APCO International

Leaders in Public Safety Communications™

APCO ANS 1.115.1-2018

Core Competencies, Operational Factors, and Training for Next Generation Technologies in Public Safety Communications

Approved American National Standard

ANSI

APCO International
351 Williamson Blvd
Daytona Beach, Fl. 32114

ISBN: 978-1-943877-25-6

APCO ANS 1.115.1-2018

Standard written by the 9-1-1 Emerging Technologies Committee. Standard approved by the Standards Development Committee *on Core Competencies, Operational Factors, and Training for Next Generation Technologies in Public Safety Communications* and received final approval by the American National Standards Institute on July 3, 2018.

Abstract: This guideline is designed to prepare Public Safety Answering Points for the impact of Next Generation Technologies.

Keywords: PSAP, Best Practices, Core Competencies, Next Generation Technologies

TABLE OF CONTENTS*

**Informative material and not a part of this American National Standard (ANS)*

*Foreword**

APCO International is the world's largest organization of public safety communications professionals. It serves the needs of public safety communications practitioners worldwide - and the welfare of the general public as a whole - by providing complete expertise, professional development, technical assistance, advocacy, and outreach.

APCO International standards are developed by APCO committees, projects, task forces, work-groups, and collaborative efforts with other organizations coordinated through the APCO International Standards Development Committee (SDC). Members of the committees are not necessarily members of APCO. Members of the SDC are not required to be APCO members. All members of APCO's committees, projects, and task forces are subject matter experts who volunteer and are not compensated by APCO. APCO standards activities are supported by the Communications Center & 9-1-1 Services Department of APCO International.

For more information regarding
APCO International and APCO standards please visit:
www.apcointl.org
www.apcostandards.org

APCO American National Standards (ANS) are voluntary consensus standards. Use of any APCO standard is voluntary. All standards are subject to change. APCO ANS are required to be reviewed no later than every five years. The designation of an APCO standard should be reviewed to ensure you have the latest edition of an APCO standard, for example:

APCO ANS 3.101.1-2007 = **1**-Operations, **2**-Technical, **3**-Training
APCO ANS 3.101.1-2007 = Unique number identifying the standard
APCO ANS 3.101.1-2007 = The edition of the standard, which will increase after each revision
APCO ANS 3.101.1-2007 = The year the standard was approved and published, which may change after each revision.

The latest edition of an APCO standard cancels and replaces older versions of the APCO standard. Comments regarding APCO standards are accepted any time and can be submitted to standards@apcointl.org, if the comment includes a recommended change, it is requested to accompany the change with supporting material. If you have a question regarding any portion of the standard, including interpretation, APCO will respond to your request following its policies and procedures. ANSI does not interpret APCO standards; they will forward the request to APCO.

APCO International adheres to ANSI's Patent Policy. Neither APCO nor ANSI is responsible for identifying patents for which a license may be required by an American National Standard or for conducting inquiries into the legal validity or scope of any patents brought to their attention.

No position is taken with respect to the existence or validity of any patent rights within this standard. APCO is the sole entity that may authorize the use of trademarks, certification marks, or other designations to indicate compliance with this standard.

Permission must be obtained to reproduce any portion of this standard and can be obtained by contacting APCO International's Communications Center & 9-1-1 Services Department. Requests for information, interpretations, and/or comments on any APCO standards should be submitted in writing addressed to:

APCO Standards Program Manager, Communications Center & 9-1-1 Services
APCO International
351 N. Williamson Blvd
Daytona Beach, FL 32114 USA

*Acknowledgements**

Special recognition goes to the committee members that provided their expertise in updating this document to successfully create this standard. At the time this version was written, the 9-1-1 Emerging Technologies Sub-Committee included the following membership:

Karen Allen
9-1-1 Emerging Technologies Chair
State of Arizona

George Long
9-1-1 Emerging Technologies Vice Chair
Willamette Valley Comm Center, OR

Stephen Ashurkoff
General Dynamics IT, VA

Gary Bates
Howard County Sheriff's Dept, IN

Roy Davis
Roanoke County Emergency
Communications Center, VA

Sharyl Dresser
Washington County Consolidated
Communications Agency, OR

Robert Ehrlich
Central Islip/Hauppauge Vac, NY

Mark Hannah
AECOM, VA

Brad Meixell
Clark County 9-1-1, IN

Don Miller
City of Long Beach (retired), CA

Darrell True
Wrentham Public Safety, MA

Jay English
APCO International

Crystal McDuffie, **RPL**, **ENP**
APCO International

APCO Standards Development Committee (SDC)*

Daniel Morelos
Tucson Airport Authority
Arizona

Sherry Taylor
Indianapolis Fire Department Communications
Division, Indiana

Chris Fischer, Past APCO International President
Des Moines, Washington

James Leyerle
OnStar

Nathan McClure, Past APCO International President
AECOM

Michael Romano
NexGen Global Technologies

Karen Allen
Phoenix, Arizona

Tracy Eldridge
Rapid SOS

Bradford S. Smith
Framingham Fire Department
Massachusetts

Bud Hicks
Grundy County, Illinois

Jackie Pace
Redwood City, California

Rick Thomas, RPL, ENP
Apex, North Carolina

Nicola Tidey, RPL, ENP
Mission Critical Partners

Stephen Ashurkoff
General Dynamics IT

Stacy Banker, RPL, ENP
Standards/ACS Program Manager
APCO International

**Informative material and not a part of this American National Standard (ANS)*

*Executive Summary**

On behalf of public safety communications professionals across the nation, the 9-1-1 Emerging Technologies Committee has created a new standard to identify the current and future challenges that Next Generation technologies bring to a Public Safety Answering Point (PSAP). The diversity of our committee which included representatives from PSAPs of different sizes, locations, and responsibilities, as well as our technologists' familiarity with what is on the technology roadmap, allowed the committee to identify many different facets that you will find in this standard.

