APPENDICES

Appendix 1. Potential Vulnerabilities of NG9-1-1 Interconnection with the NPSBN

Given that NG9-1-1 and FirstNet networks will enable significant exchange of data, all stakeholders should pay close attention to the prospect of bad actors seeking to exploit one or both of these significant pillars of the future emergency response ecosystem. The following is a detailed list of potential vulnerability points resulting from the interconnection of NG9-1-1 with the NPSBN.

- Compromised citizen devices impacting FirstNet
  - Traffic interception
    Over The Top (OTT) or IP next generation apps are vulnerable to traffic interception, particularly when utilizing the public Internet
    - Extraction of Personally Identifiable Information (PII), especially in the case of calls involving medical information exchanged with the EMS responder
    - Information passed from a PSAP to a caller may not be suited for wider consumption, especially with regards to police interactions
    - The caller information going to a first responder can be spoofed, risking false responses, response testing (reconnaissance), or denial of service attacks
    - First responder information could be intercepted, allowing future attacks on the identified device (now known to belong to a first responder)
  - Malware – caller
    Malware (worm) on an end-user device could infiltrate other systems or devices
    - Citizen device could pass malware into FirstNet
    - Citizen device could pass malware into first responder device
  - Denial of service
    Citizen devices could be used to generate DDoS attacks
    - Citizen devices could generate DDoS attack into FirstNet
    - Citizen devices could generate DDoS attack on first responder device(s)

- Compromised Originating Network impacting FirstNet
  - Traffic Interception
    Compromised Originating Network could intercept traffic interacting with FirstNet
    - Extract PII
    - Extract inappropriate information
    - Intercepted traffic in Originating Network is spoofed
    - Intercepted traffic in Originating Network identifies first responder device
  - Malware – network
    Malware in Originating Network could infiltrate other systems or devices
    - Originating Network could pass malware into FirstNet
    - Originating Network could pass malware into first responder device
  - Ransomware – network
    Ransomware in Originating Network could infiltrate other systems
    - Originating Network could pass ransomware into FirstNet
  - Denial of service
    Compromised Originating Network could generate DDoS attacks
    - Originating Network could generate DDoS attack into FirstNet
    - Originating Network could generate DDoS attack on first responder device(s)

- Compromised Internet server, interconnected via NG9-1-1, impacting FirstNet
  - Malware – network
    Malware on Internet server could infiltrate other systems or devices
    - Internet server could pass malware into FirstNet
    - Internet server could pass malware into first responder device
  - Ransomware – network
    Ransomware in Internet server could infiltrate other systems
    - Internet server could pass ransomware into FirstNet
  - Denial of service
    Compromised Internet Server could generate DDoS attacks
    - Internet server could generate DDoS attack into FirstNet

    - Internet server could generate DDoS attack on first responder device(s)

- Compromised Government server, interconnected via NG9-1-1, impacting FirstNet
  - Malware – network
    Malware on Government server could infiltrate other systems or devices
    - Government server could pass malware into FirstNet
    - Government server could pass malware into first responder device
  - Ransomware – network
    Ransomware in Government server could infiltrate other systems
    - Government server could pass ransomware into FirstNet
  - Denial of service
    Compromised Government Server could generate DDoS attacks
    - Government server could generate DDoS attack into FirstNet
    - Government server could generate DDoS attack on first responder device(s)

- Compromised LMR network/devices, interconnected via NG9-1-1, impacting FirstNet
  - Malware – network
    Malware on LMR network could infiltrate other systems or devices
    - LMR network could pass malware into FirstNet
    - LMR network could pass malware into first responder device
  - Malware – devices
    Malware on LMR devices could infiltrate other systems or devices
    - LMR devices could pass malware into FirstNet
    - LMR devices could pass malware into first responder device
  - Ransomware – network
    Ransomware in LMR Network could infiltrate other systems
    - LMR network could pass ransomware into FirstNet
  - Denial of service
    Compromised LMR network could generate DDoS attacks
    - LMR network could generate DDoS attack into FirstNet
    - LMR network could generate DDoS attack on first responder device(s)

- Compromised NG9-1-1 PSAP impacting FirstNet
  - Malware – network
    Malware in NG9-1-1 PSAP could infiltrate other systems or devices
    - NG9-1-1 PSAP could pass malware into FirstNet
    - NG9-1-1 PSAP could pass malware into first responder device
  - Ransomware – network
    Ransomware in NG9-1-1 PSAP could infiltrate other systems
    - NG9-1-1 PSAP could pass ransomware into FirstNet
  - Denial of service
    Compromised NG9-1-1 PSAP could generate DDoS attacks
    - NG9-1-1 PSAP could generate DDoS attack into FirstNet
    - NG9-1-1 PSAP could generate DDoS attack on first responder device(s)

