

NENA

Technical Information

Document

Network/System

Access Security



NENA 04-503, NENA Technical Information Document Network/System Access Security
Issue 1, December 1, 2005

Prepared by:
National Emergency Number Association (NENA) PSAP CPE Technical Committee

Published by NENA
Printed in USA

NENA
TECHNICAL INFORMATION DOCUMENT

NOTICE

This Technical Information Document (TID) is published by the National Emergency Number Association (NENA) as an information source for the designers and manufacturers of systems that are used for processing emergency calls. This document does not provide complete design specifications or parameters or to assure the quality of performance for systems that process emergency calls.

NENA reserves the right to revise this TID for any reason including, but not limited to:

- conformity with criteria or standards promulgated by various agencies
- utilization of advances in the state of the technical arts
- reflecting changes in the design of network interfaces or services

It is possible that certain advances in technology will precede these revisions. Therefore, this TID should not be the only source of information used. NENA members should consider contacting their Telecommunications Carrier representative to ensure compatibility with the 9-1-1 network.

Patents may cover the specifications, technology, or network interface/system characteristics disclosed herein. No license expressed or implied is hereby granted. This document is not to be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA or any affiliate thereof to purchase any product whether or not it provides the described characteristics.

This document has been prepared solely for the voluntary use of E9-1-1 Service System Providers, network interface and system vendors, participating telephone companies, etc.

By using this document, the user agrees that NENA will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

NENA's Technical Committee has developed this document. Submit recommendations for change to this document to the following:

National Emergency Number Association
4350 North Fairfax Drive, Suite 750
Arlington, VA 22203-1695
800-332-3911
or: techdoccomments@nena.org

Acknowledgments:

This document has been developed by the National Emergency Number Association (NENA) PSAP CPE Technical Committee, Security Working Group.

NENA recognizes the following industry experts and their companies for their contributions in development of this document.

Members:	Company
Vislocky, Mike - PSAP CPE Technical Committee Chair	Network Orange, Inc
Smith, Jeremy L. (CISSP) - CPE-Security Working Group Leader -	Plant Equipment, Inc.
Kennedy, Mike – Former CPE Security Working Group Leader	SBC
Cox, Kevin (CISSP)	Plant Equipment, Inc.
Gipson, Gordon D	911 Consulting
Hayes, David W.	Verizon
Hutchins, Gary C.	Intrado Inc.
Kelly, Gordon A.	Independent Consultant
Kleck, Kevin	Tarrant County 9-1-1 District
Palmer, Gary F.	Verizon
Corprew, Charles	SBC
Dunne, Toni D	Positron
Skain, John	Clinton County IL 9-1-1
Slivka, Joe Ben	Summit County Communications Center
Walthall, Robert	SBC
Whitehurst, Ron	Cbeyond Communications

TABLE OF CONTENTS

1 EXECUTIVE OVERVIEW 3

1.1 PURPOSE AND SCOPE OF DOCUMENT 3

1.2 REASON FOR ISSUE..... 3

1.3 REASON FOR REISSUE 3

1.4 RECOMMENDATION FOR STANDARDS DEVELOPMENT WORK 3

1.5 COSTS FACTORS 3

1.6 ACRONYMS/ABBREVIATIONS 3

2 SECURITY POLICIES & RISK MANAGEMENT 3

2.1 SECURITY POLICY 3

 2.1.1 *Executive Management Statement of Policy*..... 3

 2.1.2 *Roles & Responsibilities*..... 3

 2.1.3 *Functional Policies*..... 3

 2.1.4 *Procedures*..... 3

2.2 RISK MANAGEMENT..... 3

3 PSAP SECURITY: THREATS & RECOMMENDED COUNTERMEASURES 3

3.1 LEGACY/FUTURE ARCHITECTURE (WHERE HAVE WE BEEN/WHERE ARE WE GOING?) 3

3.2 PSAP SECURITY CATEGORIES 3

 3.2.1 *Access Control*..... 3

 3.2.1.1 Administrative..... 3

 3.2.1.2 Technical..... 3

 3.2.1.3 Physical..... 3

 3.2.2 *Network Security* 3

 3.2.2.1 Networking 3

 3.2.2.2 Firewalls & Intrusion Detection Systems..... 3

 3.2.2.3 System Configuration..... 3

 3.2.2.4 Wireless..... 3

 3.2.2.5 Remote Access..... 3

 3.2.2.6 Virtual Private Networks & Dial-In 3

 3.2.3 *Application Security* 3

 3.2.3.1 Malware 3

 3.2.3.2 Hacking/Cracking 3

 3.2.4 *Patching & Change Management* 3

 3.2.4.1 Operating System Security Patch Management 3

 3.2.4.2 Change Management..... 3

 3.2.5 *Telephony* 3

 3.2.5.1 Toll Fraud..... 3

 3.2.6 *Availability* 3

 3.2.6.1 Business Continuity Planning 3

 3.2.6.2 Disaster Recovery Planning 3

 3.2.7 *Remote Monitoring & Maintenance*..... 3

 3.2.8 *System Logs*..... 3

 3.2.9 *VoIP (Voice over Internet Protocol specific concerns)*..... 3

4 REFERENCES..... 3

4.1 DOCUMENTS 3

4.2 WEB SITES 3

5 EXHIBITS 3

5.1 EXHIBIT 1: SECURITY REQUIREMENTS FROM THE NCIC WEB SITE..... 3



1 Executive Overview

1.1 Purpose and Scope of Document

Today's Public Safety Answering Points (PSAPs) face more threats than ever before. In a post 9/11 world, the 9-1-1 community must recognize the reality of increased threats and vulnerabilities. New product paradigms are being designed and implemented by the PSAP community at a rapid pace. Today's call-centers are challenged to keep pace with the rapid shifts in technology. The threats and vulnerabilities have drastically increased with:

- impending next-generation of 9-1-1 equipment
- pervasive integration and sharing of data between multiple agencies, sites and/or systems
- rich new features and capabilities such as:
VoIP, Telematics, the Emergency Services Network (ESNet), i2/i3 and more

These challenges require innovative solutions and emphasize the necessity for truly secure computing environments in today's PSAP.

Already, many unprotected 9-1-1 networks have been infected by worms and viruses causing significant service interruptions within many PSAPs across the country. Many of these 9-1-1 networks are connected to city LANs or other external networks. With proper security policies in place, these service interruptions could have been avoided.

In a study sponsored by Microsoft and antivirus vendors, roughly one third of companies surveyed experienced major virus incidents in 2003. The study also stated that more than 80% of virus incidents involved one or more servers and resulted in an average of 17 hours of down time. Private industry reported costs ranging from \$10,000 to \$100,000 per virus incident. When virus incidents threaten the operation of the 9-1-1 system, the costs of avoidable property damage, injuries, and loss of life must also be considered.

In order for the 9-1-1 System to maintain acceptable levels of availability, it must be protected from the increasing number of threats. Security breaches can cause irrecoverable damage to systems or worse interrupt the functionality of the 9-1-1 system and ultimately result in loss of life.

The purpose of this document is to identify the importance of security for today's PSAP and to describe common types of computer and network security threats facing the industry today, as well as provide guidelines for effective mitigation strategies. The document is a guide to PSAP managers, CPE vendors, service providers, database providers, and others who design, supply, or maintain 9-1-1 subsystems interconnected with each other to form the 9-1-1 system at a PSAP.

1.2 Reason for Issue

This "PSAP CPE Security Technical Information Document (TID)" is issued to guide PSAP managers, service providers, and CPE vendors in matters related to equipment, equipment networking and communications security.

1.3 Reason for Reissue

NENA reserves the right to modify this document. Whenever it is reissued, the reason(s) will be provided in this paragraph.

1.4 Recommendation for Standards Development work

The CPE Technical Committee recommends that some of the material in this document be further developed into a NENA Standards Document. The critical interfaces between PSAP systems, and between PSAP and network elements, must be protected with a coordinated security system policy or policies.

1.5 Costs Factors

This document will not address the relative cost factors for the various suggested solutions, incorporated within this document.

1.6 Acronyms/Abbreviations

This is not a glossary! See NENA 01-002, *NENA Master Glossary of 9-1-1 Terminology* located on the NENA web site for a complete listing of terms used in NENA documents.

2 Security Policies & Risk Management

2.1 Security Policy

PSAP Security is an expansive subject and can be overwhelming to those not intimately familiar with such intricate concepts. However, as with anything, there is a beginning: The creation of a security policy is the first step in any effective attempt at PSAP Security. A Security Policy is a clearly documented statement of organizational goals and intentions for PSAP security, particularly upper management's commitment to PSAP Security. The creation of a security policy requires an organization to recognize, identify, and document its commitment to PSAP security. All too often PSAPs implement security measures without first implementing security policies. This often results in ineffective or unfocused security controls and ultimately leads to more vulnerability. A security policy should facilitate an environment of secure computing and document an organization's philosophy concerning PSAP Security.