The role of the telecommunicator has the potential to change in a variety of ways. While creating this standard, we discussed scenarios to identify the ways the role significantly changes. To help you understand what we discussed, here are a few scenarios:

1. An officer is involved in a shooting and the following is provided to the telecommunicator (TC) at their console: a sensor notification that his weapon has been removed from his holster; a GIS map displaying his location; a live feed from his body camera; available cameras in the surrounding area are displayed and his biometric sensor displays his vitals. All of this is available to the telecommunicator who either pushes it out to responders or makes it available to the responders when they need it.

2. A fire at a Smart Building notifies the PSAP by automatically submitting a call for service that includes the exact location of the fire; how many people are in the building and where; a link to unlock the doors/gates to allow responders access; links to cameras to provide a view of the fire. The telecommunicator uses this information to act as Incident Command, directing responders in to exact locations, providing details until the first unit arrives on scene and relieves the TC of their command.

3. A woman secretly contacts a PSAP through live streaming sharing a domestic violence situation in progress. The TC listens for background noise/conversations, assesses the room or location for responder details such as descriptions, weapons, location within the premise. While responders are enroute, a gunshot is heard and the telecommunicator witnesses the woman being shot by the perpetrator, repeatedly. The TC is expected to continue to provide updated details on this incident to responders without hesitation.

Telecommunicators are trained to handle the basic tasks of answering phone calls from emergency and non-emergency callers. APCO's "P43 Broadband Implications[1]" for the PSAP stated, "PSAP's of the future will be an Emergency Communications Center (ECC), managing data rich communications via broadband technology with 9-1-1 callers and first responders." The above scenarios provide examples of how these same telecommunicators may be required to take their position to another level. With additional information provided by cameras, sensors and future technology, telecommunicators may take on additional responsibilities and will be required to understand how to interact with these Next Generation systems. In addition, new "responders," are being implemented, such as drones carrying medical supplies to remote hard to reach areas. In responding to these Next Generation systems, many aspects within a PSAP will need to be evaluated, such as critical incident stress management, hiring, training, new positions, policies, technology, and more. The 9-1-1 Emerging

[1] "APCO Broadband Implications for the PSAP, Analyzing the Future of Emergency Communications," 2017

Technologies Committee has compiled this standard to provide the requirements for PSAPs to implement and prepare for the future.

*Acronyms and Abbreviations**

AACN	Advanced Automatic Crash Notification	**HIPAA**	Health Insurance Portability and Accountability Act
ACN	Automatic Crash Notification	**IP**	Internet Protocol
ANS	American National Standards	**IT**	Information Technology
ANSI	American National Standards Institute	**NG9-1-1**	Next Generation 9-1-1
APCO	Association of Public Safety Communications Officials	**PSAP**	Public Safety Answering Point
CAD	Computer Aided Dispatch	**SDC**	Standards Development Committee
CISM	Critical Incident Stress Management	**SIP**	Standard Internet Protocol
DOS	Denial of Service	**TC**	Telecommunicator
ECC	Emergency Communication Center	**TDOS**	Telephony Denial-of-Service
EMD	Emergency Medical Dispatch		
EMS	Emergency Medical Services		
ESInets	Emergency Service IP Networks		
FOIA	Freedom of Information Act		
GIS	Geographic Information Systems		

Chapter 1 Introduction

Cameras, sensors, multimedia, smart devices, and many other types of technology are used on a daily basis by members of the community allowing data sharing in a multitude of ways. Community members expect public safety to also utilize and accept multimedia during events and incidents. There are many facets surrounding the receipt and dissemination of this data that Public Safety Answering Points (PSAPs) should plan for and consider. This standard provides PSAP managers, personnel, and technologists with a guide to begin preparation to accept and utilize this data. It outlines additional training that will be needed by telecommunicators who have traditionally made decisions based primarily on voice conversations, as well as the corresponding policies agencies must develop. With the opportunity to utilize streaming video, telecommunicators will potentially be able to visually determine the number and type of responders to dispatch to a scene, provide additional information regarding a fire scene and provide details often overlooked by voice communications, such as a gun on a shelf during a domestic violence incident. Telematics data will provide specific analytics to be used by telecommunicators, responders, hospitals and others to allow for enhanced situational awareness, potentially saving more lives. Drones are being used to respond to provide emergency medical supplies to scenes much quicker than traditional public safety vehicles.

As technological changes occur within the PSAP, such as the ability to accept multimedia, public education will be an important component. Community members will need to understand the new capabilities of the PSAP, along with the expectations required of reporting parties using that technology. Additional technology changes within the PSAP, such as PSAP controlled devices, sensors and automated data, may also place greater demands on telecommunicators.

1. Scope

This APCO standard identifies the minimum requirements for both new and veteran Public Safety Telecommunicators communicating with the reporting party and operate Next Generation systems. This position is typically tasked with receiving, processing, transmitting, and conveying public safety information to dispatchers, law enforcement officers, fire fighters, emergency medical, and emergency management personnel. This document is intended to provide guidance on how to manage and process data received from Next Generation systems, including cameras, telematics, sensors, and live video.

Agency heads and management should consider the potentially changing roles of telecommunicators to better define job descriptions and classifications. Considerations should be given to the need for additional stress management and mitigation as well as potential additional liabilities associated with telecommunicator job functions relating to multimedia and stress.

Next Generation systems could require additional support staff, to handle responsibilities such as responding to public records requests, Information Technology (IT) support and specially trained data analysts. In addition, space needs may need to be considered for new Next Generation systems equipment.