- Compromised legacy PSAP impacting FirstNet
  - Malware – network
    Malware in legacy PSAP could infiltrate other systems or devices
    - Legacy PSAP could pass malware into FirstNet
    - Legacy PSAP could pass malware into first responder device
  - Ransomware – network
    Ransomware in legacy PSAP could infiltrate other systems
    - Legacy PSAP could pass ransomware into FirstNet
  - Denial of service
    Compromised legacy PSAP could generate DDoS attacks
    - Legacy PSAP could generate DDoS attack into FirstNet
    - Legacy PSAP could generate DDoS attack on first responder device(s)

- Compromised Next Generation Core Services (NGCS) element impacting FirstNet
  - Malware – network
    Malware on NGCS element could infiltrate other systems or devices
    - NGCS element could pass malware into FirstNet

    - NGCS element could pass malware into first responder device
  - Denial of service
    Compromised NGCS element could generate DDoS attacks
    - NGCS element could generate DDoS attack into FirstNet
    - NGCS element could generate DDoS attack on first responder device(s)

- Compromised Emergency Services IP Network (ESInet) element impacting FirstNet
  - Malware – network
    Malware on ESInet element could infiltrate other systems or devices
    - ESInet element could pass malware into FirstNet
    - ESInet element could pass malware into first responder device
  - Ransomware – network
    Ransomware on ESInet element could infiltrate other systems
    - ESInet element could pass ransomware into FirstNet
  - Denial of service
    Compromised ESInet element could generate DDoS attacks
    - ESInet element could generate DDoS attack into FirstNet
    - ESInet element could generate DDoS attack on first responder device(s)

- Compromised FirstNet device impacting NG9-1-1
  - Traffic Interception
    - Compromised FirstNet device could intercept traffic interacting with citizen
    - Extract PII
    - Extract inappropriate information
    - Intercepted traffic in FirstNet is spoofed
  - Malware – network
    Malware in FirstNet network could infiltrate NG9-1-1 network
    - FirstNet network could pass malware into NG9-1-1 network
    - FirstNet network could pass malware into interconnected network (Government server or Internet server)
    - FirstNet network could pass malware into Originating Network
    - FirstNet network could pass malware into citizen device
  - Malware – device
    Malware in FirstNet device could infiltrate NG9-1-1 network
    - FirstNet device could pass malware into NG9-1-1 network
    - FirstNet device could pass malware into interconnected network (Government server or Internet server)
    - FirstNet device could pass malware into Originating Network
    - FirstNet device could pass malware into citizen device
  - Denial of service – network
    Compromised FirstNet server could generate DDoS attacks
    - FirstNet network server could generate DDoS attack into NG9-1-1 network
    - FirstNet network server could generate DDoS attack into interconnected network (Government server or Internet server)
    - FirstNet network server could generate DDoS attack into Originating Network
    - FirstNet network server could generate DDoS attack on citizen device
  - Denial of service – device
    Compromised FirstNet device could generate DDoS attacks
    - FirstNet network device could generate DDoS attack into NG9-1-1 network
    - FirstNet network device could generate DDoS attack into interconnected network (Government server or Internet server)
    - FirstNet network device could generate DDoS attack into Originating Network
    - FirstNet network device could generate DDoS attack on citizen device

Appendix 2. Use of Firewalls to Control Access

Firewalls contribute to security by controlling the flow of information into and out of network entry points. By using a set of user defined configuration rules, a firewall determines which traffic will be allowed to pass through and onto the network. Traffic that doesn't satisfy the configured rules is rejected. The following provides more guidance on the use of firewalls to control access.

Firewall Basics

A firewall is either a stand-alone device or a software application running on a host with the following characteristics:

- Supports at least one internal and one external connection
- Filters information in the following ways:
  - Service control
  - Direction control
  - Behavior and content control (email, web)
- Functionality ranges from basic to complex:
  - Packet filtering
  - Application level – proxy server
  - Deep packet inspection
- Requires special expertise for proper selection and configuration

Selecting Components - Security Features that Matter

Consider the following best practices when selecting system components:

- Choose devices and protocols that support encryption, integrity, and nonrepudiation whenever possible. Encryption protects the information traversing a network by making it unreadable to unauthorized users. Integrity checks determine if any changes have been made to a network message. Nonrepudiation verifies the identity of an information source.
- Give preference to devices with logging capability, such as Syslog support. Event logging is available in a wide range of devices including routers, firewalls, backup systems, and access control systems. Logs can aid in early threat detection by recording significant network events, changes to firewall configuration, or user access to an area or device. Syslog is a logging standard that can be used to consolidate log information from multiple devices on a network.
- Look for tamper proofing, built-in locks, and other access control features when selecting mission critical components.

