PSnet

PSnet Study Report

January 31, 2007

Interisle Consulting Group

Galaxy INTERNET SERVICES

Table of Contents

1 Executive Summary

The Public Safety Network (PSnet) offers public safety agencies (initially in the metropolitan Boston area) the opportunity to connect to each other via secure, resilient, high-performance data networking infrastructure.

Built by leveraging existing networking assets and other public safety investments, PSnet provides a platform for expanding collaboration amongst public safety organizations throughout the Boston metropolitan area while improving network resilience and lowering future costs.

PSnet is a communications network, but it is also the foundation—and enabler—of a different way for public safety agencies and officials to cooperate across various agency and jurisdictional boundaries. It is concerned not just with the technology of communication, but also with the effective sharing of networking assets, of information, of applications, and of know-how, so that the best things that are developed or discovered by any participant become resources for public safety throughout the region and beyond.

The model on which PSnet is based—private and public entities at local, state, and federal levels collaborating to create and operate network infrastructure—has been proven successful from a technical, operational, and business point of view in other domains among other communities such as research and higher education.

The key features of PSnet are:

Better public safety collaboration. The core benefit of PSnet is enabling public safety officials to share important information reliably and securely, with complete confidence that the information will not be exposed either to unauthorized PSnet participants or to outsiders. PSnet brings to data what radio interoperability is bringing to voice communications: the ability for public safety agencies in different jurisdictions to collaborate effectively in real time.

Alignment with existing well-established authority. PSnet does not usurp or diminish the authority of municipal governing bodies to make local decisions about equipment and services that are right for their communities. Because PSnet is the sum of its parts, rather than a new structure imposed unilaterally from above, authority arises from (and stays with) the people and agencies that own and manage those parts, not from a new top-down bureaucracy.

Efficient incremental growth. PSnet builds on the investments in equipment, applications, and other infrastructure that each participating municipality or agency has already made—it doesn't depend on an unrealistic "and

then a miracle occurs" leap across a deep funding chasm. PSnet is a "network of networks," which benefits from everything that each participant brings to the table on day one. Funding for future growth can be local, regional, statewide, or federal.

Economies of scale. Collectively, PSnet participants can negotiate better deals for equipment and services, and can more readily find the resources necessary to develop applications that would be broadly useful. Capabilities like diverse, redundant links or 24x7 monitoring and technical support—prohibitively expensive for a single municipality or agency—become feasible at a regional level.

Standards and interoperability. Because PSnet is based on national and international standards, public safety applications, technology, and insights developed anywhere—at the local, state, regional, or Federal level—are available to the PSnet community.

Resiliency. The broad geographical scope and standards-based Internet architecture of PSnet mean that cities and towns can strike simple and very low-risk agreements with each other to provide backup when one of them encounters a connectivity problem—either internally, or with respect to a service provider.

Until recently, creating a regional network was a major undertaking, calling for purpose-built facilities and the commitment to recurring expenses for telecommunications circuits and other services. But the existence of municipally owned networking assets (for example, fiber plants delivered as part of a municipal cable franchise), the growth and ubiquity of the public Internet, and the wide availability of low-cost commodity networking technology have changed the landscape. The PSnet vision is not something hypothetically far off in the future—it is achievable today, with existing technology, as this report documents in detail.

Cooperating public safety officials in several Boston area municipalities are already running a small pilot project. The next step—to which every project participant is fully committed—is to make the vision and promise of PSnet a reality.

2 Introduction

There is a need for public safety agencies to be able to connect to each other via secure, resilient, high-performance data networking infrastructure. There is an opportunity to create such a network, without a massive new infrastructure initiative, by interconnecting existing networks and making small, incremental additions to them.

In 2006, public safety officials operating within the Metropolitan Boston Homeland Security Region (MBHSR), recognizing this need and opportunity, began a pilot project called "PSnet," for "Public Safety Network."

This report describes the motivation and background for the project and presents the results of a study whose goals were to advance the project by documenting objectives and principles, identifying requirements, resources and opportunities, and making recommendations. The study was funded using Federal Department of Homeland Security grant money administered via the Boston Mayor's Office of Emergency Preparedness and conducted from August 2006 through January 2007.

The contents of this report were derived in part from research and interviews with actual and potential project stakeholders, in part from our experience with similar efforts, and in part from our oversight of the ongoing pilot project.

The report first, in an overview and background section, explains the strategic objectives and overall direction of the project. Next, it describes the requirements, available resources, and opportunities discovered during the study. It then lays out the fundamental principles that should guide the development, operation, and governance of the PSnet network, and, in accordance with those principles, makes recommendations for PSnet's architecture, operations, and governance. The report concludes with a summary of recommendations, followed by appendices that provide some additional supporting detail.

3 Overview and Background

3.1 The need to interconnect regional public safety agencies

Public safety agencies at the municipal, state, federal, and nongovernmental levels have established a need to connect to each other via resilient, secure, high-performance data networking. Being connected enables them to:

- Access each other's existing data and data-intensive applications, for example databases used during crime analysis or investigation.
- Exchange data messages in real-time, for example to support mutual aid across jurisdictions via computer-aided dispatch.
- Enhance the interoperability of existing and planned radio systems.
- Use various media, for example video streams, to augment existing telephone communications, either for routine communications or for emergency backup.
- Develop and support new information-sharing applications such as those created for intelligence fusion or emergency operations command.
- Access central databases such as those maintained in the state Criminal Justice Information System (CJIS) or the state Automated Fingerprint Identification System (AFIS)
- Serve as a critical, enabling resource for future public safety applications such as wide area mobile data or Next Generation 911 (NG911).

3.2 Benefits of shared infrastructure

As a strategic direction, there are many advantages in moving away from a world in which individual agencies, departments, or political subdivisions each independently operate special-purpose networks supporting narrowly-focused applications, and towards a world in which resources are pooled to create shared, flexible, extensible, robust, multi-purpose infrastructure that supports an evolving array of applications and services. Some benefits associated with shared infrastructure include:

- Given the same dollar, facility, staff, and management resources that would otherwise be used to build several special-purpose networks, a shared multi-purpose network can be built to a far higher standard of performance, security, and resiliency. It can incorporate greater geographic route diversity, more robust support and management, multiple redundant operations

centers, better security measures, and other features that contribute to the effectiveness and quality of the infrastructure.

- A shared multi-purpose network can enhance existing collaboration, coordination, and data-sharing applications and can foster the development of new initiatives.
- A shared multi-purpose network built using standardized technology and operated using standardized approaches offers more flexibility for future expansion, additional interconnection, and technology refresh.
- Substantially increase the available pool of bandwidth at lower overall cost, this new approach will enable a variety of new applications that are currently infeasible or cost prohibitive due to throughput or performance requirements.

3.3 A changed landscape

Until recently, creating a regional network was a major undertaking, calling for purpose-built facilities and expensive recurring charges associated with leased circuits or service subscriptions. However, the landscape for regional networks has changed substantially as municipalities have moved toward owning or controlling networking assets (for example, community-owned fiber plants or wireless metropolitan networks). The growth and ubiquity of the public Internet, along with the general availability of low-cost commodity networking technology have also contributed to a changed landscape. PSnet is intended to make these changes work for the benefit of the communities it serves.

3.4 Strategic and policy objectives

The "PSnet vision" is of a shared infrastructure platform supporting multiple public safety applications using standardized technology. This "network of networks" is built by interconnecting many existing and planned piece parts. It is a proven approach, having led in the past to the development of quite a bit of the world's modern telecommunications infrastructure, including the Internet. Other industries (e.g., the securities industry) have demonstrated that such networks can not only increase available bandwidth at lower cost, but also substantially improve overall resiliency without increasing costs. Such a network could be achievable at relatively low cost, and would facilitate the type of "organic" growth that has characterized the public Internet but that has to date, in large measure, eluded Government networks.

PSnet itself is really three things: 1) a community of public safety agencies, 2) a data network itself, and 3) the entity that governs and operates the network.

The overall objectives boil down to:

Form a community. PSnet is self-managing community of municipalities, institutions, and agencies interested in exchanging data and/or interconnecting and pooling their network assets to achieve a result far superior to and less costly than what they could achieve by working independently. The project has already identified the early, major participants (akin to the "anchor tenants" of a real estate development); it must continue to reach out to additional participants.

Build a network. At its core, PSnet will be an IP network, built along the same general principles as the public Internet. PSnet must create, out of the available pool of fiber plants, wireless links, leased infrastructure and other networking assets, a coherent and manageable "network of networks." In addition to the networking assets owned by the participants, PSnet itself might build and operate a backbone network to help improve connectivity along with a set of central services that can more cost effectively be deployed as part of the PSnet shared infrastructure . . This "PSnet backbone" network is discussed further in Section 11.5 "Recommended Project: PSnet Network Build".

Operate and govern the network: PSnet must provide for the operation and funding of the network. It must strike a fine balance by establishing architectural, technical, operational, financial, and governance principles that are well-enough defined to promote interoperability and sharing while being open enough to draw in as many members as possible and make best use make best use of the available assets.

3.5 The PSnet study

This document presents the results of a study conducted during the fall of 2006, the purposes of which were to:

- Document the strategic and policy objectives for a shared data network serving the Boston area public safety community.
- Develop principles in the areas of architecture, security, operations, technology, and governance that would guide the builders, operators, and users of PSnet.
- Identify:
    - Potential participants
    - Immediate requirements
    - Available networking assets:
    - Short-term opportunities for interconnection

  - Gaps that can be filled in order to realize the longer-term vision

- Make specific recommendations in accordance with the policy objectives and principles.
- Use an ongoing pilot project as an opportunity to acquire practical experience about where the easy successes and the immediate challenges lie in creating and operating such a network.

4 Requirements, Resources and Opportunities

A major part of the job in building and growing PSnet is to understand the requirements for interconnectivity among members, to be aware of the potentially available networking and application assets, and to identify two types of opportunities:

1. Opportunities to improve the network (e.g., to extend its geographic reach, its capacity, or its resiliency in the face of disruptions) by making new interconnections between existing facilities.
2. Opportunities to match the available networking assets against the requirements.

We call this the "Information Clearinghouse" function, and we believe it is such an integral part of the success of PSnet that, in Section 9, we identify this as one of the most significant recommendations for moving forward.

During the PSnet study, we performed the "Information Clearinghouse" function on an interim basis, with the following results:

4.1 Requirements

Network infrastructure is an enabling technology: it allows for the development and deployment of other applications. A built-out PSnet would enhance many existing applications and enable the development of new ones. Here, we divide the requirements into three categories:

- Requirements that could be met immediately upon connection, without requiring new application development work.
- Requirements that could be met with minor modifications to existing systems or procedures.
- Significant new capabilities that could be developed given a PSnet foundation.

4.1.1 Requirements met immediately

PSnet project participants and interviewees have requested the following capabilities, which become available immediately upon connection, and which are being developed during the ongoing pilot project

Access to police department records management systems. Several local departments' records management systems offer a Web interface, meaning that anyone with network access and login credentials can search the database, for example during investigations and crime analysis.

Cambridge and Boston have already drafted a Memorandum of Understanding allowing pilot access by a small number of analysts and investigators in each department to the other's records management and other applications. This will be extended to Brookline and Chelsea and, based on lessons learned from the pilot; this access will be broadened and replicated to other municipalities.

Network transmission of fingerprints. Chelsea has requested the use of the network to transmit fingerprints to Boston.

Web EOC application. The cross-functional emergency operations system originally developed for the 2004 Democratic National Convention, WebEOC, can be hosted on a PSnet-accessible server; any public safety agency with appropriate access permissions will be able to use PSnet to access it.

Shared File Folders. Cambridge Police Department wishes to host a fileserver to which other police departments would be granted access; the fileserver would appear as a folder on the desktops of participating crime analysts and investigators and would become a place to exchange documents, pictures, notes, and other files.

Remote Viewing of Surveillance Cameras. Surveillance camera video from existing systems (e.g., Chelsea, Boston, Turnpike Authority) can be made available to authorized users at any location reachable by PSnet.

Virtual Private Network (VPN) connections from BRIC. Many officers from other police departments visit the Boston Regional Intelligence Center (BRIC). PSnet would enable secure, private connections to these officers' home department networks from the BRIC, allowing the officers to access their own records management systems and other internal department resources while at the BRIC.

4.1.2 Requirements needing some development

Desktop Videoconferencing. PSnet enables multi-party desktop videoconferencing using one or more central servers and inexpensive cameras added to existing desktop or laptop computers. The pilot project included a demonstration, although due to the timing and availability of vendor participation, the demonstration was conducted over the public Internet rather than directly over PSnet assets.

Remote Operation of Radio Equipment. Products are now available commercially that allow radio equipment to be operated from a remote location over an IP network. A device is added to a CEB (communications equipment bank), connected to PSnet, and then a PC connected to PSnet, for example

at an alternative dispatch location or an emergency operations center) can serve as a remote console or gateway switch from which the radios can be operated, or from which two or more radio channels can be patched together to gain interoperability.

Replacement of T1 lines for fire department (and other) radio. Most dispatch centers maintain leased lines to several transmit locations and multiple receive locations. Boston Fire alone has over 30 locations. To the extent these locations are reachable by municipal fiber or other networking assets connectable to PSnet, PSnet can carry the digitized audio in place of (or as a redundant backup to) the T1 lines. This would also facilitate routing of audio channels between municipalities to further extend the range offered to public safety officers that respond to requests for assistance from neighboring communities.

Remote access to Client/Server systems. When agencies want to share access to each others' systems but the applications do not support Web access, client software can be installed and configured, allowing remote access via PSnet.

Secure e-mail. PSnet can be used to deploy secure e-mail among participants that can improve the speed and utility of everyday correspondence while offering new options for securely exchanging information in an ad hoc manner. This could be especially important during a disruptive event.

Access to SWISS. PSnet provides a natural means of accessing the proposed State-Wide Information-Sharing System (SWISS), currently under development as part of the Executive Office of Public Safety (EOPS) critical incident information exchange efforts. PSnet would provide the type of high-speed access required for local police to access large databases quickly and view photos, maps, and video.

4.1.3 New Opportunities: Requirements involving new development and/or procedures

Carrier-Independent Telephone. Any location served by PSnet (e.g., a public safety agency headquarters or dispatch facility) can add a Voice-over IP (VoIP) switch to its telephone infrastructure, and connect the switch to PSnet. Any two locations so equipped could maintain telephone contact in spite of a service outage at the local telephone carrier (e.g., a fire in a central office or a major power outage).

Shared records management systems. PSnet enables the development and deployment of shared databases, for example for crime analysis.