Definitions

Automated Data: Machine to machine data, that is transmitted without human interaction such as smart buildings (ex: a hazardous materials detection that turns on cameras), sensors (ex: biometrics – heart attack, officer's gun - when un-holstered), telematics.

Advanced ACN (AACN): Immediately following a crash when certain thresholds have been exceeded, vehicle location and occupant data may send an automatic transmission of additional enhanced crash-severity data and crash pulse data collected by embedded, in-vehicle crash sensors to a PSAP.

Core Competency: The unique traits, requisite knowledge, comprehension and application of skills, and situational analysis leading to the appropriate response to the reporting party, co-worker, other public safety stakeholders, or event(s) consistent with general practices and locally defined parameters.

Denial of Service (DoS): [definition]: A distributed (DDos) or Denial of Service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users. It is usually accomplished by temporarily interrupting or suspending the services of a host connected to the Internet. NENA Master Glossary -- A type of cyber-attack intended to overwhelm the resources of the target and deny the ability of legitimate users of the target the normal service the target provides.

Multimedia: The integration and/or combination of multiple forms of media (e.g. text, images, graphics, audio, streaming video, 3rd party websites, etc.) utilized to communicate.

NG9-1-1*:* NG9-1-1 is an Internet Protocol (IP) based system comprised of managed Emergency Services IP networks (ESInets), functional elements, and databases that replicate traditional E9-1-1 features and functions and provides additional capabilities. NG9-1-1 is designed to provide access to emergency services from all connected communications sources, and provide multimedia data capabilities for Public Safety Answering Points (PSAPs) and other emergency service organizations.

Next Generation Systems*:* Include, but are not limited to, systems such as: NG9-1-1, multimedia sessions, live video feeds, vehicle telematics, sensors, PSAP operated cameras and more.

Phishing: An example of a social engineering attack, typically carried out by email, which is the favored method used by cyber-criminals (see Social Engineering).

PSAP Controlled Devices: A device that a telecommunicator or PSAP controls (ex: cameras at schools, banks, traffic; sensors – body worn cameras; drones; door controls multimedia systems).

Session Initiated Protocol (SIP): An IETF defined protocol (RFC3261) that defines a method for establishing multimedia sessions over the Internet. Enables/allows different call types such as voice, video, text, and multimedia conference sessions.

Session: An interaction between the telecommunicator and the reporting party, through voice, text or multimedia.

Skill-Based Training: Utilizing current staff with existing expertise or with the desire and/or aptitude to gain expertise on new technology to supplement an organization's training staff.

Social Engineering: The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Spam: Unsolicited usually commercial e-mail sent to a large number of addresses.

Spoofing: A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage or giving the appearance of legitimacy.

Swatting: The act of tricking an emergency service (via such means as hoaxing a 9-1-1 dispatcher) into dispatching an emergency response based on the false report of an ongoing critical incident.

Standard Operating Procedures (SOP): A written directive that provides a guideline for carrying out an activity. The guideline may be made mandatory by including terms such as "shall" rather than "should" or "must" rather than "may".

Short Message Service (SMS): A text messaging service component of phone, Web, or mobile communication systems. It uses standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages.

Telematics: A technology that uses two-way wireless communications between a vehicle and a processing center to transmit voice and data information (usually location coordinates) from the vehicle and the driver. Also used to describe the industry that uses this technology to deliver services to consumers (consumer telematics) and to commercial fleet owners and managers (commercial telematics).

Trusted traffic: IP traffic originating from a known address or network that has not been associated with a security risk.

Untrusted traffic: IP traffic originating from an unknown address or network, which may also appear on a list of known security threats.

Chapter 2 Agency Responsibilities

2 Scope

While the majority of this document addresses the handling of Next Generation systems utilized by both new and veteran telecommunicators, this chapter outlines the agency's responsibilities to provide policy and guidance for telecommunicators on many aspects of these systems. Additional recommendations are included for agencies to review hiring practices, job descriptions, stress management and mitigation, as well as potential additional liabilities associated with the changing telecommunicator job functions.

2.1 The agency shall define policies on PSAP controlled devices, such as:

2.1.1 The appropriate access and use of onsite devices owned by outside entities, such as schools, malls, and other public facilities, which are controllable by PSAP personnel.

2.1.2 Verifying proper operation of PSAP controlled devices on a scheduled basis, such as multimedia systems, door controls, traffic lights, etc.

2.2 The agency shall define policies to provide ongoing training with telecommunicators in scenario based situations, such as following a subject using multimedia sources.

2.2.1 The agency should identify opportunities to apply "skill-focused training" within the organization. Any employee with an aptitude for embracing and understanding NG9-1-1 technologies should be considered as a training resource.

2.3 The agency shall define policies identifying what multimedia sessions or multimedia from PSAP controlled device should be saved for immediate recall, to provide for on-scene responders, as needed.

2.4 The agency shall define policies identifying what multimedia will be retained and the duration, in accordance with state and local regulations.

2.5 The agency shall define policies to guide telecommunicators in handling multiple multimedia sessions related to the same incident.

2.6 The agency shall define policies identifying how the telecommunicator will process information received from PSAP controlled devices and Automated Data.

2.7 The agency shall define policies identifying how the telecommunicator will prioritize information received from PSAP controlled devices and Automated Data.

2.8 The agency shall identify policies on what pre-determined scripts should be in place for multimedia sessions.

2.9 The agency shall identify policies surrounding translation services involving multimedia sessions.

2.10 The agency shall identify policies on how to interpret incompatible language characters from multimedia sessions.

2.11 The agency shall identify policies on how and when to process non-emergency multimedia sessions.

2.12 The agency shall identify policies on logging new multimedia sources to include retention schedule, redaction procedures, data confidentiality, and the release of multimedia.

