National Institute of Standards and Technology
Department of Commerce

Mesh Technology for Network Resiliency

Federal Register Notice

Submitted: October 12, 2011

GENERAL DYNAMICS
C4 Systems

2231 Crystal Drive, Suite 600
Arlington, VA 22202

Point of Contact:
Mark Raczynski
Phone: (703) 769-1501
Fax: (703) 892-1910
Mark.Raczynski@gdc4s.com

Submitted to: Dereck Orr
Dereck.Orr@nist.gov
(303) 497-5400

"This document contains trade secrets and commercial or financial information which are privileged and confidential and exempt from disclosure under the Freedom of Information Act pursuant to exemptions (b)(3) and (b)(4). Furthermore, this information is prohibited from disclosure under the Trade Secrets Act, 18 U.S.C. 1905."

© 2010 General Dynamics

1 Introduction

The public safety community (law enforcement, fire, and emergency medical service) is experiencing a generational shift in technology that will revolutionize the way it communicates. Fourth Generation (4G) broadband wireless technology has become a commercially viable capability and offers mobile data rates that will enable a new generation of mission critical data and multimedia applications to be deployed to improve the ability of Public Safety and Law Enforcement agents to perform their mission. Traditional land mobile radio technology has limited data capabilities and suffers from a large installed base of thousands of stand-alone proprietary systems with non-contiguous spectrum assignments. Public Safety is looking for a way to leverage the latest developments in commercially available wireless technology, but has several unique requirements that are not currently reflected in broadband technology.

In August 2010, the U.S. Department of Justice Community Oriented Policing Services (COPS) office held the National Forum on Public Safety Broadband Needs. More than 20 public safety practitioners identified 15 operational requirements, each of which relate to at least four overarching themes (resiliency, availability and reliability, security, and affordability/commercial alignment). The U.S. Department of Commerce's (DoC) National Institute of Standards and Technology (NIST) is seeking input on various possible features of a new nationwide interoperable public safety broadband network, relevant to the requirements and themes identified by the COPS report. This input will be used by NIST to help determine research and development priorities in anticipation of the President's Wireless Innovation (WIN) Fund to help drive innovation of next-generation network technologies.

General Dynamics C4 Systems is pleased to submit these comments in response to the Department of Commerce request. This document will review technology from our portfolio that addresses the COPS theme of ***resiliency.***

2 Resiliency

The FCC defines **Resiliency** 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.”
http://publicsafety.fcc.gov/pshs/clearinghouse/core-concepts/resiliency.htm

The COPS report further defined 3 technology concepts essential to ensure **resiliency** in an emergency:

- Self-Organizing: Self-organizing networks dynamically manage their own configuration by automatically making changes to ensure messages reach their destinations.
- 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.
- Adaptability: The ability of the network and/or device to modify/change behavior based upon external conditions

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

Self-organizing and ad-hoc networks have tremendous potential in commercial, civil and military operations. This paper will provide a high level summary of currently available technology from General Dynamics that meets the NIST definition for resiliency.

2.1 What is "Mesh" technology?

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 setup 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 soldiers where nodes may regularly join or leave the network and the connectivity between nodes may change frequently

In short, a "mesh" network can be described as:

- ✓ **Self-forming**: Network forms with little or no user intervention
- ✓ **Self-healing**: Network can route around a failed node
- ✓ **Path optimizing**: Network uses the optimal path between any nodes

Mesh capabilities are necessary to 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.

In recent years, many vendors have created mesh networking solutions that attempt to satisfy these market requirements. These solutions differ greatly in functionality and capabilities.

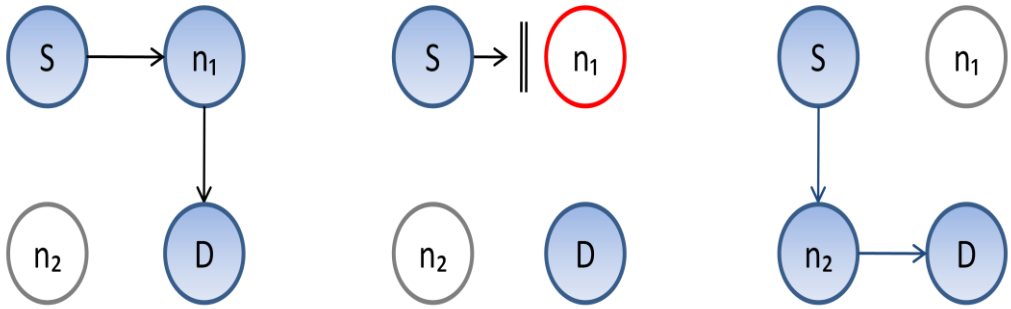

Figure 1
Node S communicates with node D through node n_1.

Figure 2
Node n_1 goes off-line.

Figure 3
Node S finds new route to node D through node n_2.

Figures 1, 2 and 3: Self-healing mesh network

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

2.1.1 Municipal vs. Mobile Mesh Networks

Many of the commercial mesh solutions are based on addressing the requirements of municipal mesh networks. A municipal Wi-Fi mesh is a hub and spoke network designed to provide broadband access to the Internet. This is provided by placing mesh points (MPs) in a grid like fashion to cover the target city geography. These MPs are attached to buildings and are thus immobile. The routing protocols are in many cases wired protocols made to operate over wireless interfaces. The primary role of these routing protocols is to compute an alternate route when an MP fails. MP failures are not very common and as such, convergence time is not a big issue. Another characteristic of municipal mesh network is that most (if not all) the traffic is destined to the Internet, with very little traffic consumed within the network and thus no peer-to-peer traffic. In addition, multicast traffic is an insignificant percentage of the overall traffic in the network. Municipal Wi-Fi mesh networks are focused on providing broadband Internet access and security is of little consequence.

Mobile mesh networks are very different. These networks are enclave and/or semi-detached networks connected to the outside world with a relatively slow (sub 1Mbps) satellite link. Much of the traffic in mobile mesh network is consumed within the network in peer-to-peer communication. In addition, multicast constitutes a significant percentage of the network traffic, sometimes, upwards of 80%, driven by video applications. In mobile environments, mesh points (MPs) are attached to individuals and vehicles. In mobile networks, a mix of RF technologies is typically employed to meet the challenging performance needs of these networks. Finally, mobile mesh networks must meet significant security requirements.

2.1.2 Requirements for tactical networks

Using radio frequency (RF) 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.

This paradigm is particularly well-suited for mobile environments such as emergency response where network nodes need to be quickly deployed and may move from one location to another. 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 Voice over Internet Protocol (VoIP). 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 wireless mesh solutions for outdoor, mobile and tactical environments can be determined in the following categories:

- **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

In order to create mobile and deployable wireless mesh networks that provide the necessary performance, coverage, mobility security and compatibility, General Dynamics C4 Systems Fortress Technologies has taken an innovative approach to Mesh technologies.

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

Figure 2: Network Diameter

2.2 General Dynamics FastPath Mesh™

FastPath Mesh is General Dynamics' mesh technology focused on mobile mesh applications. FastPath Mesh is a self-forming, self-healing, end-to-end optimal mesh solution. The main elements of the FastPath Mesh architecture are described below.

2.2.1 Routing Protocols

FastPath mesh is a highly scalable architecture based on a mix of proactive and reactive routing protocols. Proactive protocols proactively create routing adjacencies and routes with neighbors. These routes allow the system to constantly optimize the path used and quickly find backup routes when primary routes become unavailable. Reactive protocols compute routes when a packet needs to be routed a yet-unknown destination. Reactive protocols allow the network to scale to very large numbers because only relevant routes are computed and kept. FastPath Mesh utilizes a unique combination of both reactive and proactive protocols providing scalability coupled with high performance mobility.

