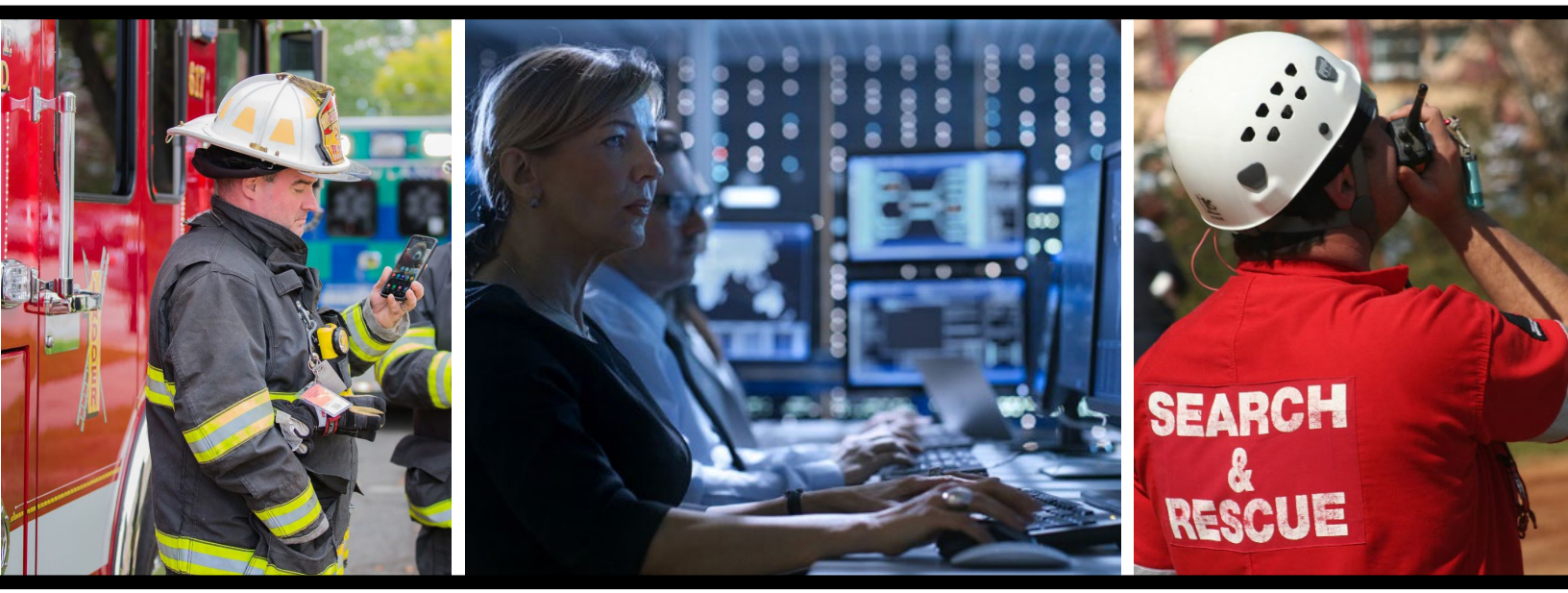



# INTEROPERABLE COMMUNICATIONS TECHNICAL ASSISTANCE PROGRAM

## Service Offerings Guide

### Version 7.2

October 2024

Cybersecurity and Infrastructure Security Agency

# Table of Contents


FOREWORD ..... 1

CISA TECHNICAL ASSISTANCE ..... 2

New and Updated CISA Technical Assistance Offerings ..... 2

Governance ..... 2

Standard Operating Procedures ..... 2

Technology ..... 2

Training & Exercises ..... 2

Usage ..... 3

Cyber Resilient 911 (CR911) TA Service Offerings Flowchart ..... 4

TA Request Process ..... 5

TA Request Form ..... 5

TA Evaluation Form ..... 5

Categories of TA Requests ..... 6

CISA Emergency Communications Coordination Support ..... 7

GOVERNANCE ..... 9

Statewide Communication Interoperability Plan Workshop ..... 9

Tribal Strategic Communication Interoperability Plan Workshop ..... 10

Rural Emergency Communications Operational Rapid Assistance Package ..... 11

Governance Documentation Review, Assessment, and Development ..... 12

Information and Communications Technology Planning & Policy Development ..... 13

Information and Communications Technology Functional Resource Assistance under Emergency Management Assistance Compact ..... 14

Grant Funding for Emergency Communications Webinar ..... 15

STANDARD OPERATING PROCEDURES ..... 16

Effective Communications During Active Shooter Incidents ..... 16

Primary, Alternate, Contingency, and Emergency Plan Development ..... 17

Standard Operating Procedures/Standard Operating Guidelines/Communications Plan Review and Development ..... 18

Tactical Interoperable Communication Plan Development/Update Workshop ..... 19

Tactical Interoperable Communications Field Operations Guide Development/Update ..... 20

Electronic Field Operations Guide Development ..... 21

TECHNOLOGY ..... 22

One-Day Cyber Threat Awareness Workshop ..... 22

911/ Public Safety Answering Point Cyber Awareness Overview ..... 23

Land Mobile Radio Cyber Awareness Overview ..... 24

Next Generation 911 and Cybersecurity Overview ..... 25

Next Generation 911 Security Operations and Administration ..... 26

Next Generation 911 Cybersecurity Plan Workshop ..... 27

Two-Day Threat Assessment and Response Planning Workshop ..... 28

Cybersecurity Kickstart Workshop ..... 29

Next Generation 911 Cybersecurity Event Tabletop Exercise ..... 30

Emergency Communications Center Cybersecurity Readiness Assessment ..... 31

Rapid Cybersecurity Assessment ..... 33

Full Cybersecurity Assessment ..... 35

Post Cyber Incident Root Cause Analysis & After-Action Report Workshop ..... 37

Post Assessment Workshop ..... 38

Next Generation 911/Strategic Planning Support ..... 39

Land Mobile Radio/Long Term Evolution Coverage Testing & Simulation ..... 40

Alerts and Warnings ..... 41

TRAINING & EXERCISES ..... 42

Communications-Focused Exercise for Information and Communications Technology Branch Trainees ..... 42

Communications-Focused Tabletop Exercises ..... 43

Communications-Focused Functional Exercises ..... 44

Communications-Focused Full Scale Exercises ..... 45

Communications Focused Drill ..... 46

Communications-Focused Exercise Design and Planning ..... 47
Communications Unit Leader Training Course ..... 48
Communications Technician Training Course ..... 50
Incident Tactical Dispatcher Training Course ..... 51
Information Technology Service Unit Leader Training Course ..... 52
Incident Communications Center Manager Training Course ..... 54
Auxiliary Communicator Training Course ..... 55
Audio Gateway Information and Training ..... 56
Resilient Communications Awareness Webinar ..... 57
Resilient Incident Communications Management Training Course ..... 58
**USAGE ..... 59**
Rural, Tribal, Territorial Emergency Communications Needs Assessment ..... 59
Operational Communications Assessment ..... 61
Regional Communications Enhancement Support – Strategic Communications Migration Plan ..... 62
Communications Focused Special Event Planning ..... 63
Communication Assets Survey and Mapping Tool Training ..... 64
Encryption Planning and Usage ..... 65
Priority Telecommunications Services ..... 66
**APPENDIX A: SAFECOM RESOURCES ..... 67**
SAFECOM Website Resources ..... 67
**APPENDIX B: ADDITIONAL TA RESOURCES ..... 68**
National Interoperability Field Operations Guide (NIFOG) 2.01 ..... 68
National Special Security Events (NSSE)/Special Event Assessment Rating (SEAR) Communications Planning Toolkit ..... 68
Primary, Alternate, Contingency, Emergency (PACE) Planning Toolkit ..... 69
Rural Emergency Medical Communications Demonstration Project (REMCDP) Planning Toolkit ..... 69
Cybersecurity PSAP Ransomware Poster ..... 70
Cybersecurity Telephony Denial of Service (TDoS) Poster ..... 70
Cybersecurity PSAP Swatting Poster ..... 70
**APPENDIX C: ACRONYMS ..... 71**