Radio System Integration. VoIP and other IP-based Land Mobile Radio techniques can use PSnet as a transport mechanism, allowing different

public safety agencies (e.g., police and fire departments based in different municipalities) to talk to each other on the radio.

EOC Support. PSnet connectivity among emergency operations centers and between EOCs and participant headquarters.

Mobile Wireless Data Integration. The municipalities in the PSnet area currently use different technologies and vendors to connect mobile laptops to central services. Cambridge and Brookline use two different mobile service providers. Brookline may potentially want to transition to its 4.9 MHz wireless network now being deployed. Boston uses a UHF Private Radio system. PSnet could potentially provide a data transport backbone related to roaming and interoperability among these systems.

4.2 Bandwidth Requirements

The requirements placed on the PSnet infrastructure will depend of course upon the mix of applications supported and the number of online users or sessions, which will, of course, change considerably as PSnet is deployed and comes into wider use . . What is presented here is extremely general; the PSnet executive and technical committees have not yet determined which applications to support and in what order, nor have the individual participants said anything about the number of users expected to be on line at any point.

Applications have widely varying profiles of bandwidth utilization, delay sensitivity, and synchrony requirements. Some, like e-mail, are tolerant of delay while others, like telephony and videoconferencing, require low, predictable latency. Interactive web services and client/server applications are in between.

At the low end of bandwidth requirements lie text e-mail and remote access to web-based records management applications. These are currently supported (e.g., at CHSB) over 56 kbps lines, although the user community generally perceives this data rate as inadequate. Because of the "burstiness" of the usage associated with these applications, there are considerable benefits to aggregation. 20 simultaneous sessions sharing 10 Mbps worth of bandwidth provides higher performance and a better user experience than 1 session with its own dedicated 512 Kbps of bandwidth. As a planning assumption, 9 municipalities each with 2 simultaneous users of interactive applications (18 sessions) might be well served by 10 Mbps of bandwidth.

At the other end of the spectrum lie telephony, remote operation of radio gear, and video conferencing, all of which are highly sensitive to network congestion and work best over networks with low latency and jitter. Voice-over-IP requires between about 10 and 90 kbps per simultaneous stream (depending upon the audio quality desired and other parameters), meaning that each 1 Mbps of

network capacity could represent (choosing a middle-of-the-range number) 32 simultaneous audio channels.

Video is a high bandwidth application. Existing video networks (such as the surveillance camera network now being developed between Boston, Chelsea, Revere, and Everett, are built using a 100 Mbps backbone, capable of transmitting many simultaneous camera streams.

We propose that the primary PSnet backbone network be built to support 100 Mbps of traffic, and that each primary connection into the backbone be either 10 Mbps or 100 Mbps. Those desiring a lower-bandwidth connection would be able to obtain service via a secondary connection via another municipality or agency with a primary connection. (See also the hybrid architecture, Section 6.3.3).

4.3 Resources

This section focuses on technical resources that were uncovered during the study.

During the interviews conducted as part of the project, we have identified the following network elements as initial elements suitable for interconnection as part of PSnet. These elements are listed here, along with their responsible agency, and relevant contact information. Appendix A provides more detail about each asset.

Note that this is just the nucleus of what will become a larger list. An important recommendation, going forward, is that PSNet establish itself as a repository of knowledge about the available networking assets within the region.

4.3.1 Existing Network Assets Included in Pilot

The assets listed here are being used in the pilot project.

Network Asset	Responsible Agency	Business Contact	Technical Contact	GIS Contact
Cambridge City-owned fiber (Reaches numerous city buildings)	City of Cambridge	George Fosque	Tom Friess / George Fernandes	Jeff Amero
Chelsea City-owned fiber	City of Chelsea	Matthew Killen	John Hyland	William Toussaint
T1 link from Brookline PD to Boston PD	Town of Brookline	Scott Wilder	Scott Wilder	
Fiber link from Cambridge to Boston[1]	Northern Crossroads	Leo Donnelly	Leo Donnelly	Leo Donnelly
Verizon TLS circuit from Boston City Hall to Boston PD	City of Boston	Ann Roper Quinn	Jerry Turner / Brian Barcelou	
Comcast Boston Fiber 1 Summer Street to Boston City Hall	Comcast	Leo Donnelly	Jerry Turner	
Harvard Fiber—William James Hall to 300 Bent Street[2]	Harvard University	Leo Donnelly	Leo Donnelly	

[1] This link is provided and managed *pro bono* during the pilot project by Harvard University

[2] Also provided and managed *pro bono* by Harvard

4.3.2 Additional Network Assets Suitable for Connection

The assets listed below have been identified during the study as highly suitable for inclusion in an expanded PSnet.

Network Asset	Responsible Agency	Business Contact	Technical Contact	GIS Contact
Boston City-owned fiber (Reaches numerous city buildings)	Boston MIS	Ann Roper Quinn	Jerry Turner	James Alberque
Surveillance Camera Network (Boston—Everett—Revere—Chelsea)	City of Boston	Unknown	Stonecrop Technologies / Doug Stringer	
MBTA SWR (Radio) fiber	MBTA	John Lewis		Bob Parfumorse
MBTA WAN fiber	MBTA	John Lewis		
Massachusetts State ITSD SONET ring	Mass ITSD	Rich Glasberg	Rich Glasberg	
Chelsea 1G Link (EOC to Soldiers' home.	City of Chelsea	John Cowhig	Stonecrop Technologies / Doug Stringer	
CJIS Network	CHSB	Curt Wood		
State Police Backbone Network[3]	State Police		Blair Sutherland	
Massport Fiber (harbor and river crossings)[4]	Massport	Bryan Corbett		

4.4 Opportunities

Analysis of the requirements against the existing networking assets point out several opportunities. We recommend the following links and connections be created.

- Connect the camera wireless network to PSnet at three locations: Chelsea Soldiers Home, Boston Police Department, and Boston City Hall. (The first

[3] To date we have been unable to obtain an interview regarding network

[4] Contact made, but detail not available as of the date of this report.

two could be done immediately; the third requires an additional fiber run). Create a VLAN on the camera network for PSnet traffic. Create a routing path through PSnet for the camera network traffic. This would create a high bandwidth connection for Chelsea, and an additional level of resiliency for both networks.

At the first two locations, the costs are entirely soft (i.e., staff time to configure routing tables; less than a week total from design through testing). The third location requires a new fiber run (next bullet point).

- Pull fiber across City Hall Plaza from JFK building to City Hall basement. (Existing conduit may be in place.) This would connect the surveillance camera network to a highly-connected PSnet node. Cost depends upon whether City, Federal, or Contractor staff are used to pull the fiber, and upon the conditions of the conduits and raceways. We do not have access to this information, but we believe the Mayor's Office of Emergency Preparedness has this information as a result of David Smith's work on the camera project.

- Demonstrate point-to-point wireless from Brookline Police Dept to Boston City Hall, via the MIT Tang Hall building or via a building at BU. At relatively low cost this would provide a fully redundant path from the western edge of the region to the center. Galaxy Internet and a radio vendor have volunteered to create this link for the pilot, pending building access being granted by MIT or BU.

  Cost estimate to make it permanent would be $2,500 worth of radio gear at each end; $2,000 for a router at the MIT or BU end, $250/month worth of cross connect at the Summer Street node (if via BU), or an additional $2,500 worth of radio gear at Boston City Hall if via MIT.

- Make fiber connection across Arlington St., Chelsea. The Eugene Wright School is on Chelsea's fiber plant; Mass ITD directly across the street is a major access node for both the CJIS network and for the Commonwealth's OC-192 ring. This would provide for additional Chelsea access to PSnet and for PSnet access to CJIS.

  Cost estimate: 2 staff days each for Chelsea and CHSB; $2,500 to $5,000 for router/switch at CHSB; $1,000 worth of incidentals.

- Make VPN connections using public Internet. Interisle Consulting Group has stepped forward to create at least multiple VPN connections between PSnet participants using the public Internet. This helps demonstrate the feasibility of establishing connections to any point that can be reached via the Internet using commodity appliances and low-cost Internet

connections employing DSL, cable or even fiber interconnects. In turn, the ability to rapidly establish PSnet connections between any two public safety operations can promote the development and deployment of shared applications without having to wait for network connectivity to be delivered by more traditional means.

Cost Estimate: Already completed for pilot using donated gear; cost to replicate is one staff week (total from planning through testing) plus VPN firewall at each location (less than $1,000), plus the cost of a low-end Internet connection if one does not already exist.

- Connect MBTA fiber and City of Cambridge fiber. If the MBTA fiber and Cambridge fiber were interconnected at two points (Alewife in West Cambridge and Lechmere in East Cambridge), then both systems would benefit. The MBTA star topology, currently vulnerable to single points of failure, would become a much more resilient ring, for parts of the Red and Green lines. Similarly, although Cambridge's infrastructure is a ring in the central portion of the city, it is a star at the edges; the MBTA fiber could close this into a ring for Cambridge.

  Cost: This is currently being investigated by Cambridge and MBTA; depends upon the difficulty of obtaining access to the MBTA communications gear rooms from public right-of-way.

- Interconnect PSnet to ITD's OC192 ring, potentially at two locations: Boston City Hall and ITSD in Chelsea. This would provide additional connectivity at several key locations, including the State Police facility in Framingham and the associated Intelligence Fusion Center.

  Cost: Subject to negotiation between PSnet and ITD, which has not to date developed a chargeback model for municipal users of the ITD ring.

- Create remote console access over IP to the Boston radio CEB.

  Cost: Details not yet available; dependent upon the availability of donated gear (Cisco LMR equipment); other costs dependent upon whether Boston does the work in-house or uses vendors.

- Connect the Web EOC server to PSnet so that WebEOC users at locations served by PSnet can access WebEOC without traversing the public Internet.

  Cost: Entirely soft; one week staff time from planning through testing.

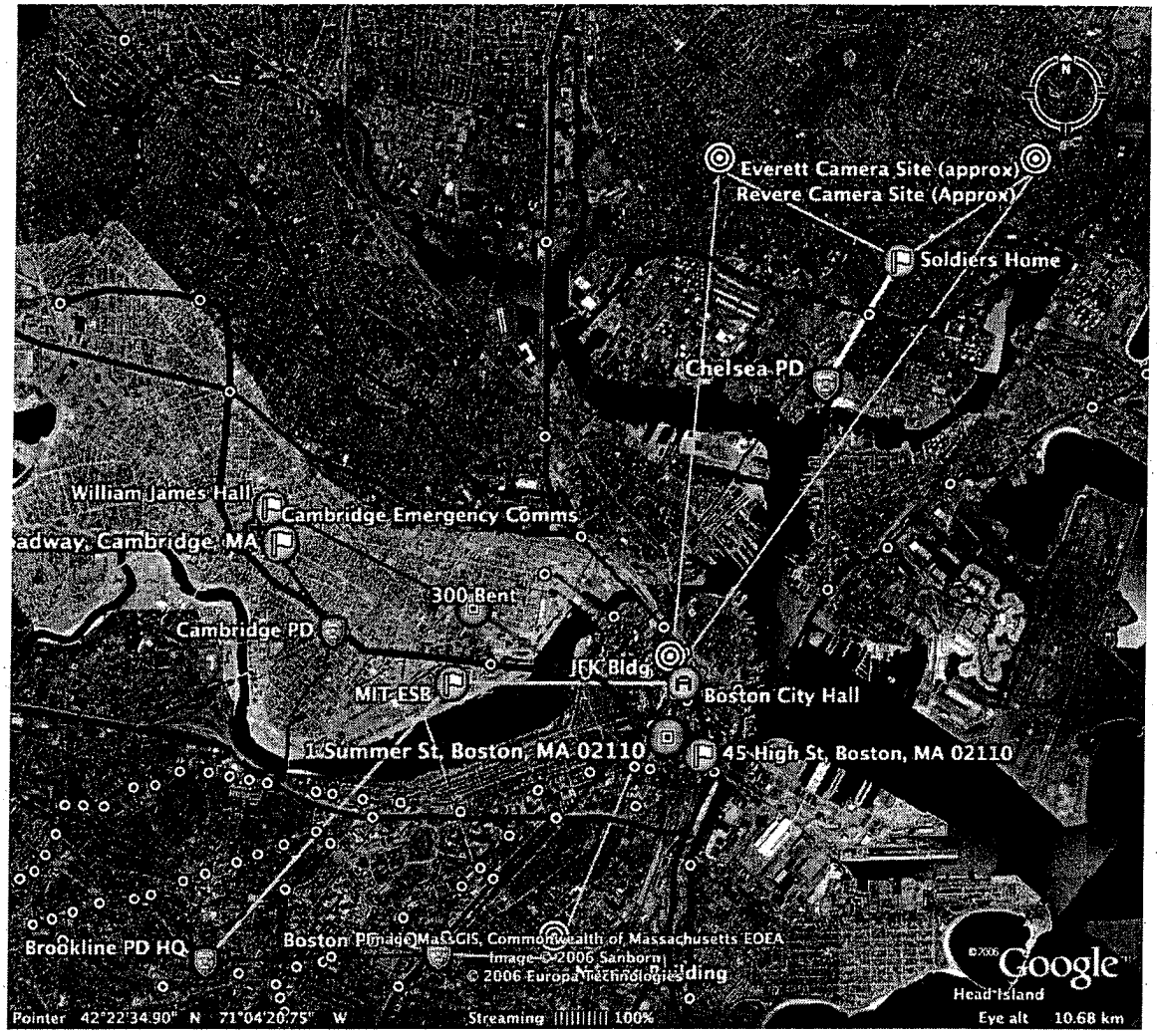

Figure 1: This map illustrates some of the existing and proposed network infrastructure elements.

5 Fundamental Principles

Several themes emerged during the study, which we believe are worth stating explicitly. In addition to the themes that emerged, we have articulated a number of fundamental principles that guide the specific policy, technology, and operational choices we recommend, and that can continue to guide further development of PSnet. This section highlights these themes and principles

5.1 Themes

- **Think globally, act locally.**
  In reality, few players have the ability to act globally, but their local actions can still contribute to a globally significant outcome. Municipal officials, acting at the local level, are in a position to influence the way public safety networking is done.

- **It's all data.**
  An important Internet principle is that **all** communications can be reduced to the transport and exchange of digital data. Convergence of many applications (e.g., phone, internet connectivity, cable TV) onto common data communications infrastructure is a "mega trend" playing out in every facet of modern life. Separate voice, video, and applications networks no longer make sense when a single network can serve all three.