2.2.2 Large, Flat Network

Many mesh implementations mandate hierarchies within it in order to scale to larger numbers of nodes. In contrast, FastPath Mesh operates as a large flat network with no inherent hierarchy within it. This allows seamless mobility of nodes anywhere within the network without regard to artificial hierarchies. That said, the administrator may create RF and/or security hierarchies to meet management or IA requirements.

FastPath Mesh supports both a large number of nodes as well as a large network diameter as illustrated below.

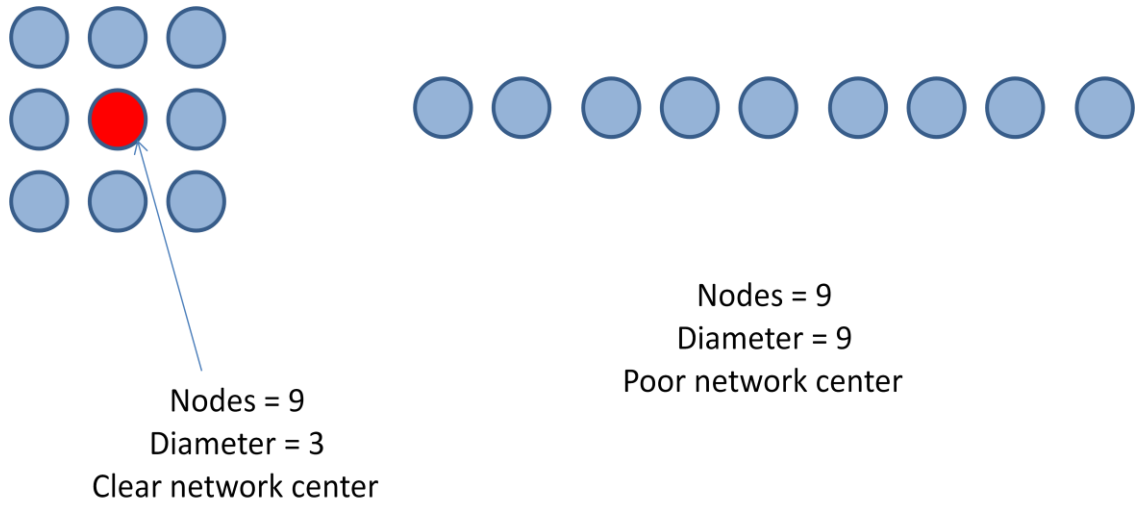

Figure 4: Network Diameter

2.2.3 Elimination of Network Flooding

One of the key design goals of FastPath Mesh is to eliminate network flooding. Network flooding occurs when a packet is retransmitted multiple times (or repeated) over the air. Network flooding is very detrimental to overall network performance. FastPath Mesh routing algorithms do not utilize any flooding. Many IP protocols such as ARP and mDNS are designed for wired network and make extensive use of flooding. When utilized over a wireless mesh network, these same IP protocols can consume a significant amount of bandwidth. Thus, FastPath Mesh implements a number of optimizations, including local ARP and mDNS proxy functions to reduce the need for flooding over the mesh network.

2.2.4 Continuous Path Optimization

As nodes move within the mesh network, the routes selected need to adapt to changing environment. In the following diagram, traffic is flowing from “S” to “D”. “S” chooses the best route through R1, R2 or R3, depending on the cost (or signal stress – RSSi in a simplified sense). This type of route refinement is possible because all nodes in the network utilize a proactive route computation.

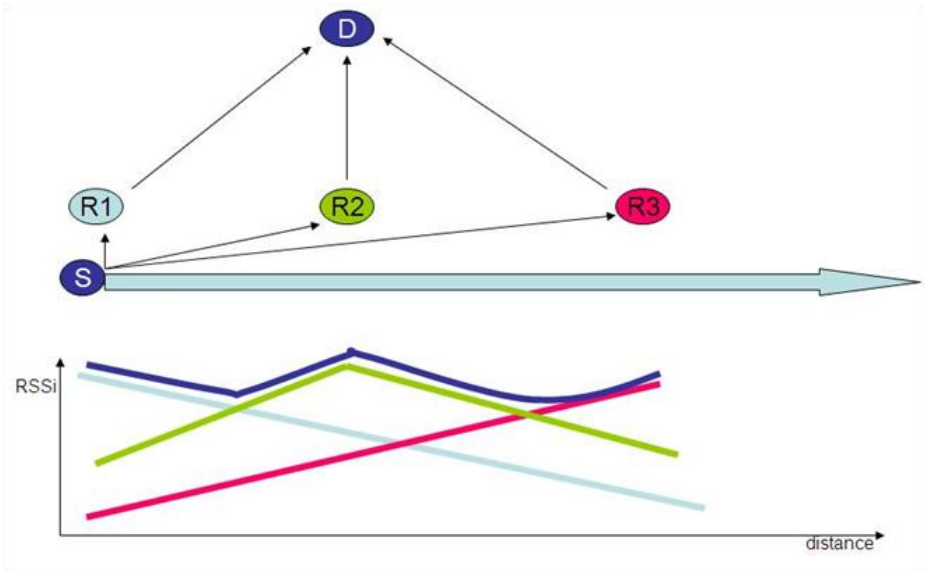

Figure 5: Continuous Path Optimization

2.2.5 Limited Control Bandwidth

FastPath Mesh limits the overhead of its routing protocols to less than 5% of the overall network capacity regardless of the network size. This allows FastPath Mesh networks to scale almost indefinitely to a very large number of nodes. This limit is possible because of the lack of flooding coupled with sophisticated set of algorithms to prioritize and compress routing updates.

2.2.6 True Multicast Operation

Applications such as streaming video, which is a critical component of situational awareness applications, commonly use multicast addressing. Many mesh implementations treat multicast traffic as broadcast – delivering every multicast packet to every node. This results in

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

indiscriminate flooding and significant loss in available network bandwidth. This is especially true as the size of the mesh network grows.

FastPath Mesh operates as multicast-aware network ala. RFC4451. FastPath Mesh snoops multicast control protocols (IGMP, MLD and MRD) and creates a multicast forwarding tree that ensures that multicast traffic is only delivered to the interested nodes in the network. The multicast forwarding trees are automatically pruned and adjusted to adapt to the varying network environment without user intervention.

In addition, FastPath Mesh uses a sophisticated set of algorithms to optimize multicast transmission over the air to conserve air time and improve robustness.

2.2.7 Media Independence

FastPath Mesh was designed from the ground up to concurrently operate over a heterogeneous mix of RF technologies. These RF technologies can be either embedded inside General Dynamics MP or connected to the General Dynamics MP via Ethernet, such as an independent WiMAX radio. FastPath Mesh is aware of and optimizes for RF links, however the routing implementation remains separate and distinct from the RF layer.

The diagram below shows a Cellular base station (BS) and three cellular subscriber stations (SS1, SS2, SS3). Cellular traffic between subscriber stations must flow through the BS. In the mesh network below, traffic between nodes A and B is optimized based on the network conditions. Traffic may follow Path#1 through the BS or hop directly between A and B using Path #2. The choice between these two (and many other paths) is dynamically determined based on end-to-end cost between the two nodes.