# Foreword

To address current and future threats to operable and interoperable communications, the Cybersecurity and Infrastructure Security Agency (CISA) partners with national security and emergency preparedness stakeholders to develop technical assistance (TA) offerings that meet their evolving needs. As part of this mission, CISA continues to deliver training that supports and promotes public safety communications, with the goal of achieving resilient, interoperable, and secure emergency communications. Our core values reflect this design and underpin everything we do at CISA in the following ways:

**COLLABORATION**

CISA engages the national security and public safety community through its Emergency Communications Coordinators (ECCs). SAFECOM, a body composed of representatives from 35 discipline-specific associations and over 30 at-large members directly representing their communities, advises on the development of resources, guidance, and offerings. The National Council of Statewide Interoperability Coordinators (NCSWIC) affords us the ability to directly collaborate with each state and territory's central node for emergency communications. This whole-of-nation approach is enshrined in the form of the National Emergency Communications Plan (NECP), which sets out a strategic, coordinated approach to strengthen and enhance emergency communications capabilities.

**INNOVATION**

Thanks to the collaborative process, we collect feedback and adapt and develop new TAs. The range of available assistance spans from TA engagements to educational offerings, such as Information Communications and Technology (ICT) training. This includes Statewide Communication Interoperability Plan (SCIP) workshops, cybersecurity, alerts and warnings, and grants for emergency communications awareness webinars and governance and standard operating Procedure (SOP) updates and development.

**SERVICE**

CISA TA offerings are provided to all states, territories, and tribal nations at no cost. TA requests are processed twice each Fiscal Year (FY), first during October and second in April, with the goal of implementing the requested TA during each six-month period.

**ACCOUNTABILITY**

CISA ECCs serve as the primary contact for Statewide Interoperability Coordinators (SWIC) and public safety practitioners to answer questions about this Guide and CISA TA services. Through the ECCs, CISA is directly accountable to the community it serves.

It is my sincere hope that this Guide will be helpful to you, and that you will join us in continually improving it. Together, we can keep America safe, secure, and resilient.

Best Regards,

Billy Bob Brown, Jr.
Executive Assistant Director for Emergency Communications
Cybersecurity and Infrastructure Security Agency

# CISA Technical Assistance

## New and Updated CISA Technical Assistance Offerings

### Governance

- ***NEW*** Rural Emergency Communications Operational Rapid Assistance Package (OP-ORAP)
- Information and Communications Technology Planning & Policy Development (GOV-ICTPLAN)
- Information and Communications Technology Functional Resource Assistance under Emergency Management Assistance Compact (GOV-ICTEMAC)

### Standard Operating Procedures

- ***NEW*** Primary, Alternate, Contingency, and Emergency (PACE) Planning Toolkit
- ***NEW*** Rural Emergency Medical Communications Demonstration Project (REMCDP) Planning Toolkit

### Technology

- ***NEW*** Emergency Communication Center Cybersecurity Readiness Assessment (CYB-ASMTCRA)
- ***NEW*** Post Cyber Incident Root Cause Analysis & After-Action Report Workshop (CYB-INCDNTAAR)
- ***NEW*** Cybersecurity Kickstart Workshop (CYB-WKSPKICKSTRT)
- ***NEW*** Next Generation 911 and Cybersecurity Overview (CYB-AWRNG911_OVRW)
- ***NEW*** Next Generation 911 Cybersecurity Plan Workshop (CYB-NG911CYBPLAN)
- ***NEW*** Next Generation 911 Security Operations and Administration (CYB-AWRNG911_ADV)
- ***NEW*** Next Generation 911 Cybersecurity Event Tabletop Exercise (CYB-NG911_TTX)
  ****See the Cyber 911 Service Offerings Flowchart on the next page.***

