

RECOMMENDED BEST PRACTICE FOR COMPLIANCE REVIEWS

Administrative

The following criteria are recommended as best practices:

Written service agreements for any and all contracted services with external, third party vendors and internal, county vendors. Some examples are:

- Building lease agreement.
- Informational Technology (IT) services.
- Tower agreements.
- Bookkeeping and/or payroll.
- Backup Center
- Shared equipment

911 Plan

The plan shall be reviewed annually at minimum to determine if alteration is necessary. Considerations for the review are to reflect a change in management of the system (including technical management), as well as call handling agreements between different jurisdictions. The Plan contains at a minimum:

- Operational considerations.
- Technical considerations.
- Fiscal considerations.
- Managerial considerations.
- Valid ballots.
- Written agreements on fund distribution (if applicable) or plan.
- Addendums

911 Board

The named board is listed in the final 911 Plan (where applicable), along with the following items:

- By-laws are defined, adhered to, and posted for the public.
- Level of authority held by the board.
- Board members include MSP, Sheriff, and fire personnel (*if established after 1994*).
- Meeting minutes.
- Public posting of meeting date(s), time(s), and location follows open meeting public act.
- Meetings are scheduled and held on a regular basis.

Contacts

The County Coordinator shall maintain a list of appropriate PSAP managers and contact information.

RECOMMENDED BEST PRACTICE FOR COMPLIANCE REVIEWS

- List is updated as changes arise and shared with the State 911 Administrative office.
 - To update the PSAP contact information, use form SNC 800 found on the State 911 website main page ([MSP - State 911 Committee](#)).

Staffing

- Establish a minimum staffing level according to the needs of the center.
- Ensure a process is in place to fill in for scheduled and unscheduled absences.
- Maintain a position management system which identifies the job type and classification number of each staff member.
- It is recommended employees provided with periodic performance-related reviews by management independently from the QA call process.

Training*

See the State 911 Committee's [Telecommunicator Training Program Manual](#).

- Possess a defined, written, in-house training program which includes evaluations.
- Process to determine selection of trainers, or Communications Training Officers (CTO).
- Apply for SNC approved training funds annually.
- Meet qualifications for a designated telecommunicator as outlined in the Telecommunicator Training Program Manual.
- Performance measures to include:
 - Identifying key personnel responsible for overseeing the process.
 - Training personnel initial training and continuing education training.
 - The activities and outcomes to be measured.
 - The measurement methodology.
 - How feedback is obtained and delivered from internal staff and to outside agencies.
 - Quarterly review at minimum, which includes review of the CTO program itself.

Education

- Public Education program includes:
 - Develop community public education policies.
 - Provide information on the community education objectives of the agency.
 - Publicize objectives, problems, and successes.
 - Convey information to citizens and agencies.
 - Improve agency practices.
 - Identify training needs for the general public.

RECOMMENDED BEST PRACTICE FOR COMPLIANCE REVIEWS

Supervision*

A clear defined chain of command shown, with the responsibilities of each level within the organization as well as a predetermination of whom has authority in emergency situations.

- A written personnel policy in place that addresses chain of command.
- A written policy in place in the event an employee is involved in an incident that may cause the agency to be questioned regarding liability.
- Written policy requiring employees to obey any lawful order of a superior, including an order relayed by another employee. This directive includes procedures to be followed by an employee who receives a conflicting or unlawful order.
- Policy establishing procedures for communication both internally and externally.
- Responsibilities of Director of the PSAP:
 - Define authority to issue, modify, or approve written directives.
 - Agency values and mission statement.
 - Requirement of employees to read, sign, and abide by the organization's Code of Ethics or Values.
 - Define off-duty code of conduct.

Operational

The following criteria are recommended as best practices:

Standard Operating Procedures (SOPs) (Duties of staff, call intake)

- Each position in the PSAP has a detailed job description that is current from call taker to director.
- SOPs are in place and current.
 - SOPs are reviewed annually by admin to include revision/review date. Telecommunicators need to sign off on each SOP as it is revised.
 - SOPs are reviewed at least semi-annually by telecommunicators.
 - SOPs are readily available at each workstation for employee reference.
 - Establish how SOPs are provided to the employees.

