
# CONSIDERATIONS FOR ESTABLISHING AGREEMENTS FOR NEXT GENERATION 911 (NG911)

Across the Nation, federal, state, local, territorial, and tribal (FSLTT) agencies are updating 911 systems to digital or Internet Protocol (IP)-based systems, known as NG911. NG911 enables a dynamic and resilient means of sharing information between citizens and public safety agencies across all disciplines. NG911 capabilities may include voice, data, and video communications. Collaboration across public safety agencies is critical to coordinate response efforts and provide greater situational awareness to promote first responder safety and protect citizens. Memorandums of understanding/agreements (MOU/As) can help FSLTT agencies interconnect to ensure a fully operable, interoperable, and secure NG911 ecosystem.

To assist agencies in the transition to NG911, the Emergency Communications Preparedness Center (ECPC) developed a considerations document for establishing MOU/As between FSLTT agencies. Written agreements provide agencies an opportunity to collaborate on mutually essential emergency response capabilities and resources. MOU/As facilitate clarity, transparency, and accountability through joint policies and procedures and clearly defined roles and responsibilities.

The ECPC Federal 911 Working Group conducted interviews with FSLTT stakeholders to develop this Considerations for Establishing Agreements for NG911 document. Paired with the ECPC's MOU/A Template, this document provides sample language and highlights considerations for establishing agreements for NG911, such as defining roles and responsibilities, resources and services, and technical requirements.

## GOVERNANCE

Agencies should consider including a governance section in agreements to establish the scope, direction, and execution of the MOU/A. The governance section establishes processes for maintaining the agreement. It provides oversight through compliance with FSLTT laws, guidelines, standards, policies, permits, and licenses applicable to the agreement.

### Governance Considerations

#### *Escape Clauses*
Identify a time frame either party may choose to terminate an MOU/A or specify in advance notice with optional alternatives in writing to authorized parties involved.

#### *Non-Performance*
Consider including non-performance clauses.

#### *Forms of Acceptable Notice/Terms of Transitioning Status*
Include terms or conditions that would trigger a review of the MOU/A, such as potential emergency communications center (ECC)/public safety answering point (PSAP) consolidation, closures, or realignments. Agencies should consider outlining acceptable forms of notification in agreements (e.g., telephone, email, or U.S. Mail).

#### *Notice Parameters*
Specify in writing the time parameters (e.g., days or months) and conditions for reaching triggers to revise, terminate, or renew the MOU/A.



ecpc@cisa.dhs.gov

### *Termination Requirements/Revision*
Identify requirements and authorities for terminating or revising agreement.

### *Procurement Laws*
Review FSLTT procurement laws to determine funding restrictions, purchasing authority for contractors, or acquisition of goods and to ensure the agreement does not violate applicable procurement laws.

## TECHNICAL-SYSTEM DETAILS

During the NG911 migration, there are various technical requirements to address when interconnecting NG911 systems. For example, geographic information system (GIS) capabilities are critical for location accuracy, call routing, and delivery of 911 calls to ECCs/PSAPs.

### Technical Considerations

### *Demarcation Point*
Determine demarcation points or mutually defined boundaries dividing areas of responsibility.[1] All parties involved in an MOU/A must agree on the location. In some instances, regulations or industry standards may determine or provide guidance on the demarcation point. The configuration may impact the NG911 network and/or cost obligations.

### *Access*
**Identity, Credential, and Access Management (ICAM)**
Establish a comprehensive approach for ICAM to protect against physical and cyber threats.

**Criminal Justice Information System (CJIS)**
Identify resources for ECCs/PSAPs, military installations, and partners, when authorized, to access criminal justice information required to protect and serve the community. Determine how information sharing between military installations and ECCs/PSAPs can be done in real-time, while also protecting sensitive data. Considerations may include location of CJIS equipment and having authorized access controls in place. MOU/As should align with laws, rules, or regulations surrounding access to or sharing of criminal justice information.

**Circuit Access to Military Installations**
Determine who has authorized access to military installations with well-defined security protocols and access control guidelines based on installations requirements for contractors, partner agencies, and "least privilege" information technology (IT) access.

### *Interoperability Interfaces*
Define policies to ensure NG911 systems and upgrades are compatible with ECCs/PSAPs and federal NG911 systems. System hardware interfaces and software applications selected independently by partner agencies must interconnect to control data and information exchange during implementation, access, testing, and auditing, without restrictions.

### *Non-Disclosure Agreements (NDAs)*
Consider an NDA, where parties agree not to discuss or share confidential information outside authorized parties.

### *Data Management*
Develop policies to address increased receipt of data, such as photos, videos, and text messages from the public. The MOU/A should outline requirements for receiving, sharing, storing, and securing data. The MOU/A should provide a clear understanding of who owns data, how long it will be retained, and requirements for partner agencies to access data.