Wireless Technology

- Choose wireless devices with built-in firewalls and support for the highest level of encryption available.
- Harden wireless access devices by following these steps:
  - Replace the default administrator name and password with strong alternatives.
  - Follow the device's "Before You Begin" protocols.

Configuring Security Features

The goal in this phase of the process is to properly configure the security features of each system component. Configuring firewalls, hardening system devices, configuring user accounts, and enabling threat detection are all tasks that contribute to secure system installation.

Configure Firewall Rules

Firewalls use a set of rules, established by the user, as the basis for determining which traffic is allowed to pass in or out of the network. For example, a rule might block all access to a specific IP address or port. Proper configuration of firewalls is essential to securing the network and should only be performed by experienced personnel. Best practices for configuring firewalls include:

- Use a combination of rules to both permit authorized traffic and deny unauthorized traffic. A typical approach is:
  - Create rules that explicitly deny access
  - Add rules to permit only the required access
  - Add a broad-based rule to deny access to all remaining traffic
- Confirm that the firewall can detect TCP "SYN-flood" attacks by tracking the state of a TCP handshake (stateful firewall).
- Include rules to restrict outbound network traffic in order to minimize the spread of damage in the event of a breach.

Appendix 3. Recommended Guidelines and Practices for Password Creation and Protection[101]

User passwords for public safety networks must balance security needs with burdens on the user. Password protection policies can help ensure the public safety network remains secure and that all users (including employees, contractors, consultants, temporary workers, etc.) adhere to the password policy. The following provides recommended guidelines and practices for password creation and protection.

Password Creation

- Strong passwords:
  - Contain at least 8 alphanumeric characters.
  - Contain both upper and lower case letters.
  - Contain at least one number (for example, 0-9).
  - Contain at least one special character (for example, !$%^&*()_+|~-=\`{}[]:”;’<>?,/).

- Poor, or weak, passwords have the following characteristics:
  - Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
  - Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
  - Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
  - Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
  - Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1, or 1secret).
  - Are some version of “Welcome123,” “Password123,” or “Changeme123.”

Additional Considerations:

- Never write down a password. Instead, try to create passwords that can easily be remembered. One way to do this is to create a password based on a song title, affirmation, or another phrase. For example, the phrase, “This May Be One Way To Remember” could become the password TmB1w2R! or another variation.
- Do not use the same password for business accounts as for personal access.
- Where possible, users must not use the same password for various business access needs.
- User accounts that have system-level privileges granted through group memberships must have a unique password for all other accounts held by that user to access system-level privileges.

Password Protection

- Regularly Change Your Password:
  - All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.
  - All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months, preferably every four months.
  - Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

- To Protect Your Password, Do Not:
  - Share with anyone. All passwords are to be treated as sensitive, confidential information.
  - Insert into email messages or any other form of electronic communication.
  - Reveal over the phone to anyone.
  - Reveal on questionnaires or security forms.
  - Hint at the format of a password (for example, “my family name”).
  - Share business passwords with anyone, including administrative assistants, secretaries, managers, coworkers, and family members.
  - Write passwords down and store them anywhere in the office, including in a file on a computer system or mobile devices (phone, tablet) without encryption.
  - Use the “Remember Password” feature of applications (for example, web browsers).

- In Administering User Accounts and Passwords:
  - Maintain a simple and usable password management 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 user level, 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.

Note

101 For additional discussion of password policy, see "Password Construction Guidelines," the SANS Institute, at https://www.sans.org/security-resources/policies/general/pdf/password-construction-guidelines.

Appendix 4. Removable Media and Access Port Security Policies

Removable media are helpful for processes such as backing up data, updating software, and transferring files without a network connection. However, removable media have historically been a source of spreading malware and viruses. A well-documented and closely followed removable media and access port policy helps ensure the integrity of the network, data, and computer systems of the agency. The following provides guidance on removable media security and access port policy.

Security of Data

- In order to minimize physical risk, loss, theft, or electrical corruption, all storage media must be stored in an appropriately secure and safe environment. At least one storage copy should be located offsite.

- Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way while in their care or under their control.

- All data stored on removable media devices must, where possible, be encrypted. If this is not possible, then all protected, restricted, or controlled data held must be encrypted.

- Virus and malware checking software approved by the agency must be operational on both the machine from which the data is taken and the machine onto which the data is to be loaded. The data must be scanned for viruses and malware before the media is loaded onto the receiving machine.

- Only data that is authorized and necessary to be transferred should be saved onto the removable media device. Data that has been deleted can still be retrieved.

- Removable media devices must not be used for archiving or storing records as an alternative to other storage equipment.

- Special care must be taken to physically protect the removable media device and stored data from loss, theft, or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

Restricting Access to Removable Media

- Some policies prohibit the use of all removable media devices. The use of removable media devices will only be approved if a valid business case for its use is developed. There are large risks associated with the use of removable media. Therefore, clear business benefits that outweigh the risks must be demonstrated before approval is given.