Security policies vary in size and shape as well as purpose or scope. At a minimum, a PSAP should have the following policies:

- Executive Management Statement of Policy
- Functional Policies
- Procedures

2.1.1 Executive Management Statement of Policy

Without executive level commitment and buy-in, a security strategy is ineffective. Consequently, upper management must be fundamentally committed to PSAP security, recognizing its importance as a 'business driver/enabler' instead of just another facet of technology. Creating an executive

management statement of policy is key to documenting the importance of the computing assets and resources to the PSAP as well as upper managements commitment to exercise due care through the definition and management of acceptable operational level standards, procedures, and measures.

2.1.2 Roles & Responsibilities

A well-written security policy should identify the important roles and responsibilities of the PSAP's security program personnel including important executive management personnel, security manager, data custodians/owners/users, and even auditors. Some common roles are listed below:

- **Executive Manager:** Executive or other department manager ultimately responsible for the security of the organization and may be responsible for the operation of all data processing, network, and access to all IT operations of an organization. This is usually a CIO or equivalent position. This person or his designated representative will define security policy as it relates to all systems, networks, and data for the organization as a whole.
- **Security Officer/Administrator:** This person has the functional responsibility for organizational security and is responsible for implementing and administrating security countermeasures in concordance with PSAP security policies.
- **Data Owner:** This employee is responsible for appropriately classifying the asset or helping the PSAP understand its importance in order to establish the necessary level of protection.
- **Data Custodian:** This is the person responsible for ensuring that any security measures required for a particular asset are implemented and maintained.
- **Data User:** The Data User is the entity that actually uses the data being secured. For example, the Dispatcher is a Data User in that they 'use' ALI data to perform their daily tasks.
- **Auditor:** Auditors may be internal or external to the organization and are responsible for examining an organizations security.

Safeguarding the assets of the organization, both physical and data, is everyone's responsibility and every individual within the PSAP should be educated and included in the PSAP's secure 'mindset.' Since 9-1-1 was originally developed, the supporting equipment and communications facilities have been generally isolated and under the control of a few responsible organizations while access to the telephone network has been tightly controlled by service providers. Interfaces between multiple CPE vendors have been restricted to clearly defined interfaces with specific data formats.

The legacy architecture limits security vulnerabilities, but is still subject to attacks. They can come in the form of "denial of service" attacks with attempts to overload a PSAP with false 9-1-1 calls. Furthermore, the next generation of 9-1-1 services (i.e. ESN, i2/i3) threatens to drastically change the aforementioned model and increase PSAP threats.

2.1.3 Functional Policies

Functional policies provide a deeper level of granularity after creating an executive management statement of policy. Functional policies must be established prior to the implementation of any actual security measures. The policy document defines the following items:

- appropriate Internet usage
- password policies
- remote access policies
- hiring practices
- security enhancements or technology that should be implemented within a PSAP
- May include baseline configurations for workstations existing on the PSAP network or standards for technology selection or router configuration.

2.1.4 Procedures

A procedure is the documented method of performing a specific task. As a PSAP's security policies begin to take shape it will become necessary to document certain tasks such as the procedures on creating new user accounts or the actual steps to allow a vendor access to a server room. Procedures are an important part of any security strategy as they take the guesswork out of certain tasks ensuring consistency and accountability.

2.2 Risk Management

Risk Management involves the identification and subsequent quantification/qualification of threats and their impacts to the PSAP. In order to avoid ineffective security countermeasures, overspending, or inefficient use of time and downtime, risk management is a process that must be conducted prior to implementing specific security technologies or measures.

Risk Management is a science and like any complex discipline must be approached in an organized manner. Risk Management for the PSAP involves the completion of a Business Impact Analysis (BIA). A BIA is a formal process (mathematical in nature) for:

- identifying all known threats
- assigning monetary (quantitative) or scenario (qualitative) values to the potential loss of critical assets
- taking appropriate measures to mitigate the realization of an actual threat by identifying methods, practices or technologies to that end

By assigning numerical (quantitative) or scenario-based (qualitative) values to different threat models it becomes easier to determine which assets are most important and therefore require a higher level of protection (and ultimately more money spent on protecting it) and can help determine where countermeasures should be applied. Risk Management is an important part of securing a PSAP and many methods, tools and third party resources are available to assist PSAPs in conducting a BIA.

Failure to properly conduct a BIA and effectively perform Risk Management can result in not only ineffective security countermeasures, overspending, or inefficient use of time but ultimately could result in PSAP downtime or worse. Risk Management is truly a mandatory and necessary exercise for PSAP Security.

3 PSAP Security: Threats & Recommended Countermeasures

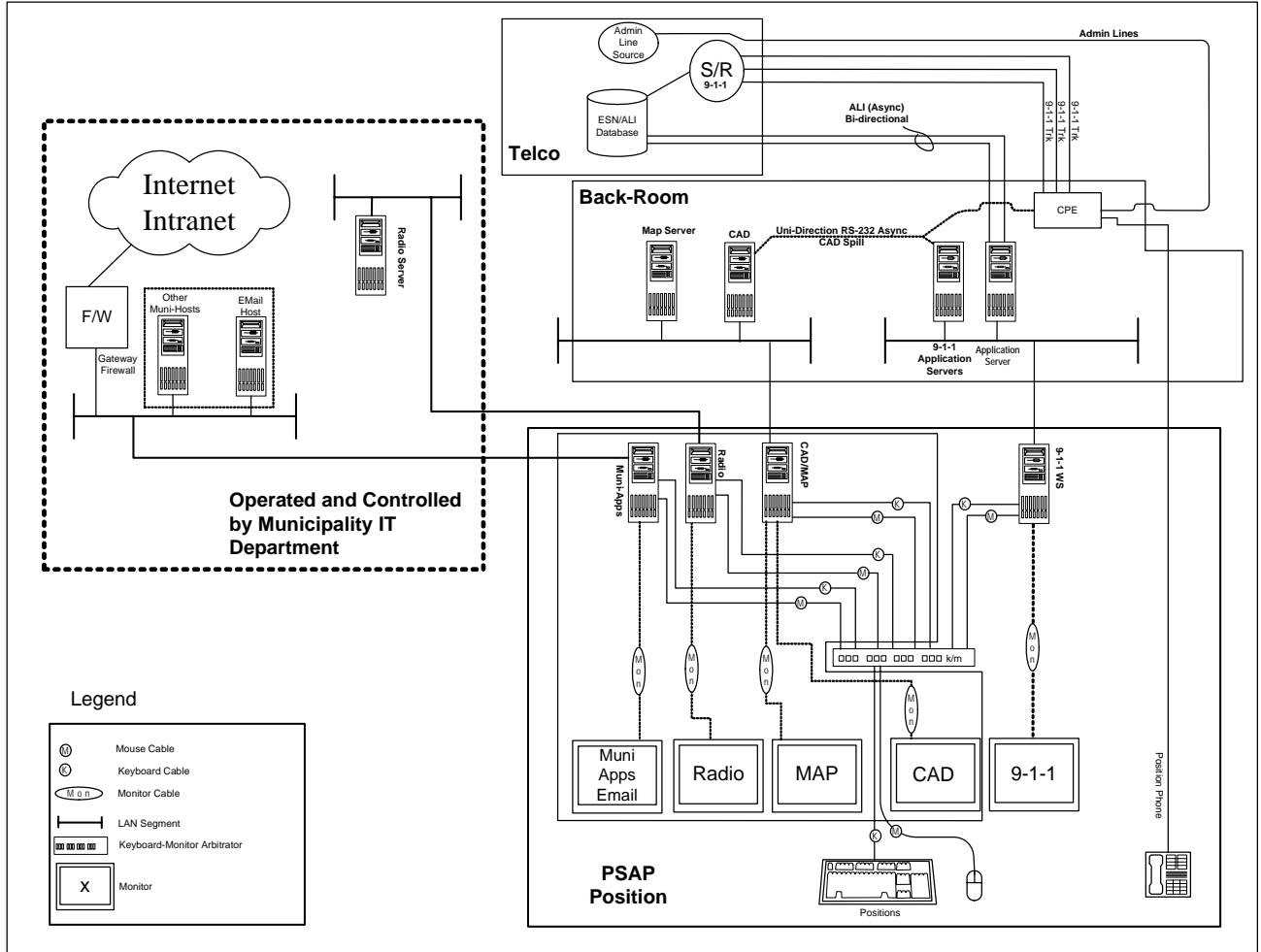
3.1 Legacy/Future Architecture (Where have we been/where are we going?)

Historically, PSAPs have normally existed in a 'closed environment', generally not connected to the Internet or to another network that might be connected to the Internet. This has been moderately successful in isolating the 9-1-1 system from many malignant activities or threats that would aim to disrupt the 9-1-1 call-taking environment. While this concept of a closed network has been an effective mitigation strategy, even closed networks are vulnerable to attack. Security strategies and effective risk management practices should be developed and enforced on all PSAP networks.