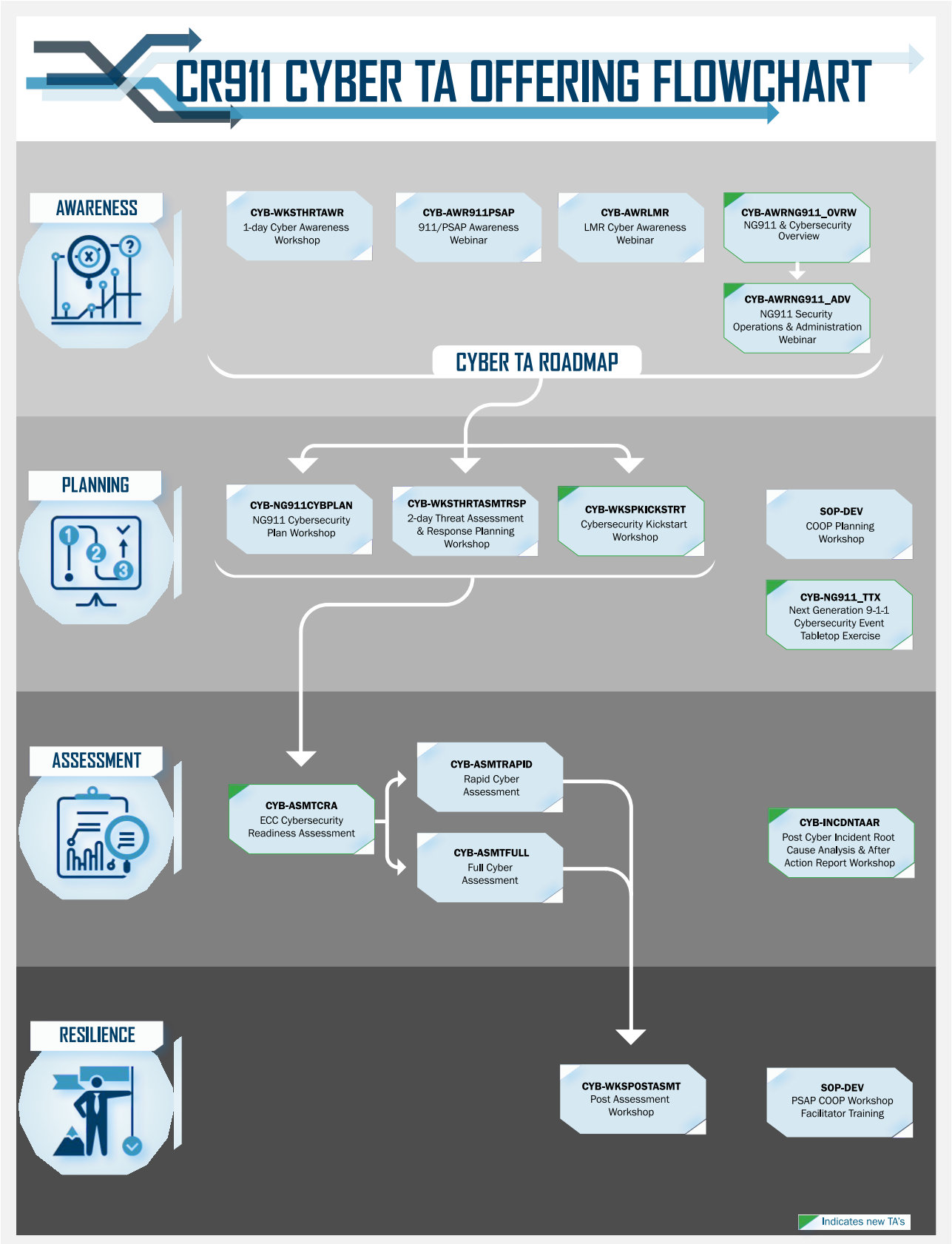
### Training & Exercises

- Communications-Focused Exercise for Information and Communications Technology Branch Trainees (OP-COMMEX)
- Communications-Focused Tabletop Exercises (OP-TTX)
- Communications-Focused Functional Exercises (OP-FE)
- Communications-Focused Full-Scale Exercises (OP-FSE)
- Communications Focused Drill (OP-COMMDRILL)
- Communications Unit Leader Training Course (TRG-COML or SS-COML)
- Communications Technician Training Course (TRG-COMT or SS-COMT)
- Incident Tactical Dispatcher Training Course (TRG-INTD or SS-INTD)
- Information Technology Service Unit Leader Training Course (TRG-ITSL or SS-ITSL)
- Incident Communications Center Manager Training Course (TRG-INCM or SS-INCM)
- Auxiliary Communicator Training Course (TRG-AUXC or SS-AUXC)
- Audio Gateway Information and Training (ENG-AG)
- Resilient Communications Awareness Webinar (TRG-RESCOM_AWR)
- Resilient Incident Communications Management Training Course (TRG-RESCOM_MGT)

## Usage

- ***NEW*** Rural, Tribal, Territorial Emergency Communications Needs Assessment (OP-ASMTRTTECN)
- Operational Communications Assessment (OP-ASMT)
- Regional Communications Enhancement Support – Strategic Communications Migration Plan (RCES-SCMP)
- Communications Focused Special Event Planning (OP-SPEV)

# Cyber Resilient 911 (CR911) TA Service Offerings Flowchart

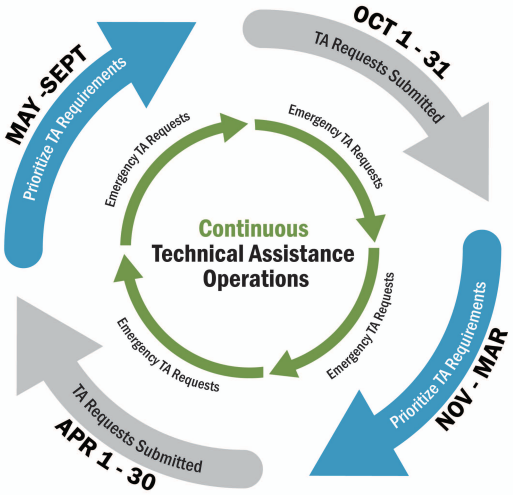


# CISA Technical Assistance

## TA Request Process

TA requests are processed twice each fiscal year, first in October and then in April, with the goal of implementing the requested TA during each six-month period.

Out-of-cycle, unplanned TA requests, and exceptions to the defined TA request periods will be reviewed on a case-by-case basis for situations that warrant immediate TA support.




## TA Request Form

To request a TA, the SWIC, Tribal Representative, or other designated SLTT point of contact should complete the fillable TA request form on the SAFECOM website at: [cisa.gov/safecom/ictapscip-resources](cisa.gov/safecom/ictapscip-resources).

Requests should be listed in Priority Order, and each request should align with the appropriate priority shown on the left side of the TA Service Offerings Selection. Select the appropriate TA category from the drop-down list under "CISA TA Offerings Pick List" section on page 4 of the TA request form.

On page 5, describe the goal or objective that the TA supports (example: advances a SCIP goal, NECP implementation initiative, advances a state marker or risk it addresses). Any additional information on the requested TA service that is being requested should be entered in this space, as well.

Once completed, click "Submit by Email" at the bottom of the form, or save the form and email it directly to: TARequest@cisa.dhs.gov.

## TA Evaluation Form

At the conclusion of a TA, the SWIC, Tribal Representative, or other designated state, local, tribal, or territorial (SLTT) point of contact will be asked to complete a TA evaluation form to provide feedback and evaluation of CISA services. CISA uses this feedback from stakeholders during TA delivery to update and improve its services. Once completed, the form should be emailed directly to: TAEvaluations@cisa.dhs.gov.

## Categories of TA Requests

**State/Territory/Tribal Prioritized TA**
TA that addresses the highest priority communications requirements for SLTT emergency communications interoperability gaps, while advancing state markers, supporting high priority risks, and implementation of the National Emergency Communications Plan (NECP).

**Statewide Communication Interoperability Plan (SCIP) Workshops**
SCIPs define the current and future direction for interoperable and emergency communications within a state or territory. The SCIP creates a single resource for all stakeholders at all levels of government so that there is a unified approach for enhancing interoperable communications. A SCIP is considered current if it is within 36 months of its creation which is a requirement of the Homeland Security Grant Program (HSGP).

**State-Sponsored Information & Communications Technology (ICT) Courses**
A state-sponsored TA course request requires that the state provides two state-qualified, and CISA recognized, instructors to teach the course.

**Regional TA**
A regional TA crosses Border/Interstate (state-to-state) Emergency Communications to establish capabilities to enable emergency communications across all components of the SAFECOM Interoperability Continuum.

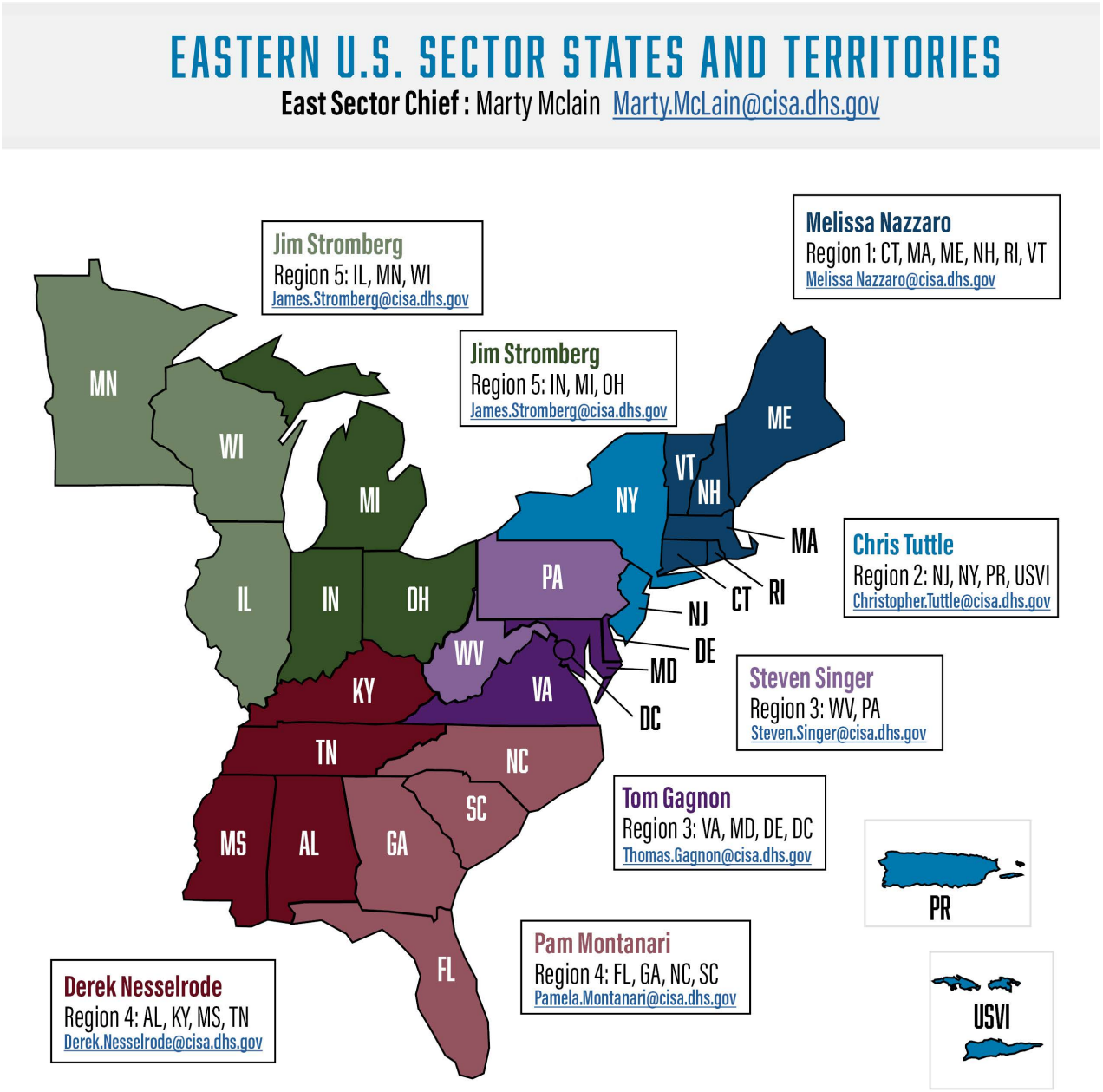
**Rural Emergency Medical Communications Program (REMCDP)**
REMCDP begins with a Rural Emergency Communications Operational Rapid Assistance Package (ORAP) TA that identifies barriers and challenges in rural emergency medical communications. This is followed by a TA that recommends enhancements to the existing emergency communications infrastructure to improve the delivery of rural medical care and addresses NECP implementation gaps.