- Requests for access to, and use of, removable media devices must be made to the department supervisor. Approval may only be given by a department manager.

Procurement of Removable Media

- All removable media devices and any associated equipment and software must only be purchased and installed by IT. Non-agency owned removable media devices must not be used to store any information used to conduct official agency business and must not be used with any agency-owned or leased IT equipment.

- Only agency purchased and IT-approved equipment and media should be used to connect to any agency equipment or network.

Network Port Access

- All open, and unused, network ports must be turned off through the management console of the respective switch, router, or firewall.

- The network device should be secured itself by adhering to password creation and protection policies.

- Any ports which will not be used for an extended period of time, for example when an employee goes on extended leave or retires, should be turned off and not accessible until it is needed again.

Appendix 5. Functional Elements Associated with NG9-1-1 and the NPSBN

Functional elements describe how NG9-1-1 will operate and integrate with origination networks and FirstNet. What follows is a more detailed description of the functional elements associated with the integration of NG9-1-1 and the NPSBN.

NG9-1-1 Functional Elements

- User Element – This is either the caller's device or a proxy for that device. This device is responsible for obtaining its current location and inserting it into the SIP call setup header to be used for call routing.

- Location Server (LS) – This element tracks and reports the current location of the 9-1-1 caller. The LS can be a static database for fixed locations, the Mobile Positioning Center (MPC) for wireless callers, or the VoIP Positioning Center (VPC) for mobile VoIP systems.

- Emergency Services Routing Proxy (ESRP) – This is a policy-based emergency call routing platform that routes a call to a PSAP based upon location, congestion, availability, language, caller impairment, PSAP capability, and other parameters.

- Emergency Communications Routing Function (ECRF) – This is a location-based emergency call routing function that provides information about the appropriate PSAP.

- NG9-1-1 PSAP – A PSAP that can handle a next generation formatted call.

- Border Control Function (BCF) – This is a combination of a session border controller (SBC) that provides security filtering SIP transactions, and a firewall that provides security filtering of all other types of transactions. There may be several BCFs to support all ingress and egress points of the ESInet.

- Legacy Gateways, Legacy Network Gateways (LNG), and Legacy Selective Router Gateways (LSRG) – These functional elements provide translations between legacy signaling (SS7) and next generation signaling (SIP) allowing calls to be transferred between legacy PSAPs and NG9-1-1 PSAPs.

- IP Multimedia Subsystem (IMS) support – At this time it is uncertain as to whether the ESInet will require a full IMS core, or just an IMS border proxy. This element would manage authentication and Quality of Service (QoS).

FirstNet

- Home Subscriber Server (HSS) – This server manages authentication at the LTE device level.

- Policy and Charging Rules Function (PCRF) – This element is responsible for managing resources for end users based upon end user role and application requirements.

- Mobility Management Element (MME) – This functional element manages call handoff between LTE cell sites when the user is in transit.

- Signaling Gateway (SGW) – This device supports a secure channel to the end user's device. A separate channel is provided and prioritized for each application.

- Packet Gateway (PGW) – The gateway provides Internet connectivity for the applications.

- eNodeB – These are the LTE cellular nodes.

- User Element (UE) – These are the end user devices.

Interconnection Between NG9-1-1, FirstNet, or IMS

- Home Subscriber Server (HSS) – The HSS manages authentication at the SIP or VoIP level.

- Proxy Call Session Control Function (P-CSCF) – This proxy either sits at the edge of the home network (FirstNet, in this case) or at the edge of the visiting network (NG9-1-1, in this case). It manages call flows between the two networks, including authentication and prioritization.

- Interrogating Call Session Control Function (I-CSCF) – This proxy serves as a central forwarding point for all external SIP service requests. It manages call flows between outside proxies and internal IMS proxies.

- Serving Call Session Control Function (S-CSCF) – This functional element is responsible for SIP client registrations, determining the appropriate application servers to use, and provides routing (typically ENUM) lookups.

- Telephony Application Server (TAS) – This application server manages advanced call features. These features include services such as conference bridging, voice mail, call forwarding, and other telephony features.

- Public Switched Telephone Network (PSTN) Gateway – This element is used when a SIP call needs to be connected to the PSTN.

- ENUM Servers – ENUM is a system that supports using the Internet DNS structure to support call routing of SIP calls to other domains without having to transit the PSTN.

Appendix 6. Sample Training Language for RFPs

When procuring broadband technology from various vendors, PSAPs should consider addressing training needs in their RFPs. The following provides sample RFP language for a variety of options for user and administrator training.