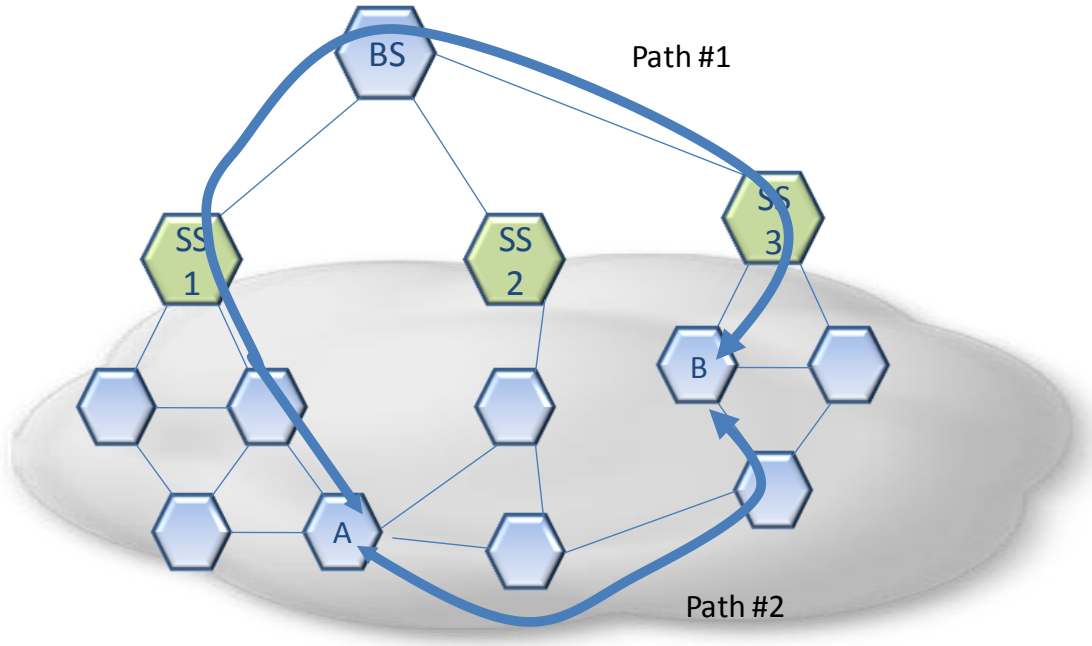

Figure 6: Media Independent Operation

In addition, as node A moves closer to node B, a more direct, less expensive route is used.

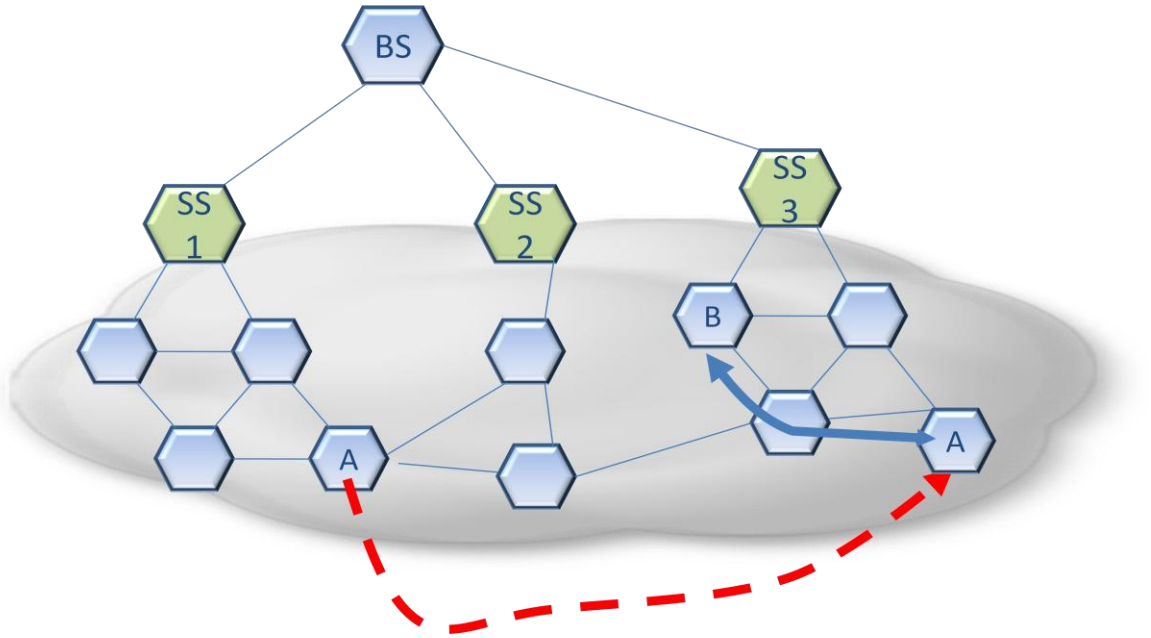

Figure 7: Media Independent Operation

2.2.8 End-to-End Security

In a mesh network, traffic usually takes multiple hops to reach its ultimate destination. Mesh Points (MPs) in FastPath Mesh create unique ephemeral keys between any pair of MPs. Traffic entering the mesh network is encrypted by the entrance MP and is only decrypted by the exit MP. This provides a number of advantages:

- High speed mobility is easily supported as no keys need to be generated when paths change
- Reduced latency eliminating unnecessary encryption and decryption of traffic
- Higher assurance as the packet is never in the clear. In fact, intermediate nodes cannot decrypt the traffic as it is encrypted using a key known only to the two end endpoints

Thus, FastPath Mesh provides high performance mobility coupled with a higher level of assurance.

2.2.9 No Single Point of Failure

In wired networks, shared resources such as DNS servers are commonly used. To avoid reliance on a single-point-of-failure, network administrators typically deploy a backup DNS server to be used when the primary one is unavailable.

In a mesh network, reliance on shared resources reduces the resiliency of the network, negating many of the benefits of mesh networks. For instance, a primary and secondary DNS severs may become unavailable for a variety of reasons. FastPath Mesh is unique in implementing a

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

fully distributed DNS capability across the entire mesh network. Thus, nodes are able to resolve name to IP mapping under all conditions. This greatly improves the reliability and survivability of the mesh network.

2.2.10 Suitability of General Dynamics FastPath Mesh™

General Dynamics FastPath Mesh™ is ideally suited to address the problems created by network clients that need access to the network even when they are widely dispersed or in mobile environments. These clients can be vehicle-based (manned or unmanned), in temporary structures, on sensors and even on personnel in the field. FastPath Mesh™ solves many real world problems, especially in the category of deployable or tactical networking.

2.2.10.1 Emergency Response

General Dynamics FastPath Mesh™ is ideally suited to Emergency Response, when temporary buildings, command centers, supplies, first responders and emergency vehicles are brought to an area where there is no reliable communications infrastructure. In these situations, FastPath Mesh™ allows for distributed assets (vehicles, personnel, sensors) to be placed and integrated into the network without the considerations and constraints associated with traditional wired networks.

2.2.10.2 Border Security

Many organizations today are challenged to extend the reach of their networks to outdoor locations and across long distances while providing as much bandwidth as possible. Often, the need is to securely link multiple locations in sites where the traditional wired approach may not be practical. General Dynamics Secure Wireless Bridges securely extend the reach of outdoor networks and are ideally suited for border security and surveillance applications.

For applications such as border security, the need is to link command posts with surveillance posts and border crossings, and to connect remote sensor networks and surveillance cameras. In these environments, the resilience of a General Dynamics FastPath Mesh™ network is critical.

2.2.10.3 Vehicle Based Networks

Many organizations need to extend broadband voice, video and data applications to their mobile and vehicle-based agents and officers. Whether the application is command and control, situational awareness, vehicle health monitoring, force protection or dismounted warrior communications, General Dynamics offers secure wireless communications while minimizing system complexity.

2.2.10.4 Deployed Operations/Event Management

In military operations, when convoys, command centers, UVs, supplies, soldiers and vehicles arrive, transit, and operate in a deployed environment, General Dynamics FastPath Mesh™ allows these units to bring the needed communications infrastructure with them, and for these distributed assets (vehicles, personnel, or sensors) to be placed and connected to the network without the considerations and constraints associated with traditional non-mesh networks.