2.13 The agency shall identify policies on releasing multimedia sessions, while considering existing local, state, and federal public disclosure and privacy laws, such as FOIA and HIPAA.

2.14 The agency shall develop a policy as to how data, such as photos and videos are to be shared or released by PSAP personnel within and outside of the receiving agency.

2.15 The agency shall develop policies to address changes in protocols to handle multimedia sessions, which may include emergency medical dispatch, police, and fire instructions.

2.16 The agency shall develop policies identifying how telecommunicators will dispatch alternative responders, such as drones.

2.17 The agency shall develop policies detailing how data is shared or transmitted to responders and other authorized entities, in coordination with the agencies they service.

2.17.1 The agency shall identify what data shall be pushed to a responder during an incident (ex: telematics to a hospital).

2.17.2 The agency shall identify what data shall be available for responders to pull during an incident (multimedia to be used during an investigation).

Example: telematics data is transmitted directly to hospitals; a Fire Incident Commander receives fire streaming video to view when appropriate and a Police Incident Commander is able to control pan/tilt/zoom cameras for incident management.

2.18 The agency shall create policies to address response and management to automated data, such as:

2.18.1 Alarm sensors that create a CAD call for service, presented directly to the telecommunicator.

2.18.2 Advanced Automatic Crash Notification (AACN) transmissions from Telematics Service Providers that create a CAD call for service, presented directly to the telecommunicator, responder or response support (i.e., hospital).

2.18.3 Responder biometric alarms that create a CAD call for service requesting the appropriate response based on the alert (i.e., elevated heart rate, not breathing).

2.18.4 A law enforcement officer sensor such as pulling his/her weapon, activating an emergency response, similar to an emergency button press on a radio.

2.18.5 Smart buildings will provide details about the facility, such hazmat data, specific location where an incident is occurring, video feeds, occupancy, and details about the incident.

2.19 The agency shall have a policy for the provision of information and employee training regarding:

2.19.1 Implementing or expanding Critical Incident Stress Management (CISM) and debriefing tools.

2.19.2 Employee assistance or health and wellness.

2.19.3 Stress recognition and management.

2.19.4 Peer Support

2.20 The agency shall identify response and mitigation policies for service interruptions or attacks.

2.20.1 The agency shall define policies ensuring telecommunicators are trained at a basic level of cybersecurity awareness and hygiene. All employees can impact cyber vulnerabilities and mitigation.

2.21 The agency shall define policies and provide cross-training to ensure telecommunicators are familiar with 9-1-1 technologies (NG and legacy) in use, as well as any other legacy technologies at neighboring agencies.

2.22 The agency shall develop policies to deal with denial of service (DOS) attacks that begin with recognition that an attack is occurring.

2.23 The agency shall develop a policy to identify verified versus unverified sessions.

2.24 The agency shall develop security policies with the introduction of NG9-1-1 to the PSAP.

2.25 The agency should enhance existing protocols for telecommunicators to provide additional pre-arrival instructions to callers while first responders are enroute, when utilizing Next Generation systems (ex: a telecommunicator viewing a live video feed may provide an elevated level of pre-arrival instructions).

2.26 The agency shall identify what skillset is needed to process incoming multimedia sessions, automated data sessions, and to manage PSAP controlled devices when developing hiring processes.

2.27 The agency shall ensure telecommunicator job descriptions encompass the skillsets and responsibilities surrounding the new technologies.

2.28 The agency shall provide critical incident stress management for telecommunicators, recognizing the impact of visual or vicarious trauma from Next Generation systems versus voice-only reports.

2.28.1 The agency shall provide telecommunicators with de-briefing tools.

2.28.2 The agency should make relief available to telecommunicators, when staffing allows.

2.29 The agency shall determine if specialty positions should be created in the PSAP to manage Next Generation systems.

2.30 The agency shall determine if the use of a fusion center, real time crime center or group of specialty positions should be utilized to manage and process multimedia sessions.

2.31 The agency shall consider staffing models that include the processing and management of Next Generation systems based on the technology utilized by the PSAP.

2.32 The Agency should develop or share positions or functions for a multimedia data or intelligence analyst to triage multiple sources of information concerning the same or unrelated incidents, in order to determine what multimedia data (still frame photos, streaming video feed, imbedded GIS interpretation, etc.) is critical to forward to responders immediately, versus what data is more “background noise” or evidentiary rather than actionable. The work of the data or intelligence analyst may at times need to be coordinated with other public safety agencies. This position as well as positions such as a remote device operator and legal liaison, may be shared among multiple agencies.

2.33 The Agency should provide skills analysis to allow existing telecommunicators the opportunity for integration in newly developed specialty positions and/or in identifying Next Generation tasks that can be incorporated with existing tasks to allow for a more efficient deployment of new technology. The Agency shall develop procedures to contend with reports made through mobile apps, social media and crime tip portals and how to handle, preserve and store the information in a way that is compliant with relevant laws and regulations

2.34 The Agency should develop procedures to coordinate numerous alerting platforms (local, regional, and national), timing of emergency notifications and compliance with applicable laws and regulations including storage and retention.

2.35 The Agency shall develop procedures to determine how operations will complement and interact with other entities, where they exist, such as fusion centers that manage multiple sources of information and data. The Agency shall develop procedures to determine which mobile applications will be utilized within, or supported by the PSAP and ensure the procedures cover questions about costs, interoperability, commitment, etc. and plan on ensuring sufficient liability protection and training.