- **A network of networks for a community of communities.**
  Our audience understands their roles within the various communities in which they participate, and they understand the increasing overlap between these communities. We want the PSnet concept to reflect this orientation. Somehow, it must be clear that if they use a network today as part of a public safety community in which they participate, then that network will be part of the PSnet network of networks.

- **Convergence of applications.**
  PSnet can evolve to support a broader array of applications, but it can also establish a framework for application convergence. Key convergence opportunities exist in messaging, records management, web applications, voice services, video, and collaboration tools.

- **Authority must follow the natural structures already in place.**
  PSnet does not require any new authority, and must reflect the existing authority relationships. This is a "federal" model that is increasingly being reflected in the structure of modern networks.

- **Leverage what's already been built to achieve new synergies.**
  By interconnecting networks that already exist, PSnet creates a whole that

is much bigger than the piece parts, but the effect is amplified by the substantial infrastructure already at hand. (Our inventory of existing network resources comprises many substantial networks that have only recently come online.)

- **Leverage commodity technologies.**
  Not just any interesting new technologies, but mature technologies that have been proven over time. Ethernet, fiber optics, routers, web applications, WiFi, radios, and VPNs are all examples of mature, standards-compliant, commodity technologies that have roles in PSnet.

- **Strengthen partnerships between public safety and other agencies.**
  Public safety cannot and should not "go it alone" when developing network infrastructure, because the widespread adoption of standards-compliant networking, and the availability of advanced security techniques, practices, and products make it possible to achieve secure networking (e.g., FIPS 140-2 compliant equipment) while traversing public or shared network infrastructure.

- **Increase community control over critical network resources.**
  Communities need to insure that the networks that are vital to their missions are built to meet the communities' needs. This includes control over costs, path diversity, geographic reach, and service levels.

- **Resiliency can be a major benefit from sharing and planning.**
  Public safety services rely on networks, but typically cannot afford to build in sufficient redundancy and diversity for every application. However, by sharing infrastructure across applications and community boundaries, greater resiliency can be achieved at lower overall cost.

- **Diversity is a goal, but also a challenge.**
  Diversity as a principle allows systems to be more flexible and resilient, but too much diversity can lead to challenges in managing complexity and uncontrolled costs. PSnet will have to strike a balance between these two sides of diversity.

5.2 Principles regarding participants

Some of the principles pertain to ensuring that PSnet serves the needs of its participants, and that it is easy for new participants to join:

5.2.1 Open-ended Structure

PSnet is expected to grow and change over time. It cannot be known in advance what entities will participate in PSnet. Therefore, all technical, operating, governance, and funding mechanisms must allow for the addition of new

participants, the removal of those who no longer wish to participate, and the merging and separation of participants.

5.2.2 Widely Disparate Service Requirements

PSnet participants will have widely varying requirements for bandwidth and availability. PSnet should not intrinsically limit the most bandwidth-hungry participants, nor force the less bandwidth-hungry to acquire more than they need. Similarly, different participants, different applications, and different geographical locations will have different requirements for network availability. Although the PSnet backbone needs to operate at the highest level of availability, connections into the backbone should offer and encourage, but not always require, multiple geographic paths and high availability.

It may be desirable to offer two types of participation: those who connect directly and those who don't (yet). The former are the active operators of PSnet; the latter are there primarily to learn and potentially to align their own future network plans with PSnet

5.2.3 Low Barrier to Entry

The barrier to entry for new participants, particularly those with low bandwidth requirements, limited in-house technical expertise, and small budgets must be low. Membership in PSnet should not automatically entail a large contribution of dollars, staff time, physical resources, or technical expertise. At the same time, PSnet should avoid getting in the business of becoming like a retail ISP and supporting large numbers of low-bandwidth connections into the backbone.

5.3 Principles regarding the nature of PSnet

A second set of principles deals with the technical nature of PSnet itself; these principles are focused on maximizing the broad applicability and easy extensibility of PSnet.

5.3.1 "Network of Networks"

PSnet participants own and control their own networking infrastructure, and they also participate in PSnet. PSnet is built by interconnecting other networks, some of which are owned and operated by PSnet participants, some of which may be built specifically as part of a "PSnet backbone" and others of which may be built and operated for other purposes. The choice of protocols and standards should encourage this interconnection. The task of connecting new networks into PSnet should minimize the disruption either to the new network being connected or to existing PSnet participants.

5.3.2 Commodity Technology

PSnet should take advantage of fundamental changes in the telecommunications market by using interchangeable, low-cost, non-proprietary, and widely available technology wherever feasible. This allows PSnet participants to shift their financial burden from recurring costs to one-time capital expenditures.

5.3.3 Neutral With Regard to Application

PSnet is not optimized for any specific application. It is not a surveillance camera network, nor a criminal justice information system network, nor a first responder dispatch network, nor is it a radio network. It is a generic data network that should be capable of supporting all of those applications and many more.

5.3.4 Neutral With Regard to Underlying Technology

PSnet is not built out of any one specific physical or data link layer. It is not a fiber network, nor a wireless point-to-point network, or a frame relay network, or an ATM network, although parts of PSnet could use any of those technologies as well as others. It must be easy to interconnect various types of networking infrastructure by complying with broadly accepted industry standards and PSnet-established practices.

5.4 Principles regarding security

An important set of principles deal with how PSnet can create a secure environment using a wide variety of shared, interconnected infrastructure:

5.4.1 Pragmatic Security

Security is often portrayed as conflicting with pragmatic goals for deploying networks and applications. However, it is both feasible and necessary to take a pragmatic approach to implementing security in modern systems. Ideally, security should be "designed into" the solutions, but the reality is that many solutions already deployed by communities are deficient relative to modern security threats. Some important principles of pragmatic security include:

- Perfect security is impossible; the challenge is in deciding what is good enough for today.
- Threats are constantly evolving, so security must also evolve. "Good enough for today, but much better tomorrow" must be the approach.
- There are threats associated with not moving forward. Preventing progress because of concerns about security is a ruse that leads to greater insecurity due to inaction.

- Compliance with statutory and regulatory requirements is essential, even when there may be resulting conflicts at the community level where multiple public service organizations share common resources and even staff.
- There will be inconsistencies in the security approaches taken by different communities. As communities share common infrastructure and services, the consequences of inconsistencies must be identified, and ultimately addressed.

In order to develop a rational approach to achieving adequate security, PSnet will have to establish priorities that consider issues of compliance with requirements and mandates, the limitations of existing systems and applications, the needs and concerns of specific communities, and the availability of expertise to implement and support security procedures and practices.

5.4.2 Support Multiple Security Policy Realms

The PSnet communities must confront many sources of policies, including security policies. As PSnet introduces new, shared infrastructure and common services, it will accumulate an increasingly complex set of policies that must be considered as security measures are deployed by each individual community. For example, CJIS policies that relate to law enforcement have already introduced challenges for communities that have consolidated radio infrastructure to support police, fire, and EMS mobility. This has led to additional measures to ensure that only police officers can access CJIS applications that might be made available over a network that also supports other public service providers.

The best way to address this challenge is for PSnet communities to collectively identify policy conflicts and develop common recommendations to deal with these conflicts. If every community tackles policy conflicts on its own, then the overall risks will be higher along with the effort to manage policy compliance.

5.4.3 Accommodate Security Mandates

Unfortunately, there are many security polices expressed as mandates by various authorities, including those that are "unfunded." Furthermore, the evolving threat environment results in its own mandates. For example, all communities must deal with threat-related mandates coming from various security watchdog organizations (e.g., CERT) and from vendors (e.g., Microsoft's first Tuesday of the month mandatory security patches).

For Police and other law enforcement agencies, the State and Federal government have stipulated various security requirements that all municipal law enforcement agencies must meet. Similarly, there are increasing sources of security mandates affecting health care providers that extend to emergency medical services. As security threats continue to evolve, and as public concerns

increase, the likely result will be more mandates governing security practices and procedures.

There is no way to avoid these mandates, but there may well be opportunities to leverage PSnet sharing to avoid duplication of effort and achieve greater efficiency in meeting mandates. As new mandates emerge, there will be opportunities to respond and address these mandates in a collective manner.

5.4.4 Utilize Existing Authorities

In today's public service environment, communities serve as local authorities, but must accept the authority of multiple regional, state and federal authorities. Even an individual public safety officer must deal with multiple authorities operating at different levels, especially as there is increasing reliance on information services provided by various authorities.

Given this context, PSnet security must reflect existing lines of authority. For example, a State criminal justice application that can only be accessed by police officers does not itself decide who is a police officer, but depends on the individual municipalities to define who is authorized to access the application.

Adherence to existing lines of authority leads to a "federated" model of security, for which technical solutions have been emerging for much of the past decade. Fortunately, some of these technical approaches have matured, and can be incorporated into PSnet plans and deployments.

What PSnet must constantly strive to avoid is the accumulation of multiple security mechanisms associated with different authorities that every individual user must somehow manage. For example, human beings cannot adequately deal with dozens of distinct userID/password combinations. Similarly, police officers already have a lot of hardware hanging off their belts; we need to be careful not to add multiple cryptographic devices (a.k.a. "security dongles") if other approaches can be followed. In particular, multi-factor authentication often requires some sort of hardware authentication device, but individuals who use such devices should not have to carry around multiple devices to access different systems and applications. Not only would this be inconvenience, it ultimately undermines real-world security while significantly increasing costs.

Today's public safety community is already based on federated models of authority, including the obvious federal, state, and local lines of authority. PSnet security practices should be oriented toward these existing models. A federated model of authority can provide a framework for addressing security requirements in ways that are practical, cost-effective, and reasonably convenient for individuals.

5.4.5 Share Security Expertise and Information

Security expertise must be constantly honed as threats and technologies evolve. However, not every community will be able to maintain local expertise on all relevant security topics. Consequently, PSnet can facilitate sharing of expertise while promoting common approaches and practices that will leverage the security expertise at hand.

Information about security concerns, including threat incidents, is another way that sharing can improve the collective ability of all PSnet constituent communities to respond and adapt to the evolving security context.

5.4.6 Compliance and Audit

As PSnet evolves, it should be possible to address some compliance and audit requirements within PSnet itself, rather than within individual communities. This presents opportunities for improving oversight without adding further cost burdens. It may also lead to ease of deployment for new applications, if the underlying network has already been deemed compliant. Even where communities operate their own networks, they may be able to inherit some audit results by maintaining consistency with the PSnet framework.

One approach already recognized by the audit community and many existing state and federal guidelines would be to have some local functions effectively "out sourced" to the PSnet infrastructure and services. This does not mean that staff or functional roles would need to shift, but merely that common procedures and practices could be handled in a shared manner. This will make it easier for all participants to benefit from compliance measures and audit results associated with the shared security procedures and practices.

5.4.7 Presume vulnerability

Because of the diversity of participants, infrastructure, and local policies, PSnet security must start with a presumption of vulnerability and exposure to a variety of threats. PSnet will carry traffic that pertains to ongoing law enforcement activity, criminal records, and other data that are highly sensitive. Many members have access to PSnet. PSnet is built using shared multipurpose infrastructure, to which others have access. The nature of PSnet implies that there will criminals, terrorists, and other groups highly motivated to disrupt the network and/or to intercept and monitor traffic.

5.4.8 Limit consequences of physical access

Physical access to the PSnet network or to the data stream it carries should not be sufficient to monitor or alter the content. E.g., sensitive data should be encrypted end-to-end. Ability to inject traffic into PSnet should not be sufficient to disrupt PSnet communications system wide. Physical access to a segment of PSnet or to a

single communications facility should not be sufficient to disrupt PSnet communications system wide.

5.5 Principles regarding how PSnet is run

A final set of principles deal with the operation and governance of PSnet:

5.5.1 Minimal but sufficient Policy Framework

It's possible for a multi-purpose network like PSnet to become paralyzed, at a policy level, by the need to "answer to many masters" – by the overlapping policy domains and (in unfortunate cases slightly contradictory) requirements imposed on the network by statute and regulation. State law (e.g. 6 MGL 168) governs the handling of criminal offender record information. Other regulations, promulgated by the FBI via the CHSB, govern other law enforcement data. Still others deal with privacy of records.

PSnet should not be a source of significant new policies. Only a minimal set of policies are needed to provide guidance on how constituent communities can share PSnet without causing additional headaches for themselves and others. Ideally, the PSnet policy framework should consolidate existing policies while introducing only new policies where there are clear gaps or the need to promote common benefits or effective sharing.

Fortunately, modern network technology permits multiple policy realms (e.g. multiple sets of rules regarding encryption or access control) to be implemented within a single physical network.

5.5.2 "Most Local" Decision Making

Although PSnet is accountable for complying with the mandates imposed by the various applicable policy realms, PSnet should be structured so that most decision-making defaults to the "most local" level. PSnet participants already have in place governance structures that work, and that are already used to acquire and operate networking technology.

PSnet must install system-wide administrative controls at the access and acceptable-use policy level; align with local public safety policies (looking down) and national/Federal public safety policies and standards (looking up). Those looking to apply regional solutions developed elsewhere should be aware of the degree to which East Coast is home-rule oriented, where local towns and governments each make their own funding decisions for public safety.

This approach also makes it possible to obtain a very high level of technical oversight by leveraging PSnet's geographical location, taking advantage of local industry and academic experts who could serve (pro bono) on the PSnet technical and advisory boards.

5.5.3 Authority must follow the natural structures already in place

PSnet might not require any new authority, and must reflect the existing authority relationships. This is a "federal" model that is increasingly being reflected in the structure of modern networks. PSnet must follow the existing authority structures that govern its design and operation.

5.5.4 Defer some policies

There is a clear distinction between (a) policies that must be established *a priori* in order to define and build PSnet at all, and (b) the policy-development apparatus that will be part of PSnet the organization. Not every policy needs to be established at the beginning, only a small essential set. The governing body can develop the rest once it is operational.

5.5.5 Separate policy from enforcement

Setting policy is not the same thing as enforcing policy. Policy-development structures need not coincide with policy-enforcement structures—for example, it's possible to have a central Interop[5] -like group debating and seeking consensus on PSnet-wide policies, but to rely on local (or more local) agencies for enforcement.

[5] Interop is a self-governing collaborative initiative

6 Architecture

The PSnet project will create two distinct tangible results:

1. A core network, to which PSnet members will connect for the purpose of exchanging network traffic. This is the network referred to in this document as "PSnet" and which is governed by the architectural principles listed here in this section.
2. A set of infrastructure sharing arrangements that are not necessarily a part of the core PSnet network. One PSnet member may share right of way, conduit space, fiber strands, private virtual circuits, antenna sites, communication closets, or other facilities with another. To the extent that they do not affect the PSnet core network, these infrastructure-sharing agreements will not necessary be subject to the same principles and policies as the core PSnet network. The PSnet organization can nevertheless serve its clearinghouse function with regard to participants wishing to make bilateral resource-sharing agreements.