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

Similarly, Public Safety and Homeland Security operations require rapid deployment of communications infrastructure to support law enforcement, security and crowd control efforts at large scale public events (conventions, sporting events, political gatherings etc.)

2.2.10.5 Unmanned Sensors

General Dynamics FastPath Mesh™ is ideally suited to support unmanned sensor networks. In such networks, with little or no setup, a large number of unmanned sensors communicate and relay information to one or more command centers. In more advanced applications, the unmanned sensors intelligently share the information and collectively act on it. In most cases the data transmitted is sensitive, so security and reliability of the delivery infrastructure is key. Owing to their size, these types of networks present significant challenges to traditional mesh architectures because of scaling limitations. For most mesh architectures, the amount of control traffic grows either linearly or exponentially with the number of nodes in the net network. FastPath Mesh™ with its unique mix of both proactive and reactive protocols allows the network size to scale essentially indefinitely while limiting all control traffic to less than 5% of the network bandwidth.

2.2.10.6 Maritime Domain Awareness

Whether the need is to support streaming video for situational awareness during vessel boarding, or to provide secure wireless backhaul for IP based applications such as Identity Management and biometric scanning, these solutions require wireless communications at the edge of the network that offer the best performance in terms of radio range, throughput and reliability.

2.2.11 FastPath Mesh Summary

General Dynamics FastPath Mesh™ is a solution for outdoor, mobile wireless mesh networking. FastPath Mesh™ meets the real-world demands of today's mobile wireless mesh networking in the following categories:

- **Performance:** General Dynamics FastPath Mesh™ provides fast link setup, low latency and broadband throughput regardless of the size of the mesh network. FastPath Mesh™ supports the use of multiple radios per node (on unique channels) for mesh links which improves throughput by minimizing co-channel interference and maximizing the spectrum in use.
- **Scalability:** General Dynamics FastPath Mesh™ supports a large number of nodes without degrading the available bandwidth of the network. Because the FastPath Mesh™ routing protocol requires only a small percentage of network bandwidth, a General Dynamics FastPath Mesh™ -enabled mesh network is far more scalable than those using traditional routing protocols. This also means that high bandwidth applications such as VoIP or streaming video are not impeded by the bandwidth requirements of the control protocol in a large mesh network.
- **Mobility:** General Dynamics FastPath Mesh™ allows the nodes to move around within the network as well as for leaving and joining the network. This is possible because the FastPath Mesh™ architecture is flat and uses the auto-configuration elements of IPv6 while providing full support for IPv4 nodes.
- **Security:** General Dynamics has a long history of providing FIPS 140-2 validated wireless solutions as well as being at the forefront of implementing NSA Suite B

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

Cryptography. General Dynamics wireless mesh products support these levels of security as well as 802.11i security.

- **Media Independence:** General Dynamics FastPath Mesh™ is not specifically tied to 802.11 networks; it also works over cellular (802.16 , WiMAX), military RF, free space optics (FSO) or standard Ethernet. General Dynamics has internal R&D programs exploring how General Dynamics FastPath Mesh™ will behave in a 4G Cellular/LTE environment. While FastPath Mesh™ is built around IPv6 as the default mode of operation, it also fully supports IPv4 and other non-IP based applications.

2.3 Software Defined Radios and Mobile Ad-Hoc Networking (JTRS)

A **mobile ad-hoc network** (**MANET)** 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 must forward traffic unrelated to its own use, and therefore be 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 kind of wireless ad-hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network.

The military Joint Tactical Radio System (JTRS) is a software-defined radio that will work with many existing military and civilian radios. It includes integrated encryption and Wideband Networking Software to create mobile ad hoc networks (MANETs) The JTRS Handheld, Manpack, Small Form Fit (HMS) Radios use advanced waveforms running on nodes that are smaller, lighter, more powerful and more capable than any other radio communications devices at the tactical edge.

The JTRS HMS Network extends network connectivity with voice, data and video communications for sensors, robots, UAVs, ground vehicles and warfighters on the move. JTRS uses MANET technology to insure every warfighter stays connected without fiber optic, cellular towers, routers and line of sight. Connectivity is maintained around buildings, mountains, tunnels, caves and in basements. JTRS HMS bridges networks together: legacy to future, terrestrial to beyond-line-of-sight, lower to upper echelons, unclassified to classified guard. General Dynamics C4 Systems believes the technology developed for JTRS is relevant to Public Safety communications. We can share more information with respect to these concepts under non-disclosure agreement.

(The MANET technologies described here are, by definition, proprietary in nature. Since there are limited global standards to address MANET networks, interoperability with other MANET products cannot be guaranteed.)

2.4 Pathfinder Network Radio

Pathfinder Network Radios provide dynamic wireless, mobile, ad-hoc networking communications without reliance on network infrastructure. Pathfinder 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.

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

The commercial/dual use Pathfinder Network Radio is a multi-band handheld transceiver device, supporting operations in the 2.4GHz to 2.48GHz and 225MHz – 450MHz frequency bands. It also may be used as a Vehicular radio. The Pathfinder Network Radio operates a commercial, advanced mobile, ad-hoc MESH networking waveform thereby allowing multiple Pathfinder Network Radios to form and joint a Pathfinder network while operating on a common channel.

2.4.1 Overview

Pathfinder radios work in a variety of situations and are ideal for use by, emergency first responders and disaster relief, law enforcement, Military and paramilitary, border patrol and drug interdiction, forest service, nation parks and monuments, and commercial industries (port authority, transit, retail, event management).

The Pathfinder Network Radio has the ability to instantly form a network where no infrastructure exist with multiple group (broadcast), group (one-to-many) and private (one-to-one) communications enable the Pathfinder Network Radios to fully support Group level and Platoon level communications.

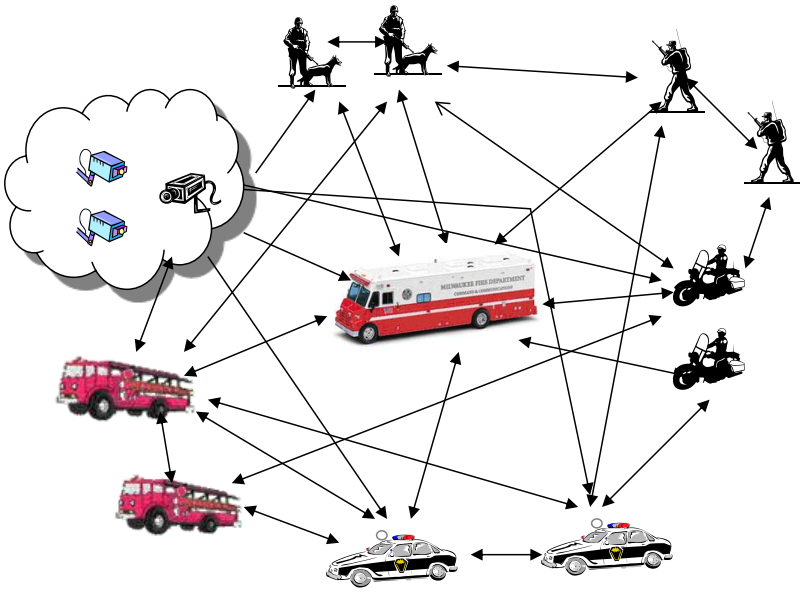

Figure 8: Public Safety Mobile Mesh Architecture

2.4.1.1 Network Features

Pathfinder radios are built for critical missions in challenging conditions and provide superior simultaneous voice, data and video communications and allow for multiple users on a single frequency to conserve spectrum space. With a maximum of 64 radio users per network, users can form traditional communications groups, or extend range and coverage by connecting to multiple networks. Pathfinder networks provide for simultaneous dynamic voice and data wireless mesh network at the individual level.

