OKLAHOMA 9-1-1 MANANGEMENT AUTHORITY

Regular Meeting

August 13, 2026 at 1:30PM

Oklahoma Capitol room 230

Oklahoma Secretary of State – Open Meetings

Login Print Page

Public Body

Subscribe to OKLAHOMA 9-1-1 MANAGEMENT AUTHORITY

Name
OKLAHOMA 9-1-1 MANAGEMENT AUTHORITY

EMail
911@oem.ok.gov

Phone
4055213193

Public Body URL
www.ok.gov/911

Description

Address
2401 N. LINCOLN BLVD.

Address 2

City
OKLAHOMA CITY

State
OK

Postal Co...
73105

Meeting

Status: New	Type: Regular	Address: 2300 N. Lincoln Blvd		
Start Date / T...: 08/13/2026 01:30:00 PM	End Time: 08/13/2026 04:00:00 PM	Address 2		
Name: Oklahoma Capitol Building	Room: 230	City: Oklahoma City	State: OK	Postal Co...: 73105
Comments: Meeeting of the Oklahoma 9-1-1 Management Authority		VM URL		
Posted By: Stacey Root				

Add Meeting to Your Calendar

Share 0 Share Post

Posted with the Secretary of State's Office on May 11, 2026 at 02:46 PM.

Oklahoma 9-1-1 Management Authority
Regular Meeting Agenda
August 13, 2026, at 1:30 PM

Oklahoma Capitol Building
2300 N. Lincoln Blvd.
Room 230
Oklahoma City, OK 73015

1. Call to order, roll call, and determination of a quorum.

2. This regular meeting of the Oklahoma 9-1-1 Management Authority ("Authority) has been convened in accordance with the Oklahoma Open Meeting Act.

   If an Authority member would like to add an agenda item to the next regularly scheduled meeting, please contact the 9-1-1 Coordinator and the Authority Chair at least one (1) week in advance of the meeting.

3. Welcome to members of the Authority and guests in attendance. All Authority members who have not taken the Oath of Office and Loyalty Oath will take group Oaths. (Handout)

4. Possible discussion, revision, and vote to approve the minutes of the June 4th meeting. (Handout)

5. Possible discussion, revision, and vote to approve the financial report for May and June 2026. (Handout)

6. Possible discussion and presentation of the "Emergency Telecommunicator of the Quarter Award." (Handout)
   a. Bianca Torrez, Shawnee 9-1-1

7. Possible discussion, revision, and vote to approve the following to the Operations Committee.
   a. Lisa Poarch, Department of Public Safety
   b. Morgan Johnson, Payne County

8. Possible discussion, revision, and vote to add the following to the Grants Committee
   a. Jodi Wolf, City of El Reno

9. Possible discussion, revision, and vote to add the following to the Technology Committee.

a. Russell Anderson, City of Norman

10. Possible discussion, revision, and vote to add members to the Ad Hoc Technology Road Map Committee. (Handout)
    a. Ben Smith, City of Woodward
    b. Jon Love, City of Oklahoma City
    c. Courtney Book, City of Lawton
    d. Jessica Carter, City of Lawton
    e. Russell Anderson, City of Norman

11. Possible discussion, revision, and vote to approve the changes to the FY26 Audit Form as recommended by the Administrative Committee pursuant to 63 O.S § 2864(7). (Handout)

12. Possible discussion, revision, and vote to establish a deadline of December 31, 2026 for quarterly updates of the NG9-1-1 Geographic Information Systems (GIS) data using version 3 of the toolkit with Authority action taken starting in February 2027. The quarterly updates to be reviewed on January 2, 2027, will be between October 1 and December 31, 2026.

13. Possible discussion, revision, and vote to approve the Cybersecurity Policy. (Handout)

14. Possible discussion, revision, and vote to approve the contract with MCP for deployment support of NG9-1-1 in Oklahoma for $233,220. (Handout)

15. Possible discussion, revision, and vote to approve travel for Mr. Curry and Ms. Brown to attend the Gold Flame Conference hosted by Virtual Academy. Funding should not exceed $4,000, to be allocated from the approved 2027 Budget from the account titled "Operations Committee- Training”. (Handout)

16. Possible discussion, revision, and vote to approve funding for two 8-hour classes at the Oklahoma Public Safety Conference, Suicide Intervention presented by Public Safety Group and How Not to Eat Our Young: A Guide to Productive Mentoring presented by Foundations Public Safety for a total amount not to exceed $8,000 to be allocated from the approved 2027 Budget from the account titled "Operations Committee- Training". (Handout)

17. Possible discussion, revision, and vote to add call handling to the Technology Roadmap. (Handout)

18. Possible discussion and action to create a Nominating Ad Hoc Committee, per OAC 145:15-3-1(c), to review and discuss possible members for the position of Authority Chair and Vice Chair, and to bring a slate of names for a vote at the October Authority meeting.

19. Possible discussion, revision, and vote to approve the new 2027 Grant Guidelines. (Handout)

20. Possible discussion, revision, and vote to approve the following grant requests: (Handout)

APPLICANT NAME	GRANT TYPE	STATE AMOUNT	LOCAL MATCH	TOTAL REQUEST AMOUNT	RECOMMENDATION
Elk City, City of	Radio	$13,710.40	$3,427.60	$17,138.00	Fund
Hobart, City of	NG911	$35,356.80	$8,839.20	$44,196.00	Fund
Osage County	TRNG	$95,609.65	$0.00	$95,609.65	Do Not Fund
Roger Mills County	TRNG	$2,900.00	$0.00	$2,900.00	Fund
Wagoner County	CAD	$127,620.96	$31,905.24	$159,526.20	Fund
TOTAL		$275,197.81	$44,172.04	$319,369.85	

20. Committee and Staff Reports: (discussion only)
    a. Programs Coordinator Update
        I. Audit Update

    b. Grants Update
        I. POP Update

    c. Administrative Committee
        I. No Update

    d. Legislative Committee
        I. No Update

    e. Technical Committee
        I. No Update

    f. Technology Coordinator Update
        I. Technical Committee Update
        II. NG9-1-1 Committee Update

III. GIS Committee Update

g. Cybersecurity
   I. Statewide Cybersecurity Awareness Training Update
      i. Homeland Security Grant Local Concent Agreement (Handout)
   II. NG9-1-1 Cybersecurity Policy Updates
   III. Cybersecurity Assessment Documentation Update
   IV. NG9-1-1 Address Standard Workshop Update

h. Operation Committee
   I. In-Person Training Update
      I. FY2027 Professional Development Pathway Budget (Handout)

i. Training Coordinator
   I. 988 Liaison Update
   II. Training Update
   III. Recruitment Campaign Kickoff July 23rd
      i. Recruitment Job Dashboard Stats (Handout)
      ii. Norman Assessments and Interviews conducted by ICG
   IV. Other
   V. Upcoming

21. State 9-1-1 Coordinator Report to the Authority
   a. Project Update
      I. Cimarron County
      II. Adair County

   b. Local, State, and Federal Coordination and Meetings (#whereisthe911guy)
      I. Bristow “Meet the New Director”
      II. Coweta “Meet the New Director”
      III. Stephens County “Meet the New Director”
      IV. Love County “Meet the New Director”
      V. City of Wagoner over consolidation
      VI. NASNA/NENA Conferences
      VII. FCC Panel “Retirement of Copper Lines”
      VIII. APCO Conference

   c. Upcoming

I. Oklahoma Field Operations Guide (OKFOG) Update- Aug. 20th
II. OTA Conference- Aug 25
III. Oklahoma Municipal League Sept 16th and 17th
IV. Oklahoma Sheriff's Association Oct 5th

22. Public Comments (Comments are to be limited to items under the purview of the Oklahoma 9-1-1 Management Authority. Each speaker shall be limited to five (5) minutes. Under the Open Meetings laws, the 9-1-1 Management Authority cannot respond to or discuss any public comment not on today's agenda.)

23. New Business

24. Chairman's Comments (discussion only)

25. Adjourment

LOYALTY OATH

(Okla. Statutes, Title 51 § 36.2A)

I do solemnly swear (or affirm) that I will support the Constitution and the laws of the United States of America and the Constitution and the laws of the State of Oklahoma, and that I will faithfully discharge, according to the best of my ability, the duties of my office or employment during such time as I am

_____

**Insert official title of Affiant (e.g., member, Oklahoma Uniform Building Code Commission OR if an employee, insert "An Employee of _____" followed by the complete designation of the employing officer, agency, authority, commission, etc.)

_____

Affiant Signature

State of _____

County of _____

Signed and sworn to (or affirmed) before me on this _____ *day of* _____, _____
(day) **(month)** **(year)**

by _____.
(**affiant's name must be stated here, print clearly**)

_____

Signature of the Notary Public OR other Notarial Officer

Commission Expires: _____

Commission Number: _____

Official seal of notary public

_____

IF a Notarial Officer (not a Notary Public) please provide Title and Rank (51 O.S. §21)

(OKSOS---11/22)

OATH OF OFFICE

(Art. XV O.C. §1)

I, _____,

(Insert printed name of Affiant, print clearly)

do solemnly swear (or affirm) that I will support, obey, and defend the Constitution of the United States, and the Constitution of the State of Oklahoma, and that I will not, knowingly, receive, directly or indirectly, any money or other valuable thing, for the performance or nonperformance of any act or duty pertaining to my office, other than the compensation allowed by law; I further swear (or affirm) that I will faithfully discharge my duties as

_____

Insert official title of Affiant (e.g., member, Oklahoma Uniform Building Code Commission)

to the best of my ability.

_____

Affiant Signature

State of _____

County of _____

Signed and sworn to (or affirmed) before me on this _____ *day of* _____, _____

(day) ***(month)*** ***(year)***

by _____.

(affiant's name must be stated here, print clearly)

_____

Signature of the Notary Public OR other Notarial Officer

Commission Expires: _____

Commission Number: _____

Official seal of Notary Public:

_____

IF a Notarial Officer (not a Notary Public) please provide Title and Rank (51 O.S. §21)

(OKSOS---09/2021)

CURRENT AVAILABLE BALANCE	**$29,293,299.83**					
REVENUE						
PROJECTED	FY26 BUDGETED					
2026 Total Budget	**$ 25,442,080**					
FY2026 Carry Over Actual	**$ 12,774,130**					
Projected Annual Income / Actual Revenue	**$ 12,382,800**	$896,246.01	$ 1,088,507.55	$ 1,042,490.48	$ 12,392,301.73	100.08%
Grant Funding / Actual Grant Reimbursement	**$ 285,150**	$7,120.88	$0.00	$ 37,026.43	$ 153,911.63	53.98%
Total Revenue Received for FY2026		$ 903,366.89	$ 1,088,507.55	$ 1,079,516.91	$ 12,546,213.36	
EXPENSES						
SALARY and BENEFITS	FY26 BUDGETED	Apr 26	May 26	Jun 26	FY26 TOTAL	% of TOTAL
Total Salaries and Benefits	$ 692,142	$ 62,226.11	$ 61,394.76	$ 60,934.91	$ 737,615.69	106.57%
MAINTENANCE and OPERATIONS						
Cellular Telephone	$ 5,500	$ 313.30	$ 330.19	$ 319.17	$ 3,855.71	70.10%
Training/Travel	$ 64,000	$ 5,885.99	$ 1,893.93	$ 7,110.84	$ 74,926.39	117.07%
Professional Memberships	$ 3,000	$ 0.00	$ 434.00	$ 0.00	$ 2,724.00	90.80%
Board Liability Insurance	$ 1,700	$ 0.00	$ 0.00	$ 0.00	$ 0.00	0.00%
Internal Services	$ 35,000	$ 723.20	$ 729.71	$ 3,286.64	$ 17,730.66	50.66%
GIS State Repository	$ 105,000	$ 0.00	$ 0.00	$ 0.00	$ 0.00	0.00%
Online Training	$ 165,000	$ 0.00	$ 88,000.00	$ 0.00	$ 95,915.00	58.13%
In Person Training	$ 250,000	$ 0.00	$ 0.00	$ 0.00	$ 0.00	0.00%
Communication & Publications	$ 25,000	$ 0.00	$ 0.00	$ 150.50	$ 150.50	0.60%
Meeting Facilitation	$ 4,000	$ 443.91	$ 170.41	$ 0.00	$ 2,999.65	74.99%
Computer Hardware	$ 17,500	$ 0.00	$ 0.00	$ 0.00	$ 0.00	0.00%
Office Furniture	$ 0.00	$ 0.00	$ 0.00	$ 0.00	$ 0.00	0.00%
Software Maintenance	$ 60,000	$ 60.00	$ 63.84	$ 0.00	$ 18,739.55	31.23%
9-1-1 Coordinator Workshop	$ 50,000	$ 0.00	$ 1,084.79	$ (169.21)	$ 915.58	1.83%
Travel Reim. for Auth Members	$ 12,000	$ 797.50	$ 0.00	$ 224.75	$ 3,263.70	27.20%
Subtotal	$ 797,700	$ 8,223.90	$ 92,706.87	$ 10,922.69	$ 221,220.74	27.73%
CAPITAL OUTLAY						
Administrative Committee						
Statewide 9-1-1 Auditing Services	$ 100,000	$ 0.00	$ 0.00	$ 0.00	$ 0.00	0.00%
Set Aside to Meet Board Goals	$ 80,000	$ 0.00	$ 0.00	$ 0.00	$ 0.00	0.00%
Mission Critical 3099005507 (Cimarron)	$ 86,505	$ 0.00	$ 7,831.79	$ 0.00	$ 85,198.54	98.49%
Training	$ 20,000	$ 0.00	$ 0.00	$ 0.00	$ 0.00	0.00%
Subtotal	$ 200,000	$ 0.00	$ 7,831.79	$ 0.00	$ 85,198.54	42.60%
Technical Committee						
Set Aside to Meet Board Goals	$ 100,000	$ 0.00	$ 0.00	$ 0.00	$ 0.00	0.00%
Training	$ 20,000	$ 0.00	$ 0.00	$ 0.00	$ 0.00	0.00%
Subtotal	$ 120,000	$ 0.00	$ 0.00	$ 0.00	$ 0.00	0.00%
Operations Committee						
Set Aside to Meet Board Goals	$ 100,000	$ 0.00	$ 0.00	$ 0.00	$ 0.00	0.00%
Training Classes	$ 20,000	$ 0.00	$ 0.00	$ 0.00	$ 0.00	0.00%
Subtotal	$ 120,000	$ 0.00	$ 0.00	$ 0.00	$ 0.00	0.00%
PROJECTS						
NG9-1-1 Planning and Deployment	$ 10,000,000	$ 0.00	$ 0.00	$ 0.00	$ 0.00	0.00%
Mission Critical 3099005408	$ 178,538	$ 0.00	$ 0.00	$ 0.00	$ 19,735.25	11.05%

CURRENT AVAILABLE BALANCE	**$29,293,299.83**					
REVENUE						
GRANTS						
2024 Grant Program	$ 1,744,417	$ 118,088.00	$ 341,347.79	$ 168,669.18	$ 1,996,517.47	114.45%
2025 Grant Program	$ 3,403,955	$ 261,615.53	$ 8,800.00	$ 329,528.55	$ 1,459,522.50	42.88%
2026 Grant Program	$ 10,500,000	$ 34,359.00	$ 14,000.00	$ 83,258.00	$ 352,976.58	3.36%
Mission Critical 3099005440 (Catoosa)	$28,056	$ 0.00	$ 0.00	$ 0.00	$ 28,055.75	100.00%
State Reimbursements	$ 15,648,372	$ 414,062.53	$ 364,147.79	$ 581,455.73	$ 3,654,184.45	23.35%
RESERVE FUND						$ 6,038,792
TOTAL EXPENDITURES		$ 484,512.54	$ 526,081.21	$ 653,313.33	$ 2,023,566.89	7.34%

EMERGENCY TELECOMMUNICATOR OF THE QUARTER

presented to

Bianca Torrez

Shawnee 911

by

APCO Oklahoma and the Oklahoma 9-1-1 Management Authority
on this the 13th day of August 2026.