6.1 Underlying assumptions

Four key assumptions underlie our recommendations for the PSnet architecture:

- PSnet is a "network of networks:" it is assembled, in part, by connecting together existing networks, many of which were originally built for other purposes.
- PSnet achieves leverage through shared, common infrastructure: portions of the network carry other traffic in addition to PSnet traffic.
- PSnet is open-ended: it is expected to grow organically over time as new participants join and as new network links are added
- PSnet leverages technology advances: it is intended to take advantages of changes in the marketplace brought about by inexpensive, widely deployed commodity networking technology.

6.2 Internet architectural principles

The PSnet assumptions are similar enough to the assumptions underlying the public Internet that we recommend the adoption of the technical standards and protocols that apply to the public Internet. These standards and protocols allow PSnet to benefit from the wide availability of commodity-priced technology and data transport, and from operating principles that have been thoroughly vetted in the real world.

In particular, we recommend that PSnet be a routed IP network.

6.3 Fundamental topology

There are three distinct approaches for the fundamental topology of the PSnet network: a backbone architecture, a peer-to-peer architecture, and a hybrid architecture.

6.3.1 Backbone Architecture

Under the backbone architecture approach, there would be a central backbone network operated by or on behalf of PSnet. The backbone network would have "access nodes" distributed throughout the region. An access node is simply a router located at a facility to which it is easy for PSnet members to obtain their own connections, for example a communications closet in a centrally located public building, or a telecommunications "carrier hotel" at which multiple carriers have points of presence. Each PSnet member would be responsible for providing and operating its own connection to the backbone; traffic exchanged among PSnet members would traverse the backbone network. Typically, PSnet members would connect to the backbone at more than one access node, to achieve a measure of path diversity and to eliminate additional single points of failure. Note that the backbone itself may be purpose-built from scratch, or it may be built by connecting network elements (e.g., fiber runs and routing infrastructure) already owned or controlled by PSnet members.

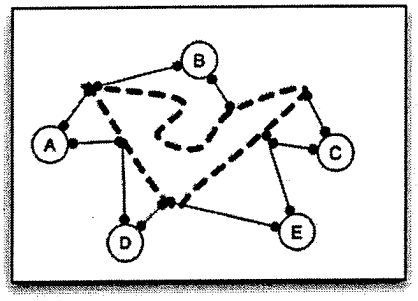

Figure 2: Under the backbone architecture proposal, each community member (circled letters) connects into the PSnet backbone (dashed red line, shown in this example as a ring.)

The backbone architecture is conceptually simple, and offers both the benefits and the drawbacks of a centrally run facility: On the one hand, it is possible, by pooling resources, to build a more resilient, higher performance backbone than anything the members could economically build acting individually. On the other hand, the backbone itself becomes critical infrastructure for all PSnet members, and must be engineered and operated accordingly, which imposes cost and administrative burdens.

6.3.2 Peer-to-peer Architecture

Under the peer-to-peer architecture approach, there would be no "PSnet backbone." Instead, each PSnet member would build and operate one or more "access nodes" of its own, and will arrange for connections with two or more other PSnet members. PSnet members wishing to exchange data would do so either over a direct connection between them, or by transiting the networks of

one or more intermediary members, who would, in effect, act as carriers for each other.

The peer-to-peer network is conceptually attractive to those who favor a grass roots, "bottoms up" approach. It makes it easy to extend the network, and the resulting network is not dependent upon any central infrastructure, and offers some theoretical advantages in the area of resiliency and survivability.[6] On the other hand, the individual PSnet members are not as likely to have round-the-clock technical staff as would a backbone operator.

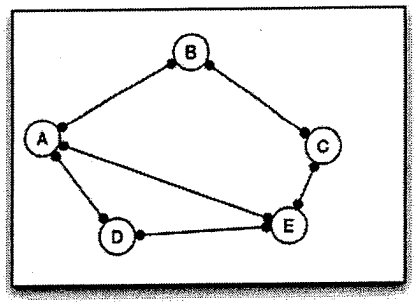

Figure 3: Under the peer-to-peer architecture proposal, each community (circled letters) connects to two or more other community members, without a backbone network.

The peer-to-peer model requires careful attention, on the part of those who act as transport providers for each other, to the question of exactly what is being offered and promised. It requires clearly documented understanding regarding the volume of traffic to be carried, network performance, availability, and support, security policies and practices, and other issues. These individual peer-to-peer arrangements would need to be standardized in some way so that participants have a clear understanding of what the network as a whole does and does not provide.

[6] Those advantages are not significant in practice—a backbone network can be designed and built with any desired level of redundancy.

6.3.3 Hybrid Architecture

Under the hybrid architecture approach, there would be a PSnet backbone with access nodes, exactly as in the backbone model, but not every PSnet member would need to connect to the backbone. Each member would connect **either** directly to a backbone access node, or to an intermediary member network that is connected to the backbone, assuming the intermediary agrees to provide transit to the backbone for that member. We believe the hybrid architecture offers the best opportunity to build a strong, high performance core network, while at the same time keeping the entry barrier low for those who cannot easily or cost-effectively connect to the backbone. We recommend that PSnet be implemented with the hybrid architecture approach. This approach requires technical staff dedicated to monitoring and supporting the backbone network (As does the backbone model).

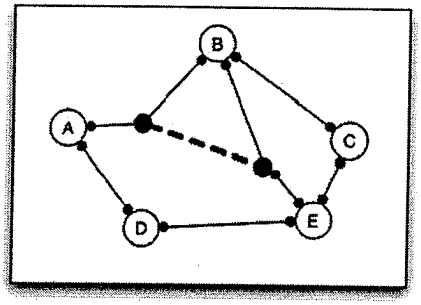

Figure 4: Under the hybrid architecture proposal, each community (circled letters) connects either to the backbone directly (e.g. A, B, E), or via an intermediary who provides transit to the backbone (e.g., C, D).

6.4 Interface to the backbone

In the interests of manageability and consistency, we recommend that PSnet limit the options for connecting to the backbone to one or two possibilities, for example, Gigabit Ethernet or 10/100Mb Ethernet. This limits the cost and complexity of the backbone routers and switches. Members wishing to connect in other ways (e.g., at lower data rates) should aggregate their traffic with another member before connecting to the backbone.

We further recommend that the interface be at the routed IP level—i.e., that no layer 2 switching, VLANs or similar services be exposed beyond the backbone or managed system-wide.

6.5 Routing architecture

The high-level decisions concerning the routing architecture of PSnet follow directly from the fact that PSnet is a routed IP network (Section 6.2) organized according to a hybrid interconnection architecture (Section 6.3.3), and from the design goal that PSnet be able to grow and change flexibly over time (Section 5.2.1) as new participants join the network, new equipment and services are deployed, and the purposes for which PSnet is used evolve. These factors combine to strongly recommend a PSnet routing architecture that recapitulates, on a smaller scale, the routing architecture of the Internet itself: locally managed

domains that exchange reachability and other routing information among themselves and with a commonly accessible core (backbone). Such an Internet-standard architecture enjoys the advantages of management simplicity, dynamic reconfigurability, and the ability to scale organically without centralized administration or control.

The details of the routing architecture—where and how to define the boundaries between intra-domain and inter-domain routing, how to provide Domain Name System (DNS) services, precisely how to manage the assignment of IP addresses and other identifiers (see Section 6.7), and how to connect PSnet to the public Internet—depend on decisions that have yet to be made about the practical organization of PSnet as a real-world deployed infrastructure:

Some PSnet participants will want to manage the routing of traffic within their own networks as an independent activity, and will be able to do so; others may choose to outsource this function to an Internet service provider (ISP) or other communications company; still others may decide to join forces and manage these functions collectively rather than individually.

PSnet could be organized to serve as an (or the) ISP for some or all of its participants, either in conjunction with existing ISP arrangements or in lieu of them. In that role, PSnet could provide the IP address, routing, and DNS management functions of a traditional ISP.

Different PSnet participants will make different policy decisions about how other participants may use their networks (e.g., for transit traffic, or as alternative-path backups), and will be free to negotiate a variety of arrangements with neighboring participants to achieve economies of scale. These decisions and arrangements will affect the way in which PSnet routing is organized, so they will have both local and PSnet-wide impacts.

Arriving at mutually agreeable decisions on these and other issues that will determine the details of the PSnet routing architecture is logically an activity of the proposed Technical Committee (Section 8.3.3).

6.6 Security architecture

The PSnet security architecture must support the security requirements discussed above in Section 5. In particular, the PSnet environment is characterized by:

- A network carrying several different kinds of traffic, each subject to its own security policies.
- A network in which there are multiple participants, each of who may wish to stipulate security policies applicable either to its own data or to others wishing to connect to it.

- Overlapping jurisdictions; overlapping security mandates.

Fortunately, modern security architectures, having evolved in a world where traffic must be carried securely over highly insecure infrastructure (e.g, the public Internet), are up to the job.

6.6.1 Defense in Depth

Adequate security can never be achieved through a single technology, counter-measure, or practice. Instead, multiple approaches to security must be employed that operate at all levels of the system. The security architecture should presume that portions of the network are compromised. A successful exploit of vulnerability in one portion of a system should be countered by other portions of the system, or at least detected by other system elements. Designing systems to employ overlapping security measures is often referred to as "defense in depth."

PSnet security architecture should provide defense in depth from several perspectives, including human controls and oversight. Several key aspects of this approach are outlined below as specific architectural guidance.

As a shared infrastructure, PSnet presents an opportunity to deploy additional defensive measures beyond what might otherwise be deployed within a specific community or application context. Again, participating communities should be able to inherit security measures and practices from PSnet that enhance security at a local level.

An important architectural objective of PSnet is to improve overall resilience of networking services used within a public safety context. By adding diversity and redundancy, PSnet will contribute to further hardening of the overall network infrastructure from a survivability perspective, which is an important element of any defense in depth strategy.

6.6.2 Layered Security Architecture

A security architecture should be "layered" in a directly analogous manner to the network architecture. This results in more effective modularization of functions as well as providing defense in depth, since a security measure implemented at one layer can serve as a backstop to security measures implemented at other layers.

6.6.2.1 Physical Access Controls

While it is impossible to protect all assets of a geographically diverse network, it is still important to provide physical access controls for critical components of the network, including switching equipment, transceivers, and network management facilities. Guidelines will need to be developed and promulgated for controlling access to vital network facilities, while recognizing that many

network elements will have to operate in environments where it is difficult to control who has access to that element.

6.6.2.2 Network Security

Security measures can be deployed at the network layer, including authentication and access control for users and nodes operating within or over the network, as well as protection of confidential information flowing through a network. Network layer security can be deployed in support of specific community interests or as generic protections that can be utilized by all users.

VPN technology, for example, is a mature network layer security measure that can be deployed to protect a single application, or a community that utilizes multiple applications. It can be used to create an isolated network that spans both trusted and untrusted networks, including paths over the public Internet. VPN tunnels can be used to connect various workgroup LANs together over an arbitrary network. Similarly, an individual workstation or server can directly support VPN connections across PSnet or the public Internet.

Firewalls are another form of network layer security commonly used in modern internets, although some firewall services are also associated with application layer security (see below). Packet filtering is one firewall technique that can be effective in providing security protections as well as preventing a variety of network failures. Network Address Translation, or NAT, is another firewall technique that offers effective protections by preventing any outside party from initiating a connection to a host residing behind a NAT firewall.

6.6.2.3 Application Security

Ultimately, every application must incorporate security measures appropriate to the application itself, and whatever policy realms govern use of the application. Unfortunately, many of the applications currently deployed by public safety organizations were not designed with security in mind, and are consequently dependent on external controls to meet security requirements. This will present challenges to extending these applications across PSnet.

In addition to network layer security measures, application gateways and firewalls can be used to augment security for applications, especially applications that have security deficiencies. For example, a web server front end might be added to an existing application to allow remote users to access portions of the application via secure SSL (or TLS) sessions.

Often, the most effective place to integrate fine-grained security measures is within an application, where it is possible to address specific policy requirements and determine which parties are allowed to access which resources or perform transactions. Such fine-grained measures can be combined with network

awareness to implement controls based on where a user is coming from or what device they are using. For example, an application might allow access to certain sensitive information for users operating within a specific office area "local" to the application, but deny access to users operating from other locations outside of controlled areas. However, the same application might provide a subset of services to remote users.

Some Internet-oriented applications (e.g., Web, email, and ftp) incorporate security measures that can be used effectively within a PSnet context. For example, both Web and email services can employ SSL (or TLS) protocols to secure communications between a client application and a server. Similarly, file transfer services and some conferencing services can leverage ssh protocols to secure communications between parties.

In the case of Web security, modern Web servers not only support https connections via SSL, they also provide moderately robust facilities for controlling access to specific resources, and even other Web servers. This flexibility can be leveraged to deploy Web-based interfaces to information resources that may well be provided by multiple communities. The Web EOC application is an example of one such application that has already been deployed.

While email is often regarded as a vulnerable application and a vector for many forms of attacks, it can also be augmented with security measures that allow for strong authentication of correspondents and encryption of email messages and associated attachments. Secure email capabilities are widely supported in nearly all email clients today, including the popular clients provided by Microsoft and various open source initiatives. A near-term win for PSnet could simply be the adoption of secure email practices amongst participating public safety agencies.

6.6.3 Generic Security Architecture

Another way to develop an effective security architecture is to introduce modular approaches that allow for reuse of common technologies and simplification of deployed solutions. In essence, promulgate the use of reusable components and modular building blocks.

6.6.3.1 Authentication

The ability to confirm the authenticity of parties over a network is a common requirement for which modular approaches can be deployed. However, authentication is a challenging security problem that also requires the use of multiple techniques. Furthermore, traditional approaches have resulted in individuals having to maintain dozens of userID/password combinations, yet passwords are widely regarded as one of the weakest ways to authenticate users.

As PSnet extends the array of applications available to users, it will also be increasing the population of users that each application will have to authenticate. This runs the risk of further burdening both applications and the people who must manage these applications.

Increasingly, public safety applications are under policy mandates to employ stronger forms of authentication, often based on multi-factor techniques that add new devices, such as crypto tokens, one-time password (OTP) fobs, or biometric scanners. These new, stronger forms of authentication can add costs while further burdening users.