**Cyber Resilient 911 (CR911)**
TA support for Emergency Communications Centers (ECC)/Public Safety Answering Points (PSAP) at the federal, state, local, tribal, and territorial (FSLTT) levels that addresses operational cybersecurity challenges and develops stakeholder-driven solutions and capabilities that address 911 cybersecurity needs and reduce risk.

**National Special Security Events (NSSEs) & Special Event Assessment Rating (SEAR)**
National Special Security Events (NSSEs) are nationally or internationally significant events that involve a large number of attendees and are attended by U.S. officials and foreign dignitaries. In addition to NSSEs, some events at the state and local level may require federal assistance to provide appropriate levels of security. A Special Event Assessment Rating (SEAR) event is a special event, typically preplanned by a nonfederal entity, that requires federal assistance to provide security but does not rise to the threshold of qualifying as an NSSE.

# CISA Technical Assistance

## CISA Emergency Communications Coordination Support



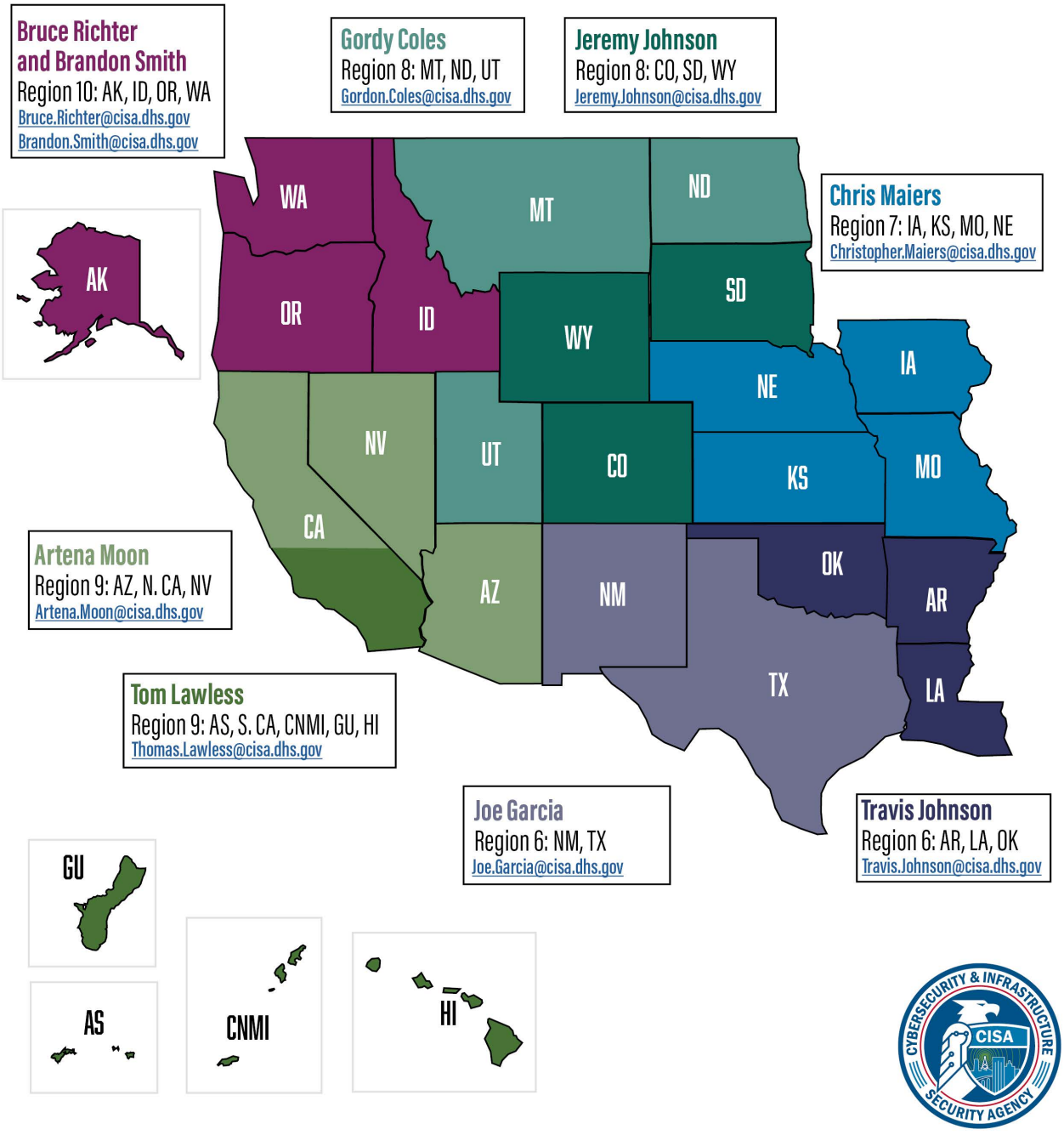

### CISA Emergency Communications Coordination Support

CISA's Emergency Communications Coordinators (ECCs) lead efforts to strengthen emergency communications capabilities across all 56 states and territories. ECCs work directly with the Statewide Interoperability Coordinators in each region to prioritize and coordinate the delivery of technical assistance service offerings to meet day-to-day operations, large special events and pre/post crisis communications support. For more information on the Emergency Communications Coordination Program, please contact ECD@cisa.dhs.gov.