OK 9-1-1 Management Authority
Board Chairman

APCO Oklahoma
President

Technology Roadmap Ad Hoc Committee Member List

Chair:
Adam Griffith, City of Oklahoma City

Technology Committee Representation:
Courtney Book, City of Lawton
Jon Love, City of Oklahoma City
Ben Curry, City of Edmond
Russell Anderson, City of Norman

Operations Committee Representation:
Joshua Huffines, Grady County **Pending*
Brandon Reynolds, City of Broken Arrow
Jessica Carter, City of Lawton
Ben Smith, Woodward County

Changes to the FY2026 Audit Form in EMGrants

- General information update on the first page to update contact information and due dates.
- Update of all phone numbers listed as contacts to reflect the change of desk phones being discontinued.
- Additional language to give more direction on how addresses are handled when a citizen calls for an address verification or registration.
- Removal of the questions asking about having a contract vendor, what software is used to update local GIS and addressing, and how mapping is maintained. This can be looked up with OKMaps now.
- Removal of the question asking how PSAP mapping data is provided in the PSAP.
- The removal of the question asking what type of calls the PSAP answers and if they are answering calls 27/7/365. This was not asked last year.
- The removal of the question asking what type of text service is provided. Everyone will soon be on a texting service, so this is no longer needed.
- The removal of the question asking if and what there is a third party for texting. This is no longer needed.
- Moving the question asking if the PSAP has a COOP plan up to the other questions asking about COOP planning and training, and adding the hint text and link to COOP planning information.
- The dates will all change to the correct requesting dates when the user chooses the 2026 fiscal year.
- Adding language that states “Not 9-1-1 fees from state funds” to the questions asking for the total amount of revenue coming from dedicated sales taxes.

GIS Repository Compliance Timeline

Key Compliance Milestones

Date	Requirement
October 1, 2026	GIS Address Standard Version 3 Required – GIS Address Standard Version 2.2 is retired. All repository submissions must comply with Version 3.
December 31, 2026	Quarterly Repository Compliance Begins – All PSAPs must upload GIS data quarterly using Version 3.

Compliance Monitoring & Enforcement Schedule

Date	Action
February 4, 2027	Board Notification – Staff notifies Board of non-compliant PSAPs and recommends a public hearing.
April 1, 2027	OK911MA Board Meeting & Public Hearing.
April 1, 2027	Board Notification – Updated non-compliance report.
June 3, 2027	OK911MA Board Meeting & Public Hearing.
June 3, 2027	Board Notification – Updated non-compliance report.
August 5, 2027	OK911MA Board Meeting & Public Hearing.
August 5, 2027	Board Notification – Updated non-compliance report.
October 2027 (TBD)	OK911MA Board Meeting & Public Hearing.
October 2027 (TBD)	Board Notification – Updated non-compliance report.
December 2, 2027	OK911MA Board Meeting & Public Hearing.
December 2, 2027	Board Notification – Updated non-compliance report.

Summary

- October 1, 2026: GIS Address Standard Version 3 becomes mandatory.
- December 31, 2026: Quarterly GIS Repository submissions are required for all PSAPs.
- Beginning February 2027: The OK911MA Board will receive recurring compliance reports identifying non-compliant PSAPs.

State of Oklahoma

Next Generation 9-1-1 Cybersecurity Policy

Approved by NG9-1-1 Ad Hoc Committee
Review Date: March 11th, 2025
Approved by OK911MA Board
Review Date: May 1st, 2025
Version 1

Table of Contents

Introduction

Purpose

This policy provides guidance on cybersecurity practices to support PSAPs in preparing for connecting to the NG9-1-1 ESInet and core services. Our mission is to protect NG9-1-1 systems and ensure the confidentiality, integrity, and availability of emergency communications. By establishing this policy and fostering a proactive cybersecurity posture, we will prepare PSAPs to identify and mitigate cyber risks, comply with relevant regulations, and maintain the resilience of NG9-1-1 services. Per **Oklahoma Administrative Code (OAC) 145:15-11-3, *Next generation 9-1-1 services (NG9-1-1),*** all PSAPs on the statewide solution must comply with cybersecurity requirements required by the Oklahoma 9-1-1 Management Authority's Strategic Plan. The requirements contained within this policy are adopted under that authority and apply to all participating PSAPs.

Scope

This policy applies to all NG9-1-1 entities connecting to the state provided ESInet and Core Services:

- Primary Public Safety Answering Points (Primary PSAPs)
- Secondary Public Safety Answering Points (Secondary PSAPs)
- NG9-1-1 third party vendor(s)
- Third party vendor(s) that provide a contracted service that performs functions or services that require securing NG9-1-1 assets
- Those who use, design, manage, or have access to NG9-1-1 assets (i.e. workstations, computers, networks, data, and systems).

Physical Security

According to the NENA NG-SEC Standard, PSAPs shall implement physical security measures to protect NG9-1-1 facilities from unauthorized access. Secure perimeters should include measures such as fencing, security cameras, adequate lighting, and guarded entry points to secure areas. Clearly marked barriers shall separate secure areas from non-secure locations to prevent unauthorized entry. PSAPs shall maintain a current list of personnel authorized to access secure locations (except for areas within the PSAP officially designated as publicly accessible). Any non-PSAP employees, such as third-party vendors or contractors, must be approved by PSAP management and documented accordingly.

All secure entry points shall be controlled, and individual access must be verified before access is granted. PSAPs should implement measures to prevent unauthorized individuals from following authorized personnel into secure areas (tailgating). Technical measures to prevent tailgating include access control systems such as badge scanning, biometric authentication, or PIN entry at all secure entry points. PSAP employees should be trained on tailgating risks and to not allow tailgating. Employees and authorized personnel should report any unidentified individuals in secure areas immediately.

Secure doors shall not be propped open under any circumstances. Access control devices, including keys and badges, must not be shared or used to provide unauthorized access.

Visitors requesting access to secure PSAP areas must be authenticated before entry and always escorted. Unauthorized visitors shall not be permitted to access secure locations under any circumstances.

Continuity of Operations Plan

PSAPs shall have established procedures to ensure continued operations in the event of a disruption. It is essential for PSAPs to account for the potential threat of a cyberattack and evaluate whether a robust business continuity plan is in place. In the event of an attack, PSAPs must be prepared to continue serving the community and supporting employees while identifying all vulnerable systems and assessing the short-term and long-term impacts of the incident.

Assessing these scenarios and determing how to prevent and prepare for them, as well as ensuring if PSAPs have a comprehensive continuity of operations plan, are critical components of the risk assessment process. Failing to prepare for cyberattacks and operational disruptions can have severe consequences, including the loss of response capabilities, harm to your organization’s reputation, exposure of sensitive personal information, and potentially life-threatening delays in emergency response.

Incident Response

PSAPs shall implement an incident response plan. An incident response plan is defined as:

A formal, written plan that details how an organization will respond to a computer security incident. It includes procedures for preparation, detecting and analysis, containing, eradicating, and recovering from a security breach. The goal of an incident response plan is to minimize the impact of a security incident and ensure business continuity.

A security incident refers to any event that compromises the confidentiality, integrity, or availability of data or systems. Examples of security incidents include ransomware attacks, virus outbreaks, critical service outages, hacking attempts, denials of service, and more.

A cybersecurity incident response plan should include the following topics based on the NIST 800-61 Standard:

- **Preparation:** Ensure sufficient security measures are in place and that a NG9-1-1 Entity is ready and able to respond. This should include when and how to bring in outside help along with a list of available resources. This outside help may be a contracted service, a Community Emergency Response Team (CERT), or through another entity.
- **Detection and Analysis:** Detection is the discovery of the incident. This may be through security tools, notification by an inside or outside party, or some other method. This phase includes the declaration and classification of the incident.
- **Containment, Eradication, and Recovery:** It is crucial to contain an incident to prevent further damage from occurring, containment is the action required to prevent an incident or event from spreading across the network. Eradication is the action required to eliminate the root cause of the security incident. Having predefined procedures to contain an incident helps speed up the process and better ensure successful containment.
- **Post-Incident Activity:** Having a post-incident activity helps ensure that lessons learned are documented, needed improvements to the cybersecurity posture are made, and the incident response plan is updated.

Roles and Responsibilities

PSAPs shall designate a security agent and/or third-party vendor that is responsible for overseeing all investigative activities related to network and computer security incidents, as well as managing the response to intrusions. These responsibilities include, but are not limited to:

- Maintaining a directory of subject matter experts, including their names, departments, contact details, and areas of expertise.
- Contacting relevant team members as necessary in response to an intrusion.
- Coordinating the overall response to the intrusion.
- Interviewing witnesses to gather information.
- Reporting information regarding the intrusion and response efforts to management.
- Collaborating with external organizations, such as neighboring PSAPs, vendors, partnering agencies, and the Oklahoma 911 Management Authority (OK911MA).
- Diagnosing the event with the assistance of the local system administrator and determining the appropriate course of action.

What details to report

When creating an incident report, it is important to gather as much detailed information as possible to ensure a prompt and accurate assessment of the situation. Discussion of the incident should be limited to individuals who have a direct need to know. Examples of key details to include in the incident report include, but are not limited to:

- The originator of the incident
- Whether the incident has been reported previously
- The type of cyber-attack (ransomware, data breach, etc.) and whether the activity is ongoing
- Availability of backups for the affected system
- The suspected business impact of the incident
- Information that has been exposed or lost
- IP addresses and domain names of the affected machines
- The network name to which the machine is connected
- Suspected method of entry or origin of the attack
- Operating system and patch levels of the systems involved
- System logs, if available
- Date, time, and duration of the activity

Reporting Timeline

A known and/or suspected attack, breach, and/or cybersecurity incident, shall be reported to the following **within 24 hours** to:

- The Oklahoma 911 Management Authority (OK911MA) Technology Coordinator and/or Cybersecurity Specialist.
- The Core/ESInet provider
- ~~OMES Cyber Command~~
    - ~~PSAPS shall report all information collected about a security incident to the email address cybercommand@omes.ok.gov~~
    - ~~For immediate assistance on reporting an incident call~~
        - ~~(405) 522-5069 during normal business hours~~
        - ~~(405) 953-6420 outside of normal business hours~~
        - ~~If no one answers, leave a voicemail and all team members will receive an email with the voicemail audio attached~~

Additional Reporting Considerations

PSAPs should additionally consider reporting a known and/or suspected attack, breach, and/or security incident to:

- State, local, and/or county officials
- Third party vendors specific to PSAPs
- The Media
- Legal Department
- Cybersecurity Infrastructure Security Agency (CISA)

Ransomware Attack Response

Public Safety Answering Points (PSAPs) are frequently targeted by threat actors seeking to disrupt emergency operations and their ability to provide critical emergency response to the public. A common attack against PSAPs are ransomware attacks. Ransomware attacks encrypt data stored on computers and attached network drives, and the attacker demands a ransom payment in exchange for the decryption key.

Providing payment in exchange for the decryption key does not guarantee the data will be decrypted, or that systems or data will no longer be compromised, therefore federal law enforcement and the State of Oklahoma does not recommend paying the ransom.

The decision whether to pay the ransom is ultimately the PSAPs decision, therefore PSAPs should have a pre-established decision-making framework in advance to guide how cyber related ransoms are handled. Deciding to pay a ransom can be a complex decision, and it's important to have clear guidelines in place beforehand. The following factors should be taken into consideration as part of the decision-making process:

- Legal and regulatory considerations
- Operational impact of the attack
- Evaluate the availability of other means to recover systems and data
- Risk of data being leaked, altered, or not being decrypted
- Cost of paying the ransom versus the cost of recovery through other means
- Reputation and public perception
- Consultation with law enforcement and subject matter experts

No matter the decision, it is critical to document the rationale behind the decision that has been made, including the factors considered and the consultation with experts and law enforcement. This documentation can help guide future decisions and improve the PSAP's overall incident response and recovery strategy.

Response and Recovery

Based on the NENA NG-SEC Standard, a NG9-1-1 entity shall have the following recovery plans, and it is recommended that they are separate plans.

- Business Continuity Plan
- Disaster Recovery Plan
- Cybersecurity Incident Response Plan

These plans shall be maintained offline and be accessible to recovery teams

These plans shall be tested and reviewed annually and updated as needed.

After a security incident has occurred, PSAPs must take several critical steps to restore systems and ensure they are secure. This includes remediating all infected IT environments, reimaging affected systems, and replacing any compromised hardware. Compromised files should be replaced with clean versions, and patches and updates should be applied to fix vulnerabilities. Passwords for compromised accounts must be reset. It's also important to develop response scenarios that account for threat actors using alternate methods for attack that go beyond the obvious or traditional methods such as DDoS, ransomware, or phishing.

Sufficient time must be allowed to ensure that all systems are free from any cyber threat persistence mechanisms. Before rebuilding and reconnecting to the network, it's critical to ensure all adversary activity is fully contained. The root cause of the incident must be identified and eliminated, and any weaknesses or vulnerabilities in the infrastructure should be addressed to prevent future attacks.

System Backups

System and data backups are crucial for recovering and returning to normal operations after a security incident. Data backups must be tested to ensure the backups are effective and useful. When determining the backup strategy, PSAPs should consider the following:

- **The type of information backed up**. Information to consider for backup are system images, log files, licensing, software, server images, databases, inventory of all hardware and software, and any information that has legal requirement.
- **Frequency of backup of the information**. The backup frequency determines how much data loss the PSAP is willing to accept. For instance, if backups are done once a week, then the most data that could potentially be lost is the last weeks' worth. The frequency for backups may be different depending on the type of

information backed up. For example, a system image may only be backed up once a year while critical data files are backed up twice a day.
- **Adherence to legal requirements** set forth by federal, state, and/or local laws, rules, and/or contracts.

According to the NENA NG-SEC Standard:

- A NG9-1-1 Entity shall have a documented backup plan.
- A NG9-1-1 Entity shall have documented recovery procedures.
- A NG9-1-1 Entity shall test their backup plan annually at a minimum.

Offboarding Policy

PSAPs should have documented procedures that must be followed when a PSAP employee separates from the organization, ensuring that all actions related to their access to NG9-1-1 systems, data, and communication are properly handled. Given the importance of the information and systems PSAPs manage, it is imperative that PSAPs establish clear, documented procedures for handling the separation of employees. Offboarding policies ensure the integrity and confidentiality of the systems and data PSAPs rely on, as it verifies that former employees cannot access or misuse sensitive information post-departure. By establishing a clear and structured approach to employee separations, PSAPs can mitigate security risks and ensure regulatory compliance.

Access Control

The termination of access to systems, networks, and other sensitive resources should be timely and comprehensive. Key actions include:

- Immediate deactivation of user accounts
- Access to critical NG911 systems is revoked
- Removal from access control lists
- Change shared passwords
- Notify relevant stakeholders

Cold storage

Cold storage refers to archiving inactive or terminated employee data in a secure, non-accessible format. This includes defining the period for which an employee's data will be retained before being deleted or archived. If an employee had access to sensitive data, ensure that the sensitive data is moved to a secure, offline storage medium (cold storage) that is encrypted and access controlled. Once the retention period has ended, securely

delete any data associated with the terminated employee to prevent unauthorized access or misuse.

Email Retention

The employee's email account should be disabled as soon as they depart, but email retention policies should ensure that any essential communications are archived or forwarded to an appropriate team member. Establish a process for forwarding the employee's email to their supervisor or another designated person who will handle urgent or relevant communications. Define the period during which an employee's email archive will be retained after their separation.

Record Retention

PSAPs should establish procedures for retaining work-related records, such as incident reports, call logs, and other documents that might be needed for legal, compliance, or operational purposes. Ensure all physical and digital records are stored securely and remain accessible only to authorized personnel. Define how records will be securely destroyed once the retention period has ended to prevent unauthorized access or misuse.