PSnet presents an opportunity for communities to pool expertise and resources to address the challenges associated with stronger authentication, while also reducing some of the burdens on users and lowering system complexity. However, this does not mean that every community will have to deploy the same technology, but it may mean that "federated" schemes will be needed that allow applications to rely on other authorities to authenticate users.

6.6.3.2 Access Controls

While "access control" depends on the ability to authenticate parties, it is a distinctly different security service that addresses the questions of which (authenticated) parties should be able to access what specific information or services. Most public safety applications must—as a matter of policy—strictly control access to the application and associated information. As communities increasingly share information and applications with other communities, the access control challenges will grow in scale and complexity.

There are two distinctly different models for sharing applications, each with its own access control issues.

- Existing applications used by one community that are shared with members of other communities. For example, a police bookings application used by the Police Department of one municipality, with access offered via PSnet to Police Detectives in neighboring municipalities.
- New applications that are designed to support multiple communities working in some collaborative manner. The Web EOC application is one such example that has already been deployed and used by multiple overlapping communities.

In each model, there must be some means for establishing the access rights and privileges for individual users, but the authority for granting access rights and privileges will reside with different officials in each case. For the second model, it becomes important to make sure that an appropriate authority is established to administer access rights and privileges.

The access control challenge represents another problem that may benefit from a "federated" approach. This might mean, for example, that individuals first authenticate and gain access to a local system that would likely be operated by their employer (the "authority" in this case). They could then access other systems beyond their local context through their local system, which would vouch for the individual and the access privileges they should be entitled to. A community that shares its application with other communities could depend on those communities to vouch for their employees on a real-time basis, which would simplify managing access rights and authentication procedures.

6.6.3.3 Common Security Machinery

Some security machinery may be appropriately offered as part of the overall PSnet infrastructure as a way to share costs and improve interoperability. One such opportunity for deploying shared security machinery is for the PSnet community to deploy a common Public Key Infrastructure (PKI) for issuing public key certificates that can be used for a variety of applications.

Public key certificates, or certs, are widely used for authentication, access control, encryption of sensitive information, and digital signatures. Many modern applications and all modern operating systems support certs, and the trend is clearly for wider use of certs. For example, secure https Web sessions based on SSL (or TLS) require that the server have a certificate to authenticate the server to users as well as to facilitate key exchange for encrypting traffic between the Web server and client browsers. However, all browsers also support client-side certificates that can be used to authenticate the user to the server. Similarly, secure email utilizes certs for both signing and encrypting email messages, and nearly all popular email clients support certs and secure email today. Certs can also be embedded in smart cards and other types of crypto tokens to further strengthen security and support multi-factor authentication. Certs are even used to authenticate parties in VPNs and to handle key exchange for encryption.

The problem is that commercial certificate issuing services (e.g., VeriSign) are not well suited to the needs of public safety agencies or state and local communities. The cost and complexity of operating a certificate issuing service has been reduced substantially in recent years, and there are significant advantages to operating this sort of machinery at a regional, or even community, level. It is important to note that, if PSnet were to provide certificate issuing as a shared service, this service would not displace any current authorities. Instead, existing communities would be able to leverage PKI services offered at the PSnet level for their own purposes under their own authority, but also in applications that are shared with the greater PSnet community.

PKI has also spawned new services that might appropriately be deployed as part of PSnet. For example, Online Certificate Status Protocol (OCSP) servers allow

any party relying on a certificate to immediately check the status of a cert in real time. Again, this capability is increasingly provided within commodity Web and email applications, but can also be easily leveraged by any modern application using both open and proprietary off-the-shelf software.

Token issuance is another PKI-related service that may be relevant to the PSnet community, especially for tokens that are based on certificates, including smart cards, USB dongles, and even some biometric authentication devices. It is also worth noting that, with the advent of TPM[7] technology, "crypto tokens" are now being built into many computers and mobile devices.

Services based on VPN technologies represent another opportunity for PSnet to deploy common machinery that could be used by all constituents. In particular, VPN services could be offered that would allow anyone working in a public safety agency to connect into PSnet via a secure VPN connection, and from PSnet gain access to shared services as well as services associated with their own local community. With many communities offering telecommuting and other ad hoc access methods via the public Internet, PSnet could consolidate these offerings in ways that would lower overall costs while increasing resilience and security. This could also help the entire UASI region improve preparedness for certain types of events, including pandemics or natural disasters, by providing ways for all public safety workers to access critical services no matter where they are located or displaced to in the event of a crisis.

To the extent that NAT firewalls are used by PSnet communities to protect specific subnets, there will need to be some "NAT traversal" services to allow parties sitting behind NAT firewalls to communicate with each other. Various NAT traversal technologies have emerged in recent years, and have been popularized by applications such as Skype and video conferencing services. If uncontrolled, NAT traversal services can undermine security in a public safety context, but if NAT traversal were incorporated into PSnet, then it would be possible to further enhance security.

6.7 Names and numbers

PSnet must incorporate a mechanism for managing the assignment of names and numbers (e.g. DNS names and IP addresses). For the pilot, this function is being managed ad hoc by Harvard University; it should be taken over by the PSnet Technical Committee or Operations Group as soon as they are formed.

---

[7] TPM stands for Trusted Platform Module, a specification developed by the Trusted Computing Group for a hardware cryptographic module that can be embedded in computers, mobile phones, and even microprocessors. For example, recently introduced Intel microprocessors that serve as the CPU chips for servers, desktops, and laptop computers, include TPM functionality built into the core processor.

7 Operations

As PSnet is envisaged as a network of networks, each existing network belonging to some community is presumed to have existing operational support in place. Connecting to PSnet should not require any change—the way in which each existing network is managed should continue even after that network is joined in to PSnet. This includes "local" network connections within the community, existing applications, and data that run on, or are accessed via, that community network.

For personnel from a "remote" PSnet community accessing resources within another community, that target community is responsible for defining the policies and procedures, and defining who is able to access which resources and how within that community.

Of interest to PSnet is responsibility for pieces that are outside a single community:

- Who is responsible for managing connections between communities, and
- Who is responsible for managing the PSnet backbone?

As PSnet is increasingly used by communities accessing each others' resources, the communities will come to rely on PSnet—and questions of reliability and responsiveness will become more important. Eventually the correct functioning of PSnet becomes a critical component of many people's jobs. Thus there is a need to:

- Keep PSnet running, sufficiently available, and responsive, so that communities can provide services to, and rely on, each other;
- Diagnose and fix problems when (some aspect of) PSnet is (thought to be) broken and adequate service is not being delivered; and
- Provide a help-desk function, to deal not only with break/fix situations, but also to answer questions, provide information, assistance, and be a source of general communications to the PSnet community.

Initially, where PSnet comprises a few isolated connections between pairs of communities, individuals (from one or the other side of each connection) will be able to take responsibility for managing and supporting those connections. But as PSnet expands, as the number of connections grows, and as the dependence of communities on intermediate communities becomes more relevant, the need for a centralized function and consolidated expertise becomes more important. And as a core backbone network for PSnet emerges, responsibility for the core

network will be seen as outside the purview of any individual community that connects to PSnet.

Such a centralized organization (or organizations) providing break-fix support, problem diagnosis, and help desk functions could be assumed by an existing organization (or coordinated among multiple existing organizations) that has (have) the capability and resources to provide those functions. Alternatively, a new, funded organization might be created to provide these functions. And it is conceivable that these functions could be outsourced to a commercial organization that has the necessary resources already in place.

7.1 Centralized services

While each community is responsible initially for its own applications and data as described above, over time there could be economies of scale realized by providing and operating centralized services in PSnet.

Clearly, providing an overall addressing plan and rules for connecting into PSnet are fundamentally critical to the overall operation and effectiveness of PSnet.

We assume that, at least initially, each community will be responsible for defining who is able to access which resources: authorization, authentication, and access control. While it may seem to be a good idea to create a central directory authority to allow PSnet-wide authorization, authentication, and access control, two things work against this:

1. Each community would doubtless want to maintain strict control over who can access what resources and how, and
2. As the scope of PSnet gets larger (in terms of numbers of communities that are connected to PSnet and the number of people within each community that are using resources available via PSnet), the ability to provide a centralized directory service facility becomes more and more difficult to achieve in a cost-effective manner.

In addition, the principle of "locality of access" works here—that is, most access to a community's resources via PSnet will be from communities in the same or adjacent municipalities, some access will be from communities that are a few municipalities away, and very little access will be from communities in remote municipalities. Thus having each community define their own authentication, authorization, and access control is not an unreasonable approach.

It seems feasible, however, that two communities might decide to provide trust (whether transitive or not) between their respective communities—so that someone authenticated to one community would be automatically authenticated to another community (though access control policies would still be used to

define whether or not a remotely authenticated user could access and use a specific local resource).

Some centralized services may make sense to include in PSnet over time. Some examples of services that could be centralized include:

- Fundamental network services: routing, system monitoring and management.
- Enhanced network services: DNS (name resolution), directory services
- Centralized management of VPN tunnels, including operation of a certification authority to issue digital certificates used for key exchange and authentication.
- Security services, e.g., the issuance and management of network-level authentication and access control (but not application-level)
- Public Key Infrastructure (e.g., issuing and validating security certificates)
- Shared file repositories
- Shared databases
- eMail services, including both secure email and gateways to the public Internet
- Audio- and video-conferencing service

7.2 Operational Support

Who will support the network core? What support (call response, time-to-repair, other?) level-of-service commitments are defined between participants? Between participants and the operator of the core network? Do participants view PSnet as primarily a local thing (they expect their local officials to be the front line of recourse to get things done or to get things fixed), or as primarily a regional or statewide thing? Will there be a "PSnet help desk?

We are unable to make specific recommendations in this area at this time; we recommend that the Executive committee take on, as one of its first assignments, the development of standards, principles, and participant agreements (all based upon participant consensus) as to how the core will be supported (i.e. by the participants directly, by a single participant on behalf of the others, or by a service organization) and what the chargeback model will be.

8 Policies and Governance

For PSnet, "governance" refers not so much to "who is in charge" as to "what structures are necessary to effectively marshal and reconcile the resources, efforts, and interests of the many individual participants in pursuit of the common public safety goals of PSnet." PSnet governance does not replace or usurp the authority of municipalities or regional or state agencies; it is the vehicle for making collective decisions and managing common resources so as to obtain the greatest benefit for all of the participants.

Although many components of a regional public safety network can—and should—be managed locally by the people and agencies directly responsible for them, some decisions and some management functions must be collective rather than distributed. Examples include:

- The deployment and management of a backbone network and its access points, which tie together the mesh of community and regional network facilities to ensure full connectivity and standardized quality of service;
- Fund-raising that depends on the favorable disposition of funding agencies toward regional, rather than strictly local, public safety initiatives; and
- Achieving economies of scale across all of the dimensions of public safety network operation: buying equipment, contracting for services, staying abreast of new developments in technology, practice, and regulation, providing technical and customer support, and educating public safety agency users and public safety beneficiaries.[8]

This section proposes a specific governance structure for PSnet, which follows from and depends on the principles and architecture described in Sections 5 and 6. A different set of driving principles or a different architecture (e.g., a pure mesh with no backbone, or a centralized star configuration) would produce a different set of requirements for governance, and therefore a different governance structure.

8.1 Scope

PSnet is directly concerned only with applications and communications infrastructure that are deployed to support public safety. Its natural constituents—and governance participants—are therefore the public safety agencies and officials within its geographical range. However, it would be foolish to ignore the many ways in which communications infrastructure deployments, in particular, can efficiently serve more than one purpose or more

[8] The public!

than one constituency within a municipal, regional, state-wide, or Federal context. An important element of PSnet governance is therefore to recognize and actively pursue opportunities to "combine forces" with other organizations.

8.2 Attributes

The essential attributes of the PSnet governance structure follow directly from the principles and architecture of PSnet itself.

8.3 Governance structures

PSnet governance is based on three representative bodies that manage the policy-making process, provide a framework for reaching collectively agreeable technical decisions, operate (either directly or indirectly) those parts of the PSnet infrastructure that are centrally owned and/or managed, and provide technical and customer support.

8.3.1 Executive Committee

The Executive Committee is responsible for policy and decision-making.

One executive representative from each organization that is entitled to participate in the decision-making process for PSnet (loosely, "stakeholder") because it is either (a) financially involved (contributing resources or funds) or (b) legally involved (regulator or other oversight agency with executive authority over public safety).

The Executive Committee is responsible for "PSnet the organization," and is supported by the Technical Committee and an Advisory Council.

8.3.2 Advisory Council

The Advisory Council advises, and serves as an expert resource to, the Executive and Technical Committees. It consists of individuals and representatives of organizations with interests and expertise in public safety but no direct executive authority (for example, Northern Crossroads, Motorola, outside consultants, MAPC, public safety officials in other (state or federal) jurisdictions).

8.3.3 Technical Committee

The Technical Committee is responsible for "PSnet the network," and directs the Operations Group and the Technical and Customer Support Group in accordance with the policies approved by the Executive Committee.

Technical representatives are to be nominated by the executive committee (that is, not strictly "one technical representative from each organization that is entitled to participate...").

8.3.4 Operations Group

The operations group will be responsible for actual operation of those parts of the network that are centrally managed, as well as any other network components that a municipality or other PSnet participant chooses to outsource ("upsource") to PSnet.[9]

8.3.5 Technical and Customer Support Group

The technical and customer support group establishes policy and provides technical support and Help Desk services to PSnet participants

8.4 Funding

Individual circumstances and opportunities will determine whether a centralized approach or a distributed approach to fund-raising is more effective. For example, a PSnet governance structure could seek State or Federal grants and other funding on behalf of its constituents, in which case funding would land on PSnet first, and accrue to the benefit of individual participants through a collective process of resource allocation. Alternatively, individual participants could seek public safety funding on their own account, some part of which would be contributed to the PSnet governance structure to be used for common purposes. Various hybrids of these two models could also be constructed.

[9] The opportunity to "upsource" local network elements or operations to PSnet is a subject for further study.

9 Pilot Project Lessons Learned

The pilot project (still ongoing) has offered a chance for us to learn key lessons about the viability and ultimate success of PSnet. Specific findings are scattered throughout this report. Four key lessons are worth highlighting here:

9.1 The basic concept works

The pilot project has demonstrated that interested public safety officials, working across jurisdictional and geographic boundaries, can assemble a high quality network out of existing piece parts without undertaking a massive procurement.

The pilot concept appears to be repeatable and extensible.