The Future Architecture of the PSAP network may well introduce shared use of centralized services or hardware and the use of VoIP for voice switching. These assumptions, and the need for remote access, will increase the need to interface with larger private networks (i.e. ESNNet) along with access to the Internet. The inherent ubiquity of appropriately connected networks introduces new risks and vulnerabilities and requires well thought out security strategies.

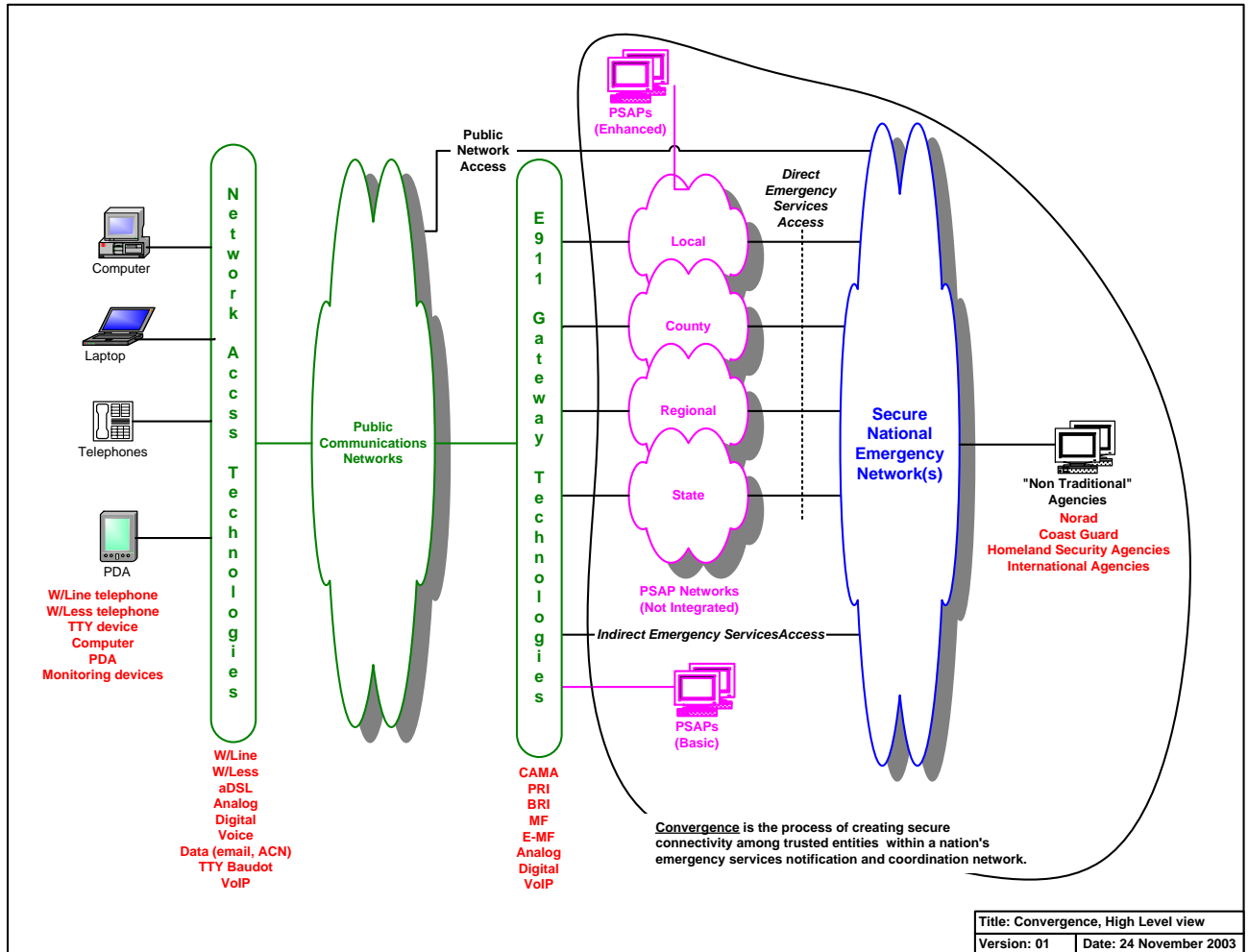
The paradigm of a closed network is beginning to fade, instead being replaced by interconnection and data sharing, tempered with effective security measures. While these new product concepts introduce rich feature-sets and revolutionary change, they also emphasize the need for a careful review of PSAP Security and implementation of effective security strategies. PSAPs moving away from the closed network model who fail to implement appropriate security measures introduce unnecessary risk into their PSAP and jeopardize the security of their organizations. Comprehensive network security plans will be mandatory for the PSAP networks of the future. A functional block diagram of a common 9-1-1 legacy architecture is shown below in Figure A. Figures B and C represents potential future architectures.

Figure A: Commonly used 9-1-1 Legacy Architecture ¹



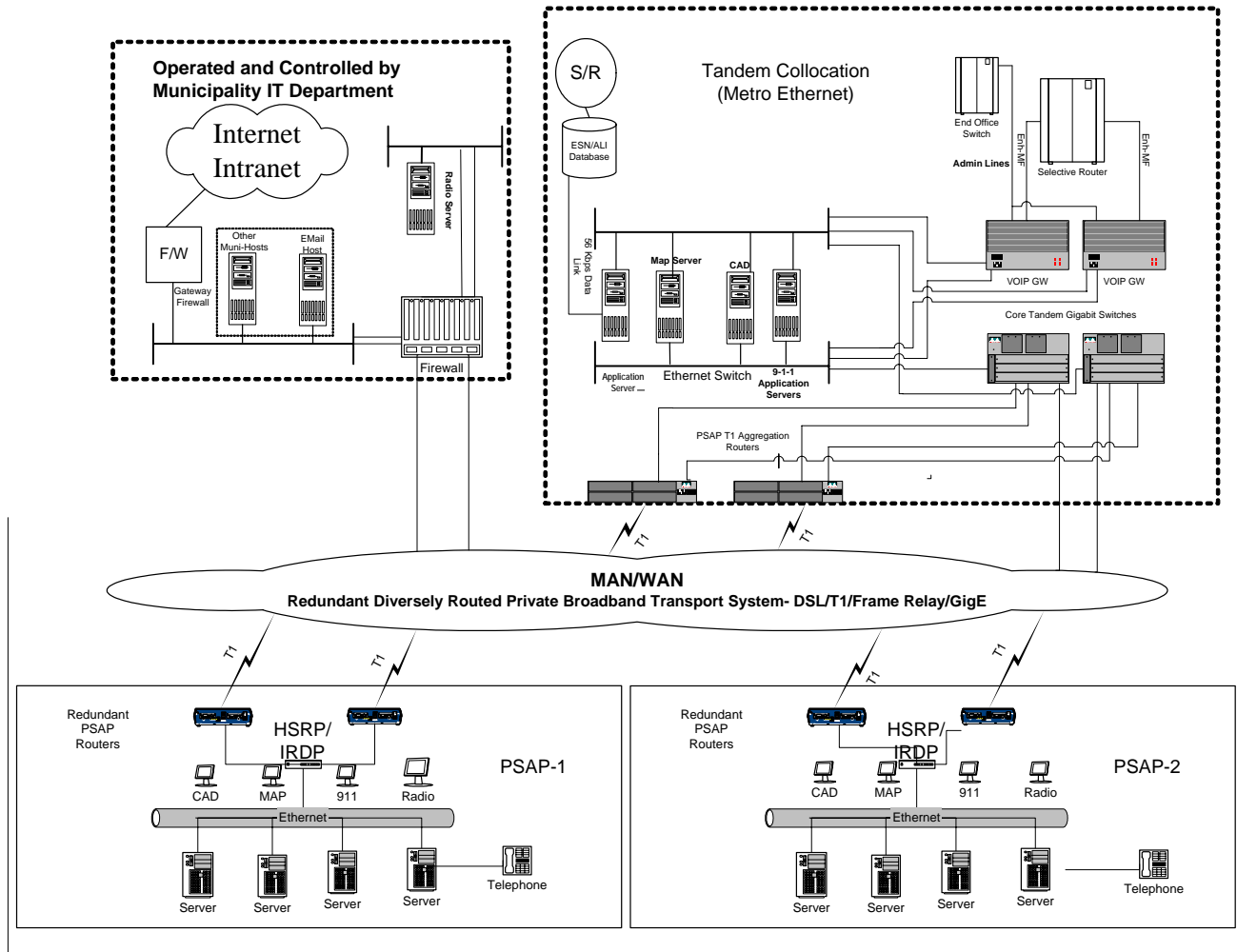
¹ Author, Mike Kennedy

Figure B: Potential Future 9-1-1 Architecture²



² Author: Gordon Kelly, TDC 2005

Figure C: Potential Future 9-1-1 Architecture³



When looking at these drawings it is important to understand that major takeaways are that future networks and PSAPs will likely be connected to ‘other’ entities and some cases multiple entities. As a result, while the connection enables new feature-sets, they also enhance the need for security.