[1] National Emergency Number Association (NENA), Master Glossary of 911 Terminology, last accessed May 6, 2022.

### *Cybersecurity*
Establish policies and procedures to protect and secure NG911 systems and data from physical and cyber threats and vulnerabilities. Conduct cyber risk assessments and develop cyber incident response and vulnerability response plans.

## OPERATIONAL

It is imperative for each agency to determine how they will respond during routine and emergency response situations to seamlessly share information. Equipment redundancy, technology upgrades, and continuity of communications are important factors. Agencies will need to develop plans to respond to and notify partners of incidents, such as cyberattacks or outages caused by weather events.

### Operational Considerations

#### *Activating/Deactivating Plans*
Update mutual aid response plans, processes, and procedures to include the continuity of operations (COOP) plan. Determine who has priority response based on delineation of geography and incorporate into response plans. Develop guidelines for activating and returning to routine operations after emergency response events to include radio channel dispositions and agency notifications.

#### *Enabling/Deactivating Interoperability*
Establish procedures to authorize and enable and/or disable interoperability solutions during an incident and return to routine operations. This includes ECCs/PSAPs roles and responsibilities, training, and multi-jurisdictional drills to practice and familiarize with new or existing resources or procedures.

#### *Allowances for Variations*
Consider including language to address events in which an agency may not be able to provide the same level of support routinely expected, such as a pandemic.

#### *Terminology, Plain Language*
Set polices to communicate in plain language to avoid confusion or misinformation. Avoid using ten-digit codes, jargon, or acronyms, unless specifically related to policy and procedures due to NG911 enhancements.

#### *Training, Testing, Exercises*
Define frequency and responsibilities associated with training and testing. Assure that training and exercise plans are developed and tested prior to cutover to NG911. Identify whether there are minimum requirements to be achieved for all personnel on NG911 operations, and that any necessary performance measures are in place. Identify costs associated with training personnel to learn new systems.

#### *Joint SOPs*
Acknowledge receipt with signature on standard operating procedures for their respective personnel. Set performance measures and determine what procedures are essential for full compliance and optimal execution. Introduce quality control and improvements within a specified timeframe to evaluate effectiveness and calibrate incidents to ensure best practices using input from all end users and project migration teams to ensure policies are working as designed.

## FINANCIAL OBLIGATIONS

Generally, if there are fiscal obligations or cost sharing arrangements to be made, an MOA is a more suitable instrument than an MOU. There may be costs associated with equipment, training, staffing, and incident response.



ecpc@cisa.dhs.gov

## Financial Considerations

### *Cost/Reimbursements*

Understand the costs associated with the NG911 migration. Determine what resources are reimbursable, if any, between agencies and clearly outline expectations for mutual aid communications response. Document whether any parties agree to provide financial consideration for any goods, services, or personnel. Incorporate how payments are made, disbursed, and documented. Consider using language for payment "subject to the availability of funds" in the event a party is unable to fulfill the financial obligation.

### *Shared Communication Systems and Infrastructure (SCSI)*

Identifying mutually agreed upon roles, equipment, training, staffing, and incident response may help partner agencies determine their shared cost with all parties involved. Cost sharing and training may enable agencies to optimize performance standards and ensure quality control. To learn more about a SCSI approach, visit www.cisa.gov/scsi.

## SUMMARY

The Considerations for Establishing Agreements for NG911 document, paired with ECPC's MOU/A Template, is intended to provide FSLTT agencies with key considerations for establishing agreements to interconnect for NG911. It provides sample language and resources to help agencies collaborate with partners to ensure operability, interoperability, and resiliency of NG911 networks.

## ADDITIONAL RESOURCES

| | |
|---|---|
| **CISA** | • *NG911 Self-Assessment Tool*<br>• *National Emergency Communication Plan*<br>• *Cyber Incident Response Case Studies for ECCs/PSAPs*<br>• *Cyber Essentials Starter Kit: The Basics for Building a Culture of Cyber Readiness*<br>• *Cybersecurity Incident and Vulnerability Response Playbooks*<br>• *Shared Communication Systems and Infrastructure (SCSI) for Public Safety Communications* |
| **Federal Communications Commission (FCC)** | • *Communications Security, Reliability, and Interoperability Council (CSRIC) VII: Report on Security Risks and Best Practices for Mitigation In 911 In Legacy, Transitional, and NG911 Implementations*<br>• *CSRIC VII: Report Measuring Risk Magnitude and Remediation Cost in 911 and NG911 Networks* |
| **National 911 Program** | • *NG911 Interstate Playbook: Chapter 5* |
| **National Institute of Standards and Technology (NIST)** | • *NIST Cybersecurity Framework* |



ecpc@cisa.dhs.gov