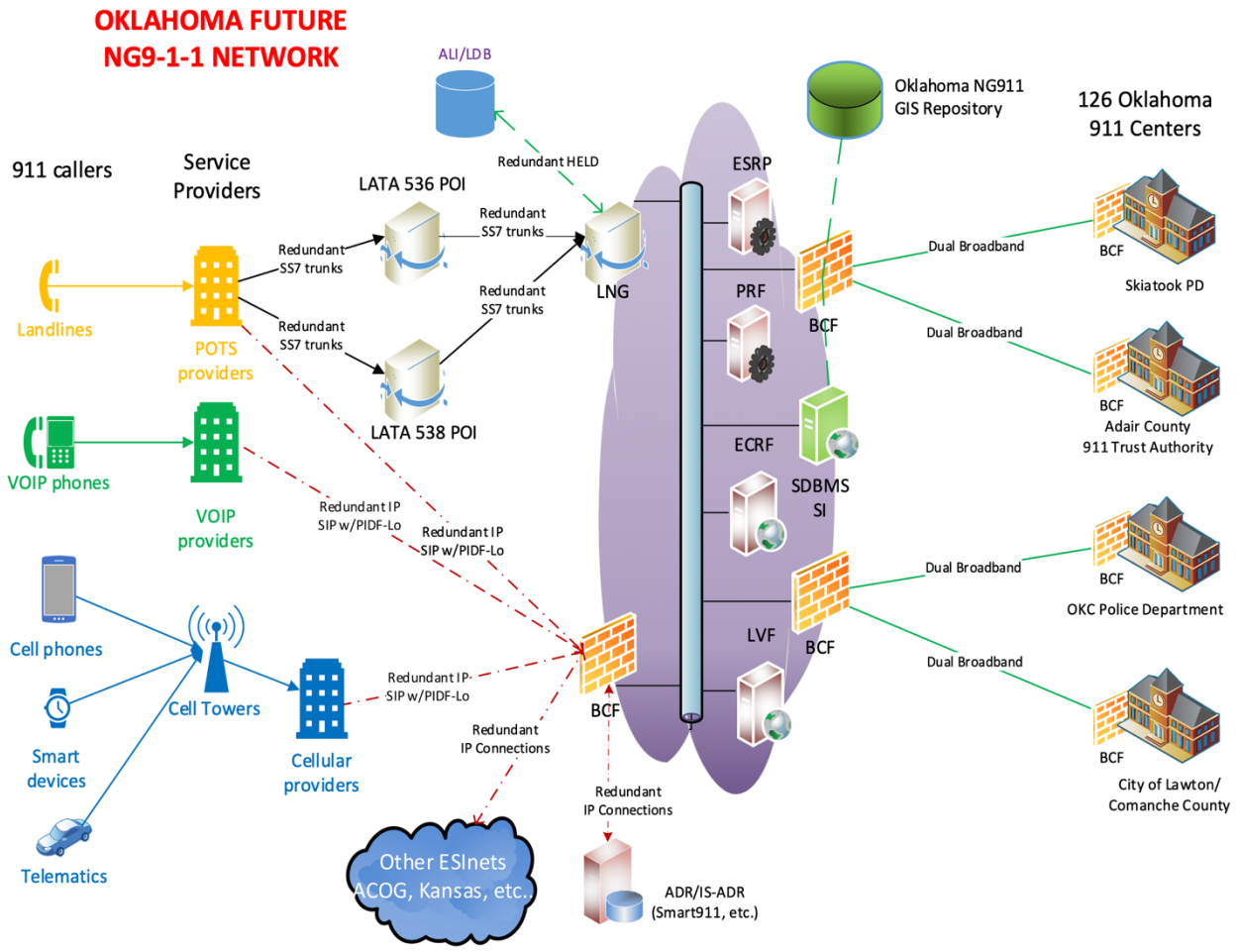
Cold Storage, Email, and Record Retention Compliance

PSAPs shall ensure that the cold storage, email, record retention, and archiving practices comply with applicable laws, regulations, and any specific requirements set forth by third parties, such as Oklahoma Law Enforcement Telecommunications System (OLETS), National Crime Information Center (NCIC), and the Criminal Justice Information Services (CJIS).

NG9-1-1 Network Architecture and Protection

The NG9-1-1 system is designed as an IP-based system and is governed by industry standards set by organizations such as NENA, APCO, and the FCC. It represents a transformative upgrade to emergency services, enabling faster, more reliable communications between callers and PSAPs. However, with this increased connectivity comes increased cybersecurity risks. The purpose of this section is to outline the critical assets PSAPs must protect, using the future NG9-1-1 network diagram for reference, to ensure the continuity and security of NG9-1-1 services.

NG9-1-1 Call Delivery Diagram



Key Assets in the NG9-1-1 System

The NG9-1-1 system is comprised of interconnected components, each of which must be protected to prevent service disruptions, data breaches, or malicious interference. The primary assets PSAPs are safeguarding include:

9-1-1 Caller Data and Communications

Data includes voice calls, text messages, multimedia (photos and videos), and location information provided by 911 callers through landlines, VoIP, cellular devices, smart devices, and telematics. Caller data must remain confidential and intact to ensure timely and accurate emergency response. Compromised data could lead to delayed or misrouted responses.

ESInet (Emergency Services IP Network)

The ESInet is the backbone of NG9-1-1 operations, handling the routing and processing of all emergency communications. The ESInet facilitates communication between service providers and PSAPs, any breach or disruption here could compromise the availability of NG9-1-1 services statewide.

Border Control Function (BCF)

The Border Control Function (BCF) is a security gateway that regulates traffic and provides security for the entire system, using admission control, firewalls, and other software tools to protect PSAPs from cybercriminals. It ensures only verified traffic reaches the network.

GIS Repository

The GIS Repository contains geographic information used for accurate call routing and location mapping. Inaccurate or unavailable GIS data could result in misrouted calls and delayed emergency response.

Public Safety Answering Points (PSAPs)

Any disruption to PSAPs operations, whether from loss of connectivity, ransomware attacks, or denial of service, could have life threatening consequences.

Interoperability Connections

Links the ESInet to other ESInets (e.g., Kansas, ACOG) and auxiliary data repositories (ADRs). Interoperability ensures seamless communication and data sharing across jurisdictions. Compromised external connections could introduce vulnerabilities into the NG9-1-1 system.

PSAPs play a vital role in protecting the NG9-1-1 infrastructure by adhering to best practices and implementing robust security measures. By understanding the critical assets within the NG9-1-1 system and implementing the proper protections, PSAPs can ensure uninterrupted, secure, and reliable emergency services. This proactive approach safeguards not only the NG9-1-1 infrastructure but also the lives of those who depend on it.

Network Security and Isolation

Closed Networks

Ensuring the security and integrity of NG9-1-1 systems requires strong network security protocols and isolation practices. Strategies to achieve this include implementing closed networks and network segmentation. A closed network refers to a secure, private communication system that is isolated from public or external networks. This type of network is used to ensure the reliability, security, and integrity of emergency communications, preventing unauthorized access or interference.

A closed network in a PSAP typically includes:

- Computer-Aided Dispatch (CAD) systems for managing emergency response.
- 911 call-handling systems for receiving and routing emergency calls.
- Radio communication networks for first responders.
- Secure data-sharing systems for transmitting critical information between agencies.

Because these networks handle sensitive and mission-critical data, they are designed with high security, redundancy, and encryption protocols to ensure uninterrupted emergency operations.

Access Control

Admin Access

PSAPs should limit the number of administrator accounts and only use them for administrative work, regular user accounts should be used for day-to-day work. Built in administrator accounts should be disabled or renamed if used. Any default credentials that are used must be changed.

User Access

PSAPs should only grant rights to users who need them and adhere to the principle of least privilege, meaning if a basic user can perform all the tasks necessary, don’t grant administrator or elevated access to them, only grant what is needed for them to perform their job. Any built-in user accounts should be disabled as these can be exploited. Audits should periodically be run against the users to determine what is their effective rights and permissions.

Each administrator and user shall have a unique account and must not be shared among others within the organization.

Define user roles and responsibilities

PSAPs should define user roles clearly and establish corresponding responsibilities to prevent unauthorized access and minimize insider threats. Roles should be assigned based on job function and the principle of least privilege. Strong authentication methods should be implemented, such as multi-factor authentication (MFA), and regular password updates as well as password complexity requirements should be enforced.

Logs of all user activities should be maintained for accountability and security analysis. Access should be removed promptly for users who change roles, leave the organization, or no longer require certain permissions. All users should be educated on the importance of access control and their specific responsibilities, regular training should be conducted on recognizing and reporting suspicious activity.

Effective access control is critical to the cybersecurity posture in the NG9-1-1 ecosystem. By defining and enforcing clear user roles, PSAPs can minimize the risk of unauthorized access, data breaches, and operational disruptions. Adopting these measures ensures that only the right individuals access critical systems and information.

Password Policies

Password complexity

According to the NENA NG-SEC Standard, all passwords shall meet or exceed the following criteria:

- Passwords/passphrases shall consist of 16 or more characters
- Passphrases shall consist of a minimum of three different words or word segments. These should be words that do not typically go together
- Passwords/passphrases shall consist of upper-case and lower-case, numbers, and symbols

Poor or weak passwords consist of the following criteria:

- Contain less than eight characters
- Contain personal information such as phone numbers, birthdates, addresses, names of family members, pets, or friends
- Contain words found in a dictionary, including public safety-related dictionary words (e.g. “firefighter”, “police”, “dispatch”, or department abbreviations like “PD”), or town names
- Contain number or letter patterns such as qwerty, 123456, or aaabbb

Passwords should never be written down. Instead, try to create passwords you can easily remember. One way to do this is to create a passphrase based on an affirmation or other phrase. For example, the phrase, “Sunflowers grow taller in the spring” could become the

password “$unfl0w3rs@Tall3r!$pr1ng!”. It should be easy for you to remember but hard for another person to guess.

Password Frequency

According to the NENA NG-SEC standard, enforced password changes should be removed, or the frequency interval extended to help prevent bad password hygiene. Passwords/passphrases shall be changed if they are expected to have been compromised.

Password Protection

- Passwords must not be shared with anyone, they must be treated as sensitive, confidential information.
- Passwords must not be inserted into email messages or any other form of electronic communication.
- Do not share passwords with anyone, including administrative assistants, IT, managers, or coworkers.
- Do not write passwords down or store them anywhere in your office or store them on your computer or mobile device without encryption.
- If you suspect your password may have been compromised, immediately notify the IT department and change all passwords.
- Passwords shall not be posted or visible to anyone within the organization, or visible to the public and/or visitors.

Password Manager

Password managers help users maintain and manage multiple passwords. When using a password manager, users only need to remember the password that is used for their password manager. The password for the password manager should be a unique phrase of at least 20 characters. The password manager should be periodically backed up in accordance with the PSAPs backup plan.
The State of Oklahoma standard is to use Secret Server as the password manager, however the decision on which password manager to use is ultimately the PSAPs decision.

Based on the NENA NG-SEC Standard:

- Only password managers approved by the security manager shall be used
- Multi-factor authentication shall be required to gain access to any password manager
- A user's password manager shall not be shared will another user
- Users shall report the loss or suspected compromise of a password manager within one working day of discovery
- All passwords stored on a lost or potentially compromised password manager, or password manager's database, shall be changed within one working day of discovery

Multifactor Authentication

PSAPs should implement multi-factor authentication (MFA) for all users who access NG9-1-1 systems. MFA provides an additional layer of security and significantly reduces the risk of credential-based attacks by requiring a second factor that attackers are unlikely to possess, such as a one-time code sent to a secure device or a fingerprint scan.

Removable Media Controls

It is also vital for PSAPs to protect removable media to PSAP computers and networks. Removable media is a cheap and easy source to spread malware and viruses and has been directly tied to the loss of sensitive information in many organizations. PSAPs should develop and include in their policy a section regarding removable media. A well-documented removable media policy will help ensure the integrity of the network, data, and computer systems of the agency.

Removable media devices include, but are not limited to:

- DVDs and CDs
- Optical disks
- External hard drives
- USB memory sticks (flash drives)
- Embedded Microchips
- MP3 players and audio tapes
- Digital cameras
- Backup cassettes
- USB chargeable devices (cellphones or e-cigarettes)

PSAPs should restrict access to removable media and only approve if a valid business case for its use is given. If removable media is used, clear business benefits should outweigh the risks that are associated with removable media before approval is given. The only media devices that should be used to connect to any agency equipment or network is media devices that has been purchased by the agency/IT. Any non-agency owned removable media devices should not be used and should not store any information used to conduct official agency business.

Network Port Access

All open network ports on routers, switches, and firewalls pose a vulnerability to network and system security. These ports are potential access points and may potentially be exploited by threat actors to gain physical access to the agency's network and computer systems. All open and unused network ports should be turned off through the management console of the switch, router, or firewall. Any ports that will not be used for an extended period should be turned off until it is needed again.

Internet of Things (IoT) Devices

The Internet of Things (IoT) is a description given to a broad category of devices that use Internet Protocols for the transmission of data and multimedia communication. It is essentially a network of devices that collect and exchange data via the internet. These devices that use IoT protocols are extremely varied with a variety of potential interactions.

Examples of IoT devices include, but are not limited to:

- Programmable thermostats
- Smart lighting systems

- Security cameras and smart surveillance systems
- Environmental sensors
- Smart speakers (Amazon Echo, Google Home, etc.)
- Smart doorbells
- IoT enabled CAD

The variety of IoT devices and systems they are integrated into make it difficult to apply consistent security measures. These devices can send alerts directly into the ESInet and users may rely on these devices for the protection of life and property, which means the impact of these devices being attacked or compromised can be severe.

IoT devices need to be hardened to prevent unauthorized usage, any default password must be changed the first time the device is configured, and best practice password strength must be applied. Any ports that are not required for normal operations of the device should be closed. Other strong security measures to harden these devices include proper network segmentation, regular patching, monitoring, and proper authentication controls.

Potential scenarios arising from malicious access to an IoT device include:

- Using the device to attack other parts of the network
- Disabling, altering, or tampering with the device to stop it from responding to a valid emergency
- Using the device as a denial of service to flood the emergency system with false data
- Interfering with location data (CAD systems)
- Compromising physical security systems such as video surveillance
- Exploiting a vulnerability in an IoT device connected to emergency communication systems and disrupting 9-1-1 systems

Acceptable Usage Policy

PSAPs should have an established acceptable usage policy which covers email usage, internet usage, social media, streaming, etc. Restrictions on such usage must be clearly defined and monitored. Some PSAPs limit access to only pre-approved websites, while others establish criteria for blocking sites that are not work-related or that pose potential security threats. Any system that reaches beyond the PSAP's internal network must be closely monitored and restricted as much as possible without adversely affecting operations.

Streaming

Streaming audio or video content for personal use should not be permitted on PSAP networks. Streaming services may only be used for training or official purposes as approved. Streaming platforms must be accessed only through secure and approved channels.

Social Media

PSAPs should include social media usage in their acceptable usage policy, stating whether it is prohibited or limited during work hours, unless required for official PSAP communication. No sensitive or operational information related to PSAP activities should be shared on social media.

Email Usage

Policies detailing restrictions on the use of email must be enacted and enforced. The improper use of email technology may jeopardize the integrity of state systems, security, and service levels. Access to email is provided to employees and contractors to assist with conducting state business, and the use of email must not jeopardize the operation of systems or the reputation and/or integrity of the state. PSAP email accounts must be used exclusively for work-related purposes.

Phishing emails pose a serious threat to internal networks and continue to be common. Employees must only open emails from known sources and must be educated on how to identify suspicious emails. Employees must not open attachments or click on links from unknown or untrusted sources. Sensitive information must not be shared via email unless it is encrypted and intended for authorized recipients.