³ Author: Ron Whitehurst

3.2 PSAP Security Categories

As mentioned in previous sections, the kinds of threats facing today’s PSAP are vast and ever changing and present PSAPs with challenges that can only be solved through creative thinking, education, awareness and application of proper mitigation strategies. This section identifies many of the common threats facing PSAPs, and provides guidelines for implementing effective mitigation strategies or countermeasures.

The following sections provide an overview of different types of threats and countermeasures and are organized into the following commonly accepted major categories as defined in Table A below. The following sections will further define these vulnerabilities and/or provide suggested countermeasures.

Note: The list below is subject to change due to new and increasing threats and technologies

Table A

<i>Categories</i>	<i>Subcategories</i>
Access Controls	<ul style="list-style-type: none"> • Administrative • Technical • Physical
Network Security	<ul style="list-style-type: none"> • Network Attacks • Traffic Protection (Confidentiality) • Traffic Integrity • Traffic Regulation (Firewall/Intrusion detection) • Wireless • Remote Access (VPN’s & Dial-up)
Application Security	<ul style="list-style-type: none"> • Malware • Secure Applications • Patching & Change Management
Telephony	<ul style="list-style-type: none"> • Toll Fraud
Availability	<ul style="list-style-type: none"> • Business Continuity • Disaster Recovery • Remote Monitoring & Availability
Access Controls	<ul style="list-style-type: none"> • Administrative • Technical • Physical

3.2.1 Access Control

A key tenet of PSAP Security involves letting the right people in and keeping the wrong ones out (physically and electronically). Access Control is a discipline specifically concerned with ensuring appropriate access methods are activated within the PSAP and is an extremely important aspect to PSAP Security.

Furthermore, the threats surrounding access control also include internal personnel. For example, internal employees can be a significant risk whether through malicious activities or plain ignorance. A list of these types of threats is provided below:

1. Insiders
 - a. Full Time Employees
 - b. Contract Workers
 - c. Visitors
 - d. Interns
 - e. Support Personnel (i.e. software/hardware vendors)
2. How Insiders can hurt you
 - a. Ignorance – Don't know security policies/practices
 - b. Carelessness – Know the security policies/practices, but get sloppy
 - c. Defiance – Know the security policies/practices, but ignore them in the name of expediency (i.e. had to ignore the policies to 'get the job done').
 - d. Malicious Intent – Know security policies/practices and intentionally circumvent them to cause damage. This is often a disgruntled employee.

Access Controls can be subdivided into three major categories, **Administrative, Technical, and Physical**. The categories may slightly overlap.

3.2.1.1 Administrative

Administrative controls can be most easily divided into two subcategories: Human Resources (HR) and System Administration (Sysadmin). This differentiation is important because different entries within a PSAP are responsible for different types of Administrative Controls. For example,

HR functions

- preventative measures such as background checks
- job rotation
- termination procedures (i.e. return all keys, etc)
- code of conduct
- workplace policies

System Administration functions/controls

- detective measures such as auditing and security reviews

- Involves non-technical ‘soft’ mechanisms, Functional Security policies should define appropriate administrative controls.

Recommendations:

- **General**
 - Create an Acceptable Use Policy
 - Ensure that an organization has hiring practices or that existing best practices are followed
- **HR**
 - Ensure that any existing security policies are adhered to as applicable to the hiring, termination and maintenance of employees
- **Sysadmin**
 - Create auditing policies and regularly perform system audits
 - Create user rights and permission policies

3.2.1.2 Technical

Technical Controls involve the use of technology to prevent or detect unauthorized access or allow authorized access. Methods for technical controls most often include user account and password mechanisms, biometrics, appropriate use of file permissions or database rights, etc. Because of their importance and commonplace within the PSAP, User Rights & Permissions and User Accounts & Password Management are discussed in detail in subsequent sections.

3.2.1.2.1 User Rights & Permissions

In order to properly protect a network and, ensure that proper access is given only to those who need it, user rights and permissions must be understood. It is at this point that a warning should be given. It is possible to create a permission structure so complicated that the administration of it will become almost unmanageable. Careful use of security groups can be very beneficial and simplify management however, it is also possible to create a situation where a user is a member of multiple groups and gains access that they should not have. As with anything else relating to network security a balance must be struck between security and usability.

It is important to understand the difference between a right and permission.

- A right is a property that is assignable to a user or a group, which will either allow or deny them the ability to perform an action. A good example of this is the ability to install a printer on a computer; this is an allowable right that can be assigned.
- A permission, on the other hand, grants or denies access to a object or resource. This would allow a basic user to see only their files while allowing management to see all of the files.

It is also important while implementing these policies to determine if there are any specific restrictions that need to be enforced, i.e., Law enforcement data can't be shared with Fire/EMS and patient records must be kept confidential.

Recommendations for Users Rights & Permissions:

- Maintain a simple, useable structure, which can be administered by the fewest number of personnel possible.
- Grant rights only to those who need them.
- Adhere to the policy of least privileged use, meaning if a basic user can perform all of the tasks necessary, don't grant administrator access to them.
- Limit the number of administrator accounts and only use them for administrative work, use a regular log on for day-to-day work.
- Disable or rename built in Administrator accounts
- Deny Anonymous or Guest accounts as these typically can be exploited.
- Periodically run audits against the users to determine what is actually their effective rights and permission. If a user is a member of several security groups it is possible for that user to have elevated privileges that were not intentional.

3.2.1.2.2 User Account & Password Management

An extremely important portion of PSAP Security is effective management of User Accounts and Passwords. The User Account is what assigned the rights and permissions and is where most of the difficulty of administration exists. Access to systems is often times provided using user accounts and passwords, however should these become compromised their purpose is rendered useless.

Because of this it is important to safeguard the passwords and create a policy, which forces them to change regularly. With enough time and/or resources, passwords can be cracked, thereby compromising the system and allowing unauthorized access. Therefore, careful thought must be taken when planning appropriate methods and policies for user account and password management.

Recommendations for User Account & Password Management:

Organizations who wish to secure access methods via user account and password policies should avoid using shared Windows accounts. Instead, each network user should have a unique Windows Account.

Furthermore, the Table below provides a listing of common password protection mechanisms (extracted from Microsoft's documentation) and a suggested value is indicated. A PSAP's password requirements should be documented in a Functional Security Policy and enforced.

Table B Extracted from Microsoft's "Creating a Strong Password Policy (Windows Server System)"
http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dsscc_aut_xbby.asp

<i>Setting</i>	<i>Explanation</i>	<i>Suggested Minimum Value</i>
Passwords must meet complexity requirements	Passwords are not based on the user's account name. Contains characters from three of the following four categories: <ul style="list-style-type: none"> • Uppercase alphabet characters (A–Z) • Lowercase alphabet characters (a–z) • Arabic numerals (0–9) • Non-alphanumeric characters (for example, ! \$#,%) 	Enabled
Minimum password length	The setting determines the minimum number of characters that a user's password must contain. It is recommended that you change this setting from the default value of 0. A minimum password length of seven characters is considered standard.	7 Characters
Minimum password age	This setting determines the number of days that must pass before a user can change his or her password. Defining a minimum password age prevents users from circumventing the password history policy by defining multiple passwords in rapid succession until they can use their old password again. The default value is 0, but it is recommended that this be reset. A value of a few days discourages rapid password recycling while still permitting users to change their own passwords if desired. Note that setting this parameter to a value higher than the maximum password age forces users to call the IT department to change their passwords, which increases costs to the organization ADD TEXT ABOUT SYSADMIN CHANGING	7 Days
Maximum password age	This setting determines the period of time (in days) that a password can be used before the system requires the user to change it. The best defense against impersonation is to require that users change their passwords regularly. This reduces the amount of time available for attackers to crack unknown passwords, and it periodically invalidates any password that has been stolen by other means. The default value of 42 days is generally appropriate, however, some IT departments shorten this to 30 days.	Refer to CJIS documentation
Enforce password history	This setting determines the number of unique new passwords that have to be associated with a user account before an old password can be re-used. It also rejects new passwords that are too similar to previous passwords. This feature prevents users from circumventing password lifetime restrictions by reusing their old password. The default value is 1. Most IT departments choose a value greater than 10.	10

3.2.1.3 Physical

The physical aspects of PSAP security are often overlooked, or incorrectly applied, if implemented at all. Physical Security of people, equipment, and other resources is critical in facilitating maximum system availability. If the battery backup system is located in an un-secure area, then it is possible to take the entire local 9-1-1 network off line with a quick flip of a switch. Physical security of servers, network routers, switches, firewalls, and other important components should be of the utmost concern when developing a comprehensive security plan. The introduction of vendor laptops/PC for the purposes of troubleshooting or routine maintenance onto a PSAP network can also potentially introduce risks that can harm the PSAP and consequently policies for such access must be implemented.