Policy & Procedure

- Procedures regarding supervision to include:
 - Indexing, purging, updating, and revising directives' statements of agency policy rules and regulations.
 - Carrying out agency activities.
 - Review of proposed policies, rules, and/or regulations prior to promulgation.
- Where and how are the policies stored?
- Establish how policies and procedures are provided to the employees.

RECOMMENDED BEST PRACTICE FOR COMPLIANCE REVIEWS

- Document receipt of policies and procedures by employees including date given to employees (Include date policy was implemented and last updated on each individual policy).

Technical Support

- Technical support is available 24 / 7 by either in-house employees or contracted technical support services, i.e. through County, Departmental, or contracted IT service.

Cyber Security

Many security breaches occur simply because the most current updates have not been applied to operating systems.

- The center has security hardware in place (firewall and intrusion detection system) to keep unwanted outside parties from accessing the center's intranet.
- Agency ensures the systems are guarded from viruses and unauthorized access.
- The center has antivirus security software on servers and PCs with current program updates and software versions.
- The center is compliant with the Criminal Justice Information Systems (CJIS) policy.
- The center has a designated Local Agency Security Officer (LASO).
- All personnel having access to CJIS have completed Information Technology Security Awareness Training (new employees with less than six months on the job, and existing employees must complete this training every two years).Mission critical 911 systems (CAD, LEIN, E911, audio recorders and radio system) servers and clients use only supported operating systems that offer updates and patches to address new cybersecurity threats.
- There is a policy in place providing guidance on when and how operating systems are updated.
- Agency has an electronic use policy.

Emergency Medical Dispatch (EMD)*

- The EMD program includes ongoing involvement, cooperation and protocol oversight with respective medical control authority, EMS agencies, and PSAPs.
- The EMD program includes 4 elements:
 - Case entry/Call Interrogation
 - Pre-Arrival Instructions
 - Collection of Information
 - Post-Dispatch Instruction

Quality Assurance (QA)*

- A quality assurance (QA) program to evaluate compliance with protocols.

Medical

- Dispatchers understand medical dispatch policy, protocol, and practice
- Dispatchers comply with medical dispatch policy, protocol and practice

RECOMMENDED BEST PRACTICE FOR COMPLIANCE REVIEWS

- Deficiencies in understanding and compliance with medical dispatch policy, protocol and practice among dispatcher are corrected in a timely manner
- Medical dispatch policy, protocols and practice are updated on a continuous basis to ensure that it is appropriate and effective
- The dispatchers tasked for medical intake calls should be EMD certified, and be able to perform medical intake from their workstations via desktop access (flip cards for backup) or flip cards.

Law Enforcement

- Dispatchers understand law enforcement dispatch policy, protocol, and practice
- Dispatchers comply with law enforcement dispatch policy, protocol and practice
- Deficiencies in understanding and compliance with law enforcement dispatch policy, protocol and practice among dispatcher are corrected in a timely manner
- Law enforcement dispatch policy, protocols and practice are updated on a continuous basis to ensure that it is appropriate and effective

Fire

- Dispatchers understand fire dispatch policy, protocol, and practice
- Dispatchers comply with fire dispatch policy, protocol and practice
- Deficiencies in understanding and compliance with fire dispatch policy, protocol and practice among dispatcher are corrected in a timely manner
- Fire dispatch policy, protocols and practice are updated on a continuous basis to ensure that it is appropriate and effective

Law Enforcement Information Network (LEIN)*

- Terminal located in a secure area.
- Assign a Terminal Agency Coordinator (TAC).
- Ensure compliance with all LEIN Security Rules & Regulations.
- For non-criminal justice agencies, have a management control agreement in place.
- Ensure approved Network Diagram, including advanced authentication requirements.
- Ensure appropriate training for staff in, LEIN, TAC, and LASO.
- Maintain LEIN Security awareness training & re-certifications of staff.
- Complete background checks for individuals who have unescorted direct or indirect access to the Criminal Justice Information Systems.
- Keep the Policy and Procedures update with the latest LEIN guidelines.
 - Establish how policies and procedures are provided to the employees.

Master Street Address Guide (MSAG)*

- Ensure MSAG is current and updated in a timely manner.
- Determine oversight of MSAG by staff or outside agency.

Mapping

- Determine oversight of mapping by staff or outside agency.