User Training and Administrator Training Options

User Training and Administrator Training programs will be provided for the system. User training shall be a minimum four hours in length and be conducted at locations within the State. Administrator training shall be a minimum six hours in length and be conducted at a central location within the State. All training documentation shall be provided prior to any PSAP installation. The Contractor must provide cost information for each training option. The State reserves the right to choose one or more options.

Training Option 1 - Just In Time Training

Contractor shall provide training to PSAP no less than three days prior to installation of the new software platform at each PSAP. Sufficient training classes at each PSAP will be provided to ensure that personnel from all shifts can be trained (no less than two classes will be conducted at each PSAP). Contractor will be responsible for providing AV equipment and sufficient equipment to conduct hands on training for all PSAP personnel. Training will be conducted in a training room outside of the active PSAP area of the answering point.

Training Option 2 - Regional Training Offsite from PSAPs

Contractor will provide training classes in dedicated classrooms offsite from the PSAPs. Sufficient classes will be conducted to ensure that all PSAP personnel are trained prior to the installation and activation of the new software platform. No less than 60 classes of 25 students each will be conducted. Contractor will provide for no less than two concurrent classes during the installation and activation period. Contractor will be responsible for providing AV equipment and sufficient equipment to conduct hands on training in the classroom. Classrooms will be provided by the State.

Training Option 3 - Train the Trainer

Contractor will provide training classes in dedicated classrooms offsite from the PSAPs. Sufficient classes will be conducted to ensure that representatives from each PSAP are trained as trainers prior to the installation and activation of the new software platform. Sufficient training will be provided to ensure that trained trainers can successfully train their respective PSAP call takers and dispatchers. Online and phone-based help desk services must be provided to ensure that all trainers can resolve training questions and problems. No less than eight classes of 25 students each will be conducted. Contractor will be responsible for providing AV equipment and sufficient equipment to conduct hands on training for trainers in the classroom. Classrooms will be provided by the State.

Training Option 4 - Self-Paced Online or CD-Based Training

Contractor will provide the capability for all users to utilize online or CD-based self-paced training. Sufficient capability or number of CDs must be provided to ensure that all training can be acquired prior to the installation and activation of the software platform. Online and phone-based help desk services must be provided to ensure that all users can resolve training questions and problems.

Administrator Training

There shall be administrator training that will provide the Department and PSAPs with any information needed to administer/manage the system. Please explain in detail the training to be provided.

Appendix 7. Suggested Modifications to Existing Training-Related APCO Standards

An important factor in improving training for broadband-capable PSAPs is the ability of training programs to reflect the characteristics of the fast-paced and ever-evolving nature of broadband technology. For the most part, APCO's standards are written to have broad applicability – both with regard to agency resources and, whenever possible, with regard to technology. Thus, many don't require modification to accommodate broadband capabilities. However, several standards could benefit from modification, described below as general considerations related to the impacts of broadband technology, followed by specific recommendations for language to change.

General Considerations

- Many APCO standards include a phrase such as "Information contained in calls for service," without specifying the type of information. In some cases, adding language such as "including text, video, audio, or photographic messages" or "NG9-1-1 and other broadband technologies" could be beneficial. Further review is suggested of the following standards:
    - Minimum Training Standards for Public Safety Telecommunicators APCO ANS 3.103.2.2015
        - Sections 3.10, 7.2.3, 8.4, 9.3.1, 9.3.3, 10.3.1, 10.4
    - Core Competencies and Minimum Training Standards for Public Safety Communications Training Coordinator APCO ANS 3.104.1-2012
        - Sections 3.11.2, 3.11.3, 4.3.17
    - Core Competencies and Minimum Training Standards for Public Safety Communications Instructor APCO ANS 3.108.1.2014
        - Sections 3.11.2, 3.11.3
    - Core Competencies and Minimum Training Standards for Public Safety Communications Supervisor APCO ANS 3.102.1-2012
        - Sections 3.11.2, 3.11.3
    - Core Competencies and Minimum Training Standards for Public Safety Communications Manager / Director APCO ANS 3.109.2.2014
        - Sections 3.11.2, 3.11.3, 4.3.10
    - Core Competencies and Minimum Training Standards for Public Safety Communications Technicians APCO ANS 3.107.1.2015
        - Sections 3.11.2, 3.11.3

- It may further be helpful to define terms such as "broadband" and "NG9-1-1" in the glossary of each standard.

- Some standards may require more comprehensive modification. For example, the Standard for Public Safety Telecommunicators When Responding to Calls of Missing, Abducted and Sexually Exploited Children APCO ANS 1.101.3-2015 may require modification to include operational considerations for PSTs who have the capability to ask callers reporting child abductions to send recent photos or videos of the child that could then be sent to field responders.