Each Pathfinder device functions as a voice and data router/repeater creating a powerful multi-hop/multi-user dynamic network that extends coverage to the edge and overcomes the daily issues of infrastructure dependency, blocked transmissions (walls, metal, dead-spots, climate,

etc.) and out of range communication. The Pathfinder Network is an Ad-Hoc, Automatically, Self organized RF network. The Unique Mesh algorithm supports up to 64 units.

- Ad-Hoc, Automatically, Self Organized RF Network
- Unique Mesh algorithm supports 64 units network with support for 7 Gateways function to other networks (GMS, CDMA, P25, Tetra, etc…)
- Simultaneous multi Voice, Data services
- Voice priority support QOS support
- PC application support (include TCP- IP interface)
- Gateway support to other wireless platforms (GSM, VHF…)

Each Pathfinder radio (up to 64 radios) on a specific radio frequency channel can be individually contacted through the Private call capability. The Pathfinder Network automatically indicates what radios are available on the Network via each radio's given alias. As radios leave and enter the network, the available alias contact list is automatically updated.

Network Features
Multi-hop, ad-hoc, self-organized network
No master/slave — no one point of failure
Quick deployment
Multiple simultaneous voice and data sessions
Multiple group (broadcast), group (one-to-many) and Private (one-to-one)
Data Rate - Up to 500 Kbps
Text messaging capability
Preemption — 4 levels for voice and 8 for data
Multiple sub-networks (groups), with up to 64 radios per group
Automatically adaptive number of hops (up to 8) according to position and mobility of users
Dynamically allocated — up to 64 registered users per channel
Up to 40 available RF channels
1km clear line of sight,

2.4.1.2 Private, Group, Broadcast & Prioritized Broadcasting

By using the Prioritize Feature radios can be configured to prioritize reception specific Groups, broadcast, or Private Call sessions over other group/broadcast/private sessions communications. Once the prioritized call has ended, the Pathfinder radio will automatically go back and receive on-going calls.

An example of prioritization allows Broadcast calls priority over (Alfa) Group Calls, which have priority over Private Session calls. Private Session call is initiated within the Alpha Group. A

Figure 9: Pathfinder Radio Private and Priority Group Calls

Group Call is prioritized over the Private Session allowing all users in the Group to listen to the Squad Leader.
Extended Group Call is prioritized over the Alfa Group call allowing contact with the Squad Leaders from both Alfa and Beta Group while still allowing the Alfa Group Call to continue within other members of the Alfa Group.

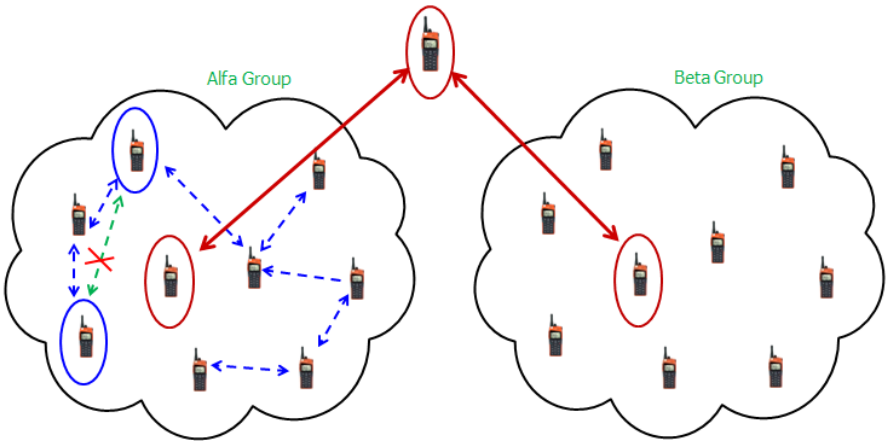

Figure 10: Pathfinder Platoon Group Calls

Once the Extended Group call is ended, Squad leader is automatically rejoined into the Alfa Group Call.

2.4.1.3 Group Radio Wireless PTT

General Dynamics C4 System has Wireless PAN technology available that can be integrated into the Pathfinder Network Radio to support Wireless PTT functionality.

2.4.1.4 Gateways for Pathfinder Network Radios

Gateways for Pathfinder Network Radios provide routing paths to connect users to other radio, satellite, IP and cellular networks, extending the reach and flexibility of the Pathfinder Network Radio system. Connecting to external communications networks is easy with General Dynamics' gateways. Where legacy network infrastructure exists, the Pathfinder Network Radio System can take advantage of those networks by providing gateways, thereby increasing the network's footprint and reach. The Pathfinder Network gateway extensions provide the interoperability with external legacy networks such as P25 land mobile radio, Cellular, VHF/UHF Analog, Internet Protocol (IP), Satellite, and PSTN.

3 Public Safety Assessment

The selection of LTE as the 4G wireless access technology for Public Safety offers the community the ability to finally have nationwide interoperable communications governed by a globally accepted industry standard. The ability to benefit from the economies of scale and market competition associated with the commercial wireless market is also an expected outcome of this action.

However, any expectation of the commercial market to meet every Public Safety feature request must be tempered with the knowledge that Public Safety represents only a small fraction of the

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

overall commercial 4G wireless market and commercial R&D investment is geared toward larger market opportunities. While LTE is a global standard, managed and administered by the 3rd Generation Partnership Program (3GPP), the ability to address vertical specific application requirements, like those identified in the COPS report, through the standards process, is limited. Public Safety must explore other avenues and technologies to meet their mission requirements.

For use in remote, geographically dispersed or dense urban areas, mobile wireless mesh technology can insure secure, reliable, mission critical communications. The products that General Dynamics has described in this response are in wide use today with civil and military customers. With the right investment and focus, Public Safety can benefit from these products.

4 Conclusion

General Dynamics C4 Systems has a long history of supporting our customer's requirements with military and dual use mobile networks. We look forward to working with NIST to help achieve the goal of the Public Safety community, Nationwide, Interoperable, secure, broadband wireless capability.

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

National Institute of Standards and Technology
Department of Commerce

Security Features Response

Federal Register Notice

Submitted: October 12, 2011

GENERAL DYNAMICS
C4 Systems

2231 Crystal Drive, Suite 600
Arlington, VA 22202

Point of Contact:
Mark Raczynski
Phone: (703) 769-1501
Fax: (703) 892-1910
Mark.Raczynski@gdc4s.com

Submitted to: Dereck Orr
Dereck.Orr@nist.gov
303- 497-5400

"This document contains trade secrets and commercial or financial information which are privileged and confidential and exempt from disclosure under the Freedom of Information Act pursuant to exemptions (b)(3) and (b)(4). Furthermore, this information is prohibited from disclosure under the Trade Secrets Act, 18 U.S.C. 1905."

© 2011 General Dynamics

1.0 Introduction

The public safety community (law enforcement, fire, and emergency medical service) is experiencing a generational shift in technology that will revolutionize the way it communicates. Fourth Generation (4G) broadband wireless technology has become a commercially viable capability and offers mobile data rates that will enable a new generation of mission critical data and multimedia applications to be deployed to improve the ability of Public Safety and Law Enforcement agents to perform their mission.

Traditional land mobile radio technology has limited data capabilities and suffers from a large installed base of thousands of stand-alone proprietary systems with non-contiguous spectrum assignments. Public Safety is looking for a way to leverage the latest developments in commercially available wireless technology, but has several unique requirements that are not currently reflected in broadband technology.