RECOMMENDED BEST PRACTICE FOR COMPLIANCE REVIEWS

- Confirm the mapping layers are current and have regularly scheduled updates.
- Ability to plot Phase II location into CAD mapping program without having to physically type the information.
- Map should include bordering jurisdictions to the PSAP boundary.

Interpreters Service*

- Translation service should be used to interpret for limited and/or non-English speaking callers.
- There should be a contract or vendor established with a translation service. Translation service provides over-the-phone voice interpretation services utilizing a staff of interpreters capable of providing translation for over 170 different languages. When a call is received from a limited and/or non-English speaking caller, a process should be in place to initiate a conference call in a short period of time, so the language can be identified, and the appropriate interpreter can be engaged.

Call Intake*

Emergency 911 Calls*

- Identify the name of the Dispatch Center upon answering the phone line.
- Establish basic information
 - Name of caller
 - Call back phone number
 - What is going on
 - Who is in need
 - Who needs to respond (i.e. law enforcement, EMS, or fire)
 - Where the emergency is
 - Follow-up questions to clarify.
- Determine policy regarding:
 - Entry and updating calls into CAD.
 - Proper call handling instructions.

Out of jurisdiction Emergency 911 Calls*

- Identify the name of the Dispatch Center upon answering the phone line.
- Establish basic information
 - Name of caller
 - Call back phone number
 - What is going on
 - Who is in need
 - Who needs to respond (i.e. law enforcement, EMS, or fire)
 - Where the emergency is
 - Follow-up questions to clarify.
 - Transfer call to the appropriate agency, ensuring the PSAP has all of the information needed to process the call.

RECOMMENDED BEST PRACTICE FOR COMPLIANCE REVIEWS

Non-Emergency Calls*

- Identify the name of the Dispatch Center upon answering the phone line.
- Establish basic information
 - Name of caller
 - Call back phone number
 - What is going on
 - Who is in need
 - Who needs to respond (i.e. law enforcement, EMS, or fire)
 - Where the emergency is
 - Follow-up questions to clarify.
 - Entry and update call into CAD.
 - Proper call handling instructions.

Equipment

The following criteria are recommended as best practices:

Network (Local Area Network (LAN), Wide Area Network (WAN), and Wireless)

- The center's network infrastructure is documented in the event of an abrupt departure of the primary technical contact. Documentation should exist so someone not familiar with the center can understand the network without extensive reverse engineering.
- The center has detailed network diagrams (or equivalent) of the network infrastructure, and can provide documentation on IP addressing, machine names, and passwords for the following systems:
 - LAN/WAN.
 - Network router/switching devices.
 - Radio/Telephone recording system.
 - CPE or Hosted E911.
 - Backup server
 - Domain controller.
 - VPNs.
 - Time server.
 - CAD.
 - Mobile VPN client.
 - Firewall.
 - Multibridge.
 - All workstations.
 - Remote access.
 - Any other servers.

Telephony (VoIP, ANI/ALI, WRLS, and WPH2)*

❖ Network

RECOMMENDED BEST PRACTICE FOR COMPLIANCE REVIEWS

- Diverse telephone entrance facilities into PSAP.
- Quantity of trunks from 911 System Service Provider adequate to provide P.01 grade of service. The NENA standard for voice grade of service is available at <https://www.nena.org/general/custom.asp?page=VoiceCircuitReqs>
- Dual-homed selective router if available.

ANI/ALI Controller

- ANI/ALI Controller should be supported by the manufacturer, not at end of life (EOL).
- ANI/ALI Controller should be running a supportable software release.
- Workstations and servers should be running an OS version that is supported by Microsoft or by the manufacturer if not a Microsoft platform.
- PSAP should have a current maintenance contract for the ANI/ALI controller with either the manufacturer or with a reseller. If the contract is with a reseller, PSAP should verify a support contract with the manufacturer.
- Remote maintenance access or web enable components to the ANI/ALI controller or workstations should comply with NENA 04-503 Network / System Access Security.
- Future ANI/ALI controllers purchased should meet NENA 08-003 – Detailed Functional and Interface Standards for the NENA i3 Solution.

Wireless

- The ANI/ALI Controller should be able to receive and display Tower location for a Phase I wireless call.
- The ANI/ALI Controller should be capable of performing a re-bid to attempt to upgrade the call to Wireless Phase II (WPH2).
- The ANI/ALI Controller should be able to receive the X/Y (latitude/longitude) coordinates including Confidence and uncertainty and the Z (elevation) coordinate of a Phase 2 call, and be able to pass the information to a CAD or a mapping system to allow the display of the caller's location on a map without having to manually type in latitude and longitude.
- System in place to verify accuracy of calls.

