold of establishing an interoperable National Public Safety Broadband Wireless Network. To foster competition and thus innovation, it is imperative that entry barriers be kept low. Lessons learned by the experience of the private sector can and should assist in

government planning. GDC4S, by virtue of its experience with wireless systems and its position as a leading system integrator for communications networks for civilian and military applications, understands the critical choices that lay before the nation as the new network is established. GDC4S has provided specific recommendations to the Interoperability Board to facilitate network development of the for the benefit of the public safety community.

Should it be of assistance to you in your deliberations, GDC4S would welcome further dialogue with the Interoperability Board and other parties interested in the future of the National Public Safety Broadband Wireless Network. Points of contact for further communication are:

James Norton
Vice President, Washington Operations
General Dynamics C4 Systems
Arlington, VA
703-769-1500

Bill Ross
Vice President, Communications Networks
General Dynamics C4 Systems
Scottsdale, AZ
480-441-6116