In August 2010, the U.S. Department of Justice Community Oriented Policing Services (COPS) office held the National Forum on Public Safety Broadband Needs. More than twenty public safety practitioners identified fifteen operational requirements, each of which relate to at least four overarching themes (resiliency, availability and reliability, security, and affordability/commercial alignment). The U.S. Department of Commerce's (DoC) National Institute of Standards and Technology (NIST) is seeking input on various possible features of a new nationwide interoperable public safety broadband network, relevant to the requirements and themes identified by the COPS report. This input will be used by NIST to help determine research and development priorities in anticipation of the President's Wireless Innovation (WIN) Fund to help drive innovation of next generation network technologies.

General Dynamics C4 Systems is pleased to submit these comments in response to the Department of Commerce request. This document will review technology from our portfolio that addresses the COPS overarching theme of security and the set of features for Strong, Dynamic Access Control.

2.0 Security Capabilities Supporting Interoperable Public Safety Broadband Network

As stated in the RFC, the network must enable security through:

> *Strong, Dynamic Access Control: Access control lists can be configured to control both inbound and outbound traffic on networks and authentication/verification of users/devices on the network. The level of access control should be sufficient to allow for entree into a broad set of systems and databases needed by public safety (e.g., criminal history databases, medical records, public work records, etc).*

Security in networks such as the nationwide public safety broadband network cannot be implemented piecemeal; it requires a systems wide perspective and understanding of the interdependencies of the components. The security approach should address all the elements: users, endpoints (handhelds, laptops, desktops, servers, etc), networking and infrastructure

equipment (firewalls, routers, switches, encryptors, etc), as well as the information on the network.

A layered approach to access control provides protection and assured availability of network resources and of the users, services, and data reached through the network. The goal must be to enable needed connectivity to and sharing of information – "the need to share" – while prohibiting inappropriate use of resources or sharing of information – "the need to protect".

We believe the following capabilities and technologies are essential for securing the nationwide public safety broadband network:

Core Security Capabilities

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
Cross Domain 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

General Dynamics C4 Systems has extensive experience developing many of the capabilities. Equally important, we have extensive experience integrating and hardening standards-based COTS devices in secure networks in both tactical and enterprise environments

2.1 Overview

Effective protection of the network, resources, and users requires a layering of access control capabilities. Network access controls are used as a first line of defense when users attempt to connect and before they can reach internal systems. This is device oriented and includes compliance checking of the device configuration. Access to services, data, and other users entails additional layers of access control and is generally tied to the user's attributes. Each instance of access control includes authentication, authorization, and accountability. Authorization is based on policy rule sets and the types and management of these rule sets enable dynamic access control.

Strong authentication is the basis for access control and current best practice is to use PKI credentials for both users and devices. Assessment of compliance of devices is strongest when based on a hardware root of trust in the device to ensure the integrity of the device, and means to measure and report the configuration. The users and networks will be interacting with multiple security domains (a domain is defined by a common security policy) such as Federal systems and

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

various forms of cross domain solutions will provide the trust to mediate information exchanged between domains. Accountability for actions and auditing of actions taken provide visibility into who is connected to what and what data has been exchanged. Finally, visualization and collaboration capabilities allow the managers of the networks and resources to determine the status, assess the risks, and select the appropriate response actions to maintain security of the operations.

2.2 Identity and Access Management

Identity and Access Management

A key capability needed on the new network is the ability to enforce secure data sharing by controlling who can access networks and data, and to control the flow of data based on document markings and metadata. All actions must be audited to provide forensic data after an event and Continuous Monitoring (CM) of network resources and client platforms provide the capabilities to identify vulnerabilities and detect anomalies so actions can be taken before malicious events occur. The data collected from audit trails and continuous monitoring are fed to a Situational Awareness (SA) function that provides alerts to administrators and provides administrators the capability to review past actions.

Identity and Access Management is comprised of the following elements:

1. Identity Provisioning and Management
2. Network Access Control
3. Attribute Based Access Control (ABAC) and Risk Adaptive Access Control (RAdAC)

Identity Provisioning and Management

The first step in Identity and Access Management is provisioning and maintaining a strong notion of a system identity. A common implementation of identity management is through the use of a PKI infrastructure. As the science and best practices of properly implementing and maintaining a PKI infrastructure have evolved, a robust PKI implementation offers desirable enterprise management qualities including: established support for identity provisioning and distribution, trust based on strong cryptographic principles, revocation abilities, and hierarchical as well as lateral chains of trust. Furthermore, new security ideas and technologies can extend the use of a PKI infrastructure, such as the introduction of non-person entity identities. Non-person entity identities allow machines, like humans, subject to similar security, registration, and handling procedures.

Following the step of using a PKI identity scheme; a common artifact of such a scheme is the credential token. As with any token, there is always the issue of adequate token protection. A common token protection scheme is to encrypt the contents of a token using a password. Unfortunately, when dealing with non-person identities the password is almost never a secret—think of the possible places a machine may store its passwords. The Trusted Computing Group (TCG) has introduced the Trusted Platform Module (TPM) as standardized, trusted, hardware module to accompany standard COTS platforms. Using the TPM specification allows the TPM device to protect a PKI token credential in a trusted manner.

Network Access Control

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

The previous section dealt with the issue of strong identity management; we now see the fruits of using these identity primitives to enable an effective network level access control mechanism. Network Access Control (NAC) provides the capability to control access to enterprise networks. Access decisions are based on rules in policies, which define access rights in regards to attributes of the requestor and the requestor's platform. The rules may also consider attributes of the network object being requested. In effect, NAC is implementing a form of Attribute Based Access Control (ABAC). NAC supports the situational awareness by providing audit events for all requests submitted to NAC. NAC encompasses authentication/authorization and interfaces. Network access controls also include the control of inbound and outbound traffic based on ports, network daemon names, hosts, and networks.

Authentication and Authorization

Most of the authentication work is largely solved by implementing a good identity management scheme. In the case of Ethernet and WLAN network authentication a standards based 802.1X compliant switch can disallow Layer-2 access until a device successfully authenticates. Likewise, in the case of a VPN tunnel, the device will need to authenticate to the VPN concentrator for further network access; unlike the wired 802.1X case, the VPN solution utilizes Layer-3 interfaces for authentication.

NAC authorization protocols are largely handled by a set of standards created by the Trusted Network Connect (TNC), a subgroup of the larger TCG body. Using the TNC body of specifications endpoint health information can be ascertained and used to implement ABAC over protected network resources. Because endpoints are fairly susceptible, health information originating from the native endpoint without additional protections should not be trusted—this is a typical case of the lying endpoint problem. In an effort to deal with this issue the TNC has embodied a set of specifications to utilize the TPM for trusted measurement and attestation of endpoint health. Additionally, using the TPM allows an endpoint to establish a root of trust at the TPM. Using the TPM as a root of trust allows the ability to extend a transitive chain of trust from the lower level computing hardware up to and including the Application layers. Establishing this chain of trust assures boot-time application trustworthiness enabling additional system health checks at the Application layer—additional checks the TPM may not have covered.

As the TPM mostly covers lower level hardware states there will exist the need to report OS and application layer states. NIST has created an evolving set of standards which define an ontological vocabulary about machine health and configuration within a body of standards known as Security Content Automation Protocol (SCAP). An endpoint scanner will evaluate and report machine configuration and health results to a NAC Policy Decision Point (PDP) using SCAP enumerations. A NAC PDP will evaluate policies using SCAP and other machine attributes over protected network resources. ABAC-enabled NAC allows expression of rich policies and policy outcomes enabling the use of access gradients. For example, access requestors compliant to a given policy are granted access to protected network resources. Requestors minimally out-of-compliance may be relegated to a "guest" or de-privileged network; while requestors markedly out-of-compliance would be assigned to an unprivileged remediation network.