# CISA Technical Assistance

## WESTERN U.S. SECTOR STATES AND TERRITORIES

**West Sector Chief :** Steve Noel Steven.Noel@cisa.dhs.gov



# Governance

| *Statewide Communication Interoperability Plan Workshop* | |
|---|---|
| TA Delivery Method: | In-Person, Virtual, or Hybrid Workshop |
| Recommended Participants: | State Interoperability Executive Committee (SIEC)/Statewide Interoperability Governance Board (SIGB) members; SWICs; SLTT stakeholders, SLTT police; Fire and Emergency Medical Services (EMS) personnel; state 911 administrators; FirstNet representatives; state information/technology officers |
| Catalog Item Description | SCIP-WKSP |

## Offering Overview

The SCIP is a stakeholder-driven, multi-jurisdictional, and multi-disciplinary statewide strategic plan to enhance interoperable emergency communications. A SCIP creates a single resource for all stakeholders throughout a state's communications ecosystem to prioritize resources, strengthen governance, identify future investments, and address interoperability gaps. It also serves to complement other state plans such as Homeland Security or Disaster Preparedness Plans. A current SCIP (created within the last 36 months) is a requirement of the HSGP.[1]

To gather a more thorough understanding of the state of the nation's emergency communications capabilities, CISA partnered with NCSWIC to develop 25 state/territory interoperability markers as a nationwide self-assessment framework to describe interoperability maturity at the state/territory level. In 2019, CISA conducted six regional workshops to collect baseline self-assessments for all 56 states and territories, which are updated on an annual basis. CISA uses this information to update SCIPs and deliver relevant technical assistance offerings to address current state/territory needs. The state/territory interoperability markers serve as a tool to support NECP implementation and to help states/territories progress towards interoperability optimization.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Draft SCIP that incorporates National Governors Association recommendations, consideration of data gathered through the state/territory performance markers baseline and NECP goals and objectives.
- One or more focused engagements:
    - Governance focused engagement to establish a governance body or strengthening existing governance and building consensus and goals,
    - Technology and Cybersecurity focused engagement to review and leverage survey results to develop land mobile radio (LMR), broadband (BRBND), 911, alerts and warnings, and cybersecurity goals, or
    - Funding sustainability focused engagement on reviewing the Homeland Security Grant Program criteria to develop funding goals
- Customized evaluation and action plan for implementation of the SCIP goals
- Evaluation and progress assessment of goals
- Strategic goals and implementation plan
- Evaluation/progress management

For additional information on the SCIP process, refer to the SCIP Overview Guide handout at: cisa.gov/statewide-communication-interoperability-plans.

[1] Additional information regarding the HSGP is available at fema.gov/grants/preparedness/homeland-security.

# Governance

| *Tribal Strategic Communication Interoperability Plan Workshop* | |
|---|---|
| TA Delivery Method: | In-Person, Virtual, or Hybrid Workshop |
| Recommended Participants: | Tribal Emergency Managers, Public Safety Officials, LMR/PSAP/IT managers, and First Responders |
| Catalog Item Description | TSCIP-WKSP |

## Offering Overview

The Tribal Strategic Communication Interoperability Plan (TSCIP) is a partner-driven and multi-disciplinary tribal strategic plan designed to enhance interoperable emergency communications. TSCIPs serve as a single document for partners throughout a tribal nation's communications ecosystem. It assists with prioritizing resources, strengthening administration, identifying future investments, and addressing interoperability gaps. It also serves to complement to other plans such as Homeland Security or Disaster Preparedness Plans. A current TSCIP (created within the last 36 months) can help support the need for grant funding and development of a Threat and Hazard Identification and Risk Assessment (THIRA) required by of the Tribal Homeland Security Grant Program (THSGP).[2]

**Customized support for this offering may look different to meet each tribal nation's unique needs. Potential design outcomes and deliverables may include:**

- Draft TSCIP performance goals baseline against NECP goals and objectives
- A three- to five-year roadmap
- One or more focused engagements, such as:
    - Communications administration and governance focused engagement to establish an administrative body or strengthen the existing administration structure,
    - Technology and cybersecurity-focused engagement to review and leverage survey results to develop land mobile radio (LMR), broadband (BRBND), 911, alerts and warnings, and cybersecurity goals, or
    - Funding and sustainability-focused engagement that can include review of the THSGP criteria to assist with development of funding and sustainment goals
- Customized evaluation and action plan for implementation of the TSCIP goals
- Evaluation and progress assessment of goals
- Strategic goals and implementation plan

For additional information on the TSCIP process, refer to the SCIP Overview Guide handout at: cisa.gov/statewide-communication-interoperability-plans.

[2] Additional information regarding the THSGP is available at: fema.gov/grants/preparedness/tribal-homeland-security.

# Governance

| *Rural Emergency Communications Operational Rapid Assistance Package* | |
|---|---|
| TA Delivery Method: | In-Person Rural Emergency Communications Assessment/Analysis/Corrective Action(s) Plan Development Workshop |
| Key Participants: | Agency EMS Rural Medical Operations Director and support Dispatch Center Director, Radio System Manager, Maintenance Vendor(s) |
| Recommended Participants: | Rural Medical Emergency Managers, 911/PSAP Officials, Public Safety Officials, Hospital Senior Leadership, First Responders, SWIC |
| Catalog Item Description | OP-ORAP |

## Offering Overview

The Rural Emergency Communications ORAP mission identifies barriers and challenges in rural emergency medical communications. Followed by a recommended TA that enhances existing emergency communications infrastructure to improve the delivery of rural medical care and addresses NECP implementation gaps.

**TA objectives:**

1. Identify immediate needs associated with rural emergency communications for rural Emergency Medical Services (EMS),
2. Provide tools (e.g., plans/policies/procedures) to immediately address those needs,
3. Train jurisdictions and communities on using those tools to address gaps, and
4. Apply and test those tools via exercises (tabletop or functional)

**Customized support for this offering may look different, depending on each community's unique needs.**
All ORAP communities receive a site assessment visit and site assessment summary report. The report provides a recommended work plan for follow-on TA offerings to address emergency communications gaps identified during the site visit. ORAP follow-on efforts will be accomplished during a power site visit where a team of subject matter experts work onsite with stakeholders to complete multiple goals.

**Examples of identified follow-on TA options:**

- Rural Emergency Medical Communications Program (REMCDP) Tool kit (Appendix C)
- Continuity of Operations Plan (COOP)
- Primary, Alternate, Contingency, and Emergency (PACE) Plan
- Alerts, Warnings, and Notifications (AWN) Plan
- Land Mobile Radio (LMR) Training
- Tabletop Exercise (TTX)
- Regional Communications Enhancement Support

# Governance

| *Governance Documentation Review, Assessment, and Development* | |
|---|---|
| TA Delivery Method: | In-Person Workshop or Webinar |
| Recommended Participants: | SIEC/SIGB: SWICs, Executive, Statutory, and Legislative Personnel |
| Catalog Item Description | GOV-DOC |

## Offering Overview

The SAFECOM/NCSWIC 2018 Governance Guide for SLTT Officials highlights the need for a formalized statewide governance body (e.g., SIGB, SIEC) or equivalent. A formalized governane body provides a unified approach across multiple disciplines and jurisdictions to address system implementation and upgrades, funding, and overall support for communications interoperability.[3]

CISA helps requestors in creating, reviewing, and evaluating existing governance structures and provides recommendations for establishing new governance bodies or structures.

For example, this TA will assist SIECs and SIGBs with the development of documentation (working group charters) for establishing governance bodies for communications-focused entities such as LMR systems, municipal agencies, and councils of government.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Existing interoperability and emergency communications-focused governance group
- Formal governance documentation (e.g., charter, executive order, etc.)
- Governance operating norms
- Robust participation by key stakeholder groups
- SWIC and/or SIGB membership needing to evaluate and assess current SCIP
- Governance charter
- Draft Executive Order to formally establish a governance group
- Best practices for establishing governance group operating norms
- Assessment of governance group representation and customized approach for improvements
- Evaluation and analysis of SCIP, progress towards stated goals and objectives, and recommendations for SCIP refresh/update

[3] The 2018 Emergency Communications Governance Guide for SLTT Officials is available at: cisa.gov/safecom/blog/2018/04/04/2018-sltt-governance-guide.