2.36 The agency should develop policies that are designed to distribute IP call loads efficiently and effectively across the PSAP, based on established call handling system capabilities and as agreed upon by all involved.

2.37 The agency shall develop a policy for handling and monitoring of cybersecurity

2.38 The agency shall review current Quality Assurance policies to ensure new functions and job responsibilities are covered.

Chapter 3 Organizational Integrity

3 Scope

This chapter discusses the issues related to organizational integrity. Topics include the mission and values of the profession in general and the agency specifically, as well as the scope of the telecommunicator's authority, confidentiality, and liability when interacting with Next Generation systems, PSAP Controlled Devices, and Automated Data.

3.1 The telecommunicator shall be able to articulate the Agency's updated vision, values, and mission statement.

3.2 The telecommunicator shall be able to articulate the Agency's expectations of professional conduct.

3.3 The telecommunicator shall demonstrate a comprehension of duties and essential functions of the position of a telecommunicator interacting with Next Generation systems, PSAP Controlled Devices, and Automated Data.

3.4 The telecommunicator shall demonstrate a comprehension of their scope of authority within the position of a Telecommunicator.

3.5 The telecommunicator shall demonstrate proper application of the Agency's written Directives when interacting with Next Generation systems, PSAP Controlled Devices, and Automated Data.

3.6 The telecommunicator shall demonstrate an understanding of the agency's chain of command.

3.7 The telecommunicator shall adhere to applicable local, state, tribal or federal statutes or codes as appropriate when interacting with Next Generation systems, PSAP Controlled Devices, and Automated Data.

3.8 The telecommunicator shall demonstrate the ability to comply with governmental or industry professional when interacting with Next Generation systems, PSAP Controlled Devices, and Automated Data.

3.9 The telecommunicator shall demonstrate comprehension and application of the agency 's confidentiality policies and rules regarding the discussion or release of information acquired in the workplace from Next Generation systems, PSAP Controlled Devices, and Automated Data to the public, the media, or others. Such information should include, but is not limited to:

3.9.1 Data systems accessible through local, state, regional, federal, tribal, or international networks.

3.9.2 Information contained in Next Generation systems, PSAP Controlled Devices, and Automated Data sessions

3.9.3 Information gained through the Next Generation systems, PSAP Controlled Devices, and Automated Data.

3.9.4 Records management systems containing information from Next Generation systems, PSAP Controlled Devices, and Automated Data.

3.10 The telecommunicator shall demonstrate comprehension of general liability concepts and terms as well as a comprehension of specific liability issues associated with the interaction of Next Generation systems, PSAP Controlled Devices, and Automated Data, including the most notable areas of litigation in public safety communications.

3.11 The telecommunicator shall demonstrate the ability to recognize when an incident changes to necessitate a telecommunicator to focus on a single incident, the telecommunicator shall hand off any additional sessions to another telecommunicator, if possible.

3.12 The telecommunicator shall demonstrate the ability to remain focused on emergencies while balancing the public's expectation for an immediate answer to their inquiries.

Chapter 4 General Knowledge and Skills

4 Scope

This chapter provides an overview of the general knowledge and specific skills needed by a telecommunicator to effectively and efficiently process calls for service by interacting with Next Generation systems, PSAP Controlled Devices, and Automated Data. The Next Generation Systems will require some additional steps and preparation, not only for what may be heard, but what may be visually viewed as well. Telecommunicators will need to be trained on the equipment and procedures to document calls for service details from Next Generation systems, PSAP Controlled Devices, and Automated Data, similar to voice calls.

The human element is the value that telecommunicators add regardless of the technology available to them, based on their training and interview skills (such as EMD questions, obtaining suspect descriptions, identifying fire exposures or entrapment data). Ultimately, it is the experience and expertise of telecommunicators that best ensure a successful response.

4.1 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:

4.1.1 Understand streaming live video from camera systems (could include portable video camera, interior camera system, PSAP controlled devices).

4.1.2 Ability to quickly identify when incoming photos/videos are related to an incident that has already been entered into the system.

4.1.3 Ability to process incoming photos/video that may contain graphic details.

4.1.4 Identify when to keep an open session, such as when monitoring a camera feed at an active scene (i.e., fire, domestic violence, bank robbery).

4.1.5 Encourage a reporting party to send any photo or video to the PSAP when safe and technically possible, while ensuring the safety of the reporting party.

4.1.6 Ability to effectively utilize 9-1-1 texting or other services in the PSAP to make contact when a phone connection is not available.

4.1.7 Ability to deliver the preinstalled EMD protocols through Next Generation services.

4.1.8 Ability to transfer data from Next Generation systems, PSAP Controlled Devices, and Automated Data to other PSAPs, in accordance with agency written directives.

4.1.9 Receive continuous training on how to quickly recognize a DOS attack.

4.1.10 Receive continuous training on how to prevent cybersecurity intrusions from inside the PSAP by using best practices for internal systems access and third-party communications.

4.2 General skills of the telecommunicator:

High-performing incumbent telecommunicators have been identified as demonstrating the ability to:

4.2.1 Analyze photos to identify specific details pertinent to the incident type.

4.2.2 Identify which agency should receive data that involved in an incident occurring in another jurisdiction.

4.2.3 Analyze streaming video to identify specific details pertinent to a real-time progressing incident.

4.2.4 Transfer control of an open session to a supervisor, another call taker or a field unit/supervisor.

4.2.5 Choose to answer incoming sessions from geographic areas outside an incident, when possible, to allow responses to unrelated incidents.

4.2.6 Manage multiple incoming sessions at one time, when safely able to do so.

4.2.7 Analyze profile information and photos to identify specific details pertinent to the incident type as well as safety issues and approach tips (specialty training – autistic and Alzheimer techniques for contact).