Recommendations for Physical Security:

- Establish an acceptable use and access policy and enforce it!
- Plan and evaluate all aspects of the physical security of a network with the worst-case scenario in mind. For example if the batteries in the UPS melt, this could cause a Hazmat incident and possibly force an evacuation of the dispatch center. Is there a single network router that can cause the rest of the system to fail?
- Place all critical systems in a controlled environment and limit the access to only those who need it, and no one else.
- Log and record all physical access to these devices just as you would log access to a computer network.
- Validate the identity of all personnel accessing these components
- Never leave an unattended terminal logged into a system, users should always terminate their sessions.
- Sometimes users will forget to terminate their sessions or may temporarily leave their positions with the intent of returning in a short while. As a result the position is now unattended. This provides personnel (both internal/external) an opportunity to negatively affect the session, the center, or worse a live 9-1-1 call. This is a real threat that should be understood and addressed carefully by PSAPs. Many operating systems offer 'inactivity timeouts' that either terminate a session or require a password to re-access a system after a configurable period of inactivity. Clearly, such a setting makes perfect sense on backroom equipment such as servers, and may offer an important layer of protection for call taking positions. However, PSAPs should be cognizant of the fact that end-user training will be necessary to ensure call takers understand the necessary procedures to terminate and log back into their systems. Many organizations suggest that the recommended inactivity timeout be set to 15 minutes. Furthermore, Windows' *Auto logon* feature, if used should always be disabled if inactivity settings are implemented.
- Work areas should be secured from non-resident personnel.
- Individual PC workstations should be password protected at the power-on level, and at the network or application level.
- PC's, workstations, and laptop type computers should be physically secured to furniture via padlock and cable mechanisms while in the end-users permanent physical location.
- While traveling, adequate safeguards including but not limited to cable and padlock mechanisms should be employed by end-users to whom such devices are entrusted, if such workstations could introduce any data into the trusted network.
- Login sequences incorporating login and password information should be stored in a location separate from the PC or workstation.
- Access levels and privileges should be periodically reviewed and adjusted based upon end-user needs and responsibilities.
- Access should never be permitted to systems via unsecured/unprotected modems.
- All remote access to systems should be authenticated prior to being authorized to the designated level. Authentication can be accomplished via:
 - Digital certificates

- Fob-based authentication i.e.: Secure-ID type card.
- PIN numbers, logins, dial access numbers, and/or passwords should be stored in a location separate from the PC, workstation, or authentication device.

3.2.1.3.1 Social Engineering

Social Engineering is defined as exploiting the weaknesses in people by tricking them to reveal information that would compromise an organization's security. Social Engineering is difficult to categorize but best fits under Physical Security. An example of social engineering is an individual posing as a valid employee of a service provider and receives access to critical equipment.

Recommendations:

- Training: An effective mitigation strategy for social engineering is ongoing awareness training.
- Security Policies: Well written, concise security policies are critically important.
- Checks and balances: Where appropriate, checks and balances systems requiring approval prior to divulging certain information can be very helpful in mitigating the effectiveness of social engineering.

3.2.2 Network Security

Today's 9-1-1 networks face a plethora of different electronic attacks. As the 9-1-1 industry and technologies have evolved, so have the threats. In some cases, current networks operate under the premise of a closed network. However, in reality, may have unaccounted for external connections violating the notion of a closed network, not to mention the threat of physical intrusion.

In the near future PSAPs will likely connect to other types of networks and closed networks may no longer be a viable/available option. Accordingly, PSAPs must understand and mitigate the different types of threats inherent with such connections. In this section, common types of threats are discussed and important precautionary measures are identified that PSAPs should be aware of.

Network security countermeasures can be categorized as follows:

- Traffic Protection (Confidentiality)
- Traffic Integrity
- Traffic Regulation (Firewall/Intrusion detection)
- System Configuration (i.e. Operating System security)
- Wireless
- Remote Access
- Physical security of network hardware

Note: The subject of Hacking is discussed in detail in Exhibit 1.

3.2.2.1 Networking

3.2.2.1.1 Traffic Protection

Because the PSAPs of tomorrow will likely be interconnected, sharing data collaboratively over networks, the data sent between sites and/or vendors can be vulnerable to interception and/or modification. Consequently the network traffic protection, including encryption and router traffic regulation may be a necessary and viable option in assuring the right data is received without modification or disclosure. The protection of traffic involves encryption, authentication, integrity, and non-repudiation. A list of common network attacks is provided below⁴:

- **Spoofing:** Refers to a situation in which one person or program is able to masquerade successfully as another
- **Eavesdropping:** Is the intercepting and reading of messages and conversations by unintended recipients
- **Teardrop:** An attack, which sends a flurry of IP fragments with malicious headers to the target machine. A bug in TCP/IP fragmentation re-assembly code caused the fragments to be improperly handled, crashing the operating system as a result
- **Smurf:** A denial-of-service attack that uses spoofed broadcast ping messages to flood a target system. In such an attack, a perpetrator sends a large amount of ICMP echo (ping) traffic to IP broadcast addresses
- **DOS, DDOS:** A computer system or network attack that causes a loss of service to users. Typically the loss of network connectivity and services consumes the bandwidth of the victim network or overloads the computational resources of the victim system

An effective means to discourage eavesdropping, spoofing and other malignant activities is the implementation of an encryption scheme where packets of data are mathematically obscured from plain text into cipher text, unreadable without knowledge of the 'key' used to decrypt the scheme.

Two methods commonly used:

- **Virtual Private Networks (VPNs)- Tunneling:** Tunneling with VPNs is a method of creating a controlled private network over an existing private or public network by using end to end encryption schemes.
- **Application Level Encryption:** Application level encryption is application specific; for example, only communication between particular applications would be encrypted vs. all traffic types as in Tunneling.

Network Traffic Protection Recommendations

- Data communications over dedicated wired media (i.e. leased modem lines, T-1s, etc.) are encrypted if practical. Keep in mind that, encrypting serial data can be very expensive).
- Data communications over shared services (especially IP-based networks) are encrypted using VPNs. If VPNs are not practical for certain applications (like incoming mobile phone

⁴ definitions obtained from Wikipedia.org, a popular online dictionary

video) be routed to a DMZ, authenticated, and then they should be brought into the 9-1-1 enclave.

- All application traffic messages are encrypted using encryption protocols (e.g. https vice http, Xenc vice XML, etc.).
- All data communications over any wireless medium are encrypted (including wireless internet access, satellite, radio links, etc.).

3.2.2.1.2 Traffic Authentication, Non-repudiation & Integrity

Authentication via encryption schemes can provide the necessary assurance that the person who sent the data, is actually who claims to have sent it. Authentication is accomplished by using digital signature protocol, which identifies the actual sending signatory as accurate.

A function of some encryption schemes is non-repudiation, which is the method by which a person cannot refute sending a message by using hashing algorithms and digital signatures. The benefits of such technology are obvious and may be a good fit for some applications within the PSAP.

Integrity is also an important function of encryption, by using hashing algorithms it is possible to determine that a message has not been altered en route. This too has obvious benefits (i.e. ALI; is this actually the right ALI?). Important Note: While obviously effective in ensuring confidentiality, encryption can be CPU-intensive. As such, appropriate performance measurements should be instituted whenever implementing an encryption mechanism.

3.2.2.1.3 Traffic Regulation (Firewall/Intrusion detection/Router Security)

The most common form of network security on the Internet today is packet regulation. This most often occurs using components such as Firewalls, Gateways, Routers, and Intrusion Detection Systems. Communication on and between networks of any shape or size involves the movement of packets, or discrete bits of data comprised in consistent ways known as protocols. Packets come in good and bad form and an effective security strategy must address proper traffic regulation.

Furthermore, it is important to protect router traffic which includes any traffic regulation that occurs on a router or terminal server (hosts whose primary purpose is to forward the packets of other hosts) and is based on packet characteristics. This does not include application gateways but does include address translation. By monitoring and regulating this traffic, different types of attacks can be identified in progress (such as a Denial of Service). Encryption, and Router regulation is likely to be a key part of the PSAP security in the very near future, if not already.

3.2.2.1.4 Router Traffic Regulation

Router traffic regulation includes any traffic regulation that occurs on a router or terminal server (hosts whose primary purpose is to forward the packets of other hosts) and is based on packet characteristics. This does not include application gateways but does include address translation.

3.2.2.1.5 Network Devices (Filters and access lists)

Regulating which packets can go between two sites is a simple procedure on the surface. Developing a plan that allows the right packets through at the right time and denies the unauthorized user packets is a considerable task. A few basic techniques are worth discussing, however.

- Restricting access in, but not out: Almost all packets (besides those at the lowest levels that deal with network reach ability) are sent to destination sockets of either UDP or TCP. Typically, packets from remote hosts will attempt to reach one of the “well known” ports. These ports are monitored by applications providing services such as Mail Transfer and Delivery, Telematics Data, Time, Domain Name Service, and various login protocols. It is easy for modern routers or firewalls to allow these types of packets through to the specific machine that supports a specific service. Attempts to send any other type of packet will not be allowed. This protects the internal hosts, but still allows all packets to get out.
- Dynamic route filters: With this technique, it is possible to have a router automatically detect suspicious activity and deny a machine or entire site access for a short time. In many cases, this will stop any sort of automated attack on a site.

Filters and access lists are typically employed on all three types of systems, although they are most common on routers.