Computer Aided Dispatch (CAD)*

- Computers should be properly licensed and copyrighted.
- Computers should have up to date Anti-Virus protection.
- System design includes provision for expansion of the system to include capabilities not required in the initial implementation, including the addition of primary and secondary PSAPs.
- A current maintenance contract with the manufacturer or an approved vendor should be in place with the ability for remote support.
- Solution should be currently supported by the manufacturer and not end of life.
- Policies for CAD include:

RECOMMENDED BEST PRACTICE FOR COMPLIANCE REVIEWS

- Administrator(s) of the system.
- Password construction.
- Redundancy.
- Backup and storage location and destruction of backup files.
- An email/internet usage policy that includes a statement that there is no expectation of privacy.
- Proper entry dependent on SOPs
- Procedures for operations when CAD is down.

Radio System*

- The center has a 24-hour, two-way radio capability with continuous communication.
- The center has multi-channel radio capabilities with two-way operation on joint public safety, interjurisdictional, and/or regional frequencies.
- A current maintenance contact with the manufacturer or an approved vendor should be in place with the ability for remote support.
- Solution should be currently supported by the manufacturer and not end of life.
- Interoperability within the system and neighboring radio systems
- A written directive that lists the following:
 - All equipment.
 - Frequencies.
 - Persons responsible for monitoring.
 - Available means of communication.
 - Annual interoperable equipment testing.
 - Annual review of personnel assignments.
 - Storm plan.

Recording System*

- The center has the ability to immediately playback recorded phone and radio conversations while it maintains a continuous recording of all phones and radios within the centers.
- Recordings are retained for a minimum of 30 days, or as indicated in retention schedule.
- A current maintenance contract with the manufacturer or an approved vendor should be in place with the ability for remote support.
- Solution should be currently supported by the manufacturer and not end of life.
- Policy for recording includes:
 - Secure handling and storage of recordings.
 - Criteria and procedures for reviewing recorded information.

Video Relay Service (VRS)/Teletypewriter (TTY)/Telecommunications Device for the Deaf (TDD)/Real-Time Text (RTT)*

RECOMMENDED BEST PRACTICE FOR COMPLIANCE REVIEWS

- The center has a TTY/TDD/RTT or an equivalent system at each emergency answering point.
- Policies for processing calls via TTY/TDD/RTT include:
 - Initial training.
 - Retraining of personnel every six months.
 - Documented monthly testing of TTY/TDD/RTT equipment.

Mobile Data Terminal (MDT)/Automatic Vehicle Locator (AVL)*

- If the center has software allowing other agency's mobile devices to connect remotely, the center has the following in place:
 - System memorandum of understanding (MOU)/memorandum of agreement (MOA) between the center and connecting agencies.
 - User policy for all connecting agency users.
 - Only devices with operating systems that are currently supported by the manufacturer are allowed to connect.
 - The connecting agencies agree to stay current with operating systems updates.
 - The connecting agencies have antivirus software installed with automatic checks for software and data file updates.
 - MDT connectivity shall be conducted in compliance with CJIS network security requirements.

Time Server

- Agency uses a hardware or software time server that synchronizes all mission critical 911 systems (CAD, LEIN, audio recorders, E911, and radio system) to the same time, down to the second.

Facility

- Equipment room should comply with NENA 04-502 - E911 PSAP CPE Site Characteristics.
- Bathrooms: Accessible within the communications center's secure area.
- Break Room: Accessible within the communications center's secure area.

Communications Center

- Staff have access to the following equipment:
 - LEIN.
 - Resource materials.
 - Consoles/Radio playback.
 - Fax machine.
 - TTY/TDD.
 - Weather monitoring.*
 - Weather Alert system*

RECOMMENDED BEST PRACTICE FOR COMPLIANCE REVIEWS

- Internet.*
- CPE.
- Access to American Disabilities Act (ADA) compliant work stations.
- Adequate seating.

Backup

The following criteria are recommended as best practices:

Trouble Reporting*

- Supervisor(s) (if applicable) / employees understand any trouble reporting procedures and have all contact information available 24 / 7.