4.2.8 Identify specific details that affect a public safety response, such as smoke dynamics, telematics data deciphering, and scanning the initial scene for hazards.

4.2.9 Effectively utilize translation services during a texting session.

4.2.10 Read and understand information from shot detection and other sensors.

4.2.11 Maintain proficiency on the current trends within the industry.

4.2.12 Remain cognizant when an incident changes to identify when to:

4.2.12.1 Focus on a single incident.

4.2.12.2 Hand off any additional sessions to another telecommunicator, if needed.

Chapter 5 Tools, Equipment, and Technology

5 Scope

This chapter addresses the need for all telecommunicators (both new and veteran workers) to demonstrate proficiency on all NG-9-1-1 multimedia tools, PSAP controlled devices, automated data, and equipment within the public safety communications center. Technology is changing at a pace faster than seen in the past.

There will be continuous innovation producing technologies that PSAPs cannot anticipate. Thus, adaptability, already a key trait of successful telecommunicators, will be even more important as broadband technologies change emergency communications because the technology may be developed and introduced more rapidly than training programs can keep up with.

Smart buildings will send data such as a sensor alarm that includes temperatures in the area of the fire, hazmat data elements located in the facility, access points, and PSAP controlled cameras. Citizens with phones will communicate via live video, send recorded videos, as well as photos of incidents in progress when not able to speak freely. Non-traditional responders, such as drones, will be available. Telecommunicators must be trained to comprehend and process all types of calls for service from a variety of technology sources, as received and/or controlled by the PSAP. Training should be ongoing to ensure skills are kept proficient, especially for those critical technologies that are not used on a routine basis, such as school cameras available for an active shooter event.

5.1 The telecommunicator shall demonstrate the ability to create, access, and update incident data in accordance with Agency directives.

5.2 The telecommunicator shall demonstrate the ability to recognize service interruptions and/or attacks, such as; a Denial of Service (DOS) attack; spamming; swatting;

5.3 The telecommunicator shall demonstrate the ability to activate the agency’s plan to take immediate steps for response & mitigation of a service interruption or attack.

5.4 The telecommunicator shall demonstrate the ability to recognize verified vs. unverified sessions and proceed based on agency policy.

5.5 The telecommunicator shall demonstrate the ability to document and report recognized successful or unsuccessful service interruptions or attacks for an agency after action report.

5.6 The telecommunicator shall demonstrate the ability to operate PSAP controlled devices, such as; multimedia systems, cameras, door controls, traffic lights.

5.7 The telecommunicator shall demonstrate the ability to control the camera movement flow from one camera to another.

5.7.1 The telecommunicator shall demonstrate the ability to view camera feeds and know where the camera does not cover.

5.7.2 The telecommunicator shall demonstrate the ability to understand how a subject is moving from one camera to another and which direction the subject is moving.

5.8 The telecommunicator shall demonstrate the ability to operate multimedia logging sources in compliance with agency policies and procedures.

5.9 The telecommunicator shall demonstrate the ability to recognize unfamiliar character sets and utilize translation services within multimedia sessions.

5.9.1 The telecommunicator shall demonstrate the ability to recognize emojis.

5.9.2 The telecommunicator shall demonstrate the ability to recognize texting abbreviations and slang.

5.10 The telecommunicator shall demonstrate the ability to utilize and process automated data received by the PSAP, including vehicle telematics, sensors, alarms, etc.

5.11 The telecommunicator shall demonstrate the ability to dispatch non-traditional responders, such as drones.

5.12 The telecommunicator shall demonstrate the ability to operate the agencies NG9-1-1 telephone system.

5.13 The telecommunicator shall demonstrate the ability to visually verify call details when utilizing streaming video.

Chapter 6 Professional Competence

6 Scope

This chapter identifies those components within Public Safety Communications that are critical for enhancing the professional competence of all telecommunicators. Some of these components have been outlined Minimum Training Standards for Public Safety Telecommunicators within this document while others have been identified as being necessary for developing, maintaining, and enhancing the knowledge and skills of telecommunicators. While the Agency has some responsibility for supporting and facilitating the development of the telecommunicator's professional competence, this chapter places primary accountability on the telecommunicator.

6.1 The telecommunicator is responsible for asking clarifying questions to ensure a thorough knowledge and understanding of the equipment installed to handle NG9-1-1 sessions.

6.2 The telecommunicator is responsible for providing honest and specific feedback to their agency regarding the processes involved in learning new procedures.

6.3 The telecommunicator is responsible for providing input to improve or enhance the agency procedures in an effort to ensure current information is taught.

6.4 The telecommunicator is responsible for always presenting themselves in a professional manner, being on time, being prepared, ready to learn and actively participate in their own learning.

6.5 The telecommunicator shall comply with the requirements and rules of the learning environment or training facility.

6.6 The telecommunicator shall be responsible for being aware of the resources available to deal with stress from multimedia sessions involving disturbing content.

6.7 The telecommunicator shall demonstrate the ability to meet and/or exceed performance standards set by the Agency.

6.8 The telecommunicator shall demonstrate job proficiency in assigned job tasks.

6.9 The telecommunicator shall demonstrate compliance with Agency expectations of interpersonal communications, personal conduct and ethical behavior.

6.10 The telecommunicator shall comply with department, local, state, tribal, or federal regulations.

6.11 The telecommunicator shall actively seek and be receptive to feedback and review of their performance, including during the agency's established quality assurance or quality improvement process.

6.12 The telecommunicator shall identify professional goals that can be supported by the Agency.

6.13 The telecommunicator shall take responsibility for their own professional career development by actively seeking developmental opportunities to enhance their job knowledge and skills.