9.2 Infrastructure is widely available

Municipal, State, Federal, and interested nongovernmental agencies have significant telecommunications assets: Fiber in the ground, radio towers, leased infrastructure that can be repurposed, etc. The summary in Section 4.3 tells part of the story; we expect that the clearinghouse function (Sections 10.5 and 11.3) to continue to discover useful assets and potential interconnections.

9.3 Application requirements will take time to develop

PSnet facilitates new ways of interaction among agencies that have previously interacted informally. As a result, the requirements are not entirely clear in advance, and are expected to change over time as people learn about the capabilities of the network. For example, we do not know at this time how many people in one municipality are going to be accessing the records management system of another at any given time until patterns of usage emerge. Similarly with new technologies such as voice-over-ip or videoconferencing, there seems to be a group of potential participants who are eager for the technologies and those who see the value as peripheral. Actual demand is very difficult to project at this time; our recommendation is to allow for experimentation and significant expansion as usage patterns warrant.

9.4 "Remote-readiness" of applications varies

There are several ways to take advantage of a network connection to support interdepartmental collaboration (for example, if a crime analyst in one municipality wants to obtain data from a records management system in another).

Some applications offer a web interface, which makes it easy for any connected party with a web browser and appropriate authentication credentials to make use of the application.

Other applications require the installation of remote client software at the user end. In some cases this is easy, in others it causes problems when applications designed to work locally over high bandwidth low-latency LANs are asked to run remotely. In most cases, vendors either have or are working on a solution.

Ideally, in some future state, the presence of PSnet will encourage automated data sharing; applications will be specified and built with sharing in mind, and the job of the analyst looking across multiple jurisdictions (or of the computer-aided-dispatch system implementer looking at remote backup) will be made easier.

9.5 Trust is key

In one sense, public safety agencies have always cooperated, as evidenced by mutual aid agreements among fire companies or collaborative work by police departments. On the other hand, sharing technical infrastructure and letting "outsiders" access critical public safety systems is new territory for many agencies, and requires a great deal of trust.

PSnet can support trust in three ways. Through well-managed regional working groups, individuals will have the opportunity to work closely together in developing policies and procedures for the sharing of assets and data. Through well-crafted Memoranda of Understanding and other agreements, PSnet can help to codify those policies and procedures. And, through careful implementation of solid security principles, PSnet can create a network that gives its users confidence in the security it provides.

9.6 Volunteers can do only so much

PSnet got its start in the voluntary collaboration of a group of forward-looking public safety officials. "Volunteers"—individuals for whom PSnet was not originally in their capital or operating budget or annual plan, put the pilot project together. Good things have happened.

At the same time, one's official day job will (and should) always take precedence over a volunteer project. People are overbooked and offices are understaffed. Getting the pilot built took a great deal longer than was expected.

The ongoing growth and success of PSnet depends on taking what has been an ad-hoc activity driven by the enthusiasm and vision of a few individuals and legitimizing and institutionalizing it.

9.7 Strong governance / project management are needed

Because PSnet will continue to be a collaboration of many independent departments and agencies, it will require strong governance, effective information sharing, and a higher degree of everyday project management than

would normally be expected for a project of this size and scope. The governance and information clearinghouse recommendations of Sections 10.2, 11.2, and 11.3 are particularly important in this regard.

10 Summary of Recommendations

This section summarizes the recommendations made throughout the document. It is intended to serve as the basis for near-term decision-making. Because there are a large number of individual recommendations here, those rated by project participants as most critical and most accomplishable have been consolidated into a small number of larger projects, which are discussed in Section 11 along with order-of-magnitude cost estimates.

There are two kinds of recommendations – those that pertain to launching PSnet as a coordinating entity, and those that can be undertaken now by individual municipalities or agencies without waiting for PSnet to become formally established. This latter group of actions are, in general, consistent with good network design and operations and do not represent a speculative "investment in PSnet".

10.1 Develop the PSnet Community

10.1.1 Convene PSnet Workshops

To move PSnet forward requires that a broader audience from the constituent communities and related State agencies be briefed on what PSnet is, why it is important, the benefits it will deliver, and how it will be formed. Plan and hold a series of progressively broader workshops to bring together key players with experts and representatives from similar efforts elsewhere. The workshops would serve as a "launch event" to bring all interested parties up to speed on the core concepts behind PSnet, and the initial plans for moving PSnet beyond the pilot stage.

10.1.2 Identify Representatives

At a minimum, PSnet needs to gain commitments from every constituent municipality or agency to appoint a "PSnet Point-of-Contact" and to share information about plans, available resources, applications, and expertise. The workshop events can serve as a useful starting point for gaining these commitments, but some continued follow-up with each community would be required.

10.1.3 Begin Coordinating Network Procurements Now

Negotiate a memorandum of understanding (PSnet MoU) among potential PSnet participants (the 9 municipalities in the UASI region), relevant state agencies (CHBS/CJIS, State Police, State ITSD, others) that all development, procurement, and deployment of public-safety related networking capabilities would be

coordinated through PSnet. This MoU will not be asking participants to give up control, merely to agree to coordinate and share plans and information.

10.2 Form the Governance Structure

While the PSnet governance structures should be "light weight," there is still a need to coordinate collective efforts in order to move PSnet forward.

"Volunteers" will continue to be essential to getting PSnet established, but there will need to be some focal point established to facilitate *people communications*—i.e., a host for the workshops, and a place where the "PSnet phone" and email gets answered. Steps must also be taken to get the word out that PSnet is "real," and to let a broader audience learn about it, and how it will make a difference to the communities it serves.

10.2.1 Establish Executive Committee

Form an Executive Committee as soon as possible to bring together representatives from every participating community and organization. The initial resource commitment expected from participants is to appoint a representative, and expect them to engage with other Executive Committee members on establishing minimal governance of PSnet in accordance with the principles in this document, or as modified by the stakeholders

10.2.2 Establish "Technical Planning Committee"

This committee should comprise the experts who can develop technical plans for advancing PSnet within both the pilot context and as an evolving resource. This will eventually become the technical community referred to above in Section 8.3.3 Committee members should be chosen based on expertise and ability to contribute to PSnet technical initiatives.

A near term objective will be to either ratify or modify the basic set of technical standards developed during the pilot and articulated here, in particular those that govern how participants connect into, and provide resources to, PSnet. Another important early objective will be to identify application requirements that PSnet will need to address.

10.2.3 Convene "Advisory Council"

The role of the Advisory Council (see Section 8.3.2) is to leverage available outside experts, including experts from other similar projects. Participation on this Advisory Council should be by invitation from the Executive Committee. The Council will support planning efforts undertaken by both the Executive and Technical Committees.

10.2.4 Sanction Operations Support for PSnet Pilot

At least some minimal operational support plan will be needed to move the PSnet pilot from a *skunkworks* project to one that has institutional support. The Technical Committee will make the key recommendations for establishing operational support, which may initially comprise cooperative agreements, and no permanent allocation of staff. Eventually, the Operations Group (Section 8.3.4) will subsume this function.

Determine who should be involved in operational matters, and establish basic practices for resolving problems or introducing extensions into PSnet. The pilot is a good place to start with initial operations practices, and can serve as a means to evaluate what works, and what needs improvement.

10.3 Secure Rights to Infrastructure

10.3.1 Obtain Rights to Conduits and Poles

Several communities (e.g., Cambridge, Somerville, Everett) already have municipal ordinances allowing the city to use existing underground conduit and utility poles for municipal signaling purposes (e.g., to pull its own fiber or to add radio gear). Communities that do not have such an ordinance should consider adopting one.

10.3.2 Ensure Quality of Municipal Networking Plants

Several communities have fiber plants and/or wireless mesh networks that have been or are being provided by a cable or telecommunications vendor as part of a franchise agreement. Municipalities should recognize, when negotiating and overseeing these arrangements, that the resulting network is not just a "nice to have", but is part of the region's critical networking infrastructure, and should be built and operated accordingly.

10.4 Expand the PSnet Pilot

The PSnet Pilot is just now becoming operational, and there is a lot of benefit to continuing the pilot to gain experience and demonstrate the value of the PSnet approach.

Section 4.4 outlines several specific interconnections and network links that represent likely next steps for the pilot. The order in which they should be undertaken will be determined by the ability of the participants to secure administrative commitment, contractual agreement, and funding.

10.4.1 Leverage Initial Fiber Backbone with Additional Applications

Add applications that utilize the connectivity offered by the initial fiber backbone, including bandwidth intensive applications such as:

Video conferencing.

Remote viewing of Surveillance video.

Remote radio. See also Section 10.4.8 below

10.4.2 Interconnect Agencies for Resiliency

Section 4.4 suggests interconnecting Cambridge and MBTA fiber at East and West Cambridge. Although there is no immediate short-term need for data exchange between the MBTA and the City of Cambridge, the interconnection would create a ring topology, adding a layer of resiliency and making both entities' networks far less vulnerable to single points of failure. Such a link would demonstrate the value that PSnet coordination can provide, even if only two communities enter into a sharing arrangement.

10.4.3 Introduce Point-to-Point Wireless Links

By leveraging the camera surveillance network that is already in place, the PSnet pilot can demonstrate the unique role that point-to-point wireless technology can play in building a more robust and resilient network. This should also serve to illustrate how PSnet can acquire access to critical communications pathways, while offering back additional communications links that result in both the camera network and PSnet being more resilient. This approach to growing aggregate bandwidth represents significant upside potential to participants. At the same time, camera surveillance becomes a new application that can be more broadly shared throughout the greater Boston region.

The pilot should also introduce at least one new link involving commodity wireless technology and unlicensed spectrum. The proposed radio link between Brookline and Boston via a rooftop in Cambridge can be used to evaluate the role that such technology can play in building out PSnet at reasonable cost while further improving path diversity.

10.4.4 Utilize VPN Tunnels for ad hoc Connections

Incorporate VPN tunnels as a means for establishing "PSnet" initial connections between any two participating organizations. For example, a VPN connection between Cambridge and Brookline Police Departments can help to demonstrate the ease with which such connections can be established with adequate security and minimal cost. The goal would be to eliminate network availability as an impediment to application sharing.

10.4.5 Expand Participation to other Communities

PSnet has been promoted so far by only a handful of communities, even though the interest is broader than just the initial pilot participants. The next step must be to engage other communities, and demonstrate that the concepts can extend to a variety of players, including:

- Other municipalities not currently involved in the PSnet Pilot
- Introduce at least one State agency into PSnet Pilot (e.g., CJIS, State Police)
- Include public safety organizations at major universities
- Include emergency medical services at major hospitals
- Add transportation organizations, such as MBTA, Massport, or the Massachusetts Turnpike Authority

10.4.6 Add New Applications to Pilot

The existence of PSnet Pilot can be leveraged to stimulate interest in adding new applications that can be shared across community boundaries. Some examples include Web EOC, camera surveillance, video and audio conferencing, access to State services, secure email, shared document repositories, etc.

Ultimately, the justification for PSnet is the applications it supports, and the resulting efficiencies gained through greater cooperation and reduced friction. Therefore, it is important to continue to associate PSnet with familiar and new applications that are compelling for the benefits they will deliver.

10.4.7 Continue to "Learn from Doing"

While a lot has been learned from implementing the initial PSnet Pilot, even more can be learned from actually using the pilot to support shared applications. By continuing to build on PSnet lessons, future planning will be better informed and better suited to the collective requirements.

10.4.8 Integrate PSnet into Radio Networks

PSnet can support public safety radio systems in at least three ways:

- As a replacement for the T1 lines currently used to carry audio signal between a dispatch facility and remote transmitter or receiver locations. This is highly cost effective in cases where PSnet can be brought to sites housing radio equipment.
- To enable remote console operation of radio equipment, via a PSnet link between a radio Communications Equipment Bank and an ordinary PC at a remote location; the PC runs software which allows it to emulate a radio

console. This would be an effective tool for operating public safety radio systems from alternative locations, e.g., emergency operations centers

- To enable interoperation between municipalities. PSnet can carry audio traffic as voice over IP, allowing users of mobile radios from different municipality to talk to each other, or allowing the dispatcher in one municipality to talk to radios issued by another.

We recommend that at least one of these radio applications be added to the PSnet pilot.

10.5 Solidify the Clearinghouse Function

Perhaps the most essential ingredient in the strategy to grow PSnet organically is the concept of a "clearinghouse" to aggregate information that will be essential to planners and any organization that needs to find new solutions to problems with their current networks or applications resources.

The biggest challenge to be addressed with the clearinghouse is getting PSnet constituent communities to contribute information to it. This will take some prodding and chasing, but it will also take senior management endorsement. Concerns about security and access control to the information maintained by the clearinghouse will have to be addressed, although these challenges can be met on an incremental basis as the information is accumulated.

A dynamic, secure project web page (as is being offered by Cambridge) is an excellent start; what is also essential is that there be an individual or group whose job it is to ensure the quality and currency of the information.

10.5.1 Identify Available Sources of Expertise

Massachusetts communities are fortunate to have access to world-class expertise in application and network technologies. Existing staff resources within many of the participating communities have substantial expertise and knowledge accumulated through years of supporting their communities. Identifying these individuals is the first step to being able to tap their collective depth and breadth of expertise.

While this is a different form of sharing, it has the potential to provide similar synergistic benefits to sharing of network and application resources.

10.5.2 Collect Plans from Communities for Network and Application Expansions

PSnet will likely evolve most efficiently when plans are developed that include interconnection with, and use of, PSnet resources. However, unless plans are shared, many of the opportunities to grow PSnet in an organic manner could be

easily overlooked. Therefore, the clearinghouse needs to collect information about the plans for upgrading networks and applications throughout the community of participants. The Memorandum of Understanding discussed above in Section 10.1.3 forms the starting place; the clearinghouse becomes the place to collect and manage the information: the place planners come to first, as they develop their plans, and every participating organization should be committed to sharing its plans with the overall PSnet community.

10.5.3 Expand Inventory of Physical Resources

This study has created an initial inventory of physical resources, listed in summary form here and in detailed form on a GIS map distributed separately. This information becomes stale rapidly; the clearinghouse must take ownership of it and keep it up to date.

10.5.4 Inventory Network Resources

With modern internetworking technologies, any existing network can be extended to become part of a larger whole. Most communities have networks today that serve their needs, and many of these networks could become initial extensions of PSnet. By developing an inventory of networks used within the PSnet community, it will be possible to assess where opportunities exist to extend connectivity and organically evolve PSnet.

In some cases, existing networks may have little to offer PSnet, but their existence may still be important, as they may represent opportunities for a more cost-effective PSnet solution to displace or augment networks that are struggling to satisfy growing demands. Including such networks in the overall inventory may be as useful to planners as including the most modern and bandwidth rich networks.