3.2.2.2 Firewalls & Intrusion Detection Systems

3.2.2.2.1 Network Firewalls

Network Firewalls (sometimes called security gateways) are designed to prevent unauthorized access to (or from) an internal/private network or “enclave” and can exist in either hardware or software format⁵. These enterprise firewalls, which can proxy most services, should be configured to allow only those ports and protocols required. They should implement a “deny all but” posture unless specifically allowed where a port or protocol is blocked. In addition, wherever possible, firewall rules should permit these protocols only between specific network entities (e.g. if database updates are received from specific external servers, the rule allowing the ports for the update protocol should specifically define the external servers and allow those services only to specific internal servers). These firewalls also generate log files, and qualified personnel should be provided access, to review the logs for anomalies. Firewall logs should be retained for at least one year unless local or state records retention policy requires longer retention.

3.2.2.2.2 Personal Firewalls (Host Firewalls)

Personal Firewalls (Host Firewalls) are applications such as the firewall included with Windows XP SP2 or Zone Alarm. Because IT Security involves a layered or defense-in-depth approach, personal firewalls can help provide an additional layer of security to intrusions. Some can also monitor outgoing traffic and both block and alert users to a possible rogue application running on their system. However, be aware that personal firewalls can sometimes cause applications to cease

⁵ reference Webopedia.com

functioning. Ensure proper testing is conducted and contact vendors or first tier maintenance providers if problems occur.

Firewall Recommendations

- Network Firewalls should always be implemented whenever any 9-1-1 entity accesses any other entity; be it another agency, service provider, or the Internet.
- Workstations and servers should implement software firewalls when appropriate, especially when applications are supported for firewall-enabled inter-network operations.
- In addition, if the agency has control of an external router, access control lists (ACL's) should be implemented to filter unwanted or undesired protocols.

3.2.2.2.3 Intrusion Detection/Prevention Systems

“An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system”⁶. IDS/IPS systems should be installed and operational within all 9-1-1 centers. The IDS system should be set to alarm on critical events and the logs should be frequently reviewed.

3.2.2.3 System Configuration

System Configuration Security refers to the physical and software hardening of the PC's/Servers and Operating Systems. System Configuration can include things like disabling unnecessary services, implementing security policies, ensuring systems are patched, etc., because this field is so broad it is difficult to provide specific recommendations in this document. However, there are many accepted Security Standards that provide details on this subject. A small list is provided below:

- Center for Internet Security (CIS)
 - <http://www.cisecurity.org/>
- Defense of Information Systems Assurance (DISA-DoD)/National Institute for Standards (NIST):
 - <http://csrc.nist.gov/pcig/cig.html>
- The SysAdmin, Audit, Network, Security (SANS) Institute:
 - <http://www.sans.org/aboutsans.php#stepbystep>

3.2.2.4 Wireless

The prevalence of wireless technologies has now made wireless affordable and likely a future reality for the PSAP. However, wireless technologies, while rich in features and flexibility, require careful consideration from a security perspective.

⁶ reference Webopedia.com

Physical security of the actual Wireless Access Point is obvious as well as encryption of the data traveling wirelessly. Several forms of wireless encryption are available including WEP and WAP. The IEEE standard encryption algorithms WEP and WEP2 (Wired Equivalent Privacy) that were designed to secure wireless communications have been cracked. Tools are posted on the Internet to exploit the vulnerabilities. There are other methods of securing wireless communications. WPA (WiFi Protected Access) is an alternate encryption mechanism that may fix the weaknesses in WEP.

Papers that identify exploitable design flaws in the 802.1X (WEP) encryption algorithms are provided below:

- W. A. Arbaugh, N. Shankar, and J. Wang. Your 802.11 Network has no Clothes. In Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks, December 2001. <http://www.cs.umd.edu/~waa/wireless.pdf>
- Mishra, W. A. Arbaugh, An Initial Security Analysis of the IEEE 802.1X Standard. <http://www.cs.umd.edu/~waa/1x.pdf>

Administrators should restrict access point installation on the PSAP LAN without authorization. Conducting RF site surveys would enforce this rule.

Recommendations for Wireless Security:

- Avoid unnecessary wireless networks
- Ensure that wireless networks, when needed, adhere to the highest level of manufacturer supported security

3.2.2.5 Remote Access

Many vendors and telecommunications companies offer enhanced support capabilities through monitoring and/or remote maintenance. The benefits of such services are obvious, however they also introduce risks to the PSAP that must be carefully analyzed and mitigated. The two major types of remote access are Virtual Private Networking (VPN) and Dial-In Access. As a general rule, no matter if VPN or Dial-In access, the highest levels of security should always be maintained for remote maintenance connections. The next sections further define these concepts as well as provide security recommendations.

3.2.2.6 Virtual Private Networks & Dial-In

Virtual Private Networks or VPNs allow secure, high-speed remote connections for maintenance purposes including real-time support, monitoring, patch or antivirus definition delivery, and more. Oftentimes, firewalls are modularized to allow secure VPN connections. Whenever implementing a high-speed connection, strongly consider the use of a secure VPN.

In many cases, high-speed connections are not supported or cost-prohibitive. In such cases, dial-in connections provide a reasonable method to remotely access and support a system. However, it is important to ensure that appropriate security measures are implemented for any dial-in connections.

Recommendations for secure access:

- Monitoring/maintenance connections to PSAPs over high speed access should be secured with VPN level access
- Remote networks should be expected to adhere to commonly accepted industry security practices
- Modem or fax lines should avoid being directly connected to any PC or workstation that is connected to a database server or PSAP LAN
- Dial-out modems should not be capable of receiving incoming calls/traffic.
- Dial-out modems should not allow system access at the receiving end of the path.
- Password authentication should always be enabled for dial-in modem connections
- Auditing should be enabled whenever possible to track remote access connections

3.2.3 Application Security

Application Security covers a wide range of topics subdivided into the following prominent categories:

- Malware
- Patching & Change Management
- Application Security

3.2.3.1 Malware

Malware (Malicious Software) is defined as any program or file that is harmful to a computer and encompasses a broad range of threats such as Viruses, Worms, Spyware/Adware, and Trojan Horses.

- Viruses
- Worms
- Spyware/Adware
- Trojan Horses

3.2.3.1.1 Viruses

Whatis.com, an online Information Technology dictionary, defines a computer virus as “program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector, or document. Viruses can be transmitted as attachments to an e-mail note or in a downloaded file, or be present on a diskette or “CD.”

Viruses come in many shapes and sizes with differing payloads (or malicious intents). Viruses are delivered through a variety of means including email, network replication, or media. A virus can render a 9-1-1 computer completely inoperable, and/or have a detrimental effect on the call taker’s ability to respond to a call. Subcategories of viruses are Worms and Trojans.

3.2.3.1.2 Worms

A worm is a virus that replicates and propagates itself from system to system but generally does not alter files or data. Worms generally propagate rapidly and can ultimately cause a Denial of Service. A Denial of Service (DOS) is any service degradation or loss of service.

3.2.3.1.3 Trojan Horses

A Trojan horse is a program that contains malicious code while appearing to be harmless. For example, a user might download a seemingly desirable screensaver program that secretly causes harm to the PC by slowing it, deleting or damaging files, or worse rendering the system inoperable. Trojan horses are different from viruses in that they generally do not replicate themselves.

3.2.3.1.4 Spyware/Adware

Spyware and **Adware** are two of the most significant causes of user angst today.

Spyware is designed to snoop or monitor the user with or without their express consent, generally without. Spyware, is generally installed on the user's machine during an Internet session and oftentimes without the user's knowledge or through confusing the user into accepting something they should not. In its less harmful, but nonetheless invasive form, spyware can track and collect such things as visited Internet sites, for the purpose of transmitting the information back to its source in order to help advertisers send unsolicited pop-ups and e-mails to an Internet user's account.

In its harmful and invasive form, it can collect sensitive personal information including but not limited to:

- logins & passwords
- Social Security information
- names
- addresses
- birth dates
- PIN Numbers
- credit card numbers which are used by on-line shoppers.

In some cases, spyware can run in the form of actual processes (programs) on a desktop or workstation and can actively track all keystrokes and activity on that device. These programs can run at a lower and un-noticeable level, or they can run at a high priority to a point where they consume significant system resources.

Adware,⁷:

“any software application in which advertising banners are displayed while the program is running. The authors of these applications include additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on a computer

⁷ according to Whatis.com

screen. The justification for adware is that it helps recover programming development cost and helps to hold down the cost for the user.

Adware has been criticized because it usually includes code that tracks a user's personal information and passes it on to third parties, without the user's authorization or knowledge. This practice has been dubbed Spyware and has prompted an outcry from computer security and privacy advocates, including the Electronic Privacy Information Center."

Malware often opens the door for Hacking/Cracking, which is explained in section 3.2.3.2.