Software Updates and Patch Management

Software updates and security patches provide protection against vulnerabilities and threats. Following a patch management plan ensures that vulnerabilities are addressed promptly and minimizes the risk of cyberattacks. Best practices for patch management include:

- Maintain an up-to-date inventory of all hardware and software assets to ensure that no system is overlooked during patching. This list should include network devices such as routers, firewalls, and VPN concentrators, as well as application and operating system software.
- Ensure all software is updated regularly and enable automatic updates whenever possible.

- Use a method of prioritizing patches to distinguish whether the patch is a routine update that can be implemented according to a schedule or if it's a critical patch that should be implemented immediately upon release.
- Use vendor issued firmware updates, service packs, and hot fixes.
- If possible, use patches with digital signatures which validates a patch's source and integrity.
- Test all updates and patches in a controlled environment before deployment to ensure compatibility and to avoid disruptions.
- Subscribe to vendor notifications and security bulletins to stay informed about the latest updates and vulnerabilities.

Vulnerability Management

Configure Firewall Rules

Firewalls determine which traffic is allowed to pass in or out of the network based on a set of rules established by an admin user account. Proper configuration of firewalls is essential to securing the network, best practices for configuring firewalls include:

- Using a combination of rules to both permit authorized traffic and deny unauthorized traffic by:
    - Creating rules that explicitly deny access.
    - Adding rules to permit only the required access.
    - Adding 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 that restrict outbound network traffic to minimize the spread of damage in the event of a breach.

As a best practice, CISA recommends all firewalls and software be patched for vulnerabilities within 15 days for critical vulnerabilities and 30 days for vulnerabilities rated as high.

Hardening system devices

The National Institute of Standards and Technology (NIST) defines system hardening as reducing the attack surface of a system. A system can be hardened by:

- Removing all non-essential software programs and utilities from the computer
- Using the principle of least privilege to control access to sensitive system and application files and data
- Limiting user accounts to those needed for legitimate operations and disabling or deleting the accounts that are no longer required
- Disabling or removing network services that are not required for the operation of the system
- Disabling removable media, or disabling automatic run features on removable media and enabling automatic malware checks upon media introduction
- Disabling network ports that are not required for the system operation
- Activate built-in security features to ensure that the device's security capabilities, such as encryption, firewalls, access controls, intrusion detection, and user authentication, are enabled and properly configured
- Install and configure firewall software on host devices to block unauthorized access
- Ensure automatic operating system updates are enabled where possible. Use a centralized management system for updates to maintain consistency across all devices

Risk Management and Assessment

Cybersecurity Training

Cybersecurity training for employees is key to building awareness about the role each person plays in maintaining security of NG9-1-1 systems.

Trainings should include:

- How to recognize and report cybersecurity threats such as phishing, swatting, Distributed Denial of Service (DDoS), ransomware, etc.
- Password policies and proper handling of account credentials
- The dangers of plugging in personal devices such as phones, tablets, e-cigarettes, etc. into the agency's system.
- The cybersecurity risks of removable media including USB drives, hard drives, SD cards, etc.
- Reasons behind various security policies and procedures.

- Roles and responsibilities of each person in maintaining security.

All PSAPs connected to the statewide ESInet/NGCS shall ensure personnel complete cybersecurity awareness training on an annual basis. Upon implementation of the Oklahoma 9-1-1 Management Authority's statewide cybersecurity awareness training program, all PSAPs connected to the statewide ESInet and NGCS shall participate in the state-provided training program. New employees shall complete cybersecurity awareness training as part of the onboarding process and prior to receiving access to agency systems or networks whenever practicable.

The statewide cybersecurity awareness training program will be provided to participating PSAPs at no cost. PSAPs shall sign and return the Local Consent Agreement form to the Oklahoma 911 Management Authority in order to participate in the statewide cybersecurity awareness training program.

The statewide cybersecurity awareness training program will include cybersecurity awareness training, phishing simulations, and compliance reporting tailored to emergency communications environments.

Data Protection

Data should be protected as part of each PSAPs security policy. Data can be lost, stolen, leaked or altered. Steps should be taken to limit access to data to an "as needed" condition. Administrators can create levels of passwords used to limit access to the agency's data. Physical means add additional layers of data protection. Data storage devices, both local and hosted, should be encrypted. Access to data storage facilities should be limited and defined in the physical security policy.

Cryptographic implementation should use industry standard cryptographic algorithms and standard modes of operations. It is recommended that the algorithm Advanced Encryption Standard (AES), which is certified by the US National Institute of Standards and Technology (NIST), be used. Sensitive data in transit and at rest should be encrypted to prevent unauthorized access.

Conclusion

The advancement to NG9-1-1 also introduces an increased amount of cybersecurity risks. As cybersecurity threats continue to evolve and PSAPs connect to the NG9-1-1 ESInet and core services, it is essential to remain prepared and proactive in safeguarding critical assets. By adhering to these cybersecurity practices, PSAPs will not only protect

themselves from cyberattacks but will also contribute to the resilience and reliability of the NG9-1-1 system. The protection of sensitive data, uninterrupted service delivery, and the ability to quickly respond to cyber incidents are crucial for maintaining the trust and safety of the public we serve.

This policy outlines key principles for preparing for and responding to cyber threats. Incorporating these cybersecurity measures into everyday operations ensures that PSAPs remain ready to respond to emergency situations, despite the growing complexity of the digital landscape and cyber threats.

Glossary

Acronym/Term	Definitions
Access Control Lists (ACLs)	A list that specifies which users or systems can access specific resources or data within a network.
ADR (Auxiliary Data Repository)	A secure location for storing backup or auxiliary data.
AES (Advanced Encryption Standard)	A widely used encryption algorithm to secure data.
APCO (Association of Public-Safety Communications Officials)	A professional organization that provides training, standards, and resources for emergency communication professionals.
BCF (Border Control Function)	A function in network security that controls access at the network's boundary to protect against unauthorized data exchanges.
Business Continuity Plan (BCP)	A strategy ensuring that essential functions and operations continue during and after a disruption, such as a cyberattack or natural disaster.
CAD (Computer-Aided Dispatch)	A system used by PSAPs to manage emergency calls and dispatch resources.
CERT (Community Emergency Response Team)	A volunteer organization that assists in responding to local emergencies and disasters.
CISA (Cybersecurity and Infrastructure Security Agency)	A U.S. government agency responsible for protecting the nation's critical infrastructure from cyber threats.
Cold Storage	Secure, offline storage of data that is not actively used, often for compliance or archival purposes.

Containment	Actions taken during a security incident to limit the spread of damage or further compromise across systems.
Cryptographic Algorithms	Mathematical procedures used to encrypt or decrypt data, ensuring that the data remains confidential and intact during transmission or storage.
Cybersecurity Incident Response Plan	A comprehensive strategy to address and respond to cybersecurity breaches, attacks, or incidents.
Data Archiving	The process of storing inactive data that must be preserved for legal, regulatory, or operational reasons.
Data at Rest	Data that is stored on a system, such as on hard drives or cloud storage, and is protected to prevent unauthorized access or theft.
Data in Transit	Data that is being actively transmitted across a network or between devices, and which needs to be encrypted to protect it from interception.
Decision-Making Framework	A set of criteria or guidelines used to make decisions during a crisis, such as whether to pay a ransom in a ransomware attack.
DDoS (Distributed Denial of Service)	A cyberattack that floods a system with traffic to overwhelm and disrupt its service.
Digital Signatures	A cryptographic technique used to verify the authenticity and integrity of data, ensuring it hasn't been tampered with.
Disaster Recovery Plan (DRP)	A detailed plan to recover and restore IT infrastructure and data after a disaster or significant security event.

Eradication	The process of eliminating the root cause or source of a security incident to prevent recurrence.
ESInet (Emergency Services IP Network)	A dedicated, secure IP-based network designed to support emergency services and NG9-1-1 systems.
FCC (Federal Communications Commission)	The U.S. government agency that regulates communication infrastructure, including emergency services and 9-1-1 systems.
GIS (Geographic Information System)	A system that analyzes and visualizes geographical data, used for location-based services in emergency management.
GIS Repository	A database or storage system that holds geographic data used in emergency response systems, such as for routing 9-1-1 calls.
Hardening	The process of strengthening a system or device's security by eliminating unnecessary features, closing unused ports, and applying security patches.
Hot Fix	A patch or update deployed quickly to address a specific vulnerability or issue without waiting for a scheduled update.
Incident Classification	The process of categorizing a security incident by its type, severity, and potential impact.

Incident Response Plan	A formal plan detailing the procedures and protocols an organization follows to address cybersecurity incidents and minimize damage.
Interoperability Connections	Links or integrations between different systems or networks (e.g., between PSAPs or external databases) to ensure smooth data and communication exchanges.
Internet of Things (IoT)	Devices connected to the internet that collect and exchange data, ranging from household items like smart thermostats to critical devices used in emergency services.
Intrusion Detection	A security system that monitors network traffic or system activities for signs of malicious behavior or unauthorized access.
IoT (Internet of Things)	A network of interconnected devices that can communicate and exchange data over the internet.
MFA (Multi-Factor Authentication)	A security method that requires more than one form of identification to access a system.
NENA (National Emergency Number Association)	The organization that represents and provides standards for 9-1-1 systems in the United States.
NENA NG-SEC (National Emergency Number Association Next Generation Security)	A set of standards by NENA to address security in NG9-1-1 systems.
NG9-1-1 (Next Generation 9-1-1)	The next generation of 9-1-1 systems designed to handle modern communications technologies such as text, video, and data transmission.
NIST 800-61 (National Institute of Standards and Technology Special Publication 800-61)	A guide for handling computer security incidents issued by NIST.

Network Segmentation	Dividing a network into smaller, isolated segments to limit the spread of security breaches and to reduce exposure to threats.
Operational Impact	The effect a security incident or attack has on the day-to-day functioning and ability of an organization to deliver services.
Patch	A software update released to fix vulnerabilities or bugs in an application or system.
Phishing	A type of cyberattack where attackers impersonate legitimate entities to steal sensitive information, often through deceptive emails.
Post-Incident Activity	Steps taken after a security incident to evaluate the impact, improve future response, and strengthen security measures.
PSAP (Public Safety Answering Point)	A call center where emergency calls are received and managed.
Recovery	Restoring systems, services, and data to their normal functioning after a security incident.
Reimaging	Restoring a device to its original state, often through reinstallation of the operating system and required applications.
Remediation	The process of fixing vulnerabilities, errors, or weaknesses after an incident to prevent future risks.
Security Incident	Any event or breach that compromises the confidentiality, integrity, or availability of data, networks, or systems.

Smart Devices	Internet-connected devices that can be remotely controlled and monitored, such as security cameras, thermostats, or lighting systems.
Social Engineering	A tactic used by cybercriminals to manipulate individuals into revealing confidential information, often by exploiting human psychology.
Stateful Firewall	A firewall that monitors and tracks active network connections, ensuring that incoming data packets are part of an established connection.
SYN (Synchronize - TCP Handshake Process)	A signal used in the TCP handshake to establish a connection between two devices.
TCP (Transmission Control Protocol)	A standard network protocol that ensures reliable data transmission across networks.
Threat Persistence Mechanisms	Techniques used by attackers to maintain access to a compromised system even after initial detection or remediation.
Vulnerability	A flaw or weakness in a system, network, or application that can be exploited by cybercriminals.
VPN (Virtual Private Network)	A secure network that allows remote access and encrypts data traffic to protect privacy.

References

APCO Cybersecurity Committee. (2016). *An introduction to cybersecurity*. https://www.911.gov/assets/An-Introduction-to-Cybersecurity-A-Guide-For-PSAPs-1638566090.pdf

Barker, E., Smid, M., Branstad, D., Computer Security Division, G2, Inc., & NIST Consultant. (2015). *NIST Special publication 800-152*. U.S. Department of

Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-152.pdf

Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). *CISA INSIGHTS*. https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-RemediateVulnerabilitiesforInternetAccessibleSystems_S508C.pdf

The future of 9-1-1: Securing next generation infrastructure. (n.d.). https://www.thecall-digital.com/nenq/0324_issue_50/MobilePagedArticle.action?articleId=2028995#articleId2028995

National Emergency Number Association, & National Emergency Number Association. (2020). Impact of IoT devices and emergency calling applications. In *NENA Impact of IoT Devices and Emergency Calling Applications Information Document* (Report NENA-INF-030.1-2023; pp. 1–36). NENA. https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/nena-inf-030.1-2023_iot_&_ap.pdf

National Emergency Number Association (NENA) Systems Security & Resiliency Committee, Security for NG9-1-1 Working Group. (2024). *NENA Security for Next Generation 9-1-1 Standard (NG-SEC)*. https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/STA-040.2-2024_SecurityforNG.pdf

National Institute of Standards and Technology. (2018). Framework for improving Critical Infrastructure Cybersecurity. In *National Institute of Standards and Technology*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Protecting your center from ransomware. (n.d.). In *CISA PSAP Ransomware Poster* [Report]. https://www.cisa.gov/sites/default/files/publications/CISA%20PSAP%20Ransomware%20Poster%20Fact%20Sheet_20210204_FINAL%20508.pdf

Proposal

NG911 Implementation Support

June 5, 2026

Oklahoma 911 Management Authority, Oklahoma

MissionCriticalPartners

Table of Contents

Introduction Letter

June 5, 2026

Lance Terry
Executive Director
Oklahoma 911 Management Authority
2401 N. Lincoln Blvd.
Oklahoma City, OK 73105

Re: OK911MA - NG911 Implementation Support

Dear Lance:

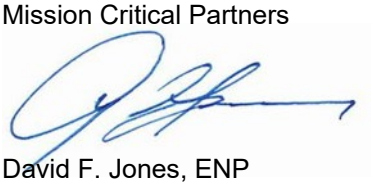
Mission Critical Partners® (MCP) appreciates the opportunity to provide this proposal to the Oklahoma 911 Management Authority (OK911MA) for implementation support of Next Generation 911.

MCP is prepared to serve OK911MA by assisting you with achieving optimal delivery of emergency communications services—**because the mission matters.** If you have any questions regarding the information submitted, please feel free to contact me at 864.809.9911 or via email at DavidJones@MissionCriticalPartners.com.

On behalf of our entire team, we stand behind the Oklahoma 911 Management Authority to serve as your partner and your advocate.

Sincerely,

Mission Critical Partners



David F. Jones, ENP
Senior Vice President

Mission Critical Partners

Putting Our Clients' Missions First

A Firm Unlike Any Other

At Mission Critical Partners, our mission is simple: to improve public safety and justice outcomes. Our client commitment is to act as a trusted, independent advisor, always striving to solve problems, deliver value, efficiency, and fresh ideas – all while mitigating risk.

We stand behind the significance of the work our clients do and how critical their missions truly are – not just for their organization, but for their entire community. Our greatest pride is partnering with clients to implement the best solutions that drive their mission, building upon our expertise and experience – because their mission is what matters.

We bring highly specialized expertise in public safety, justice and in other critical infrastructure sectors. Many of our professionals have been in our clients' shoes and are well attuned to their unique needs. Our vision is to transform mission-critical and public-sector networks and operations into integrated ecosystems.

A **Halo Effect** Over the Critical Communications Ecosystem

MCP provides its clients with a holistic approach to enhance and evolve critical communications systems and operations across the entire ecosystem. The "MCP Halo Effect" is our comprehensive integrated series of products and solutions to dramatically effect collaboration and situational awareness, improve decision-making, and ultimately influence outcomes.

3,900+ projects
supporting 2,200+ public-sector and critical communications agencies since 2009

We serve clients in
50 states
and 95% of the nation's largest metropolitan areas

200+
subject-matter experts on staff with an average of 25 years of experience

90%
of our clients remain with us from project to project

15%
average project cost savings for our clients—sometimes more

SecureHalo™
Family of Cybersecurity and IT Solutions

We're designing and monitoring highly reliable, secure and easy-to-manage integrated public safety networks.

Consulting
Consultive & Advisory Solutions

We're providing expertise across all areas of the constantly evolving public safety, justice, and broader public sector ecosystem.