Specific Recommendations

- Minimum Training Standards for Public Safety Telecommunicators APCO ANS 3.103.2.2015
    - Modify Section 4.2:
        - "4.2 General Knowledge of the Telecommunicator The following general areas of knowledge have been identified for the Telecommunicator regardless of their area of public safety expertise:
            - 4.2.1 An awareness of and respect for diverse populations,
            - 4.2.2 Comprehension of jurisdictional boundaries and geography,
            - 4.2.3 Proper application of Agency terminology,
            - 4.2.4 The ability to identify and properly utilize Agency resources, and
            - 4.2.5 Comprehension of their role in:
                - 4.2.5.1 Incident Command Systems (ICS),
                - 4.2.5.2 National Incident Management Systems (NIMS), including, but not limited to required training, Tactical Interoperable Communication Plan (TICP), and
                - 4.2.5.3 State or local emergency operations plans, and
                - 4.2.5.4 Use and development of emerging technologies."

- Core Competencies and Minimum Training Standards for Public Safety Communications Training Officer (CTO) APCO ANS 3.101.2-2013
  - Chapter 3 – Organizational Integrity:
    - "3.15 The CTO shall demonstrate comprehension and application of the Agency's confidentiality policies and rules regarding the discussion or release of information acquired in the workplace to the public, the media, or others. Such information should include, but is not limited to:
      - 3.15.1 Data systems accessible through local, state, or federal networks,
      - 3.15.2 Information contained in calls for service, including but not limited to information obtained through text, video, audio, or photographic messages to the PSAP,
      - 3.15.3 Information gained through the 9-1-1 or E9-1-1 system,
      - 3.15.4 Records Management Systems, and
      - 3.15.5 System security."

- Minimum Training Standard for TTY/TDD Use in the Public Safety Communications Center APCO/NENA ANS 3.105.1-2015
  - Section 2.2.7:
    - "The Agency shall provide the Telecommunicator with practical instruction on identifying and processing TTY/TDD calls including:
      - 2.2.7.1 The importance of recognizing silent or open line TTY/TDD calls, and
      - 2.2.7.2 Using proper syntax, abbreviations, and protocol when responding to TTY/TDD,
      - 2.2.7.3 Recognizing when an individual who is communications impaired (i.e. deaf, deaf-blind, hard of hearing, or a person who has a speech disability) is using text-to-911 or text-to-TTY based on the language of the message or how the call is presented to the Telecommunicator."
  - Section 2.2.12.4:
    - "The Agency shall evaluate the trainee on use TTY/TDD protocol, such as:
      - 2.2.12.4.1 Abbreviations,
      - 2.2.12.4.2 Etiquette, and
      - 2.2.12.4.3 Language,
      - 2.2.12.4.4 Recognizing when an individual who is communications impaired (i.e. deaf, deaf-blind, hard of hearing, or has a speech disability) is using text-to-911 or text-to-TTY based on the language of the message or how the call is presented to the Telecommunicator."
  - Section 5.3:
    - "The Telecommunicator shall demonstrate the ability to receive, process and initiate calls of an emergency and non-emergency nature utilizing the agency's primary and backup TTY equipment, detection equipment, telephony equipment, records management system, and other related tools or equipment all appropriate tools, equipment, and technology they may be expected to operate within the public safety communications center and/or training facilities."
  - Chapter 7 – Core Competencies of the Telecommunicator
    - Section 7.3: "The Telecommunicator shall demonstrate the ability to process emergency and nonemergency calls for service for individuals who are communications impaired (i.e. deaf, deaf-blind, hard of hearing or have a speech disability or other disabilities)."
      - Add: "7.3.4 The Telecommunicator shall demonstrate the ability to communicate directly and indirectly with callers via all appropriate tools, equipment, and technology."

Appendix 8. Training Courses from Other Sectors with Applicability to PSAPs

Standards and best practices related to IT, Fusion Centers, Real-Time Crime Centers, and Emergency Management are worth considering for PSAPs implementing broadband technology. The following is intended to be a non-exhaustive selection from each sector.

Information Technology

The FCC's TFOPA, particularly its cybersecurity working group, conducted a review of IT standards and best practices and made recommendations for the public safety community. Among other things, TFOPA reviewed the NIST Cybersecurity Framework, a voluntary framework of standards and best practices, and recommended implementation of appropriate elements to PSAP operations. Regardless of the approach a PSAP takes to managing IT challenges, employees will benefit from understanding IT basics so that they can have a productive collaboration. The following best practices and standards should be considered:

- PSAP employees should have at least a basic level of IT training, which may include awareness of a cybersecurity plan to protect data and lower the risk of cyber incidents.
- PSAPs should have a basic understanding of cyber hygiene, meaning steps computer users can take to improve cybersecurity and protect their systems and data. This includes:
  - Establishing strong passwords by using a combination of numbers, letters of varying sizes, and symbols,
  - Having a strong firewall,
  - Installing and consistently updating antivirus protection software,
  - Updating computers and programs regularly,
  - Physically securing laptops, cell phones, and other electronics,
  - Using encryption software,
  - Backing up data regularly,
  - Being wary of emails, instant messages, and downloads from the web,
  - Limiting and managing the number of people who have administrative privileges to change, bypass, or override security settings,
  - Limiting and monitoring any devices that physically or wirelessly connect to the system,
  - Reporting on IT issues and suspected cyber incidents at all levels, and
  - Regularly reviewing and updating policies and standards.