Recommendations for protection from Malware attacks:

- Implementation of Acceptable Use Policies (Internet, Network, email, etc) and users should receive awareness training. Direct connections to the Internet should be avoided. Sites that do allow direct Internet access should do so with caution. Acceptable Use Policies and if necessary 3rd Party Web Filtering Software can be used to enforce the policy (i.e. Websense Enterprise, or SurfControl Web Filter)
- Antivirus software should be mandatory for all systems (Coordination with local support contract provider and CPE Vendors may be necessary). It is extremely important to enact a detailed plan for virus definition updates, virus scans, and other configuration settings in order to achieve the highest levels of effectiveness.
- PC and Internet computer browsers security settings should be set to their highest level that while still allowing required functionality. This will include limiting the download of unsolicited files and/or programs, first and third party cookies that do not have a stated security policy, blocking first and third party cookies that use personally identifiable information without the users express consent, and allowing only per-session cookies. You can adjust your browser settings so that you are notified when a cookie is being placed in your browser. You can also set your browser to decline (or accept) all cookies.
- As a precaution, Internet users should never launch or activate unsolicited programs or pop-up windows, and never accept downloads from unsolicited sources.
- Firewalls can help limit certain types of malware attacks and should be mandatory for PSAP networks.
- Spyware/Adware removal tools should be installed on all systems. Anti-Spyware software is available also from reputable sources. It is cautioned that there are several sites on the Internet that claim that they are effective anti-Spyware, when in reality these have been known to be Trojan-horses, but are very sophisticated Spyware packages that are extremely difficult to remove, once loaded to a PC. As such, programs of this nature should always be installed by trained professionals and in concordance with documented software installation policies.

3.2.3.2 Hacking/Cracking

Hacking is a somewhat misunderstood term and is often confused with Cracking.

- **Hacking:** Hacking is the process of a person learning about a particular programming language or system, or actually doing the programming rather than just theorizing about it. A hacker does not have any intended malice or malignant purpose behind his or her activities. A hacker may be competent enough to ‘understand’ or ‘identify’ weak points within a particular system.
- **Cracking:** Cracking involves an entity or person breaking into someone else’s computer system, often on a network; bypassing passwords or licenses in computer programs; or in other ways intentionally breaching computer security. The cracker may be doing this for profit, maliciously, for some purpose or cause.

The key differences between Hacking and Cracking are fairly obvious despite their universal confusion; Cracking has a malicious intent in mind, while Hacking is more exploratory in nature. Regardless, hacking has achieved a notable stigma within the industry and despite what it may be called, protection against unauthorized electronic access is a threat that must be understood and mitigated.

Today’s attacks are very sophisticated – just to name a few:

- exploiting known vulnerabilities
- self replicating code
- password cracking
- backdoors
- stealth diagnostics
- packet forging/spoofing

Systems connected to external/untrusted networks (such as the Internet) are constantly being scanned for vulnerabilities and are susceptible to attack at all times.⁸

- Default installations of Red Hat 6.2 servers are routinely scanned, probed, and exploited within 72 hours of connecting to the Internet.
- Default installations of Windows are routinely compromised within 24 hours of being connected to the Internet
- The most popular attack method is an overflow associated with rpc.statd for Intel based systems.

Intel based systems are commonly used in the PSAP environment. The most commonly used attack for an Intel based system is a buffer overflow⁹. A buffer overflow attack can be executed from across the Internet. These attacks often target services that are running by default, silently in the background. The attack inputs more information than the service is designed to accept. A buffer overflow can have a number of different results such as crashing the machine or service, this type of

⁸ statistics were gathered from the HoneyNet Project (<http://www.honeynet.org/>)

⁹ Per “Honey net” statistics

attack is often designed to cause the service to crash in a way that enables the attacker to gain access to the command prompt. At which point the attacker can enter arbitrary commands. A commonly used approach is to compromise the system using a buffer overflow attack, install a backdoor which enables the attacker to easily gain access to the compromised host in the future, clean up the logs to remove any trace of compromise, and then use the compromised host to perform any number of illegal activities.

Recommendations for protection against Hacking/Cracking:

- Ensure systems are patched
- Install and update antivirus software
- Install Firewalls
- Leverage other security measures mentioned in this document

3.2.4 Patching & Change Management

3.2.4.1 Operating System Security Patch Management

The Operating Systems in use today are not foolproof; as a result, Microsoft and other O.S. Vendors release critical security patches periodically. Failure to test and install these security patches can result in systems becoming vulnerable to different types of attacks that could ultimately result in downtime to the 9-1-1 center. Consequently, PSAPs must include a comprehensive security patch management strategy as part of any efforts towards effective PSAP Security.

When planning a security patch management strategy there are several items to consider:

- **Identification/Scope/Ownership**
 - Determine who owns the Security Patch Management Process.
 - What are the roles and responsibilities and who owns them?
 - Who is responsible to support systems?
 - Who is responsible to test?
 - Determine who is responsible to deploy/install critical updates (generally 1st-Tier maintenance provider although some vendors offer enhanced or managed security services)
 - Determine timeframes for patch testing and deployment
 - Determine what systems will fall under the Security Patch Management Policy
 - Determine where patches will come from and what method will be used to identify their existence
 - Determine and comply with any Vendors patch management policies/constraints
- **Testing**
 - Determine what needs tested (i.e. what software is installed on the different systems—maybe multiple test efforts)
 - Determine depth/breadth of testing
- **Deployment**
 - Determine how to install

- Manually
- 3rd Party Tool
- Vendor enhanced or managed security service
- Determine when (or if) to install
 - Least disruptive but still sensitive to closing the security vulnerability as quickly as possible

3.2.4.2 Change Management

In reality a security patch management strategy should be part of a larger ‘change management’ strategy which is concerned about not only security patches but also product updates (i.e. feature updates/service packs, upgrades, etc) and new software. However, for the purposes of clarity, the two are separated. While this section does not intend to be an all-encompassing discussion of change management, an effective change management strategy should at least address the following concerns:

- **New Software**
 - Who determines the need?
 - Who is responsible for regression testing the software?
 - Does the vendor support the software in my current environment?
 - Are there third party components that may require additional testing?
 - Identify who will load new software and register it on the computer
- **Updates to existing software**
 - Who determines the need?
 - Who is responsible for testing the software?
 - Has the vendor tested the upgrade in my environment?
 - Are there third party components that may require additional testing?
 - Who installs the upgrade?
 - Determine an acceptable schedule for outage of workstation or system

3.2.5 Telephony

The Telephony Infrastructure faces many threats; however, the most significant of these is toll fraud, described in the next section.

3.2.5.1 Toll Fraud

The most costly type of a telecommunications system security breach, **Remote Access Toll Fraud**, involves hackers who gain direct access to **Customer Premise Equipment (CPE)** and make long distance calls. Unfortunately, most of these are International calls from payphones to payphones. The hackers are able to break into Voice CPE—such as PBX’s, Automatic Call Distributors, auto-attendants, call diverters, and voice mail systems via Direct Inward System Access (DISA) features or manipulation of system features.

Example:

Hackers randomly call selected 800 number or regular telephone numbers. They will focus on numbers that answer with an Automated Attendant, DISA Tone, or Voicemail. They will then input codes until the second dial tone is obtained. ***Since this task typically takes numerous attempts, you should take notice of any multiple short hold time calls on your CDR records.*** After the hacker gains access to the telephone system they will access an outside line and call anywhere in the world. It gets worse. Once the hacker finds a usable target number, they sell the information to others and your network becomes the international “gateway” for people to “Phone Home.”

To minimize risks on DISA and voice mail:

- Limit the number of employees given access codes
- Remove manufacturer/vendor-installed default passwords.
- Change codes frequently and use the maximum number of digits your system will allow.
- Deactivate all unassigned codes immediately.
- Restrict after-hours and weekend access to DISA.
- Deactivate your voice mail system’s second dial-tone feature if you don’t need it.
- Require voice mailbox users to change their codes and check their greetings often.
- Never use a telephone number as a DISA access code.
- Block telephone access to area codes not relevant to your business operations.
- Monitor call detail reports closely and investigate any patterns that indicate the likelihood of unauthorized calls.
- Ensure that operators never connect an internal call to the external network without proper authorization.

Another simpler method hackers use to access CPE and telephone lines to make unauthorized calls is the Internal Operator Transfer to “0” method. The hackers will call into the main switchboard and ask to be transferred to the outside operator. Unfortunately, most switchboard operators are so busy they do not stop and ask who the caller is and why do they need the operator. They simply access a line, dial “0,” and connect the caller. Believe or not this is one of the most successful methods used by hackers today. ***Instruct your switchboard operators never to transfer to the outside operator unless they know the caller, and the caller has authority to ask for this type of call completion.***

3.2.5.1.1 Preventing Toll Fraud

- Be sure that you are taking advantage of the security features built-in to your phone system to eliminate any obvious invitations to fraud. Remote access to your PBX or voice mail system, especially for outbound calling, should be restricted to as few employees as possible.
- Use multiple layers of password protection i.e. an additional code should be required to gain dial tone once a caller has entered the voice mail or PBX system.
- Toll restrict lines from long distance access for forwarding messages to pagers, cell phones etc.
- Set up voice mail to restrict the digit 1 for dialing access to any extension or outside lines, i.e. 10288, 1 (XXX) XXX-XXX, 1 (800) ATTcall.