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

While the use of the aforementioned technologies enables a more secure operating environment they must work in tandem within present day IT frameworks, paradigms, and equipment. A naïve incorporation of new security technology may raise numerous denial-of-access headaches. Infrastructure, to support legacy devices and platforms owned by unanticipated users,—whose devices may not yet be provisioned for the targeted operating environment—must exist to facilitate a productive seamless environment. More importantly than the presence of this infrastructure is the ability for the constituent infrastructure sub-systems to communicate effectively, and in a standards based compliant manner.

Interfaces
The TNC's prescience had recognized the need for inter-device communication, and thus created a common repository to facilitate device collaboration. IF-MAP, a specification which composes a part of the TNC set of specifications, defines a Metadata Access Point (MAP) along with interfaces to access the MAP repository. The MAP database can store, amongst other information, all relevant platform and network metadata. Additionally, the MAP database's graph-centric structure enables cognizant searches based on system connectivity and operational flows. The authoritative, standards based collection, storage, and communication of machine attribute data enables the use of rich multi-grained policies on attribute metadata not only at the NAC level, but also for the purposes of Data Access Control.

Attribute Based Access Control (ABAC) and Risk Adaptive Access Control (RAdAC)
Today's need-to-share paradigm succinctly requires the explicit sharing of sensitive information with authorized entities, all the meanwhile maintaining adequate protection mechanisms from unauthorized access. Furthermore, sharing must be performed across administrative, organizational, and governmental boundaries, accommodate unanticipated users, support dynamic communities of interest (COIs), meet the demand of changing mission needs, and keep pace with increased mission tempos.

ABAC enables information sharing based on the identity and attributes of the user, platform attributes, resource attributes, environmental attributes, and the policy defined by the data steward while simultaneously protecting valuable assets. ABAC supports the situational awareness by providing audit events for all requests submitted to ABAC, whether allowed or rejected.

An ABAC implementation consists of a security gateway placed in front of a protected resource; all network connections addressing the protected resource must first be processed by the security gateway. This security gateway is called a Policy Execution Point (PEP). The PEP takes direction from a Policy Decision Point (PDP). The PDP's responsibility is evaluating policies on resource metadata. The PEP or PDP may possess intelligence to determine the context of a request; that is they could contain a Context Handler. It is the Context Handler's responsibility to marshal and present attributes required by the policy to the PDP. Design pattern variations may be influenced by attribute metadata flows, such as the ratio of local vs. federated (remote) attribute queries. An ABAC implementation aware of the XACML profile may recognize the aforementioned subject matter; but in fact there are many open security standards and frameworks that can be employed one can employ to implement an ABAC solution.

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

As resource and requestor attribute metadata become prevalent, so will ABAC expressions and functionality. ABAC controlled information is not limited to the typical request/access pattern discussed up to this point, but may include RSS feeds, broadcast transmissions, custom portals, subscriptions, etc. Furthermore, when dealing with cross-domain environments content can be automatically—with assurance—redacted; or alternatively multiple versions of content appropriately distributed to authorized parties.

RAdAC

The need to keep pace with ever changing mission needs and increasing mission tempos will drive the need to evolve to Risk Adaptive Access Control (RAdAC) mechanisms. Risk adaptation includes the adoption of multiple policies over a single protected resource; policy selection is chosen according to a defined risk profile. RAdAC also includes capabilities to assess threat and need levels. RAdAC allows information sharing in situations where the data steward has allowed and provisioned for the risk in the form of another policy. Conversely, a RAdAC implementation could restrict access to a protected resource when the system observes evidence that a resource's observed risk profile exceeds the risk profile associated with the current selected policy. Automation of such a function serves as a foundational dynamic defense piece within the context of Computer Network Defense (CND). ABAC implementation naturally lends itself to performing RAdAC since operations are still performed over attribute metadata.

Insider Threat Protection Prototype Using Trusted Computing Technology

Complete mitigation of insider threat requires enhancements across the full spectrum of people, processes, policies and IT security. However, significant improvement in the risk posture can be gained via advancements in trusted computing and assured information sharing capabilities. With the right mix of monitoring and access control tools, combined with better data protection, agencies can make accidental or malicious exposures of sensitive information much more difficult. These same capabilities are also needed in mobile and cloud environments, where the distributed nature of data and users necessitates increased trust in humans, devices and access mechanisms.

A hardware root of trust, Trusted Platform Module (TPM) enabled endpoint is foundational to clearly knowing the user requesting access, understanding the state of the endpoint, whether fixed or mobile, making access decisions to networks, services, and data in the cloud, and gaining clear visibility of your overall information and security posture, all of which is imperative in an ever changing environment with increasing threats.

Anchored by the hardware root of trust in the TPM, an endpoint can attest to the integrity of its configuration, the operating system state, and applications based on trusted measurements collected by the TPM-enabled endpoint. Coupled with the strong authentication of a user bound to an authenticated TPM endpoint, network and data decisions can be made with higher confidence, using the identity of the user and the trusted characteristics of the endpoint. These capabilities enable smartly tagged information to be confidently and securely shared and protected against any anomalous activity in enterprise, secure mobility, and cloud environments.

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

We have developed a proof-of-concept system to deliver these capabilities by integrating COTS products with internally-developed security management and visualization capabilities. Specifically, the proof-of-concept:

1. Uses a commercially-based standards Trusted Network Connect (TNC) approach for collecting hardware-based measurements and verifying platform integrity.
2. Increases the fidelity of endpoint assessment, to include Security Content Automation Protocol (SCAP) checklist and vulnerability scan results, patch levels, application versions, firewall settings, browser settings, and the existence of potentially malicious applications specifically defined in policy to focus on insider threat activity.
3. Standardizes, aggregates, correlates, and makes insider threat related endpoint information available for network access and information sharing decisions and situational awareness.
4. Information tagged with DoD/IC standards based metadata enables strong access controls and end-to-end protection, whether information is stored in conventional stores or made available via cloud services.
5. Provides a common visualization point for situational awareness of the information sharing posture and anomalous events.

This technology advances trusted computing technologies and provides a stepping stone to an integrated, standard based, commercial solution to the insider threat challenge.

2.3 Cross Domain Solutions

Although the use of security controls such as access control lists and user/device authentication may be sufficient to control access to resources and information on a network when a single level of information (e.g., public, sensitive, classified) is on the network and a single organization controls the entire network, they are not sufficient when multiple levels of information are on the network and no single organization controls the network. In this case, much stronger security controls are required to meet governmental requirements for information assurance (IA) and certification and accreditation (C&A).

The nationwide public safety broadband network will make it “easy” (i.e., possible, fast) to share information between the law enforcement agencies (LEA) – Federal, State, Local, Tribal – that use the network. Each LEA will have some information – text messages, chat sessions, static images, streaming images, file transfers, database queries, web browsing, etc. – it wants to share and some information it wants to keep private. Sharing information between LEAs, while essential in an operational context, must be controlled to ensure that sensitive or restricted information is not shared inappropriately. The network must therefore implement security controls that allow information to be shared in a secure manner.

In the lexicon of information assurance, each LEA would be described as a *security domain* and the sharing of information between security domains would be described as a *cross-domain* transfer of information. The security controls that allow the sharing of information between security domains in a secure manner go beyond simple network access control lists and user identification. Cross-domain security controls provide discretionary access controls (DAC), mandatory access controls (MAC), role-based access controls (RBAC), attribute-based access controls (ABAC), content inspection, and auditing functionality that meet government information assurance requirements for certification and accreditation (C&A), which

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

significantly exceed commercial best practices. Cross-domain security controls are typically not found in commercial information systems and networks. These security controls are found in information systems and networks used by the Department of Defense (DoD) and the Intelligence Community (IC).