DataHalo™
Family of Data Solutions

We provide data analytics and software solutions that improve collaboration, productivity, and decision-making.

Corporate Headquarters: 690 Grays Woods Blvd, Suite 100, Port Matilda, PA 16870 Phone: 888-862-7911

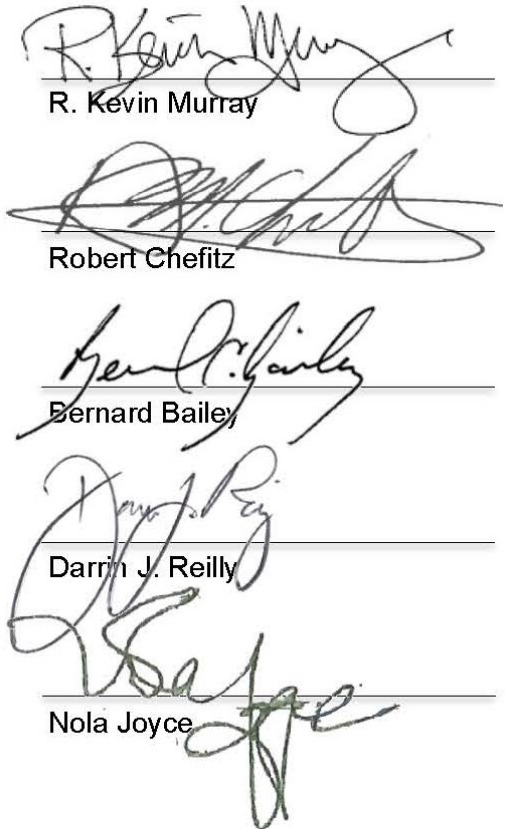
Our Commitment to Our Clients

Partnering with a firm that brings an independent, objective perspective to every engagement is our clients' top priority. We stand behind our commitment to always put the fundamental interests of our clients first.

From our inception, vendor-neutrality is a value that underpins every aspect of what we do. Our goal is to determine the most favorable solution for our clients based on their unique requirements, budget, governance structure, operations, and existing technologies. We provide a holistic perspective regarding the entire mission-critical communications ecosystem, free of bias or favoritism to any specific product or service provider. Our recommendations are always based solely on the value and the benefit provided to the client.

For clients, this approach means more control and greater visibility into the systems they ultimately are responsible for operating and maintaining, and—more importantly—a successful project that improves outcomes.

Board of Directors



Scope of Work

Phase 4: NG911 Implementation Support

Mission Critical Partners® (MCP) will provide technical subject-matter expertise assistance for Oklahoma 911 Management Authority (OK911MA) in support of preparation and transition to the Next Generation 911 (NG911) solution, including vendor oversight and coordination. This assistance ensures that OK911MA information is provided consistently and timely to the Next Generation 911 Core Services or Next Generation Core Services (NGCS) Emergency Services IP Network (ESInet) vendor to support the NG911 transition. In addition, MCP will assist OK911MA in maintaining an overall schedule for the ESInet migration based on NG911 system service provider commitments for onboarding the service and avoiding delays regarding data collection and vendor coordination for data accuracy.

As an independent advisor with extensive experience supporting statewide and regional NG911 implementations, MCP's role is to ensure that all design, implementation, testing, and operational decisions remain aligned with OK911MA's long-term operational objectives, contractual requirements, and desired end-state architecture. Independent oversight is particularly critical during NG911 implementation efforts, where service providers may prioritize approaches that align with their existing operational models, standard deployment methodologies, or cost-containment objectives rather than the optimal long-term solution for the OK911MA and their stakeholders.

Partnering with MCP helps mitigate the risk of incomplete implementation planning, overlooked technical dependencies, insufficient testing criteria, or design compromises that can result in significant downstream operational limitations, change orders, schedule delays, or increased lifecycle costs after deployment. MCP will provide objective technical validation and strategic guidance to help ensure OK911MA receives the full benefit of the contracted NG911 capabilities while preserving flexibility for future operational and technological evolution.

To successfully and efficiently transition the State's legacy public safety answering points (PSAP) to NG911, OK911MA will need to determine an optimal order for implementation. The deployments will necessitate a detailed and well-planned effort by State leadership, local leadership, and NG911 providers to define the elements of success and agree on a transition schedule.

A deployment plan should identify and rank the factors for cutover and provide strengths, weaknesses, costs, and other considerations for the various cutover strategies. The order of cutover might be driven by selective router locations, regional 9-1-1 service groups, or those PSAPs most technologically ready, best funded, with the closest access to network connections, or even having the greatest need. These factors can be prioritized, weighted, and scored to arrive at the "best" deployment plan.

MCP will provide technical subject-matter expertise and assistance to OK911MA to support preparation and transition to the ESInet and NGCS, including vendor oversight and coordination. NG911 implementations frequently involve large multidisciplinary vendor teams operating across network engineering, NGCS configuration, cybersecurity, geographic information system (GIS) integration, provisioning, and project management functions. While these resources are necessary for implementation execution, they can unintentionally create an imbalance in technical influence during planning and decision-making activities. MCP serves as an experienced client representative and technical advocate for OK911MA, providing independent analysis and recommendations that enable the OK911MA to make informed decisions based on operational readiness, industry best practices, contractual compliance, and long-term sustainability rather than implementation convenience alone.

MCP's technical leadership will also help ensure that implementation decisions do not unnecessarily constrain future interoperability, governance flexibility, operational workflows, or integration opportunities. Through independent review of project plans, technical deliverables, testing procedures, and operational readiness activities, MCP will help identify risks early and support proactive issue resolution before impacts to schedule, cost, or service quality occur.

MCP will support OK911MA from project initiation through acceptance of the network and NGCS. MCP has supported the implementation and operational oversight of numerous regional and state ESInets, including the various project tasks outlined by the selected vendor, including:

- Project initiation
- Design and document review
- Project status call support
- Contract compliance
- Testing preparation review and support
- Training review
- Operational readiness assessment

MCP's technical SMEs will provide OK911MA with independent validation that the selected vendor(s) deliver services in accordance with contractual commitments, industry standards, NG911 best practices, and OK911MA's operational objectives. MCP will independently assess implementation progress, technical deliverables, testing outcomes, and operational readiness to help identify gaps, risks, or deviations early enough to support corrective action before they affect deployment timelines, system functionality, or long-term operational effectiveness. In addition, MCP will support coordination between the vendors and OK911MA stakeholders as needed to help avoid delays regarding data collection, regional PSAP coordination, and vendor coordination.

With implementation support, MCP will work closely with OK911MA to ensure the goals and objectives are being met and support necessary actions should escalation be needed.

On a monthly basis, MCP will issue a project status update document for OK911MA's leadership.

With more than 200 technical requirements, each having multiple sub-requirements or vendor commitments, this task also supports OK911MA in preparing a comprehensive test plan for independent validation and verification of vendor commitments agreed to within the procurement process. MCP will ensure acceptance testing criteria are based on contractual agreements between OK911MA and the selected NG911 service provider.

The value of independent implementation oversight is not measured by duplicating vendor project management functions, but by protecting the Authority from avoidable technical, operational, and contractual risk throughout the lifecycle of the NG911 transition. MCP's experience supporting numerous statewide and regional ESInet and NGCS deployments (with the Authority's chosen vendor and multiple other industry-leading vendors) enables the Authority to benefit from lessons learned across prior implementations, including identification of common implementation pitfalls, operational readiness gaps, testing deficiencies, governance challenges, and design decisions that may create unintended long-term impacts. This expertise helps reduce the likelihood of costly post-implementation remediation efforts and supports a more stable, scalable, and operationally effective NG911 environment for Oklahoma's PSAP community.

MCP will provide technical subject matter expertise for operational readiness testing and for PSAP testing. MCP has included support for up to three trips of three days each in support of testing.

Deliverables:

- Conduct project initiation meeting
- Deliver redline edits to the vendor-provided plan
- Function as OK911MA's subject-matter expert (SME) regarding planning, ordering circuits, and executing the ESInet and NGCS transition
- Provide:
  - Monthly project status update
  - Independent minutes capturing MCP's perspective of the weekly vendor project meetings
  - Independent validation of the vendor's project plan, identifying risks to the proposed schedule and plan
  - Independent validation and verification test plan
  - Acceptance testing criteria and strategy
  - Recommendations for early-warning escalations of issues that may affect the overall schedule

Project Team

With more than 225 staff members, MCP's specialized professionals are integral members of our team:

MCP's Specialized Professionals	
• Former public safety communications operations staff, managers, directors, and executives • Technology, forensic, and policy specialists • Operations and training specialists • GIS Specialists	• Emergency Number Professionals (ENPs) • Project Management Professionals (PMPs) • Former law enforcement, fire, and EMS • Programming, design, and construction specialists

MCP has identified in the figure below the key team members that we plan to assign to this important project.

Organizational Chart

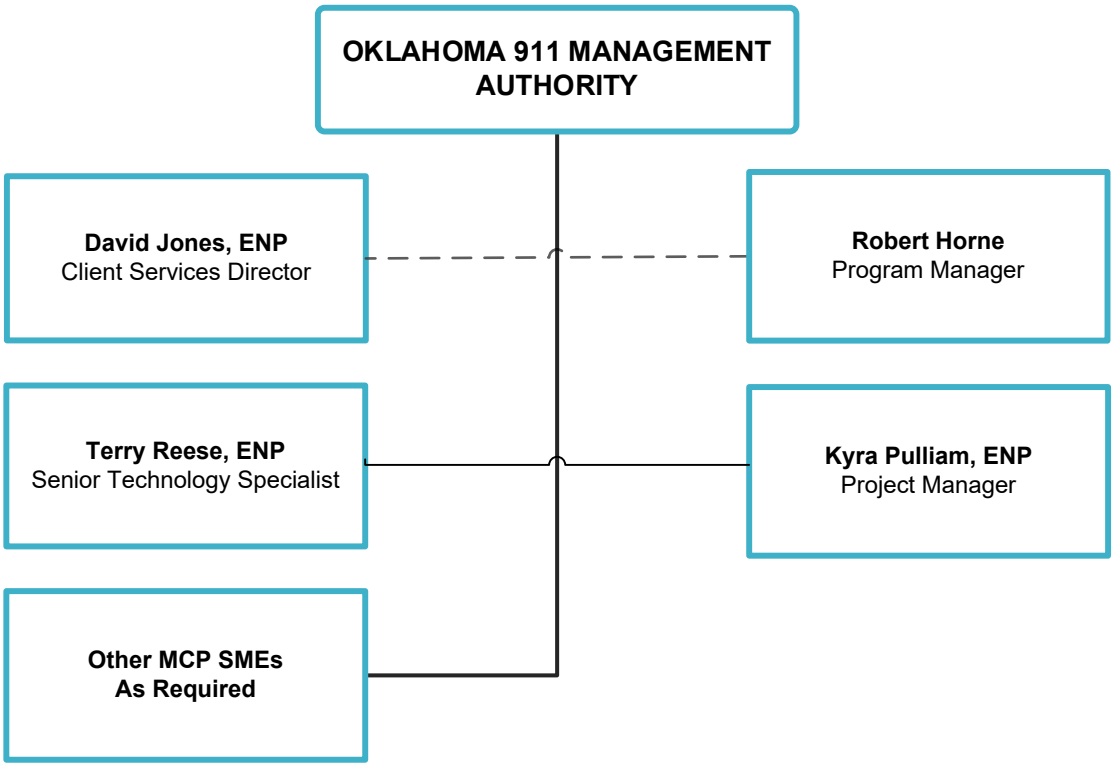


Figure 1: Organizational Chart

Each team member brings a unique skill set and depth of experience in NG911 implementation. Additional resources and subject-matter experts are available also, as we are a full-service firm focused on all aspects of public safety communications.

Resumes

Resumes highlighting our qualifications and experience are included on the following pages.

David F. Jones, ENP

Co-Founder, Senior Vice President of Strategic Accounts, Mission Critical Partners

David provides executive-level consultative services and expertise in NG911, government affairs, public policy, and legislation. He is an internationally known SME on 911, NG911, and emergency services and has advocated emergency services-related issues throughout North America, Asia, South America, and Europe.

While serving as President of NENA, he testified before the U.S. Senate Commerce Committee on 911 and next-generation telecommunications networks. He was among the first professionals in the U.S. to be certified as an ENP and has decades of experience in the public sector administering, directing, managing, and operating emergency service agencies and 911 departments. Areas of specialization include client management, program management support, and executive-level consultative services.

Representative Experience

State/Regional Experience

- Arizona—FirstNet-related support, NG911 planning and implementation, executive-level support
- 911 Association of Central Oklahoma Governments (911 ACOG)—NG911 design, acquisition, and deployment
- Kansas—NG911 support
- Minnesota—Statewide 911 implementation, technology support, and procurement support
- Nebraska Public Service Commission—NG911 study and professional general consulting
- New Mexico—NG911 planning and implementation support
- Oklahoma—NG911 support
- Tennessee Emergency Communications Board (TECB)—Technology consulting
- Texas—ESInet facilitation for the Commission on State Emergency Communications and applications development for the Department of Public Safety
- North Central Texas Emergency Communications District (NCTCOG)—911 master planning, executive mentoring, GIS assessment, NG911 implementation, and PSAP feasibility study

City/County Experience

- Horry County, SC—911, NG911, and radio support
- Shelby County, TN, Emergency Communications District—CAD consulting, automatic vehicle location (AVL) procurement assistance, and radio procurement for the Memphis Police Department
- Charleston County, SC—Public safety system review and ESInet
- Tarrant County, TX—911 District customer premises equipment (CPE) review and implementation and Regional Interoperability Communications Committee (RICC) study
- Dallas, TX—NG911 system planning, 911 CPE replacement, and LMR system implementation
- Houston, TX—CAD replacement
- Austin, TX—Radio System Needs Assessment and Procurement
- Lubbock Emergency Communication District, TX—Radio Communications System Assessment, Network Security Assessment and Monitoring Services
- Potter Randall ECD, TX—Cybersecurity Assessment and Network Monitoring
- Spartanburg County, SC—Director, Emergency Services—911, Emergency Management Agency, Fire Marshal, and Emergency Services Training Academy

Industry Experience

41 years

Education

B.A., Political Science, Wichita State University, KS

Certifications

Emergency Number Professional (ENP)

Associations

National Emergency Number Association (NENA)

NENA, President, 2005-2006; Executive Board, 2001-2007

Association of Public-Safety Communications Officials (APCO)

Awards

"Order of the Palmetto," by South Carolina Governor, October 2005. Highest civilian award in the State for "efforts to improve emergency services and communications"

Robert Horne

Vice President of Network 911, Mission Critical Partners

Robert is an executive-level leader who has built a successful career fostering prosperous relationships between local, regional, state, and federal technology programs. He has experience with integrating people, processes, systems, and data into 911 PSAPs, EOCs, fire and police command centers, and fusion centers across the country. Areas of specialization include federal, state, tribal, and regional interoperability, strategic and implementation planning, data modeling and reporting, business process reengineering, and standard operating procedures development. Robert is the Vice President of Network 911 Technologies teams. Robert provides strategic leadership for the Network 911 and GIS Teams, helping to further strengthen operations, innovation, and client support initiatives.