- Restrict voice mail from permitting dialing of any PBX soft key's that reconfigure the switch itself.
- Restrict voicemail from passing through phone numbers or extensions that start with 7, 8 or 9 which are normally used to make outside calls.
- Do not allow your voice mail system or telephone switch to be configured remotely. If your system is connected to a modem and that modem goes to an outside line, disconnect it. No matter how convenient it is to the installer to remotely configure and make changes, this is not an option unless you personally are at the office, personally plug the line in, and personally unplug the line when changes are completed. The remote access is the most serious point of entry.
- Reports – If your PBX/key system has a Station Message Detail Recording (SMDR) or Call Detail Reporting (CDR) feature, **turn it on**. The SMDR/CDR reports will record all telephone transactions throughout the day. This is a good place to monitor phone transaction on a regular basis to detect toll fraud. If you do not have time to review the reports on a daily basis, then make it a practice to look every Monday morning. In most cases, toll fraud happens on the weekends when there is no one in the office to notice that every line is in use.

Toll charges originating from CPE is the customer's responsibility. Carriers will not automatically remove the disputed charges from your bill. However if you have determined your network has been compromised and have not identified the source, notify your carrier's fraud department immediately as they will typically work with you to prevent further charges.

3.2.6 Availability

PSAP availability is perhaps the most prominent aspect of PSAP Security. Keeping critical resources up and running requires careful and well thought out planning. Availability can be separated into two major categories: Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP). The following sections provide an introduction to these important concepts and identify some important recommendations on how to ensure the PSAP is protected in this regard.

3.2.6.1 Business Continuity Planning

Business Continuity Planning or BCP is primarily focused with the planning necessary to AVOID a disaster. For example, conducting a Business Impact Analysis to determine what assets are important and what risks (including probability of different threats occurring) are relevant to the PSAP is an important process to ensure proper expenditure of resources (i.e. purchase of uninterruptible power supplies/generators, protected server storage (such as Redundant Array of Independent Disks hard drives, Hot Sites, etc).

An important part of the plan is to have back-up procedures for all computers in the PSAP. A serious security breach or even a total device failure, leaving compromised or unusable software may require a complete system reload. A recent software back up of user files and data plus documented changes made since the back-up will greatly speed the restoration process.

Recommendations:

- Ensure the PSAP has a BCP in place
- Conduct a Business Impact Analysis
- Keep your BCP up to date

3.2.6.2 Disaster Recovery Planning

A Disaster Recovery Plan (or DRP) is more concerned about what a PSAP does when a disaster actually occurs (note the difference between a BCP and DRP). A disaster would be an instance that makes the PSAP non-operational. The DRP would detail how to begin the recovery such as detailed instructions on how to roll calls to another PSAP in order to maintain service. Next would be a plan on how, when and where the PSAP would be put back into full operation. This would depend on the nature of the disaster. A DRP is a crucial part of a PSAP security strategy.

Recommendations:

- Ensure the PSAP has a DRP in place
- Keep your BCP up to date
- Educate everyone on their role in the DRP
- Test and practice your DRP

3.2.7 Remote Monitoring & Maintenance

9-1-1 Systems must achieve high levels of availability and the implementation and management of a security strategy can be a challenging exercise. Remote monitoring and maintenance services can be an effective mitigation strategy to help maintain high levels of availability.

Real-time monitoring and response of alarm events and the automation of operating system patches and antivirus pattern file update services to PSAP networks can provide significant benefit and help to relieve the burden and complexity of security management. However, remote monitoring & maintenance in itself must be evaluated from a security perspective. Such access must always be secure and from trusted entities or risk inadvertently introducing security risks into the PSAP.

3.2.8 System Logs

All system logs should be recorded with accurate time/date data, using a hardware-based, UTC-traceable timeserver.¹⁰ This applies to all of the PSAP Security Categories having logs, such as firewalls, so that all logs can be compared and analyzed easily, and that the logs will be admissible as evidence in court. This method is used to synchronize the ANI/ALI switch, voice recorder, radio console, CAD, and other PSAP system logs. By using the same traceable timing method all logs, from networking equipment to PSAP operations systems, will be synchronized for interoperability requirements.

3.2.9 VoIP (Voice over Internet Protocol specific concerns)

When the deployment of VOIP is being considered or is being deployed all resulting security issues shall be considered. A VoIP PBX architecture and a VOIP network architecture can create two

¹⁰ Reference NENA #04-002 for the PSAP Master Clock

different security threats to the existing PSAP and its infrastructure. For instance, using an **Internet** connection as opposed an **intranet** connection creates completely different security issues.

As standards and policies are developed to include VOIP security technology, this document will be updated to include those standards and policies.

4 References

4.1 Documents

CJIS Security Policy	AUGUST 2003, Version 3.2
NIST Special Publication 800-60	Version 1.0 Initial Public Draft
NENA 04-002, PSAP Master Clock	Issue 3, May 17, 2000

4.2 Web Sites

www.nena.org **National Emergency Number Association (NENA)**

NENA's mission is to foster the technological advancement, availability, and implementation of a universal emergency telephone number system. In carrying out its mission, NENA promotes research, planning, training and education. The protection of human life, the preservation of property and the maintenance of general community security are among NENA's objectives.

www.fas.org/irp/agency/doj/fbi/is/ncic.htm **National Crime Information Center (NCIC)**

www.fbi.gov/hq/cjisd/cjis.htm **Criminal Justice Information Services (CJIS)**

www.nist.gov **National Institute of Standards and Technology (NIST)**

csrc.nist.gov **National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC)**

The De Facto repository of all government documents relating to data security for the PSAP and law enforcement agencies. This site has an excellent repository of recommended practices, programming templates, and security templates.

www.cert.org **C.E.R.T**

Computer Emergency Response Team. Also called US CERT this is a joint cooperation between Carnegie-Melon University and the Federal Government to establish a site for tracking and processing of computer threats and vulnerabilities. This site provides excellent links to training and reference material for data security and an excellent source of up-to-date knowledge and fixes.

www.grc.com **Gibson Research**

Gibson Research is a private firm that provides data security testing however they have an excellent program on their website which is a free tool to check the integrity of a workstation

isc.sans.org **Internet Storm Center**

The Internet Storm Center is a tracking tool put together by the SANS institute which is updated in close to real time with port vulnerability information, latest security threats and recommended fixes and workarounds.

www.sans.org **SANS Institute**

An excellent source for data security training and instruction, as well as links to online resources to help answer questions. This site focuses more on security auditing and system hardening versus active defense but it does provide a excellent foundation. It provides a good source of hardening checklists.

Following are vendor web sites that provide an excellent source of virus definitions, removal tools, and patches:

securityresponse.symantec.com **Symantec Anti-Virus Response Team**

vil.nai.com **Network Associates AVERT anti-virus team.**

5 Exhibits

5.1 Exhibit 1: Security Requirements from the NCIC Web Site

1. Computer Center:

- a. The criminal justice agency computer site must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any of the stored data.
- b. Since personnel at these computer centers can have access to data stored in the system, they must be screened thoroughly under the authority and supervision of an NCIC control terminal agency. (This authority and supervision may be delegated to responsible criminal justice agency personnel in the case of a satellite computer center being serviced through a state control terminal agency.) This screening will also apply to non-criminal justice maintenance or technical personnel.
- c. All visitors to these computer centers must be accompanied by staff personnel at all times.
- d. Computers having access to the NCIC must have the proper computer instructions written and other built-in controls to prevent criminal history data from being accessible to any terminals other than authorized terminals.
- e. Computers having access to the NCIC must maintain a record of all transactions against the criminal history file in the same manner the NCIC computer logs all transactions. The NCIC identifies each specific agency entering or receiving information and maintains a record of those transactions. This transaction record must be monitored and reviewed on a regular basis to detect any possible misuse of criminal history data.
- f. **Each State Control terminal shall build its data system around a central computer, through which each inquiry must pass for screening and verification.** The configuration and operation of the center shall provide for the integrity of the database.

2. Communications:

- a. Lines/channels being used to transmit criminal history information must be dedicated solely to criminal justice, i.e., there must be no terminals belonging to agencies outside the criminal justice system sharing these lines/channels.
- b. Physical security of the lines/channels must be protected to guard against clandestine devices being utilized to intercept or inject system traffic.

3. Terminal Devices Having Access to NCIC:

- a. All agencies having terminals on this system must be required to physically place these terminals in secure locations within the authorized agency.
- b. The agencies having terminals with access to criminal history must screen terminal operators and restrict access to the terminal to a minimum number of authorized employees.
- c. Copies of criminal history data obtained from terminal devices must be afforded security to prevent any unauthorized access to or use of the data.
- d. All remote terminals on NCIC III will maintain a manual or automated log of computerized criminal history inquiries with notations of individuals making requests for records for a minimum of one year.