Real-Time Crime Centers

Real-Time Crime Centers (RTCCs) leverage a variety of data to prevent and respond to crime. This can include live video feeds, social media, 9-1-1 call information, incident mapping, historical data, license plate readers, arrest information, and other sources of information. While RTCC training information was not readily available, publicly-available material reveals the following best practices:

- Training will vary based on the complexity, breadth of technology, and data used/gathered by the RTCC, but given the complex nature of the tools used in a RTCC, training may require six to nine months.
- Training should address information sharing and storage policies, as well as legal requirements.
- Depending on the software, there could be an operational benefit to training even non-programmers in structured query language (SQL), a special-purpose programming language designed for managing data held in a database management system or for relational data stream management, to enable them to fully leverage the capabilities of the available systems.
- Field units may require education and training on the RTCC to make them aware of its capabilities and increase the likelihood of collaboration and use for field operations.

Fusion Centers

Fusion centers operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal, state, local, tribal, territorial, and private sector partners. The U.S. Department of Justice and Department of Homeland Security developed guidelines for developing and operating a fusion center within a state or region. These guidelines include several considerations for training that may be relevant to PSAP operations:

- Identifying training needs of center personnel.
- Providing specialized training, as appropriate.
- Providing training on the fusion center operations, NCISP, intelligence cycle, and the fusion process.
- Providing information collection training for fusion center participants.
- Providing training in tactical and strategic intelligence.
- Seeking accredited or standards-compliant training programs for government personnel.
- Utilizing private security entities for subject-matter training (e.g., cybersecurity).
- Emphasizing analysis and its link to intelligence-led policing.
- Developing materials and integrating outreach efforts.
- Adhering to other training mandates.
- Ensuring that personnel assigned to specific crime desks receive crime-specific training.
- Utilizing scenario-based training, simulations, games, and tabletop and field exercises.
- Participating in public safety and private sector tabletop, functional, and full-scale exercises.
- Participating in college- and university-sponsored intelligence and analyst training programs.

Emergency Management

The U.S. Department of Justice and Department of Homeland Security have issued “Considerations for Fusion Center and Emergency Operations Center Coordination,” which includes a list of training courses relevant to PSAPs.[102]

Note

[102] https://www.fema.gov/pdf/about/divisions/npd/cpg_502_eoc-fusion_final_7_20_2010.pdf.

Appendix 9. Likely Impacts on Job Tasks Following Adoption of Broadband Technology

PSAPs will need a workforce capable of handling a wide range of calls for service, from "basic" 9-1-1 calls (e.g., voice-only) to calls containing incident-related pictures and video. The following describes the likely staffing impact with the adoption of broadband technology by comparing staffing considerations before and after broadband implementation. These charts are designed to reflect job tasks rather than specific job titles.

SMALL PSAP (1-15 employees)	**Before Broadband Implementation**	**After Broadband Implementation**	**Impact on Staffing**
Call Taking: Non-Emergency Call Processing	Y	Y	N/A
Call Taking: Emergency 9-1-1 Voice Calls	Y	Y	N/A
Call Taking: Text-to-911	N	Y	Moderate
Call Taking: NG9-1-1 Call with Video and Images	N	Y	Moderate
Call Taking: NG9-1-1 Call from Sensors/M2M	N	Y/Y	Minor
Call Taking: Incoming PSAP to PSAP Data Sharing	N	Y	Minor
Dispatching: Law Enforcement Voice Dispatch	Y	Y	N/A
Dispatching: Fire/Rescue Voice Dispatch	Y	Y	N/A
Dispatching: EMS Voice Dispatch	Y	Y	N/A
Dispatching: Management of First Responder Video	N	Y	Moderate
Dispatching: Management of First Responder Sensors	N	Y	Minor
Dispatching: Management of Interoperable Data	N	Y	Minor
Supervising: Support to Telecommunicators	Y	Y	Significant
Supervising: Oversight of Technology and Systems	Y	Y+	Significant
Supervising: Coordination with External Entities	Y	Y+	Moderate
Supervising: Coordination with Agency PIO on Data	Y	Y+	Moderate
Admin: Database and Table Maintenance	Y	Y+	Moderate
Admin: Creation of 9-1-1 Call Records for Release	Y	Y+	Moderate
Admin: Creation of CAD Records for Release	Y	Y+	Moderate
Admin: SOP Documentation	Y	Y	Moderate
Admin: GIS Maintenance	Y	Y+	Moderate
Training: Length/Complexity for New Employees	Moderate	Extended	Moderate
Training: Length/Complexity for Recurring Training	Moderate	Extended	Moderate
IT: Equipment, Application, Network Management	Minor	Significant	Moderate
IT: Physical and Cybersecurity Management	N	Y	Moderate