# Governance

| *Information and Communications Technology Planning & Policy Development* | |
|---|---|
| TA Delivery Method: | In-Person and Virtual Workshops |
| Recommended Participants: | SIEC/SIGB; SWICs, STOs, Key Public Safety partners as identified by the SWIC |
| Catalog Item Description | GOV-ICTPLAN |

## Offering Overview

This TA develops or updates planning and policy documents to support states, territories, and tribes. The policy documents help to establish and maintain a formal program that develops, recognizes, deploys, and maintains Informaton and Communications Technology (ICT) position resources.

The updated planning process takes a holistic approach when assessing the jurisdiction's personnel resource needs (for both personnel and instructors) in each position within the Incident Command System's ICT Branch. The positions are then matched to the life-cycle requirements to train, qualify/recognize, and deploy personnel. It also assists with maintenance and attrition/seccession planning.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Identify long-term goals for staffing and sustainability
- Establish and document credentialing/recognition requirements
- Identify each individual's path from training to qualification/recognition
- Identify and develop opportunities that provide experience, training, and exercises to develop or maintain qualification/recognition and experience
- Establish and operate a Qualifications Review Board (QRB)
- Identify currency, qualification/recognition maintenance requirements or loss of qualification/recognition status
- Establish the performance measures of the ICT Program
- Identify tracking and reporting methods

# Governance

| *Information and Communications Technology Functional Resource Assistance under Emergency Management Assistance Compact* | |
|---|---|
| TA Delivery Method: | In-Person Workshop or Webinar |
| Recommended Participants: | SWICs, Emergency Managers and Administrators, COMLs, Agency Radio Officers, ESF #2 Coordinators, and State Warning Officers |
| Catalog Item Description | GOV-ICTEMAC |

## Offering Overview

This CISA service offering is designed to familiarize states/jurisdictions with EMAC. EMAC is the nation's preeminent state-to-state mutual aid system for facilitating the exchange of services, personnel, and equipment during incidents/emergencies. EMAC is implemented through state Emergency Management Agencies and has been passed into law in all 50 states and four U.S. territories. However, EMAC is greatly under-utilized for deployment of ICT Function resources due to a lack of awareness of the resources available and how to utilize the process.

This service offering provides states/jurisdictions an awareness of how EMAC functions; the advantages the state/jurisdiction gains by having predetermined Mission Ready Packages (MRPs); the process for requesting assistance to share resources within their state and with other EMAC members; how to handle similar requests for ICT Function assets; the preparations required to ensure personnel resources are deployable under EMAC; and guidance on how to streamline the internal EMAC request process and expedite the procurement and deployment of communications resources via the Mutual Aid Support System (MASS) and predetermined MRPs.

This offering can be delivered in-person or virtually, and can be a one- or two-day offering depending on the needs of the state/jurisdiction. The one-day version provides basic familiarity with EMAC, and provides training in creating MRPs. The two-day version allows for completion of a specific MRP which will serve as the first ICT Functional Resource MRP, and will be a reference for any additional MRP's created by the state/jurisdiction.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Overview of EMAC functions and benefits
- Information regarding in-state procedures/legislation
- List of participating in-state agencies and available resources
- Interstate agreements and resources
- Assistance with developing EMAC policies/procedures and building completed MRPs
- Other types of mutual aid across state borders
- EMAC's origin, provisions, structure, roles, and responsibilities
- Role of each state's EMAC Coordinator
- Overview of in-state EMAC procedures
- Resources available through EMAC
- Properly identifying and credentialing of personnel for interstate deployment under EMAC
- How EMAC is activated/Requesting EMAC assistance/EMAC Approval Process
- Deployment Procedures (briefings/lessons Learned)
- Defining, building, and formatting MRPs
- Overview of the MASS
- Reimbursement procedures
- EMAC training and exercises

# Governance

| *Grant Funding for Emergency Communications Webinar* | |
|---|---|
| TA Delivery Method: | Webinar |
| Recommended Participants: | SLTT Officials/SIEC/SIGB Members |
| Catalog Item Description | GOV-GRANT |

## Offering Overview

Public safety agencies should consider all available funding sources to procure, maintain, and upgrade mission-critical emergency communications systems. However, grant funding remains one of the most vital funding mechanisms available for state, local, tribal, and territorial officials to meet their communications needs. This CISA technical assistance webinar details how to identify financial assistance opportunities, reviews recommended activities during each stage of the grants lifecycle, and provides tips to help agencies apply for and manage federal grants. In addition, the webinar highlights several resources published by CISA in coordination with SAFECOM/NCSWIC that identify alternative funding mechanisms and offer best practices and considerations for emergency communications project planning and implementation.[4]

**This offering is applicable to states, tribes, or localities with some or all the following challenges:**

- Identification of available grant funding and alternative sources of funding.
- Understanding of eligibility requirements, program goals, and allowable costs.
- Management and administration of federal grant funding.

**This offering covers the following resources:**

- *SAFECOM Guidance on Emergency Communications Grants* includes typical activities that can be funded through federal grants; best practices, policies, and technical standards that help improve interoperability; and resources to help agencies comply with grant requirements.
- *List of Federal Financial Assistance Programs that Fund Emergency Communications* includes available grants, loans, and cooperative agreements that may fund various emergency communications activities.
- *Funding Mechanisms Guide for Public Safety Communications* provides an overview of various methods of funding emergency communications systems (e.g., bonds, special tax, surcharges), and specific examples of where these methods have been used to fund state and local systems.
- *Land Mobile Radio Trio of Fact Sheets; Brochure and Action Memorandum* provide stakeholders with basic information they can give to state and local decision-makers and elected officials on why it is important to fund and sustain public safety radio systems.
- *Emergency Communications System Lifecycle Planning Guide* aids stakeholders in their efforts to fund, plan, procure, implement, support, and maintain public safety communications systems, and eventually to replace and dispose of system components.
- *Contingency Considerations When Facing Reductions in Emergency Communications Budgets and Contingency Planning Guide for Emergency Communications Funding* help state, local, tribal, and territorial government agencies maintain or adjust their budgets in a time of constrained funding.

[4] Additional information regarding SAFECOM funding resources is available at: cisa.gov/safecom/funding.

# Standard Operating Procedures

| *Effective Communications During Active Shooter Incidents* | |
|---|---|
| TA Delivery Method: | In-Person Workshop |
| Recommended Participants: | Communications supervisors and dispatchers; law enforcement, fire and EMS supervisors; radio technicians and PSAP IT support; emergency management; hospital personnel; mutual aid partners; and Public Information Officers |
| Catalog Item Description | OP-COMMS_ASI |

## Offering Overview

After-action reports for large, public-safety incidents, particularly active shooter mass casualty incidents (MCIs), consistently document significant emergency communications challenges and gaps. In an effort to address these gaps, CISA offers a workshop that focuses specifically on the communciations challenges of active shooter MCIs. The goal of this workshop is to identify lessons learned in interoperable emergency communications from previous active shooter/attacker incidents across the nation and discuss strengths and weaknesses in local plans, policies, procedures, training, and equipment if the host community or tribe faced a similar incident.

**The workshop has three objectives:**

1. Identify interoperable emergency communications lessons learned in mass casualty incidents.
2. Discuss how national gaps in mass casualty incidents relate to local capabilities.
3. Develop courses of action to resolve locally identified capability gaps for mass casualty incident communications.

The workshop features a localized scenario and facilitated small group discussions where participants identify challenges and strengths against the scenario. During brief-backs, groups share their findings and discuss issues across disciplines. Gaps discussed by participants are aligned to the Interoperability Continuum, a national tool that identifies five critical success elements that must be addressed to achieve a sophisticated interoperability solution: governance, standard operating procedures (SOPs)/standard operating guidelines (SOGs) and field operations guides (FOGs), technology, training and exercises, and usage of interoperable communications.