Representative Experience

Federal Experience

- National Highway Traffic Safety Administration (NHTSA) National 911 Program—National GIS capabilities gap analysis and strategic plan

State/Regional Experience

- Maryland 911 Board—NG911 Spatial Interface (SI) data analysis and readiness assessment, and statewide NG911 GIS strategic plan and implementation support: continuous contract since 2018
- Pennsylvania Emergency Management Agency (PEMA)—NG911 GIS strategic planning and statewide implementation coordination: continuous contract since 2017
- Pennsylvania Region 13 Task Force—NG911 GIS readiness gap analysis and five-year strategic plans for each of the 15-member jurisdictions and the region
- Arizona 911 Program—NG911 GIS strategic plan and statewide education and outreach
- Arizona 911 Program—NG911 GIS readiness gap analysis for every local 911 system
- Virginia Information Technologies Agency (VITA)—GIS needs analysis and implementation planning, and NG911 strategic planning roadmap
- Nebraska Public Service Commission (NPSC)—NG911 strategic planning, GIS support, and wireless integrity testing
- Minnesota Department of Public Safety, Emergency Communications Networks—NG911 strategic planning and GIS support
- District of Columbia Homeland Security and Emergency Management Agency (HSEMA)—Creation of a geospatial program for EMA, providing support for 3 presidential inaugurations, 78 federal national security special events, and more than 100 natural and human-created disaster activations; management of a team of six analysts
- Washington, DC, Washington Regional Threat Analysis Center (WRTAC)—Development and management of geospatial intelligence program, providing law enforcement sensitive and classified analysis of law enforcement, health, and homeland security data for steady-state operations, national security events, and emergency response

City/County Experience

- Atlanta, GA—CAD and GIS integration and migration support
- Fairfax County, VA—NG911 GIS readiness assessment project support
- Carroll County, MD—NG911 GIS readiness assessment and data improvement
- Charles County, MD—Fire and EMS assessment and strategic plan
- Burke County, NC—NG911 GIS readiness assessment and project management
- Wake County, NC—Emergency management study and gap analysis

Industry Experience

32 years

Education

M.B.A., Western Carolina University, NC

B.S., Computer Science, Business Information Systems, Columbia Southern University, AL

Certifications

Federal Emergency Management Agency (FEMA) Emergency Management Institute, Certified Emergency Operations Center Manager

The State of Florida, Disaster Recovery Operations (G385) “Train the Trainer”

Associations

National Emergency Number Association (NENA)

Maryland State Geographic Information Committee (MSGIC)

Theresa Reese, ENP

Senior Technology Specialist, Mission Critical Partners

Theresa brings years of telecommunications expertise, with nearly three decades specializing in 911 initiatives. A key focus of her career has been the development of industry standards for transitional and end-state NG911 architectures. She has led the specification of gateway system standards critical for transitioning from legacy E911 to NG911 environments and has spearheaded industry efforts to mitigate spoofing of critical information in 911 calls. Theresa has chaired and co-chaired numerous forums, committees, and working groups for the National Emergency Number Association (NENA) and the Alliance for Telecommunications Industry Solutions (ATIS). In recognition of her contributions, she was inducted into the NENA Hall of Fame in 2022.

Representative Experience

State/Regional Experience

- State of Illinois—Provided support for tracking NG911 deployment activities
- Gulf Coast Region, TX—Tracked NG911 call-handling equipment (CHE), NGCS, and ESInet deployment activities
- Pennsylvania Emergency Management (PEMA)—Provided input regarding system-sharing between PSAPs
- Minnesota Public Safety—Supported the development of the PSAP self-assessment checklist
- Oklahoma 911 Management Authority ESInet/NGCS—Supported the development of an ESInet/NGCS RFP and an interoperability policy for NG911, as well as NG911 RFP response evaluation
- Indian Nations Council of Government, Tulsa, OK—Provided 911 assessment, developed a CHE RFP, evaluated RFP responses, and facilitated vendor interviews
- State Office of Interoperable and Emergency Communications, New York—Supported Division of Homeland Security and Emergency Services (DHSES) NG911 planning, assessment, RFI response analysis, and CHE requirements development
- Commonwealth of Kentucky—Supported ESInet/NGCS RFP development and provided NG911 implementation support
- City of Longview, Texas—Supported NG911 procurement by developing an ESInet/NGCS RFP, evaluating responses, and facilitating vendor interviews
- State of Hawaii—Supported NG911 readiness assessment
- State of Arizona—Supported development of ESInet/NGCS RFP requirements
- Louisiana 911 Director's Consortium—Provided ESInet/NGCS procurement support through vendor due diligence and RFP development
- North Central Texas Emergency Communications District—Developed CHE RFP requirements

Additional Experience

- Chair, ATIS Emergency Services Interconnection Forum
- Co-Chair, ATIS ESIF Next Generation Emergency Service Subcommittee
- Co-Chair, NENA 9-1-1 Core Services Committee
- Chair, NENA Spoofing Mitigation Working Group
- Co-Chair, NENA Demarcation Points Working Group

Industry Experience

40 years

Education

M.S., Engineering-Economic Systems, Stanford University, California

B.S., Mathematics, Manhattan College, New York

Certifications

Emergency Number Professional (ENP)

Associations

National Emergency Number Association (NENA)

Kyra Pulliam, ENP

Project Manager, Mission Critical Partners

Kyra is a seasoned professional with a background in public safety communications and consulting. Kyra has experience in targeted stakeholder outreach, support, and education via facilitated sessions and served as an operations supervisor in a busy 911 center in the metropolitan Washington, D.C. area. Her strengths include communications center operations and project management.

Representative Experience

Federal Experience

- U.S. Department of Transportation (USDOT), National 911 Program
    - Recommended Minimum Training Guidelines for Telecommunicators Update
    - Pre-hospital Blood Program Support

State/Regional Experience

- Association of Central Oklahoma Governments (ACOG)—Grant Program Development
- Maryland 9-1-1 Board—NG911 Commission and subcommittee support
- Maryland Association of Counties (MACo)—Subcommittee support
- Metropolitan Washington Council of Governments (MWCOG)—Co-location Feasibility, Continuity of Operations Planning (COOP)
- National Capital Region (DC, VA, and MD)—NG911 call overflow/abandonment playbook
- Oklahoma—NG911 consulting
- Pennsylvania Emergency Management Agency (PEMA)—NG911 support

City/County Experience

- Alexandria, VA—Workforce optimization
- City of Philadelphia, PA—Vesta translation upgrade support
- City of Longview, TX—Next Generation Core Services (NGCS) and Call Handling Equipment (CHE) RFP support
- Dorchester County, MD—Training program development
- Oakland County, MI—CHE RFP support
- Pottawatomie County, OK—911 Assessment
- Salt Lake Valley, UT—Organizational Health Assessment
- Salt Lake City, UT—Organizational Health Assessment

Additional Experience

- Managed communications team, program website, and program stakeholder outreach efforts
- Liaison with the program legal team, aligning the website, and handling inquiries from stakeholders to contact center personnel/dispute resolution
- Updated training program content, requirements for career progression, and provided effective trainee/trainer evaluations
- Launched a critical incident stress management peer support team to support fellow dispatchers following September 11, 2001

Industry Experience

41 years

Certifications

Emergency Number Professional (ENP)

National Incident Management System/ Incident Command System (NIMS/ICS)—022, 100, 100B, 200B, 247A, 546A, 700, 800B courses

Associations

Association of Public-Safety Communications Officials (APCO)

National Emergency Number Association (NENA)

Pricing

Professional services outlined in the scope of work for **Phase 4** will be provided for a **fixed fee of $233,220**, including expenses.

The cost for services is detailed in the table below based on MCP's knowledge of similar efforts in scope and size across the nation:

Service	Hours	Price
Program Management	120	$37,920
Project Management	300	$78,900
Technology SMEs	400	$116,400
Phase 4: NG911 Implementation Support		**$233,220**

These services are provided under the State of Oklahoma – Deliverable Based Information Technology Services SW1050MI.

Mission Critical Partners recognizes that it is responsible for costs related to the project. Any additional services contracted in subsequent years will be performed at MCP's then-current fee schedule. Prior to initiating any such additional work, MCP would require a formal letter of authorization from the Oklahoma 911 Management Authority.

An invoice shall be submitted each month and include the percentage of work completed relevant to the fee and shall be reviewed and paid within 30 days of receipt.

Based on the current MCP understanding of what is to be accomplished, the pricing identified above represents an estimate of the work anticipated to achieve project success. MCP's priority is for this project to be successful for the Oklahoma 911 Management Authority.

GOLD FLAME

CONFERENCE

Igniting Excellence in Emergency Communications

SCHEDULE AT A GLANCE

TIME	TUESDAY, NOVEMBER 3	TIME	WEDNESDAY, NOVEMBER 4
	OPENING KEYNOTE -		***PANEL DISCUSSION -***
9:00 AM	Leading the Way: Organizational Wellness in Emergency Communications - Michelle Lily	**9:00 AM**	Creating a Culture that Thrives in 9-1-1 - Jamison Peevyhouse, Monica Milion, Leslie Whitham, Jennifer White
10:15 AM	• Peak Resiliency and AntiFragility - JC Ferguson • The Power of Your Passion - Sara Weston	**10:15 AM**	• The Art of Communication: Giving and Receiving Feedback - Dru Clarke • Leveraging Public Speaking for Career Advancement - Derek Dugas
11:30 AM	• Changing Perception. Strengthening Support. Advancing 9-1-1 - Laura Ehrhart • The Anchor Approach: Crisis Call Taking -Brandi Powell	**11:30 AM**	• Effective Strategies for Dealing with Workplace Conflict - Jason Long • The Imposter Within: Real Stories. Real Strategies -Jen Poole
1:30 PM	• Never Forgetting: A Story of September 11th and Beyond - Chris Carver • Owning the First 600 Seconds: Elevating T-CPR in 9-1-1 - Dawn Shumway	**1:30 PM**	• Leading With Empathy Without Losing Authority -Shantelle Oliver • Stop Training the Symptom: Build a Performance-Focused Culture in 9-1-1 -Dominique Mathis
2:45 PM	***PANEL DISCUSSION -*** Wellness, Retention, and Supporting the Modern ECC Professional - Joe Serio, Steve Martini, Julianna Davis, Kim Anderson	**2:45 PM**	***CLOSING KEYNOTE -*** Leave A Legacy -Doug Showalter

FRANKLIN, TENNESSEE | NOVEMBER 3-4 2026

OKLAHOMA 911 MANAGEMENT AUTHORITY - OPERATIONS COMMITTEE

2026 OKLAHOMA PUBLIC SAFETY CONFERENCE COURSE INFORMATION

Course Name:

Suicide Intervention

Instructor:

Public Safety Group

Course Description:

A one-day interactive class designed to educate Public Safety call-takers in crisis intervention. Topics include: Suicide Attitudes, Risk Assessment of Caller, Risk Assessment of Responder, and Call-Taker Intervention.

Course Name:

How Not to Eat Our Young: A Guide to Productive Mentoring

Instructor:

Foundations Public Safety

Course Description:

Explores the formal mentoring relationship and its distinction from education and general professional development. Highlights why mentoring is critical to leadership development and organizational culture. Participants engage in dialogue about mentoring successes and challenges while gaining practical strategies to improve mentoring effectiveness – a role that strengthens both the mentor and mentee.

9-1-1 Technology Roadmap

Date Approved: August 13, 2025

Version: 2.0

Vision

- To build a resilient, interoperable, and future-ready emergency communications system that ensures rapid response, seamless coordination, and public safety across Oklahoma.

Strategic Priorities

1. Statewide Mapping & GIS Integration

Objective

- Establish a unified, accurate, and continuously updated statewide GIS dataset to support 9-1-1 operations.

Key Actions

- Standardize address data collection and maintenance across jurisdictions.
- Deploy a central GIS repository accessible by all PSAPs.

Pros

- Improves caller location accuracy and response times.
- Creates consistency and eliminates data silos.
- Supports Next Generation 9-1-1 (NG9-1-1) compliance.

Cons

- High upfront cost for data remediation and repository setup.
- Requires ongoing coordination between multiple agencies.

2. Satellite Emergency Communication Infrastructure

Objective

- Ensure uninterrupted emergency communication during outages of terrestrial networks.

Key Actions

- Identify strategic locations where emergency satellite terminals can be available.
- Train staff on usage, testing, and maintenance.
- Develop a policy for deployment, usage, and operational needs.

Pros

- Provides redundancy during outages of cellular and landline systems.
- Critical for rural, remote, and disaster-affected areas.
- Independent of terrestrial infrastructure.

Cons

- Ongoing subscription and service costs can be high.
- Limited coverage indoors or in heavily obstructed areas.
- Requires periodic testing to maintain readiness.

3. Push-to-Talk (PTT) Technologies

Objective

- Enable secure, real-time voice communication across agencies and jurisdictions.

Key Actions

- Deploy PTT over LTE and/or LTE/FirstNet for interoperable communication.
- Integrate with legacy radio systems to ensure compatibility.
- Establish common talk groups and protocols for multi-agency incidents.
- Ensure the application and device are vendor agnostic.

Pros

- Faster coordination between agencies and responders.
- Scalable and cost-effective compared to traditional radio systems.
- Enhances interoperability during multi-jurisdictional incidents.

Cons

- Dependent on cellular/LTE coverage for reliability.

- May require device upgrades or new equipment.
- User adoption and training are critical for success.

4. CAD-to-CAD

Objective

- Deploy a CAD-to-CAD model that allows all PSAPs within the State of Oklahoma to connect their CAD systems to a centralized hub.

Key Actions

- Establish seamless CAD-to-CAD interoperability between:
  - Public Safety Answering Points (PSAPs)
  - Emergency Communications Centers
  - Response agencies
- Improve incident response coordination across jurisdictions.
- Reduce call-processing delays.
- Eliminate redundant data entry.
- Enhance situational awareness for all participating entities.
- Utilize a cloud-hosted design to eliminate single points of failure for all participants.

Pros

- Faster dispatch and response times.
- Elimination of duplicate call entry.
- Improved accuracy and situational awareness.
- Better data for analytics and quality assurance.
- Stronger mutual aid and interoperability.

Cons

- High maintenance fees.
- Complex integration.
- Increased points of failure.
- Training challenges.
- Data duplication and/or conflicts.
- Multiple interfaces increase exposure to cybersecurity attacks.

5. Computer-Aided Dispatch (CAD)

Objective

- Deploy Computer-Aided Dispatch (CAD) systems for all PSAPs to support effective emergency response operations.

Key Actions

- Provide a cost-effective, cloud-hosted CAD platform that supports resource management and call-for-service tracking, with reporting capabilities to a database managed by OSBI.
- Support optional, upgradeable features, including:
    - Two-tone and fire station alerting
    - NCIC records checks with multi-factor authentication (MFA)
    - 9-1-1 CHE integration
    - Paging capabilities
    - iOS and Android mobile applications with AVL/GPS

Pros

- Provides a true CAD solution to agencies that currently lack one.
- Upgradeable and compatible with other systems already in use statewide.
- Cloud-hosted architecture increases uptime during outages or COOP activations.
- Faster implementation compared to on-premises solutions.
- Improves data security while eliminating the need for individual agencies to maintain primary databases.
- Data can be replicated to an OSBI-hosted server to support statewide and agency-specific reporting.
- Agencies are not required to purchase features they do not need or cannot afford.

Cons

- Even with modular, upgradeable features, the overall cost may remain significant.
- Training requirements are both a benefit and a challenge; training documentation must be developed and maintained and should not be the sole responsibility of the vendor.
- A governance body will be required to make configuration, policy, and operational decisions.
- Participating agencies must reach consensus on standardized call type codes, unit naming conventions, and administrative access protocols.

6. Call Handling Equipment (CHE)

Objective

- Implement standardized, NG911-compliant Call Handling Equipment (CHE) that meets the NENA i3 Standard, enabling Public Safety Answering Points (PSAPs) to receive, process, and manage emergency communications over an IP-based network while improving interoperability, resiliency, cybersecurity, and support for current and future emergency communication technologies.

Key Actions

- Develop statewide CHE standards to ensure interoperability.
- Procure a list of state approved CHE vendors that meets current NENA i3 standard.
- Integrate CHE with the Emergency Services IP Network (ESInet) and Next Generation Core Services (NGCS).
- Develop migration plans to minimize service interruptions during cutover. interoperability and acceptance testing prior to deployment.