10.5.5 Identify additional "Concentration Points"

In any network, there are "nexus" points where the pathways of the network converge. These nexus points represent natural locations where switching equipment, and even some network-based services, can be located. However, what makes a nexus point valuable is not just the convergence of multiple pathways, but also facilities where equipment can be safely located, powered, and maintained.

The project has created two nexus points—one in Cambridge and one in Boston. Additionally, it has identified additional existing nexus points, for example the basement of Boston City Hall and others listed on the map

Keeping the map of nexus points up to date, and identifying potential paths into these points is one of the most important objectives for the clearinghouse. Not only should the concentration points "owned" by the participants be mapped,

but it would help to also map and inventory concentration points created by the telecommunications carriers, ISPs, and major corporate data centers.

At the same time, knowing where the nexus points are can be sensitive information, and so protections must be in place to prevent unauthorized access to this information. However, failure to map the nexus points can lead to unforeseen vulnerabilities, or (worse) vulnerabilities that are only observed by adversaries.

10.5.6 Create additional "Concentration Points"

Any current or potential PSnet participant can proceed with the creation of its own nexus points, secure in the knowledge that these will be of use independent of the status or progress of PSnet. Well-defined nexus points are the key to efficient network communication with the outside world.

10.5.7 Identify Critical "Sites"

Most of the PSnet constituent communities utilize one or more critical sites where data processing and networking resources are maintained. There are also important workplace sites where key personnel conduct community business, typically requiring access to networks and information. In addition, there are command and control sites, disaster recovery sites, hosting centers, and workplace recovery sites.

Knowing where these sites are located, and what their purposes are, is vital to any PSnet planning exercise. The clearinghouse should serve to assemble this information from all participants, and make it available with sufficient protections to authorized planners.

It is worth noting that this information may well be useful for other planning exercises, including disaster recovery planning. For example, rather than building out new facilities strictly for the purpose of housing systems used in disaster recovery, communities could use the clearinghouse to discover compatible sites where sharing arrangements could allow two or more parties to "back each other up."

10.5.8 Create Repository for Relevant Legal Documents

In the real world, cooperation is predicated on agreements between the parties. Often, these are legal in nature, and problems with legal agreements can be one of the biggest impediments to sharing and collaboration.

One way to facilitate establishment of effective working agreements is to collect and make available all worked examples of bilateral and multilateral agreements, including memoranda of understanding. In some cases, covenants, regulations, charters, bylaws, executive orders and even laws or court rulings may be useful

to collect in order to assemble a complete picture of the complex legal context that could affect PSnet evolution.

10.6 Security Next Steps

Public safety services require strong security against a variety of threats where the risks can sometimes by considerable. Consequently, expanded sharing between communities tends to exacerbate concerns about security as the perimeters of information access grow beyond familiar boundaries. At the same time, security challenges can, in many cases, be addressed more effectively at a collective level. This leads to the conclusion that security must be "baked into" all PSnet plans and deployments, starting with the pilot and subsequent early developments.

10.6.1 Enable use of Secure eMail

A simple, first step to promoting security within the broader PSnet community could be to introduce secure email that can be used to authenticate correspondents and encrypt sensitive information shared amongst individuals and groups. Since email is widely used today, this relatively straight-forward step can serve as the foundation for sharing information more broadly in an ad hoc, yet secure manner. If nothing else, this will help facilitate planning and coordination activities across the various community boundaries.

Since secure email technology is already included in the email client applications used by most (all) PSnet participants, this exercise is a matter of enabling existing machinery, instead of deploying new machinery. Experience with public safety crises in the past decade has demonstrated time and again the utility of basic email; so equipping public safety organizations to communicate via a secure channel they already use provides substantial opportunities to respond more effectively to future events. Furthermore, deploying secure email can help bootstrap awareness of new security measures and the PSnet opportunity for broader sharing.

10.6.2 Develop Requirements for Secure Web Access to Applications

Put forward common requirements that can be presented to every application vendor to facilitate convergence on common methods for shared access using off-the-shelf software and widely supported security protocols, specifically the SSL family of protocols that includes the latest TLS standard. By stating requirements in terms of standards, application developers and vendors can choose between compliant proprietary or open source solutions.

These same requirements can also serve as the foundation for deploying new generations of applications on PSnet, including applications that extend beyond traditional Web approaches. For example, new applications can utilize proven TLS (SSL) protocols and related infrastructure to provide real-time, application-to-application exchanges with strong authentication and protection for confidentiality.

10.6.3 Introduce Common VPN Services within PSnet

In recent years, so-called VPN technologies have become increasingly common as a way to securely extend connectivity for sensitive applications over insecure networks. Many of the PSnet constituent communities have, or plan to, deploy VPN solutions to allow remote access or support telecommuting. In many cases, these new services are not just conveniences; they represent vital components of disaster recovery plans where critical personnel can access the applications they depend on from any location.

PSnet can aid communities by setting interoperable standards for use of VPN technologies, and even deploy common VPN services that could be used by all communities. For example, VPN access to PSnet could be used by personnel from any community to gain access to that community's critical applications by way of PSnet.

10.6.4 Develop Plans for PKI Services

Most modern security protocols depend to some degree on public key (asymmetric) cryptographic measures for performing authentication, controlling access, exchanging encryption keys, and signing documents or transactions. This, in turn, has led to the need for techniques to exchange and access the public keys of communicating parties. Increasingly, public key certificates have become the preferred means for distributing and accessing public keys.

To make effective use of public key certificates (a.k.a., digital certificates), a Public Key Infrastructure (PKI) is required. While the cost to set up and operate PKI services has declined dramatically in the past decade, there are still hurdles to be overcome in terms of expertise and having appropriate plans in place to make effective use of PKI services throughout a community. PSnet presents an excellent opportunity for the constituent communities to pool expertise and PKI service deployments in a way that increases access to certificates for all applications, while lowering collective costs and risks.

It is worth emphasizing that secure email, secure Web services, and VPNs can all utilize certificates to ease integration and improve manageability of production systems. By providing common infrastructure to support this technology base throughout the PSnet community, it will be far easier to deploy effective security measures.

10.6.5 Establish a "Federated" Model for Authentication and Access Control

As noted previously, the PSnet communities already operate within a federated model of authority, or they exist as peer entities. The security models for supporting authentication and access control across the various organizational, community, and application boundaries should reflect the existing lines of authority. This will require development of rational plans for establishing "federated" models for authentication and access control.

Fortunately, PSnet can leverage recent industry developments to support federated models that are well suited to this context. What is needed is to choose appropriate technical approaches, and promulgate plans that will guide the development and evolution of all secure applications.

11 Making PSnet Happen

The list of recommendations above is long. In order to create a tractable plan going forward, we have identified a few tasks of critical importance (as voted by the PSnet project team) and we have grouped them into five larger scale pragmatic projects that provide some overall structure.

11.1 Critical early items

Reviewing the list, the PSnet project team identified several as being of vital importance over the short term. These include:

- Convening PSnet workshops (item 10.1.1)
- Identifying representatives to sit on the governing body (item 10.1.2)
- Establishing the Executive and Technical Planning committees (items 10.2.1 and 10.2.2)
- Expanding and maintaining the inventory of available network infrastructure (item 10.5.3)

11.2 Recommended project: Establish PSnet Governance

11.2.1 Project overview

A well-functioning governance entity will be essential to getting things done. Planning, operation, and management of PSnet must become institutionalized rather than run *ad hoc* by volunteers.

Therefore, staffing the Executive and Technical Planning committees and having them begin their work is a low-cost, high-impact activity. The necessary steps are:

- A burst of outreach activity (presentations and meetings) in February and March 2007, to make public safety officials at all 9 UASI region communities aware of PSnet and to solicit their participation. (see also "Outreach" at 11.4 below)
- Identify representatives for the governing bodies.
- Identify agencies willing and able to take on operational responsibility for any aspects of PSnet
- Agree upon the charter for each committee (as described here, or as modified by the committee itself)

- Establish collaboration infrastructure (web site, file repository, mailing lists, etc.)
- Establish administrative support
- Facilitate the regular meetings of the committees.
- Begin work on the pragmatic work of getting PSnet built.

11.2.2 Cost estimate

This project has no capital costs, but will require a fair amount of senior and executive staff time, especially during the first three months when undertaking the outreach and set up activity, up to half time or more for a single senior individual or equivalent labor conducted by a group of staff, with administrative support. On an ongoing basis, it should require approximately one-quarter time staff member (or equivalent), with administrative support.

11.3 Recommended project: PSnet Clearinghouse

11.3.1 Project summary

The Clearinghouse serves two purposes:

1. A means for PSnet participants to share information, align policies, and coordinate strategic and technical plans.
2. A resource for potential participants to explore opportunities available to them as a result of engaging in the development of PSnet.

The Clearinghouse collects and maintains the following types of information and provides secured access to this information by authorized community representatives:

- Resource information: Maps and tables showing available network and facility resources
- Technical information: Network designs, addressing plans, performance metrics, security measures, "how-to" guides
- Administrative information: Schedules, meeting minutes, action items,
- Policy information: Documented agreements, MoUs, statements of policy, etc.
- Project information: Status of project activities, budgets, funding levels, roadmaps
- Project participant information: Contact details for all players, organization charts, problem resolution trees, sources of expertise

- (Possibly) Operational information—: Status of network and equipment, test results, network utilization trends

The Clearinghouse provides a single telephone number and a single e-mail address by which interested parties can obtain authoritative information.

Much of the work in managing the clearinghouse involves contacting the relevant regional agencies and reaching out to new ones to obtain and update information.

11.3.2 Cost estimate

The Clearinghouse project also requires no capital outlay.

It requires the use of a hosted web-based collaboration infrastructure, which can be built internally or optionally purchased at a cost of between $350 and $500 per month, depending upon the number of active participants.

Setup requires a full time senior staff person for nearly a month (or equivalent); ongoing operation requires a quarter-time administrator and, initially, as much as half time for a manager to oversee setup of the Clearinghouse and collection of necessary information.

11.4 Recommended project: Outreach

11.4.1 Project summary

Plan and host a series of workshops that engage a broader circle of participants in PSnet, probably three four-hour workshops in Spring 2007, and a larger workshop in the Fall of 2007. Also, on an ongoing basis, provide an "evangelism" point of contact—an executive staff person who is available to make PSnet briefings to other regional public safety groups, to get PSnet onto their meeting agendas, and generally to serve as the "PSnet Ambassador.". Potentially this is the person who would return phone calls and e-mail queries to the Clearinghouse.

11.4.2 Cost estimate

The Outreach activity requires no capital outlay.

Running a workshop requires an estimated one week of senior staff time per workshop, plus additional time for follow-up

The ongoing "evangelism" function requires 2 or 3 executive staff days per month.

11.5 Recommended Project: PSnet Network Build

11.5.1 Project summary

We recommend that each member of the UASI region establish a 'PSnet Access Node' (Sections 10.5.5 and 10.5.6). PSnet Access Nodes are interconnection points at which a municipality's own internal network connects to PSnet. A typical access node would be a router or a switch with a fiber connection to one or more PSnet backbone nodes. For example, Cambridge has a PSnet access node located at Cambridge Police Department headquarters; the node connects Cambridge Police, City of Cambridge, PSnet VPN, and PSnet backbone networks together at a single switch.

Once an access node exists, then any facility with access to that municipality's own internal network can obtain access to PSnet. In addition to expanding basic connectivity, this project will require that a number of the security and operational recommendations be addressed.

Cambridge and Boston have already established interconnection points for the pilot that could easily become permanent access nodes. The access node project can be undertaken in parallel with the EOC interconnection project described below in Section 11.6.

Separate from the individual participant access nodes, we recommend that the existing two pilot project backbone nodes (located at Bent St. in Cambridge and Summer St. in Boston and on loan to the project from Harvard University) be made permanent, and that one or two additional backbone nodes be built, each redundantly connected to the other backbone nodes. The technical planning committee would develop specifics of where these backbone nodes should be built.

11.5.2 Cost estimates

The cost estimates are separated into the costs for building a participant access node and for building a backbone node

11.5.2.1 Participant access node

A participant access node requires the following capital equipment, which may already be in place for some communities, but would need to be acquired by others:

- Equipment rack space, approximately 5 U, in a location with good physical security, reliable power, access to the municipality's network plant, and access to telecommunications carrier lines.

- Router/Firewall/Switch: details may vary by community. A Cisco 3745 at $5,000 is a reasonable high-end placeholder for planning assumptions while various middle-of-the-road products (e.g., Secure Computing SG720) can be acquired for around $2,000.
- 100 Mbps fiber connection to nearest backbone node (2 for resiliency). This might be a capital expense or a recurring telecommunications expense, depending upon how the municipality obtains the lines; the recurring expense will be highly variable depending upon the location of the facility and the proximity to competing carriers' facilities.
- 50 Mbps connection to nearest wireless network access point (see Section 11.6 below). Note that if the access node is collocated with the EOC, this is a local connection. Otherwise, the pricing his highly variable as is the 100 Mbps connection immediately above.
- Cross-connect at each backbone node: from $0 to $250 per month.

11.5.2.2 Backbone node

For the pilot, Bent Street and Summer Street are the two backbone nodes. This section discusses the costs of replicating these nodes.

A backbone node requires the following. It can either be provided by a participant or obtained from a service provider.

- Equipment rack space, 4—8 U, located in a "carrier hotel" or similar facility with power, security, and access to multiple carriers' telecommunication lines. PSnet may benefit from facilities that can be donated at little or no incremental cost to the donor. This is because carrier hotels typically rent only in increments of an entire rack, at $500 to $1,000 per month; many users will not require an entire rack and will therefore have "extra" space to donate to PSnet, as is currently being done for the pilot project by Harvard University / Northern Crossroads.
- Switch / Router combination. As a placeholder, use $12,000 for a Cisco 7207VXR with NPE-G1 and $5,000 for a fully featured switch.
- 100 Mbps connection to at least one other backbone node. (2 for resiliency), including cross-connect. If unable to find donated fiber, budget $1,500 per month for each node-to-node connection, plus $0 to $250 per month per cross-connect.
- Public Internet connectivity of at least 10 Mbps. May be possible to share this with other subscribers, e.g., the donor of the rack space, otherwise budget $250 per month.

11.6 Recommended project: EOC connectivity

11.6.1 Project Summary

Build a wireless network that connects all 9 municipal Emergency Operations Centers and selected additional regional emergency facilities.