Additionally, communities may elect to add an additional day or half-day to the workshop that focuses on solutions. During the solutioning session, participants will discuss and prioritze steps the community or tribe can take to close its identified gaps. After the workshop, the host receives a summary report containing self-identified gaps and solutions (if discussed).

**Expected Outcomes:**

- **1 Day Workshop**
  - Report detailing self-identified gaps
  - Limited solution development
- **1.5/2 Day Workshop**
  - Report detailing self-identified gaps
  - Detailed solution development specific to host needs
  - Solution implementation roadmap

**Prerequisites for Attendance:**

- None

| ***Primary, Alternate, Contingency, and Emergency Plan Development*** | |
|---|---|
| TA Delivery Method: | In-Person Workshop or Webinar |
| Recommended Participants: | Public safety personnel including PSAP/911, law enforcement, fire and emergency medical services, emergency management, and any persons responsible for critical government services. |
| Catalog Item Description | SOP-PACEPLN |

## Offering Overview

PACE is a methodology developed by the U.S. military to build resilient communications for field operations. PACE plans provide a framework that ensures decision-makers and critical government services can communicate and coordinate, regardless of impacts from incidents or events. The purpose of this TA is to assist agencies and/or communities with developing PACE plans.

**The workshop covers the following topics:**

- What is PACE?
- Communications methods
- CISA Communications Ecosystem (i.e., public to public, public to government, government to public, and government to government)
- Communications systems failures, case studies and reporting
- PACE Planning (e.g., triggers to switch methods, when and how to switch PACE levels along with PACE in more detail)
- Resources (e.g., PTS, National Oceanic and Atmospheric Administration [NOAA] Weather Radio, Integrated Public Alert and Warning Systems [IPAWS], etc.)
- Examples of PACE development
- Practice PACE plan development

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Facilitated PACE plan development
- Pre-workshop review of existing plans and subject matter expert (SME) recommendations on PACE strategies
- PACE Infographic

# Standard Operating Procedures

| ***Standard Operating Procedures/Standard Operating Guidelines/Communications Plan Review and Development*** | |
|---|---|
| TA Delivery Method: | In-Person Workshop or Webinar |
| Recommended Participants: | SWICs, Public Safety Stakeholders/Mid-Senior Level Managers |
| Catalog Item Description | SOP-DEV |

## Offering Overview

SOPs and SOGs are formal written guidelines or instructions that contain both operational and technical components. In many cases, SOPs and SOGs are designed to facilitate cross-discipline and cross-jurisdictional operations on a day-to-day or emergency basis.

Clearly defined interoperable communications SOPs/SOGs facilitate an orderly and efficient response to multi-agency incidents and events as routine as daily calls for service and as catastrophic as large-scale disasters. In addition to that, various state/territory, urban area, regional, and/or tribal planning documents include specific communications components.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Emergency Operations Plans
- Continuity of Government (COG) and Continuity of Operations Plans (COOPs)
- Capabilities assessment planning
- ECC/PSAP operational plans
- Incident Communications Planning

| ***Tactical Interoperable Communication Plan Development/Update Workshop*** | |
|---|---|
| TA Delivery Method: | In-Person Workshop or Webinar |
| Recommended Participants: | SWICs, Tribal Communications Coordinators, Communications Unit Managers, and Personnel |
| Catalog Item Description | TIC-WKSP |

## Offering Overview

TICPs are designed to document a state, territory, tribal nation, region, county, or urban area's interoperable communications technology assets, usage policies, and procedures. Public safety can use a TICP to clearly define the breadth and scope of interoperable assets available in the area and how those assets are shared and their use shall be prioritized, and the steps individual agencies should follow to request, activate, use, and deactivate each asset.

In this service offering, a facilitator, data specialist, and communications specialist coordinate and execute a workshop to create or update an existing TICP for a state, territory, tribal nation, region, county, or urban area. Developing a TICP requires the collaborative efforts and inputs of public safety organizations in the geographic area. In order to document the input of all relevant stakeholders and develop the TICP in the most efficient and effective manner, CISA provides a list of the assets and information needed for the plan prior to the workshop. The requesting area also receives a copy of the plan template that the participants will populate during the workshop.

Workshop attendees should include communications and operational representatives from multiple agencies and jurisdictions across all public safety disciplines, including tribal, non-governmental organizations and volunteer entities in the geographic area covered by the plan. The working group should mirror the responders and support personnel needed for a major incident in the area.

Once developed and approved, the TICP should be disseminated to all stakeholder agencies. Ensuring that communications users are knowledgeable about the plan and able to implement its components immediately increases the area's ability to maintain appropriate and effective interoperable communications during an event or incident of any size or scope.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Quick reference for regional channel data
- Use of mutual aid channels
- Situational area maps
- Technical support contacts and Communications Unit personnel
- Formal procedures for interoperable communications equipment requests
- Updated information about encryption capabilities
- Communication Assets Survey and Mapping Tool (CASM) entry/update

# Standard Operating Procedures

| *Tactical Interoperable Communications Field Operations Guide Development/Update* | |
|---|---|
| TA Delivery Method: | In-Person Workshop or Webinar |
| Recommended Participants: | SWICs, Tribal Communications Coordinators, Communications Unit Managers and Personnel |
| Catalog Item Description | TIC-FOG |

## Offering Overview

Based on the CISA National Interoperability Field Operations Guide (NIFOG), a state/tribe/territory-specific TIC-FOG is a compendium of interoperable communications that may include information such as frequencies, Government Emergency Telecommunications Service (GETS)/Wireless Priority Service (WPS) information, radio caches, alerts, and warning message formats, among others. In addition, reference material for use by emergency response and communications personnel responsible for establishing and maintaining interoperable communications during events or incidents may also be included. A printed copy TIC-FOG is designed as a pocket-sized quick reference guide that can be carried by radio operators and technicians at all times.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Quick reference for regional channel and encryption data
- Listing of mutual aid channels
- Situational area maps
- Listing of technical support contacts and Communications Unit personnel
- Formal procedures for interoperable communications equipment requests
- Contact information for technical support and Communications Unit personnel
- Interoperable communications equipment requests
- TIC-FOG development/update
- CASM entry update

# Standard Operating Procedures

| ***Electronic Field Operations Guide Development*** | |
|---|---|
| TA Delivery Method: | In-Person Workshop or Webinar |
| Recommended Participants: | SWICs, Tribal Communications Coordinators, State/Tribal Communications Managers and SMEs |
| Catalog Item Description | APPS-FOG |

## Offering Overview

CISA offers to make FOG document content available through CISA's Public Safety Library mobile app. This mobile app allows users to easily access coordinated communications information offline. These radio frequency interoperability field guides are the go-to reference for emergency communications planning and for radio technicians responsible for radios that will be used during disaster response. This technical assistance delivers eFOG mobile apps for both Apple and Android mobile devices. The eNIFOG or eAUXFOG mobile apps can be downloaded from either app store as an example of eFOG capabilities.