6.14 The telecommunicator shall demonstrate improvement of performance deficiencies.

6.15 The telecommunicator shall demonstrate the ability to operate within all written directives and plans established by the Agency.

6.16 The telecommunicator shall remain current and informed of all policies, guidelines, and plans.

6.17 The telecommunicator shall demonstrate the appropriate application of policies, guidelines, or plans.

6.18 The telecommunicator shall recommend updates to policies, guidelines, and plans when appropriate.

6.19 The telecommunicator should demonstrate the ability to utilize networking opportunities when appropriate.

6.20 The telecommunicator should take advantage of opportunities to network both within the public safety community and within the community for which they provide service.

6.21 The telecommunicator should recognize networking opportunities presented in concert with training, professional affiliations, and community outreach.

6.22 The telecommunicator should review professional publications in order to enhance professional competence and remain up-to-date on developments within the profession.

6.23 The telecommunicator should read professional publications, when possible, to remain up-to-date on current events affecting the public safety communications industry.

6.24 The telecommunicator should have an awareness of professional publications that identify, regulate or mandate activities associated with public safety emergency communications.

Chapter 7 Telecommunicator

7 Scope

This chapter identifies the minimum training requirements for a telecommunicator interacting with Next Generation systems who serve as a Public Safety call taker, Law Enforcement, Fire, and/or EMS dispatcher. The function of the telecommunicator is to process incoming calls both traditionally and through the Next Generation of multimedia possibilities to include, but not limited to, video from camera systems, drones, texting services and shot detection systems. As Next Generation multimedia systems/equipment are installed and the PSAP has the capability, the telecommunicator must maintain proficiency on the current trends within the industry as the Next Generation Systems will require some additional steps and preparation, not only for what may be heard, but what may be visually viewed as well.

Stress management and employee well-being will need to be considered using the understanding of the influx and type of exposure related to the viewing of incidents, such as the sights and/or sounds of disasters or medical emergencies.

7.1 The telecommunicator shall demonstrate the ability to ascertain whether the caller is in an unsafe situation and then take appropriate protective actions in compliance with existing agency policies and the following considerations:

7.1.1 The telecommunicator shall demonstrate the ability to avoid asking the reporting party to get unnecessarily involved in a situation.

7.1.2 The telecommunicator shall demonstrate the ability to consider that people behind a camera/video may have a different perspective on a scene.

7.1.3 The telecommunicator shall demonstrate the ability to provide direction to encourage the initial safety of the 9-1-1 reporting party when processing incoming sessions.

7.1.4 The telecommunicator shall demonstrate the ability to advise the reporting party to stay a safe distance from the incident when trying to take a photo or video.

7.2 The telecommunicator shall demonstrate the ability to discourage the reporting party of involving themselves in an incident at the scene when trying to obtain a photo or video.

7.3 The telecommunicator shall demonstrate the ability to process information received from incoming multimedia sources to determine an appropriate public safety response.

7.3.1 The telecommunicator shall demonstrate the ability to dispatch appropriate resources, apparatus or specialty units based on telematics data received.

7.3.2 The telecommunicator shall demonstrate the ability to dispatch appropriate resources, apparatus or specialty units based on visual data received, such as live video feeds.

7.3.3 The telecommunicator shall demonstrate the ability to provide data such as telematics and live video to response support units such as hospitals, doctors or incident commanders.

7.4 The telecommunicator shall demonstrate the ability to recognize all resources available in the PSAP, such as cameras, to gather specific details.

7.5 The telecommunicator shall demonstrate the ability to properly document multimedia sources requiring a public safety response by visually gathering details that are traditionally gathered by questioning a caller.

7.6 The telecommunicator shall demonstrate the ability to identify when incoming traffic is from an untrusted source.

7.7 The telecommunicator shall demonstrate the ability to identify the meta data from photos, videos and notes, such as location and date/time.

7.8 The telecommunicator shall demonstrate the ability to rely on information gathered from a caller, using multimedia to correlate the sources.

7.9 The telecommunicator shall demonstrate the ability to save a portion or entire multimedia session on their desktop for immediate recall, following agency policies.

7.10 The telecommunicator shall demonstrate the ability to coordinate with responders and other authorized personnel to share multimedia sessions, following agency policies.

7.11 The telecommunicator shall demonstrate the ability to manage multiple incoming multimedia sessions, following agency policy.

7.12 The telecommunicator shall demonstrate the ability to recognize when to focus on one critical incident and transfer non-related multimedia sessions to other telecommunicators.

7.13 The telecommunicator shall demonstrate the ability to follow all agency policies, including privacy policies regarding multimedia.

7.14 The telecommunicator shall demonstrate the ability to instruct the caller on how to provide the multimedia to the PSAP.

7.15 The telecommunicator shall demonstrate the ability to respond to sensor data from responders, such as biometric data or when a weapon is pulled.

APPENDIX A: Validation and Security

PSAP personnel need to be secure in the knowledge that their ability to receive 9-1-1 communications from the public is not compromised and data they receive is valid. The network sources that this data can be received from can be categorized as trusted or untrusted. A bad tag or misclassification should not be the reason why someone in need is prevented from reaching those who can help. By allowing the reception of all such data, PSAP's have a further concern that they do not become victim to any malicious data attacks which can negatively affect operations. For this reason, having or updating security policies with the introduction of NG9-1-1 to the PSAP should be a priority.