This will enable the EOCs to communicate with each other (via access to each other's data applications, access to centralized services like WebEOC, via voice or video conference, remote operation of radio gear, etc.). It will provide an independent backup for telephone connectivity between EOCs. It will also provide for connectivity between the EOCs and any other PSnet-connected entity (e.g., PSAPs, dispatch centers, police and fire headquarters).

The following locations should be connected as part of this project:

Boston	EOC	85 Bragdon St.,	Roxbury
Brookline	EOC	879 Hammond St.,	Brookline
Cambridge	EOC	249 Alewife Brook Pkwy	Cambridge
Chelsea	EOC	45 Washington Ave	Chelsea
Everett	EOC	45 Elm St	Everett
Quincy	EOC	1 Merrymount Parkway	Quincy
Revere	EOC	400 Broadway	Revere
Somerville	EOC	220 Washington St.,	Somerville
Winthrop	EOC	1 Metcalf Square	Winthrop
MBTA	HQ	45 High St.	Boston
MEMA	Bunker	400 Worcester Rd	Framingham
State Police	Troop E	50 MassPort Haul Road	South Boston
Massport	Logan Airport	Logan Airport	East Boston

The technical committee will determine the best way to achieve this, but as an overall strategy we recommend the following:

- Build one or two Wireless Aggregation Points. An aggregation point should have good connectivity to a PSnet backbone node, and should also have access to a high rooftop or other location with line-of-sight views to as many EOC locations as possible.
- Build a Wireless Endpoint at each EOC, capable of connecting to a Wireless Aggregation Point.
- Connect each EOC to the corresponding municipality's PSnet Participant Access Node. (This may be a local connection if the Access Node is collocated

with the EOC, or it may be accomplished via municipal fiber, or it may require a leased line. It may also be already planned as part of the EOC build-out.

11.6.2 Cost estimate

11.6.2.1 Wireless Aggregation Point

A wireless Aggregation Point requires the following:

- Antenna site—rooftop, hilltop, tower location, including fiber drop to building basement. If this is not donated (or piggy-backed on existing facilities such as BAPERN towers), assume $2,000 to $3,000 per month for planning purposes
- Antenna and Radio gear—approximately $23,000 (3 sectors of 120 degrees each at $7,500 per sector)
- Switch or router (unless physically collocated with another PSnet facility), assume $2,500 to $3,000
- Installation and wiring—presume soft costs.
- 100 Mbps connection to nearest access node (unless already collocated.) Cost is too variable to estimate until the locations are known; from $0 (if collocated with a PSnet node) to $3,000 per month.

11.6.2.2 EOC end node

An EOC end node requires the following:

- Rooftop antenna and radio gear—approximately $2,500
- Installation and wiring and configuration—assume 5 days from planning through testing.
- Available port on existing EOC switch to connect radio gear—already exists
- Additional port on existing EOC switch to connect to municipal network (if not already connected)—already exists

Appendix A Inventory

This appendix provides additional detail for each of the items listed in the tables in section 4.3. A detailed GIS map of existing assets is under development and will be provided as a separate document.

A.1 Boston City-owned fiber delivered by Comcast

As a part of the municipal cable franchise contract between the City of Boston and Comcast, Boston has a fiber plant which interconnects many of the public safety facilities in Boston.

Responsible Agency: Boston MIS

Business Contact: Ann Roper Quinn

Technical Contact: Jerry Turner

GIS contact: James Alberque

Available capacity[10]: Boston has 10 pairs of single-mode fiber in its core network, with smaller number of fibers reaching various endpoints. In some, but not all cases, an extra pair can be dedicated for PSnet. There is more than ample capacity here to support any anticipated PSnet need, using any of the options discussed in the footnote below.

A.2 Boston Legacy fiber

48 strand single mode fiber that runs from the Boston City Hall MXP room out to Boston Fire Alarm at 59 Fenway, with patch panels at Boston Public Schools Administration Building (24 Court), Parkman House (33 Beacon), Boston Public Library (700 Boylston), Engine 33 Firehouse (941 Boylston), then on to Fire Alarm. There is also a fiber run from Engine 33 across the street to the Prudential Center (800 Boylston—T1 Room

[10] Anyplace where fiber exists, it can be used for PSnet in any of four ways: A strand of fiber can be dedicated to PSnet, a "lambda" on an existing can be dedicated to PSnet, a "Virtual LAN" or VLAN can be allocated to PSnet, or PSnet traffic can be routed over the network along with other traffic. The first two options create essentially a dedicated circuit for PSnet. They offer the greatest flexibility to the PSnet architects and a considerable range of long-term expansion options, at the cost of tying up significantly more of a resource (Fiber strands or lambdas) than PSnet is actually using. A VLAN is essentially a dedicated slice of bandwidth allocated to PSnet on an existing link. It consumes only the bandwidth allocated to it (as opposed to requiring its own fiber), while offering that bandwidth without interference either way between PSnet and other traffic on the same link. The fourth option, routed traffic, requires only the bandwidth that is actually being used by the PSnet application at the moment, at the cost of potential bandwidth contention between PSnet and non-PSnet users of the same link.

Responsible Agency: Boston MIS

Business Contact: Ann Roper Quinn

Technical Contact: Jerry Turner

Available capacity: Similar to Boston Comcast fiber. Dedicated strands may not be available to all locations, but ample bandwidth exists, relative to the currently envisioned PSnet requirements[11].

A.3 Cambridge City-owned fiber

The City of Cambridge is responsible for their own fiber plant, which interconnects many of the public safety facilities in Cambridge.

Responsible Agency: City of Cambridge

Business Contact: George Fosque

Technical Contact: Tom Freiss, George Fernandes

GIS contact:

Available capacity: Similar to Boston Comcast fiber. Dedicated strands may not be available to all locations, but ample bandwidth exists.

A.4 Surveillance Camera Network

In connection with the surveillance camera project, there exists a 100Mbps full-duplex wireless ring connecting the JFK building, a location in Revere, the Soldiers' home in Chelsea, a location in Everett, and back to the JFK building. From there, a 100Mbps wireless link connects to the Nurses' building, and from there to Boston PD headquarters at Schroeder plaza. There are Cisco 3550 switches at each location. There is also a 1GB link from Chelsea EOC to the Soldiers' home

Responsible Agency: City of Boston

Business Contact: Unclear—use MOEP / Cynthia Chang

Technical Contact: Doug Stringer, Stonecrop Technologies

GIS contact: ?

Available capacity[12]: Needs to be negotiated with the primary users of the network. Existing capacity is 100 Mbps, which is believed to be much more than

---

11 We use the term "ample" in cases where existing surplus capacity is difficult to assess quantitatively, e,g. for systems now under construction and not yet deployed, but where we believe the capacity is either sufficient to the needs of PSnet or easily scalable (e.g., by replacing fiber transceivers.)

adequate for the camera network, although the actual usage pattern of the camera network has not yet been determined because it is so new. Our unsupported guess is that 10 Mbps could be made available to PSnet.

A.5 Chelsea City-owned fiber

Chelsea fiber connects most municipal locations in Chelsea

Responsible Agency: City of Chelsea

Business Contact: Matthew Killen

Technical Contact: John Hyland

GIS contact: William Toussaint

Available capacity: Similar to Boston Comcast fiber. Dedicated strands may not be available to all locations, but ample bandwidth exists.

A.6 Fiber link from Cambridge to Boston

Fiber connection on loan from Harvard University, between the carrier hotel at 300 Bent Street, Cambridge and the carrier hotel at 1 Summer Street, Boston.

Responsible Agency: Northern Crossroads

Business Contact: Leo Donnelly

Technical Contact: Leo Donnelly

GIS contact: Leo Donnelly

Available capacity: For the purposes of the pilot project, the entire bandwidth is available, which is vastly more than PSnet will require.

A.7 MBTA radio fiber

SWR Fiber is dedicated to support RF-over-fiber network for the SWR (system-wide radio) project.
All fiber runs are 72 strand.
There are four fiber runs from the MBTA facility at 45 High Street to each of the MBTA facilities at: Downtown Crossing; Park Street; Government Center; State Street. From each of these MBTA stations, the fiber is routed to all tunnel communications rooms.
There is sufficient spare fiber to go from one station's communications room to

[12] With a wireless network, the "dedicated fiber" and "dedicated lambda" options do not exist. The switch gear used in the camera network does, however, support both the VLAN and routed options discussed in the previous footnote.

another station's communications room in the same tunnel (i.e., along the same branch of the subway line).

Responsible Agency: MBTA

Business Contact: John Lewis

Technical Contact: Ken Sliby

GIS contact: Bob Parfumorse

Available capacity: The radio fiber is dedicated and cannot be shared with other applications. It may be possible to use some of the spare fiber for PSnet purposes.

A.8 MBTA WAN fiber

WAN fiber handles IP traffic and is used for MBTA applications other than radio. It also runs along MBTA rights of way.

Responsible Agency: MBTA

Business Contact: John Lewis

Technical Contact: Ken Sliby

GIS contact: ?

Available capacity: Similar to Boston Comcast fiber. Dedicated strands may not be available to all locations, but ample bandwidth exists.

A.9 ITSD SONET ring

ITSD operates an OC192 ring that connects ITSD in Chelsea, Boston City Hall, several other downtown Boston locations, and State Police in Framingham

Responsible Agency: Mass ITSD

Business Contact: Rich Glasberg

Technical Contact: Rich Glasberg

GIS contact: ?

Available capacity: This OC192 ring has ample capacity to carry 100 Mbps worth of PSnet traffic.

A.10 T1 link from Brookline PD to Boston PD

Responsible Agency: Town of Brookline

Business Contact: Scott Wilder

Technical Contact: Scott Wilder

GIS contact: ?

T1 Circuit #70DBZE241732

Available capacity: Has 1.5 Mbps total capacity, part of which is already allocated to Brookline PD access to Boston. Suitable for additional application load but not suitable as part of the PSnet backbone.

A.11 Proposed Wireless Link Brookline to Boston via MIT Tang Hall

Responsible Agency: Galaxy Internet Services

Business Contact: Sandy Bendremer

Technical Contact: Sandy Bendremer

GIS contact: ?

Galaxy Internet Services has offered to provide hardware and establish, for the pilot, a line-of-sight wireless link from Brookline Police Department to Boston (City Hall?) via Tang Hall at MIT in Cambridge.

Available capacity: Up to 50 Mbps depending upon radio propagation factors

A.12 Proposed Wireless Link Via Boston University

Boston University may be willing to provide a rooftop antenna site, power, a fiber drop through the building, and fiber to the 1 Summer St. facility.

Responsible Agency: Galaxy Internet Services / Boston University

Business Contact: Sandy Bendremer

Technical Contact: Sandy Bendremer

GIS contact: ?

Available capacity: Up to 50 Mbps depending upon radio propagation factors

A.13 VPN from Brookline PD to Cambridge PD

Using off-the-shelf hardware (Snap Gear SG300 and SG560 VPN firewall appliances) provided by Interisle Consulting Group located at both the Brookline Police Department and the Cambridge Police Department, a secured tunnel connection can be set up to allow a direct "connection" which is routed across the public Internet. At the Cambridge end, the VPN terminates on the PSnet backbone

Responsible Agency: Interisle

Business Contact: Chuck Wade

Technical Contact: Chuck Wade

GIS contact: n/a

Available capacity: Subject to the limit of the DSL line serving Brookline—768 kbps but can be upgraded

A.14 VPN from Chelsea PD to Cambridge PD

Identical to the VPN from Brookline to Cambridge

A.15 Verizon TLS circuit from Boston City Hall (?) to Boston PD

There is a circuit connecting Boston City Hall with Boston PD headquarters. Separate VLANS can be established under the control of Boston MIS.

Responsible Agency: City of Boston

Business Contact:

Technical Contact: Jerry Turner

Available capacity: Subject to negotiation with the other users; can be upgraded by Verizon. More than adequate for pilot project.

A.16 Comcast Boston Fiber 1 Summer St. to Boston City Hall

Fiber runs from City Hall to Engine 50 in Charlestown and from there to Summer St. (purely for the pilot, to take advantage of available fiber; a production implementation would take a more direct and resilient route)

Responsible Agency:

Business Contact: Leo Donnelly

Technical Contact: Leo Donnelly

GIS contact:

Available capacity: Two strands dedicated for the pilot. Ample for PSnet.

A.17 Harvard Fiber - William James Hall to 300 Bent St.

Responsible Agency: Harvard University

Business Contact: Leo Donnelly

Technical Contact: Leo Donnelly

GIS contact:

Available capacity: Two strands dedicated for the pilot. Ample for PSnet.

Appendix B Project Interviews

As part of the PSnet Study, Interisle Consulting Group conducted a number of interviews with as many people who could be contacted.

The following people gave their time to provide their perspectives on PSnet, detailing what they could provide into PSnet, and what their aspirations were for using PSnet. In many cases, we also sought opinions on topics relating to architecture, operations, and governance of PSnet.

- Jim Alberque—City of Boston MIS
- Brian Barcelou—Boston Police Department
- Bryan Corbett - Massport
- George Fernandes—Cambridge City Electrical Department
- James Fitzpatrick—Boston Police Department
- John Hyland—City of Chelsea
- Matthew Killen—City of Chelsea
- Steve Lenkauskas—Cambridge City Electrical Department
- William Oates—City of Boston MIS
- Ken Pitts—City of Cambridge
- Kavita Reddy—Massachusetts ITD
- Jerry Turner—City of Boston MIS
- Curt Wood—Criminal Systems History Board
- Jim Slater—Executive Office of Public Safety
- Kenneth Sliby—MBTA
- Charles VonLichtenberg—Boston University
- Gregg Hollenbeck—US DOT Volpe center
- Carl Walter - Boston Regional Intelligence Center (BRIC)
- Federal Protective Services—Eric Johnson

Despite reasonablein attempts to secure interviews with additional people, via a number of different sources, we were unable to schedule interviews with the following organizations:

- Massachusetts State Police

Appendix C Core Project Team

The following people comprised the core project team for the PSnet Study:

- Cynthia Chang—Boston Mayor's Office of Emergency Preparedness
- George Fosque—City of Cambridge
- Leo Donnelly—Northern Crossroads/Harvard University
- John Cowhig—City of Chelsea
- Ken Pitts—City of Cambridge
- Ann Roper Quinn—City of Boston
- Scott Wilder—Town of Brookline

And the following people provided consulting services for the PSnet Study:

- Sandy Bendremer—Galaxy Internet Services
- Chris Owens—Interisle Consulting Group
- Chuck Wade—Interisle Consulting Group
- Colin Strutt—Interisle Consulting Group
- Lyman Chapin—Interisle Consulting Group