Pros

- Supports voice, text-to-911, images, video, and future multimedia communications.
- Improves interoperability between PSAPs and neighboring jurisdictions.
- Enables seamless transfer of calls and associated data.
- Supports remote call-taking during emergencies or disasters.
- Improves caller location accuracy through NG911 data integration.
- Reduces reliance on aging legacy telephone infrastructure.

Cons

- Significant upfront procurement and implementation costs.
- Requires reliable, redundant broadband connectivity.
- Training requirements for telecommunicators and technical staff.
- Migration may temporarily increase operational workload.
- Vendor interoperability may vary without standardized requirements.
- Ongoing software licensing and maintenance costs.
- Cybersecurity responsibilities increase as systems become more IP-based.

Oklahoma 9-1-1 Management Authority
FY2027 Grant Program Guidelines Changes
(Proposed Changes Highlighted in Yellow Below)

PURPOSE

In 2016 the Oklahoma legislature passed HB 3126. This legislation authorizes the Oklahoma 9-1-1 Management Authority to administer grants for the purpose of:

1. Assisting public agencies with funding for consolidation of facilities or services;
2. Deployment of Phase II or successor technology;
3. Development of NG911 regional emergency service networks;
4. Other purposes the Authority deems appropriate and necessary.

The goal of the grant program is to provide the highest quality of 9-1-1 services to the citizens of Oklahoma.

APPLICATION DEADLINES/PERIOD OF PERFORMANCE

Rolling Deadlines: Grant applications may be submitted at any time. Applicants can track the application progress in EMGrants. Typical processing time is 60-90 days. Applications will be accepted until June 30, 2027 or until funding is depleted. Period of Performance: The period of performance for the FY2027 Grant Program is July 1, 2026 – June 30, 2028. Grant projects must be completed and closed out no later than June 30, 2028.

WHO IS ELIGIBLE TO APPLY?

Only governing authorities of a primary Public Safety Answering Point (PSAP) will be eligible to apply for this grant as authorized by O.S. §63-2864.5. All applicants must also be an eligible entity of local government or tribal organization as defined in 47 CFR §400.2 to apply for the Oklahoma 9-1-1 Management Authority grant. Eligible entities include primary PSAPs including:

1. City, County, and Tribal Governments;
2. City or County Fire Departments;
3. City or County Law Enforcement Agencies;
4. Councils of Governments (COGs);
5. Public Districts, Public Trusts, and Public Authorities;
6. Other governmental entities that provide 9-1-1 services.

~~**Please note: PSAPs are eligible to only apply in the GIS category unless their local GIS data has been successfully uploaded to the State repository.**~~ **(Can be removed?)**

ELIGIBLE PROJECTS

The Oklahoma 9-1-1 Management Authority has determined that the following projects will qualify for consideration for grant funding. Funding can be used for the purpose of developing a plan, purchasing equipment, hardware or software, procurement of services to create a final product, or payment of one-time expenses related to the following:

1. **Geographic Information Systems (GIS)** – Creation, maintenance, or improvement of GIS maps to meet or exceed the OK Geographic Information NG911 and Addressing Standard as outlined in State contract (SW1177), including any hardware and/or software needed. **Computer Aided Dispatch (CAD) GIS** – this may include hardware, software or aliasing necessary to ensure that the location received during a 911 call matches the location within the CAD system, this only includes the initial cost and not the maintenance of the CAD GIS components or periodic updates.

2. **Consolidation** – Consolidation or virtual consolidation of call centers; **Capital Improvement Projects (eligible as part of a Consolidation Only)** – including new buildings, additions, or renovations of existing buildings (maximum State contribution allowed is $400,000). **Radio Tower (eligible as part of a Consolidation Only)** – located at the 911 center that is necessary to ensure the call is delivered (including toning) to the proper police, fire and/or EMS.

3. **NG9-1-1 Deployment** – Development or deployment of NG9-1-1 technology to meet the State NG9-1-1 deployment plan. This includes NG9-1-1 recording equipment and Call Handling Equipment (CHE). For all CHE requests, funding is limited to a maximum of $100,000 per position for a five (5) year cost funded at 80% state/20% local match. Also, a total amount (maximum) of $2.5 million per grantee can be awarded per year. [See below for more details].

4. **Training & Protocols** – Call taker training and certification; 9-1-1 administrator training; Protocols, including necessary hardware and software.

5. **Computer Aided Dispatch (CAD)** – CAD systems that are GIS centric; Emergency Incident Data Object (EIDO) (i3) capable; and/or a universal hub or data sharing server/cloud services that are used to share data between CAD systems. Custom, one off, CAD to CAD interfaces do not qualify for this category. **ASAP to PSAP** – A CAD interface to receive Automated Secure Alarm Protocol (ASAP) to CAD systems for alarm reporting from alarm monitoring services.

6. **Continuity of Operations Plan (COOP)** – Tools and/or technology necessary to mitigate any gaps within COOP necessary to mitigate the downtime in the delivery of 9-1-1 call processing. (PSAP must submit their current COOP to qualify for this category).

7. **Radio Consoles** – Radio consoles and necessary radios needed by the console to transmit 911 calls to the local or state radio system. Please Note: only public safety grade radios on the Authorized Equipment List (AEL) are eligible for funding. AEL link for grant approved radio equipment: https://www.dhs.gov/science-and-technology/approved-grant-eligible-equipment. **Encoding or Toning Equipment** necessary to deliver the call to the proper police, fire and EMS agency.

8. **ADA Compliant Equipment** – Furniture/chairs necessary to provide the proper ergonomics to reduce on the job injuries related to the stationary sitting common in 24/7 call centers; **ADA Compliant Structural Modifications** – modifications to existing structures such as entrances, ramps, doorways, and restrooms to allow access for physically disabled employees.

9. **Cybersecurity Penetration Testing** – To offer PSAPs comprehensive guidance and remediation strategies in preparation for the deployment of NG911 in Oklahoma. Penetration testing (pen testing) is a controlled and authorized simulation of a cyberattack on systems, networks, or applications. The main objective is to help organizations identify security weaknesses that can be exploited my malicious actors in a controlled environment.

MATCHING FUNDS REQUIREMENT

No in-kind match will be accepted - the match must be monetary (cash) unless the applicant demonstrates the inability to provide matching funds. A 20% cash match of the total project cost is required for all grant categories with the following exceptions: GIS and Training & Protocols grants are funded 100% with no match required.

INELIGIBLE EXPENSES*

The following are **NOT** eligible for funding through the 9-1-1 Management Authority grant program:

1. Costs to operate 9-1-1 systems; purchase and/or maintenance of radios unless the radio is necessary to connect to the radio consoles in order to transmit 911 calls to local or state radio system.

2. In field radios/subscriber units (Mobile and Portable radios).
3. Radio infrastructure outside of the items specifically related to consolidation or the components of the radio consoles listed under Eligible Projects (above); this includes repeaters, combiners, towers, radio tower buildings, etc.
4. Construction/capital improvement projects not related to consolidation and/or outside of construction projects listed in Eligible Projects.
5. Purchase of buildings; building operating costs including rent, utilities.
6. Purchase of vehicles; vehicle maintenance costs.
7. Oklahoma Law Enforcement Telecommunications System (OLETS/NCIC).
8. General administrative costs including salaries and wages.
9. Purchases or purchase agreements entered into prior to grant award.
10. Costs associated with any college or university degree, such as tuition, fees, etc.
11. Costs associated with prizes; fundraising events/expenses.
12. Outside of the state of Oklahoma travel expenses (except in rare cases).
13. Grant writer fees.
14. Fines/penalties/taxes; offsetting of debt; legal or audit fees; lobbying expenses.
15. Food/refreshments.
16. Decoding equipment used by field responders.
17. Cybersecurity vulnerability assessments, which are completed by the OK911MA Cybersecurity Specialist upon request.

*This list is not all-inclusive, final determinations will be made on a case-by-case basis by the Oklahoma 9- 1-1 Management Authority.

GRANT FUNDING LIMITATIONS

1. For all grant categories, only the first year of maintenance, warranty or system support will be considered for funding; future years are ineligible for funding. Additionally, the applicant must demonstrate the ability to maintain the project financially in future years.
2. Applicants are not eligible to apply for any product (including software, hardware, equipment, etc.) that has received funding through the Oklahoma 911 Management Authority Grant Program within five (5) years of the initial grant award.
3. Only after an award has been made and a State & Local Agreement (SLA) has been signed by the OEM Director and the local authorized contact may funds be expended by the applicant.
4. Applicants may submit no more than one (1) application per category per fiscal year.
5. No general planning excluding consolidation, administration, or promotional activities will be funded.
6. Assets funded by this grant must located on property either owned by or leased to the applicant or partnering entity.
7. Successful applicants will be required to submit a change request in EMGrants for approval prior to any changes being made to the project.
8. Funding Limitation – A total amount (maximum) of $2.5 million per grantee can be awarded per year.
9. Radio Console Category - only public safety grade radios on the Authorized Equipment List (AEL) are eligible for funding. AEL link for grant approved radio equipment: https://www.dhs.gov/science-and-technology/approved-grant-eligible-equipment.

NG9-1-1 GRANTS (CHE Grants Only)

In support of the rules outlined in the Federal Communications Commission report and Order in the Matter of Facilitating Implementation of Next Generation 911 (NG911) Services, **the grant applicant must ensure** that the provider of the requested Call Handling Equipment (CHE) solution must agree and include in the contract that they will support the transition to NG911 utilizing the State provided EsiNet and i3 Core Service when it becomes available. The provider must also agree and include in the contract that they will certify the grant funded CHE using the State provided testing lab. This includes any modifications or upgrades required to ensure the CHE is technically ready to receive 9-1-1 calls and texts in the IP-based format and the requirement

set forth in policy and rules set forth by the Oklahoma 911 Management Authority.

In addition, CHE solution providers must commit to facilitating and completing connectivity testing with Originating Service Providers (OSPs) within the compliance timeframe applicable to the OSP. Applicants must upload a copy of the draft contract with the CHE provider with their application and note the section number and/or page number on the contract that agrees to the above requirement. After the grant has been awarded and an SLA (grant contract) has been signed, the applicant must upload a copy of the signed contract including these terms. Failure to upload the contract within 90 days of the grant approval may result in a delay in payment or the grant being withdrawn.

GIS GRANT REQUIREMENTS

GIS grant funding must be used to bring GIS data to the OK Geographic Information NG9-1-1 and Addressing Standard for uploading into the State 9-1-1 repository. PSAPs that want to partner with an eligible governing body as defined within these guidelines may also be approved for a grant for GIS remediation services, hardware, software and maintenance.

All GIS applicants are required to use one of the vendors listed on Oklahoma State contract SW1177 that have been vetted by the Oklahoma 9-1-1 Management Authority as a result of competitive bidding. All GIS applications should include a minimum of two quotes from the vendors listed on State contract.

Throughout the duration of the grant, the vendor shall provide monthly written reports to the local PSAP regarding the progress of the mapping project. The progress report will indicate the percent complete of mutually pre-determined milestones and tasks. The following milestones shall be included: assessment, centerline, map point, polygons, validation using the State tool, and upload or delivery of completed work to the state. The vendor's recommended milestones and associated tasks should be included in the vendor's quote. The agency reserves the right to include additional milestones and/or tasks prior to the finalization of a contract. The agency must include this milestone progress information in the required quarterly reports. Final payment is contingent upon all milestones being completed. GIS applicants are eligible to apply for one year maintenance costs from their state approved vendor.

CYBERSECURITY GRANT REQUIREMENTS

All Cybersecurity applicants are required to use one of the vendors listed on Oklahoma State contract SW1042 (see SW1042 here: Central Purchasing: Division of Office of Management and Enterprise Services (OMES) - Solicitations). The state cybersecurity vendors are: Go Security Pro; CBIZ Risk & Advisory Services; Elegant Enterprise Wide Solutions; Soft Stages; and True Digital Security. All Cybersecurity applications should include a minimum of two quotes from the vendors listed on State contract. All cybersecurity applicants must define the scope of the project. The penetration test may include but not limited to: internal network(s), external network(s), wireless network(s), social engineering, web applications, and mobile apps.

APPLICATION SUBMISSION & AWARD PROCESS

The 9-1-1 grant is a competitive grant. If the submitted grant application package does not meet the requirements set forth in these guidelines, the grant application will not be considered. Failure to comply with any of the required application steps may disqualify the application from funding. Applications shall be submitted online through EMGrants and contain the following:

1. Project narrative, including an explanation of how this project will achieve compliance with the goals and objectives of the Oklahoma 9-1-1 Management Authority;
2. Explanation of proposed method of funding the cash match requirement;
3. Project timeline (milestones);
4. Most recent fiscal year PSAP budget;
5. Resolution from the Local Governing Authority;
6. Vendor Quote(s);
7. Vendor Brochure(s);

8. Local 9-1-1 Deployment Plan – if deploying initial E911 Phase II;
9. **GIS Applications Only** – a signed GIS Memorandum of Understanding between the applicant and the Oklahoma 9-1-1 Management Authority is required if not already on file. All GIS applications must also include a signed commitment from the GIS remediation provider to comply with all technical requirements of state contract SW1177 as stated in its RFP;
10. **Consolidation Applications Only** – consolidation grant applicants must provide the information listed in the Master Plan for Deployment checklist. If requesting a Radio tower at the 911 center location, an independent coverage study must be included showing the current radio coverage for the County on each necessary frequency needed for primary and backup operations.
11. **Training Grant Applications Only** – training grant applicants must submit a Training Grant Questionnaire found at (www.ok.gov/911) with all Training grant applications.

Grant awards are made solely at the discretion of the Oklahoma 9-1-1 Management Authority. The Authority may choose to modify the amount of any grant request. Each applicant will be notified via EMGrants of the Authority's funding decision for each grant application.

GRANT REIMBURSEMENT

The 9-1-1 Grant Program is a reimbursement grant. Invoices must be paid up front by the awardee Funds will be reimbursed only with confirmation that invoices have been paid in full. Proof of payment documentation required to receive reimbursement includes: (1) copies of the front **and** back of cancelled checks; or bank statements; and invoices.

Applicants generally must have a minimum of $5,000 in reimbursable expenses in order to request a reimbursement (payment); however, final closeout payment may be less than $5,000. For project awards less than $5,000, applicants must request one draw for the total amount of the project. Reimbursement requests will generally be processed within seven (7) business days; however, please allow up to twelve (12) weeks to receive payment.

All 9-1-1 grant reimbursements must be: (1) deposited back to the account that the grant invoices were paid from originally; or (2) deposited in the account that has been designated by the governing body to carry out the requirements of the Oklahoma 9-1-1 Management Authority Act as required by State Statute 63-2868.C.

63-2868.C. states, "Money remitted to public agencies pursuant to the Oklahoma 9-1-1 Management Authority Act and any money otherwise collected by any lawful means for purposes of providing 9-1-1 emergency telephone services shall be deposited in a separate 9-1-1 emergency telephone service account established by a public agency or its governing body to carry out the requirements of the Oklahoma 9-1-1 Management Authority Act.

Failure to abide by State Statute 63-2868.C. is considered diversion of 9-1-1 fee revenues which is a violation of state and federal rules, regulations and laws.

Prior to applying for a grant, please ensure that you have the following: (1) an EIN number; (2) an updated SAM.gov registration; and a (3) state Vendor Number for EFT direct deposit. All grant awardees must enroll in the Oklahoma State Treasury EFT (direct deposit) system in order for payments to be made.

ONLINE GRANT APPLICATION

To register for access or to log in to the online application system, OEMGrants, go to ok.emgrants.com.

QUESTIONS?