Incoming Call Validation

Review Available Metadata Associated with the Call

Multimedia messages sent to Public Safety Answering Points (PSAPs) via industry standard NG9-1-1 network connections will arrive with IP address information that can be pre-validated by the originating service provider. Its source will be classified as trusted; originating from a known address or network, or classified as untrusted; originating from an unknown source or a network address known to be a threat. With Internet Protocol (IP) communications, each message has an originating IP address embedded in the message, Session Initiation Protocol (SIP) packet. Addresses that are associated with Internet Service Providers (ISPs) outside the United States, or included on the alert lists due to prior malfeasance, would be likely to trigger the untrusted classification. Originating service providers and receiving public safety agencies would need to agree on a policy for the treatment of untrusted messages.

How these untrusted sources will be identified to the call taker has not yet been standardized. In general, it is expected that the two categories will be easily distinguishable from each other. However, the information that is received from either source will be evaluated at the PSAP level and disseminated accordingly. It is possible that valid data may be received by a source that is classified as untrusted. Also, simply because a source is categorized as trusted, does not mean that it is delivering honest information relative to the call specifics or needs. Regardless of the categorization, the PSAP shall decide the relevance, applicability, and evidentiary value of any data it receives.

New operating procedures would start by checking to see if the SIP message has been tagged. If the call has been tagged as coming from an untrusted source, the call taker should follow standard operating procedures for their agency regarding call queue prioritization and call handling. One approach would be to place untrusted messages at the end of the queue and only answer them after all trusted sessions have been processed. Most, if not all NG9-1-1 call handling solutions are expected to have the ability to prioritize sessions based on certain characteristics, including security parameters. It is recommended that all agencies develop a policy for NG9-1-1 sessions coming from untrusted sources.

Review Any Notes Associated with the Specific x-y Coordinates Associated with the Calling Party Number

Many NG9-1-1 Call Handling and Computer Aided Dispatch (CAD) systems have the ability to maintain notes, information entered from past experience or applied from external alerts, specific to x-y coordinates. Examples of notes would be prior law enforcement activity at the same address, disability registrations for public transport, or proximity to known fire hazards. The Call Taker should check to see if the reporting party's x-y coordinates have notes and follow the agency's standard operating procedures accordingly.

For example, high-profile cases of a call type known as "swatting" can receive media attention and result in copy-cat cases in other locations. Classic characteristics of this type of call include: outrageous claims that, if true, would necessitate a maximal departmental response (e.g., SWAT Team), upon unit arrival the reported situation seems eerily untrue (the reporting party has reported multiple gun shots but neighborhood and reported homes are silent), Bystanders, and those unaware that a call has been made, exhibit genuine surprise. If the x-y coordinates are associated with a known swatter or frequent false alarms, best practice suggests that the dispatched first responders should be given this information.

Security Policies

Agency Response Capability Compromised by IP Traffic from External Sources

There are several ways that illegitimate data can impact a PSAP ranging from unintentional to malicious. In much the same way that a voice caller on an uninitialized cellular phone can repeatedly call a PSAP and tie up a line, unwanted data could also cause a disruption.

Denial of Service Attacks (DOS)

Agencies should develop standard operating procedures to deal with denial of service (DOS) attacks that begin with recognition that an attack is occurring. With NG9-1-1 technologies, authorized users (typically an Administrator or on-duty Supervisor) can review available metadata on high call volumes to identify suspicious traffic. Once an attack has been recognized (for example hundreds of sessions a minute from the same black-listed IP address) it will be possible for agencies to choose how all sessions from the same address will be routed. This is very different from a Telephony Denial of Service (TDOS) attack where options are more limited.

Key elements of any DOS operating procedure are:

Continuous training on how to recognize an attack and how to minimize internal vulnerabilities

Have a plan in place on immediate steps for response & mitigation

Pre-determine your options for ensuring legitimate calls get answered

Follow a disciplined post-event documentation & reporting process

SPAM

There can be cases where high-volume IP traffic can be directed at your agency without a specific intent to compromise 9-1-1 traffic. Spamming, sending unsolicited bulk e-mail messages, is one example.

Although the threat will be new to 9-1-1 agencies as they migrate to NG9-1-1 platforms, this type of nuisance traffic has been present in the commercial world for some time. Many information technology tools exist today to mitigate the impact. Agencies may need a new operating procedure to address these occurrences.

It is recommended that agencies coordinate policy creation, adoption, and implementation with their in-house IT department or external IT service provider.

Minimizing Threats Enabled Within the Trusted Network

With the advent of NG9-1-1 and IP networks delivering (SIP) messages, agencies should adopt or create policies which address how employees can protect the trusted network. These policies should include best practices for opening e-mail from unknown sources or activating links to untrusted websites. It should also prevent unauthorized physical access to the workstations and any adjunct equipment with an IP connection. Higher levels of exposure to external networks (internet or e-mail for example) result in higher risk levels. The lowest level of risk exists when the trusted network is fully contained and traffic is limited to 9-1-1 sessions from originating service providers connected through NG9-1-1 based Emergency Services IP Network (ESINet).

Information Sharing on Threats & Mitigation Strategies

Many states have centralized resources for sharing information about existing threats and mitigation techniques against known attacks. At the Federal level (available to all local jurisdictions), the Department of Homeland Security regularly issues security information that can assist agencies in anticipating specific threats and utilizing the best available information on how to defend against the attacks and/or mitigate damage. The Federal Communication Commission's Task Force on Optimal Public Safety Answering Point Architecture (TFOPA) introduced the concept of an Emergency Communications Cybersecurity Center (EC3). Each Agency, or group of agencies acting collaboratively, should designate a resource to monitor available cyber security information and share updates with Agency supervisors daily. Depending on the threat or defensive action required, the supervisor may decide to share the information more widely within the agency.

Notes

APCO International
Leaders in Public Safety Communications™
351 N. Williamson Blvd.
Daytona Beach, FL 32114 USA