Uninterruptible Power Source (UPS)

- All critical equipment, i.e. 911 phone system, CAD (if applicable), records etc. are connected to a UPS with a 30 minute capability under full load.
- Maintenance of UPS is documented and system is tested on a regularly scheduled basis.

Generator

- The emergency backup power with an automatic transfer switching is connected to primary call center, tower sites, and backup center (where applicable).
- Generators are tested under load on a scheduled basis.
- Generator testing is documented.

Call Rerouting*

- Call rerouting / transfer is in place in case of a primary site failure or evacuation.
- All employees are aware of how to reroute calls in the case of an emergency.
- Written policy and agreement with re-route location for receipt of calls.

Backup Center*

- A backup center is available in case of an emergency, or documented agreements are in place with surrounding PSAPs in case of evacuation.

Disaster Recovery Plans*

- A Continuation of operation plan (COOP) is available.

RECOMMENDED BEST PRACTICE FOR COMPLIANCE REVIEWS

Funding

The following criteria are recommended as best practice:

- 911 budgets for each PSAP in the county for the current year and for at least, the two years prior.
- Copies of written agreements for fund distribution between the county and PSAPs (where more than one PSAP exists within said county).
- Copies of budgetary reports or journals including the line items for 911 fund receipts and expenditures for each PSAP for the current year and at least two years prior to that.
Additionally:
 - Copies of vouchers may also be requested.
 - Proof of earned interest following principal.
- Copy of indirect and administrative costs and its calculation, if being charged to 911.
- Copy of the SNC training funds receipts, revenue journal entries and expenditures, and completed DTS-510 forms to date for each PSAP receiving State 911 Committee training funds.
- Written description of fund distribution (wireless and wireline) for all PSAPs.

Resources

<http://www.911.gov>

<http://www.nena.org/>

<http://www.michigannena.org/>

<http://www.apcointl.org/>

<http://www.miapco.org/>

<http://www.fcc.gov/>

<http://nasna911.org>

<http://www.michigan.gov/snc>

<http://www.calea.org>

<http://www.michigan.gov/emhsd>

<http://www.michigan.gov/mpscs>

RECOMMENDED BEST PRACTICE FOR COMPLIANCE REVIEWS

**Items marked with an asterisk within the document must have a policy and procedure.*
Required Policies and Procedures

Appendix List of Required Policy and procedures

Index Reference	Section and Subsections	Compliance Y/N
	Establish Agency Values	
	Establish Agency Mission Statement	
	Establish Code of Ethics or Values	
	Establish Off-Duty Code of Conduct	
	Define Chain of Command and Communication Procedures	
	Responsibilities of the Director	
	Responsibilities of the Dispatch Supervisor	
	Responsibilities of the Dispatcher	
	Responsibilities of the CTO	
	Responsibilities of the Trainee	
	Insubordination to include an employee who receives a conflicting or unlawful order.	
	Clear procedure on how policies are updated and provided to employees	
	Training Manual	
	Process for updating the training manual	
	Emergency Medical Dispatch	
	LEIN	
	MSAG	
	Mapping	
	Interpreter Service	
	Call Intake	
	Emergency 911 Call	
	Phase I (WRLS)	
	Phase II (WPH2)	
	VoIP	
	Text to 911	
	Emergency 911 Call Out of Jurisdiction	
	Non-Emergency Call	
	Dispatch	
	Law Enforcement	
	Fire	
	Medical	
	CAD	
	Administration of the system	
	Password Construction	
	Backup and storage	

RECOMMENDED BEST PRACTICE FOR COMPLIANCE REVIEWS

	Email/Internet usage	
	Radio	
	Recording System	
	Process for requesting and reviewing recorded information	
	Video Relay Services (VRS), Teletypewriter (TTY)/Telecommunications Device for the Deaf (TDD)	
	Mobile Data Terminal (MDT)	
	Automatic Vehicle Locator (AVL)	
	Weather Monitoring/Alerting	
	Trouble Reporting	
	911 Phone Lines	
	Non-emergency Lines	
	Radio	
	CAD	
	LEIN	
	Generator	
	UPS	
	Call Rerouting	
	Backup Center	
	Disaster Recovery Plans	
	Evacuation	
	Fire	
	Flood	
	Towing	
	Overtime Call In	