KEY: Y = Yes; N = No; Y+ = Yes, but will increase

MEDIUM PSAP (16-75 employees)	**Before Broadband Implementation**	**After Broadband Implementation**	**Impact on Staffing**
Call Taking: Non-Emergency Call Processing	Y	Y	N/A
Call Taking: Emergency 9-1-1 Voice Calls	Y	Y	N/A
Call Taking: Text-to-911	N	Y	Significant
Call Taking: NG9-1-1 Call with Video and Images	N	Y	Moderate
Call Taking: NG9-1-1 Call from Sensors/M2M	N	Y/Y	Moderate
Call Taking: Incoming PSAP to PSAP Data Sharing	N	Y	Moderate
Dispatching: Law Enforcement Voice Dispatch	Y	Y	N/A
Dispatching: Fire/Rescue Voice Dispatch	Y	Y	N/A
Dispatching: EMS Voice Dispatch	Y	Y	N/A
Dispatching: Management of First Responder Video	N	Y	Moderate
Dispatching: Management of First Responder Sensors	N	Y	Moderate
Dispatching: Management of Interoperable Data	N	Y	Moderate
Supervising: Support to Telecommunicators	Y	Y+	Significant
Supervising: Oversight of Technology and Systems	Y	Y+	Significant
Supervising: Coordination with External Entities	Y	Y+	Moderate
Supervising: Coordination with Agency PIO on Data	Y	Y+	Moderate
Admin: Database and Table Maintenance	Y	Y+	Significant
Admin: Creation of 9-1-1 Call Records for Release	Y	Y+	Significant
Admin: Creation of CAD Records for Release	Y	Y+	Significant
Admin: SOP Documentation	Y	Y	Moderate
Admin: GIS Maintenance	Y	Y+	Significant
Training: Length/Complexity for New Employees	Moderate	Extended	Significant
Training: Length/Complexity for Recurring Training	Moderate	Extended	Significant
IT: Equipment, Application, Network Management	Minor	Significant	Moderate
IT: Physical and Cybersecurity Management	N	Y	Moderate

KEY: Y = Yes; N = No; Y+ = Yes, but will increase

LARGE PSAP (76+ employees)	**Before Broadband Implementation**	**After Broadband Implementation**	**Impact on Staffing**
Call Taking: Non-Emergency Call Processing	Y	Y	N/A
Call Taking: Emergency 9-1-1 Voice Calls	Y	Y	N/A
Call Taking: Text-to-911	N	Y	Significant
Call Taking: NG9-1-1 Call with Video and Images	N	Y	Significant
Call Taking: NG9-1-1 Call from Sensors/M2M	N	Y/Y	Significant
Call Taking: Incoming PSAP to PSAP Data Sharing	N	Y	Significant
Dispatching: Law Enforcement Voice Dispatch	Y	Y	N/A
Dispatching: Fire/Rescue Voice Dispatch	Y	Y	N/A
Dispatching: EMS Voice Dispatch	Y	Y	N/A
Dispatching: Management of First Responder Video	N	Y	Significant
Dispatching: Management of First Responder Sensors	N	Y	Significant
Dispatching: Management of Interoperable Data	N	Y	Significant
Supervising: Support to Telecommunicators	Y	Y+	Significant
Supervising: Oversight of Technology and Systems	Y	Y+	Significant
Supervising: Coordination with External Entities	Y	Y+	Significant
Supervising: Coordination with Agency PIO on Data	Y	Y+	Significant
Admin: Database and Table Maintenance	Y	Y+	Significant
Admin: Creation of 9-1-1 Call Records for Release	Y	Y+	Significant
Admin: Creation of CAD Records for Release	Y	Y+	Significant
Admin: SOP Documentation	Y	Y	Significant
Admin: GIS Maintenance	Y	Y+	Significant
Training: Length/Complexity for New Employees	Moderate	Extended	Significant
Training: Length/Complexity for Recurring Training	Moderate	Extended	Significant
IT: Equipment, Application, Network Management	Minor	Significant	Significant
IT: Physical and Cybersecurity Management	N	Y	Significant

KEY: Y = Yes; N = No; Y+ = Yes, but will increase