There are aspects of cross-domain information sharing in the LEA environment that will be different from the usual DoD/IC environment:

1) The LEAs will share/protect information on a dynamic case-by-case or operation-by-operation basis, so the network must allow cross-domain security controls to be implemented rapidly, as operational needs arise. Equally important, the network must allow operation specific cross-domain security controls to be removed when the operation is complete.
2) Participation in operations will be variable across the LEAs on the network; some LEAs will have many users participating and other LEAs will have no participation.
3) Some operations will be long lasting (weeks, months) and other operations will be short (hours, days). The network must be able to support both without imposing unnecessarily administrative burden on the LEAs.
4) The network will not have a centralized user identification and authorization function that spans all LEAs. Rather, each LEA will be responsible for authenticating the identity and privileges of their personnel and all LEAs will have to trust the authentications from other LEAs. Because the LEAs exist at many different levels, establishing the policies and security controls to implement a system of mutual trust will be particularly challenging.

The implementation of cross-domain security controls in this multiple LEA environment will require a trade-off between “the need to share information” and “the need to protect information” as well as an understanding of C&A requirements and process.

Because of our history of working with DoD/IC customers to solve their cyber security problems, we have products and technology that provide cross-domain functionality such as:

1) Computing platforms – handheld, laptops, desktops, embedded – that allow access to multiple security domains at the same time
2) High Assurance Guards that control the transfer of information between security domains
3) Systems – network, desktops, servers, storage, databases, gateways, etc – that consolidate information from multiple security domains into a single enclave
4) VoIP desktop phones and handheld smart phones that provide Type 1 encryption of voice communication
5) Encryptors that provide Type 1 encryption at bandwidths up to 1 Gb/s
6) Encryptors for hard drives in both tactical and enterprise computing platforms
7) Enterprise security management (ESM) software for all of the key elements of ESM: (a) Attribute Management, (b) Audit Management, (c) Configuration Management, (d) Credential Management, (e) IA Metadata Management, (f) Identify Management, (g) Key Management, (h) Policy Management, (i) and Privilege Management.

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

Additional information on these products and technologies has been included as appendices to this submission.

2.4 Transactional and Asset Inventory Audit

Further utilization of strong identity management technologies and process result in higher assurance transaction and asset inventory audit systems. Binding human subject and platform identities through the use of NAC and DAC reduces anonymous network activity. The ability to tie fragmented network event data to a human user and platform reduces uncertainty when supporting incident response tasks such as event reconstruction. The benefits of strong identity management are not localized to network events, however. The Insider Threat prototype system discussed earlier records all transaction requests; regardless of the request's success of failure. An audit trail of such quality might sufficiently establish a chain-of-custody in support of forensics or other detailed analyses.

2.5 Situational Awareness

As with any security system, people are needed to continuously monitor and maintain awareness of system state, as well as tend to any reports the system may have generated. As systems become more complex and a greater wealth of information becomes available we are left with an information sifting problem. While analytic functions are still necessary, some of the pattern recognition may be performed by human using charting, visual cues, and highlighting. A visualization tool used to analyze data must support data interaction and collaboration. Dashboard type views are easy to use, but are limited in capability to what they can convey using pre-defined views. Interactivity or the ability for analysts to drill-down into the data using custom visualizations unlocks unique human analytic capabilities. The need to collaborate and communicate ideas reflected within the data is another essential function a visualization tool must have. These pillars of visualization are reflected in CoMotion™, a product developed by General Dynamics C4 Systems.

The CoMotion™ product has been developed by General Dynamics C4 Systems as a visualization system to enable analysts to have better views of information. The CoMotion™ product collects data from many sources including events generated by NAC and PBAC subsystem. The CoMotion™ product includes an Aggregation and Recomposition Manager (ARM) subsystem that supports the user's need to organize, understand and make sense of large amounts of data. Standard visualization capabilities are supported: 2D and 3D geospatial visualizations, timelines, network diagrams, scatter plots, histograms, and other charts.

CoMotion™ is based on a collaborative visualization engine that has been used in applications ranging from the US Army's Command Post of the Future (CPOF) to logistics for USTRANSCOM, as well as medical clinical trial management applications where situational awareness is critical to rapid and informed decision-making.

Situational Awareness Subsystem Goals Focus

1. Collect and analyze forensic-quality data
2. Models represent both normal and abnormal insider activity

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

3. Better techniques to determine user intent from strict observation
4. Counter multiple colluding insiders
5. Architecturally integrated response strategies

2.6 Applicability of Security Capabilities to Other Desirable Features in the Public Safety Broadband Network

The implementation of the robust security capabilities described above is beneficial to the network in other key areas as well. Security adds to the resiliency of the network by enhancing the ability of the network to operate in the presence of an attack and by allowing network resources to be reallocated based on need during an attack. Security adds to the affordability of the network by increasing the compatibility of the network to commercial networks by allowing standard interfaces to be used in a secure manner, rather than requiring the development and implementation of custom interfaces. Security also enhances the ability of the network to scale as needed by the users on the network.

3.0 Considerations for Implementing Security Capabilities in Public Safety Networks

Access control is highly important to maintaining the availability of resources for those who need them. If unauthorized users and mis-configured devices are allowed into the network, the integrity and availability of resources will be in jeopardy. The network must protect itself and the hosted services in order to be ready to support its intended missions. The proper implementation of access control with appropriate policy rules and dynamic adaptability is also critical in order to avoid the problem of denying access when it is most critically needed.

3.2 Gaps, Challenges and Research Opportunities

Gaps include

- Trust on the mobile device – hardware root of trust and hardware virtualization support are being developed but not yet fielded and when fielded will need application and infrastructure support. Research is needed into use of planned capabilities for compliance assessment/integrity verification and for device audit and accountability. Also need to develop and pilot infrastructure support such as issuance of attestation and identification certificates.
- Digital policy management for access control and RAdAC capabilities are in early adoption and not yet complete, scalable, and standardized across vendors.
- Visualization of information across integrated, cross functional data sources can provided improved situational awareness and risk assessment of a national network but piloting and research is needed to determine the operational requirements and data needed.
- Use of NAC, RAdAC, digital policy management, trusted computing, and cross domain solutions can all contribute to network resiliency, availability, reliability, and recovery options as well as security. Conversely, methods to dynamically reconfigure and reconstitute networks need to address continuity of security services. Research is needed into the coordinated capabilities and features providing these overarching themes.

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.

3.3 Industry and Government Best Practices

Enterprise networks and Federal users such as DoD have begun implementing these features for fixed users and are investigating and planning for support of mobile devices and users. For instance, ABAC, NAC, hardware root of trust, and CDS are implemented for fixed user networks and best practices can be examined.

3.4 Importance of Standardization and Vendor Diversity

Both standardization and diversity are important. The security features obviously involve interoperation between a number of systems (identity management, policy management, access control, compliance assessment, SA) and this includes interoperation with similar functions in external networks and systems (Federated PKI, access control to existing systems). Diversity not only serves to maintain competition and supply availability but provides a valuable security attribute for defense in depth – different vendor implementations tend to not share the same vulnerabilities so layering diverse implementations is generally stronger than two of the same.

3.5 Establishment of a Core Public Safety Network

In a recent report, the President's Council of Advisors on Science and Technology suggested the need to develop methods for implementing a ``survivable core'' of cyber-infrastructure that would be relied upon to provide truly essential services in the event of a catastrophic cyber-attack.

Our recommended approach would be to design the primary network for rapid reconstitution. We have addressed network recovery and reconstitution requirements for networks and have some insights. New capabilities for dynamic policy control (networking and security), ad hoc network formation, adaptable security features, and common identification can all contribute to reconstitution rather than being roadblocks.

3.5 Network Features or Requirements Not Identified in the RFC

Our response has identified the security features needed overall to provide strong, dynamic access control as well as general security support for the mission and goals of the new nationwide public safety network.

Use or disclosure of data contained in this document is subject to the restrictions on the title page of this document.