Contact Karen Douglas, 9-1-1 Grants & Compliance Officer karen.douglas@oem.ok.gov
(405) 833-4959

STATE APPROVED GIS VENDORS

GEO-COMM, INC
Stacen Gross, Territory Sales Manager
1100 W. Saint Germain St.
Saint Cloud, MN 56301
Phone: 320.281.2186
www.geo-comm.com

SURVEYING AND MAPPING (SAM)
Kimberly Myers, Project Manager
501 N. Market Street
Maryville, MO 64468
Phone: 620.617.5915
www.sam.biz

SPATIAL DATA RESEARCH
Penny Knight, Vice President
PO Box 684
Olathe, KS 66051
Phone: 800.238.1911, ext 701
www.sdrmaps.com

DATAMARK/MICHAEL BAKER INT'L
Robert Murphy, AVP, Director of Business Development
2316 Killearn Center Blvd
Tallahassee, FL 32309
Phone: 412.512.4407
www.mbakerintl.com

STATE APPROVED CYBERSECURITY VENDORS

Go Security Pro
Geoffrey Wilson, CEO & Founder
3527 E 102nd ST
Tulsa, OK 74173
Phone: (877) 909-0507
Email: geoff@gosecuritypro.com

CBIZ Risk & Advisory Services
Tiffany Garcia, Managing Director
11044 Research Boulevard Suite C500
Austin, TX 78759
Phone: (512) 340-7423
Email: tiffany.garcia@cbiz.com

Elegant Enterprise Wide Solutions
Vikas Arora, Sr. Program Manager
25961 Hartwood Dr
Chantilly, VA 20152
Phone: (703) 909-1289
Phone: (703) 722- 0603
Email: govt@elegantsolutions.us

Soft Sages
Rohan Patel
20 Mystic Lane 2nd Fl
Malvern, PA 19355
Phone: (484) 321-8314
Email: rohan@softsages.com

True Digital Security
Angela Baker, Account Executive
PO Box 35623
Tulsa, OK 74153
Phone (405) 400-7418
Email: Angela.baker@ciso.inc

Oklahoma 911 Management Authority

Grant Approval Form

Organization Information

Applicant Organization Name: Elk City, City of

Address: PO Box 1100, Elk City, OK, 73648-1100

Phone: 580-562-5041

Email: lisa@swoda.org

County:	**Type:**	**DUNS#:**	**EIN#:**
Beckham	City or Township Govt	135800675	73-6005191

Primary Contact Name/Title:	**Authorized Contact Name/Title:**
Elesia Church (Grant Writer/Administration)	Micah Kilhoffer (Mayor)

Project Information

Project Title: Elk City PD – 911 Radio Project

Project Type:	**Project Category:**
Radio Consoles (911 Use Only)	Radio Consoles (911 Use Only)

Brief Project Description: The Elk City Police Department is requesting funding under the Radio Consoles/NG911 Deployment category to procure and implement an additional dispatch console workstation. This request does not include the purchase of any radios.

Request Amount:	**Award Amount:**	**Project Start Date:**	**Project End Date:**
$17,138.00	$17,138.00	July 1, 2026	October 29, 2026

Approvals - Required Signatures ☐ Approved ☐ Not Approved

911 Management Authority Chair	**Date**
911 State Coordinator	**Date**

State Office Use Only

Funding Sources
a. Federal $0.00
b. State $13,710.40
c. Local $3,427.60
d. Other
e. TOTAL $17,138.00

Oklahoma 911 Management Authority

Grant Approval Form

Organization Information

Applicant Organization Name: Hobart, City of

Address: PO Box 231, Hobart, OK 73651-0231

Phone: 580-726-2424

Email: chiefofpolice@hobartok.gov

County:	**Type:**	**DUNS#:**	**EIN#:**
Kiowa	City Government	102388089	73-600256

Primary Contact Name/Title:	**Authorized Contact Name/Title:**
Strider Estep (Chief of Police)	Strider Estep (Chief of Police)

Project Information

Project Title: Hobart NG911 Recording System

Project Type: NG911 Deployment

Project Category: Recorders/Loggers/Call Handling Equipment

Brief Project Description: Request is to update our recorder as our current one is not fully compatible with NG911 infrastructure. As regional partners transition to NG911, it is critical that Hobart's 911 system be upgraded to ensure interoperability, reliability, and continued delivery of emergency services to the public.

Request Amount:	**Award Amount:**	**Project Start Date:**	**Project End Date:**
$44,196.00	$44,196.00	April 5, 2026	Oct 30, 2026

Approvals - Required Signatures ☐ Approved ☐ Not Approved

911 Management Authority Chair	**Date**
911 State Coordinator	**Date**

State Office Use Only

Funding Sources
a. Federal $0.00
b. State $35,356.80
c. Local $8,839.20
d. Other
e. TOTAL $44,196.00

Oklahoma 911 Management Authority

Grant Approval Form

Organization Information

Applicant Organization Name: Osage County

Address: PO Box 1569, Treasurer's Office, Pawhuska, OK 74056-1569

Phone: 918-287-4911

Email: kkelleyoc1@gmail.com

County:	**Type:**	**DUNS#:**	**EIN#:**
Osage	County Government	078665288	73-6006403

Primary Contact Name/Title:	**Authorized Contact Name/Title:**
Kay Kelley (911 Director)	Kay Kelley (911 Director)

Project Information

Project Title: Osage County EMD

Project Type: Training & Protocols	**Project Category:** Protocols

Brief Project Description: Upgrading the EMD program will help maintain the highest quality 911 service possible. Given Osage County's large rural landscape, this upgrade is highly beneficial to both EMS services and residents, ensuring better emergency response and support.

Request Amount:	**Award Amount:**	**Project Start Date:**	**Project End Date:**
$95,609.65	$95,609.65	May 3, 2026	August 1, 2026

Approvals - Required Signatures ☐ Approved ☐ Not Approved

911 Management Authority Chair	**Date**
911 State Coordinator	**Date**

State Office Use Only

Funding Sources
a. Federal $0.00
b. State $95,609.65
c. Local $0
d. Other
e. TOTAL $95,609.65

Oklahoma 911 Management Authority

Grant Approval Form

Organization Information

Applicant Organization Name: Roger Mills County

Address: PO Box 708, County Treasurer, Cheyenne, OK, 73628

Phone: 580-303-6048

Email: chris.clift@rogermillsso.org

County:	**Type:**	**DUNS#:**	**EIN#:**
Roger Mills	County Government	011205531	73-6006413

Primary Contact Name/Title:	**Authorized Contact Name/Title:**
Christopher Clift (Dispatch Supervisor)	Christopher Clift (Dispatch Supervisor)

Project Information

Project Title: Govworx Training

Project Type: Training & Protocols

Project Category: General technology training

Brief Project Description: The proposed project will implement GovWorx CommsCoach HIRE and CommsCoach Simulations to strengthen the agency's ability to recruit, evaluate, hire, train, and retain qualified 9-1-1 telecommunicators.

Request Amount:	**Award Amount:**	**Project Start Date:**	**Project End Date:**
$2,900.00	$2,900.00	July 15, 2026	September 15, 2026

Approvals - Required Signatures ☐ Approved ☐ Not Approved

911 Management Authority Chair	**Date**
911 State Coordinator	**Date**

State Office Use Only

Funding Sources
a. Federal $0.00
b. State $2,900.00
c. Local $0.00
d. Other
e. TOTAL $2,900.00

Oklahoma 911 Management Authority

Grant Approval Form

Organization Information

Applicant Organization Name: Wagoner County

Address: 14608 S 385 E Ave, Coweta, OK 74429

Phone: 918-485-7727

Email: mketchum@wagonercounty.ok.gov

County:	**Type:**	**DUNS#:**	**EIN#:**
Wagoner	County Government	796675226	73-6006421

Primary Contact Name/Title:	**Authorized Contact Name/Title:**
Mark Ketchum (Director of Communications)	Mark Ketchum (Director of Communications)

Project Information

Project Title: Wagoner County CAD Modernization Project

Project Type: CAD

Project Category: Shared CAD systems

Brief Project Description: Wagoner County and Coweta 911 have partnered to implement a shared CentralSquare CAD system. This project will improve interoperability, real-time information sharing, and coordinated emergency response. The coalition is requesting $159,526.20 to support implementation, increasing efficiency, reducing costs, and strengthening public safety services across both jurisdictions.

Request Amount:	**Award Amount:**	**Project Start Date:**	**Project End Date:**
$159,526.20	$159,526.20	August 16, 2026	August 16, 2027

Approvals - Required Signatures ☐ Approved ☐ Not Approved

911 Management Authority Chair	**Date**
911 State Coordinator	**Date**

State Office Use Only

Funding Sources
a. Federal $0.00
b. State $127,620.96
c. Local $31,905.24
d. Other
e. TOTAL $159,526.20

ROHIT RAI
DIRECTOR

TIM TIPTON
DPS COMMISSIONER
HOMELAND SECURITY ADVISOR

STATE OF OKLAHOMA
OFFICE OF HOMELAND SECURITY

State of Oklahoma
Fiscal Year 2025 State and Local Cybersecurity Grant Program
Local Consent Agreement

I, _____ (print name), the duly appointed authorized agent on behalf of _____ (the "Local Government Entity"), located at _____ _____ (address) hereby expressly consent to the Oklahoma Department of Emergency Management/OK 911 Management Authority and the State of Oklahoma State Administrative Agency (SAA), the Oklahoma Office of Homeland Security a division of the Oklahoma Department of Public Safety, undertaking the following acts in accordance with the State and Local Cybersecurity Grant Program (SLCGP) for Fiscal Year (FY) 2025, Federal Award Number EMW-2025-CY- 05007, as authorized by Section 2220A of the Homeland Security Act of 2002, as amended (Pub. L. No. 107-296) (6 U.S.C. §665g):

1. Retain $ in SLCGP fund for FY 2025 at the State level; and
2. Utilize $ in SLCGP funds for FY 2025 as follows:
    a. $ for training.

This consent is given because it is in the best interest of the Local Government Entity and is provided without duress or fear of reprisal. This consent is only effective for the FY 2025 SLCGP Funds.

Signed, on _____ day, _____ month, and _____ year, in _____ Oklahoma.

_____
Signature

_____
Printed Name

_____
Title

FY2027 In-Person Training				
Total budget	**$ 250,000**			
Total Annual expense	**$ 247,750**			
Professional Development Pathway	Location	# of classes	Cost Per Class	Total
Annual training				
Dispatcher				
Advance Fire (2 day)	TBD	4	$ 8,750	$ 35,000
Advance Police (2 day)	TBD	4	$ 8,750	$ 35,000
Enhanced Caller Management (1 Day)	TBD	2	$ 4,400	$ 8,800
Preventing 911 Tunnel Vision (1 Day)	TBD	2	$ 4,400	$ 8,800
911 Customer Service (1 Day)	TBD	2	$ 4,400	$ 8,800
Total				**$ 96,400**
CTO				
CTO training (3 day)	TBD	3	$ 11,500	$ 34,500
Communication Center Liability (1 Day)	TBD	3	$4,500	$ 13,500
Total				**$ 48,000**
Supervisor				
Middle Management Leadership Training (3 days)	TBD	1	$ 8,900	$ 8,900
Lead, Follow, or Get Out of the Way	TBD	3	$ 4,500	$ 13,500
NENA Supervisor class (prereq for CMCP)	TBD	2	$ 11,000	$ 22,000
Total				**$ 44,400**
Technologist				
Demistifying NG911 Call Flow (2 days)	TBD	2	$ 8,000	$ 16,000
911: Hacked, Attacked and Where's That	TBD	2	6,475.00	$ 12,950
Total				**$ 28,950**
Director				
CMCP	TBD	1	$ 30,000	$ 30,000
Total				**$ 30,000**
GRAND TOTAL		**31**		**$ 247,750**

OKLAHOMA PUBLIC SAFETY JOB DASHBOARD

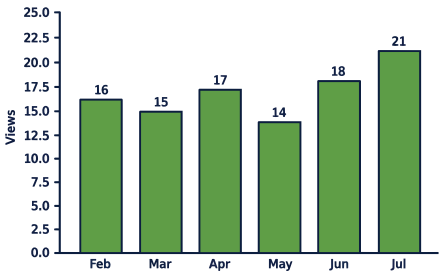
OVERVIEW
FEBRUARY 2026 - JULY 2026

KEY INSIGHTS

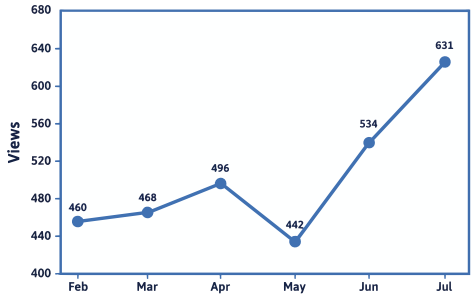
- 39 JOBS POSTED SINCE FEBRUARY
- 29 POSITIONS CURRENTLY ACTIVE
- MORE THAN 3,460 DASHBOARD VIEWS
- DASHBOARD TRAFFIC AVERAGES 21 VISITS PER DAY

TOTAL JOB APPLICATIONS	ACTIVE APPLICATIONS	EXPIRED APPLICATION	TOTAL DASHBOARD VIEWS	AVERAGE HOURLY SALARY
39	29	10	3,460	$18.45 PER HOUR

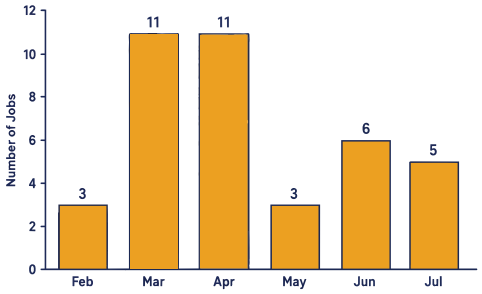
AVERAGE DAILY VIEWS



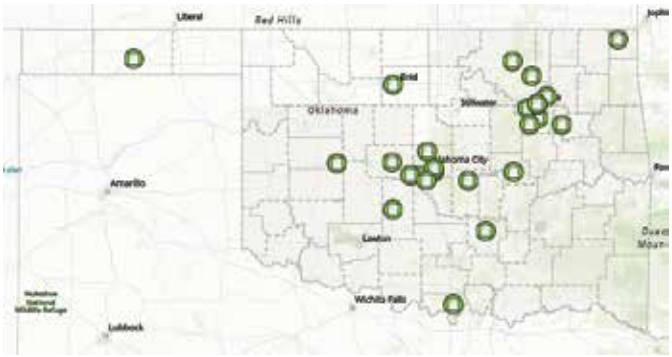
DASHBOARD VIEWS OVER TIME



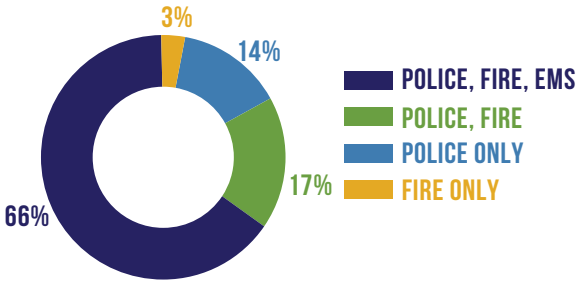
JOBS POSTED BY THE MONTH



ACTIVE AGENCY APPLICATIONS



JOBS BY MANAGES CALLS FOR



PARTICIPATING AGENCIES

AGENCIES WITH ACTIVE JOB POSTINGS

Ada/Pontotoc County 9-1-1
City of Chickasha 9-1-1
City of Lawton/Comanche County 9-1-
City of Midwest City 9-1-1
City of Tulsa Public Safety Communications
Coweta PD
Creek County 9-1-1
Edmond Public Safety Communications
El Reno PD
Love County E 9-1-1
Moore PD
Mustang PD
OHP - Enid
Okfuskee County/Okemah PD
Oklahoma City Community College Police
Oklahoma County Sheriff's Office
Osage County Sheriff's Office
Ottawa County 9-1-1
Owasso 911
Sand Springs 9-1-1
Shawnee 9-1-1
Skiatook PD
Stillwater PD
Texas County 911 Trust Authority
Tulsa 911
Weatherford PD

WE ARE HIRING

OKLAHOMA 911 MANAGEMENT AUTHORITY

GIS Project Coordinator

See full job description
and apply at
https://bit.ly/911projectscoordinator