**A key requirement for developing an eFOG is that the state must provide CISA with their most current/up-to-date FOG for conversion.**

The process involves four distinct phases, each of which involves significant, though remote, interaction between CISA and the state:

- **Legal Agreement Phase:** This phase completes the review and signing of legal documents between the state and CISA before CISA begins development. In order to begin this phase, the state needs to provide CISA with the name of the agency with authority to sign the documents. Templates of the documents may be provided enabling the state to determine signing authority. This phase takes at least three weeks, depending on the state process, and can be completed in parallel with the Configuration Phase.
- **Configuration Phase:** This phase involves CISA's receipt of the required inputs from the state for the development of the mobile apps. This includes a current Microsoft Word version of its FOG document. The state will also be asked to decide on some options offered, such as high-resolution tables and maps. This phase takes two weeks on average.
- **Build and Beta Test Phase:** This phase completes CISA's build of the beta version of their eFOG. The state is then asked to identify and coordinate beta testers for a two-week test of the beta version, providing user feedback to CISA. This is the main development phase and will take at least two months.
- **Release Phase:** This phase completes CISA's update of the eFOG based on beta test feedback. When ready, the state approves release of the eFOG to CISA in writing (an email). The eFOG content is then added to CISA's library of eFOGs available through the Public Safety Library mobile app (downloadable from Google Play Store and Apple's App Store).

**The state is responsible to inform their users of the eFOG availability. This phase takes one month on average. The Public Safety Library mobile app provides the following features for each eFOG in its library:**

- Offline mobile app Field Operations Guide information for state or region
- Live links to reference websites, emails, and phone numbers (with connectivity)
- Personal FOG notes and favorites bookmarking
- Multi-word search of FOG content
- High-resolution imagery or tables with pan/zoom enabled
- Ability to easily share FOG with out of area personnel
- TIC-FOG updates identified through state beta testing
- A single portal for all eFOGs developed by CISA

# Technology

| *One-Day Cyber Threat Awareness Workshop* | |
|---|---|
| TA Delivery Method: | In-Person Workshop |
| Recommended Participants: | SWICs, Tribal Communications Coordinator, State/Tribal 911 Coordinators, 911 Operators/ECC/PSAP/LMR Managers and System Operators |
| Catalog Item Description | CYB-WKSTHRTAWR |

## Offering Overview

This workshop is focused on helping PSAP/ECC leadership and emergency managers understand the common cybersecurity threats and vulnerabilities affecting PSAP and LMR environments. This workshop also discusses best practices to secure their daily operations and govern third party service providers. The day will end with an exercise meant to reinforce the learning objectives delivered during the day.

**Workshop Objectives:**

- Build awareness about the threats and vulnerabilities common to public safety
- Provide an overview of cyber hygiene best practices
- Develop an understanding of how to identify and manage cyber-risks
- Establishing adequate third-party governance and risk management
- Promote the other cyber offerings available through CISA

***NOTE:*** The session is not meant to be technical. IT personnel are welcome; however, they may find the content to be remedial.

# Technology

| *911/ Public Safety Answering Point Cyber Awareness Overview* | |
|---|---|
| TA Delivery Method: | In-Person Workshop or Webinar |
| Recommended Participants: | SWICs, Tribal Communications Coordinators, State/Tribal 911 Coordinators, Call Takers, 911 Operators/ECC/PSAP Managers and System Operators |
| Catalog Item Description | CYB-AWR911PSAP |

## Offering Overview

While the evolution of public safety communications (including the ongoing transition to Next Generation 911 [NG911]) has dramatically improved voice and data communications, both legacy 911 and NG911 systems are vulnerable to cybersecurity attacks. 911/PSAP/ECC functions are considered high-value cyber targets to those looking to disrupt public safety services, extort local governments through ransomware[5], or create mischief. Also, ECCs are sometimes an unintended target, becoming "collateral damage" when a municipality or a supporting managed service provider is attacked. The critical nature of 911/PSAP/ECC operations means cyberattacks against them can result in a large-scale impact on public safety operations, impacting the public's ability to obtain assistance.

This offering introduces public safety communications stakeholders to common cybersecurity threats and vulnerabilities affecting 911/PSAP/ECC environments. Topics include ransomware attacks and their impact, Telephony Denial of Service (TDoS) attacks against administrative lines and 911, exposed networks and devices, why individual logons and password protection is critical, cryptojacking and email phishing. The 911/PSAP Cybersecurity Awareness Webinar also discusses basic best practices to improve the secure use of emergency communications technologies in daily operations. In addition, guidance is provided on responding to and reporting cyber incidents.

In collaboration with the CISA Cybersecurity Advisors (CSAs) and Protective Security Advisors (PSAs) in the region, CISA offers a customizable cyber awareness webinar to inform concerned public safety officials, managers, and technical staff on cyber risk management best practices and how to recognize and address cyber threats and incidents. The webinar is typically less than two hours long and is oriented to non-technical audiences at the local or regional level and may be customized to stakeholder audience needs. This allows for discussion around specifics that pertain to the attendees' environment and helps managers decide whether an expanded cybersecurity one or two-day planning workshop is needed as a follow-on. The webinar is typically given to participants statewide through a one-time, secure URL but can also be provided to participants on a regional or local level, if required.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Cyber awareness and education webinars on the types of cyber threats and attacks affecting public safety communications, especially 911, PSAP, and ECC operations
- Tailoring to emphasize specific topics or audiences such as managed services providers
- Sessions recorded for later reuse
- In-person or webinar delivery using a unique URL provided to attendees identified by the SWIC or Tribal Communications Coordinator
- Introduction to CISA phishing awareness and dedicated offerings available through CISA Assessments[6]

[5] Additional information related to ransomware can be located at: cisa.gov/stopransomware.
[6] Additional information regarding CISA Assessments is available at: cisa.gov/cyber-resource-hub. Further information regarding CISA Cyber Hygiene Services is available at: cisa.gov/cyber-hygiene-services.

# Technology

| *Land Mobile Radio Cyber Awareness Overview* | |
|---|---|
| TA Delivery Method: | In-Person Workshop or Webinar |
| Recommended Participants: | SWICs, Tribal Communications Coordinators, ECC/LMR Managers and System Operators |
| Catalog Item Description | CYB-AWRLMR |

## Offering Overview

While the evolution of public safety communications has dramatically improved voice and data communications, LMR systems are vulnerable to cybersecurity attacks. LMR/ECC functions are considered high-value cyber targets to those looking to disrupt public safety services, extort local governments through ransomware[7] , or simply create mischief. Also, ECCs are sometimes an unintended target, becoming 'collateral damage' when a municipality or a supporting managed service provider is attacked. The critical nature of LMR/ECC operations means cyberattacks against them can result in a large-scale impact on public safety operations, impacting the public's ability to obtain assistance.

This offering introduces radio system owners to common cybersecurity threats and vulnerabilities affecting LMR environments. Topics include ransomware attacks and their impact, exposed networks and devices, why individual logons and password protection is critical, cryptojacking, and email phishing. The LMR Cyber Awareness Overview also discusses basic best practices to improve the secure use of emergency communications technologies in daily operations. In addition, guidance is provided on responding to and reporting cyber incidents.

In collaboration with the CISA Cybersecurity Advisors (CSAs) and Protective Security Advisors (PSAs) in the region, CISA offers a customizable cyber awareness webinar to inform concerned public safety officials, managers, and technical staff on cyber risk management best practices and how to recognize and address cyber threats and incidents. The webinar is typically less than two hours long and is oriented to radio system owners, emergency communications managers, and other staff supporting communications that could be affected by a cyber-threat and may be customized to stakeholder audience needs. This allows for discussion around specifics that pertain to the attendees' environment and helps managers decide whether an expanded cybersecurity one or two-day planning workshop is needed as a follow-on. The webinar is typically given to participants statewide through a one-time, secure URL but can also be provided to participants on a regional or local level, if required.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Cyber awareness and education webinars on the types of cyber threats and attacks affecting public safety communications, especially LMR and ECC operations
- Tailoring to emphasize specific topics or audiences such as managed services providers.
- Sessions recorded for later reuse
- In-person or webinar delivery using a unique URL provided to attendees identified by the SWIC or Tribal Communications Coordinator
- Introduction to CISA phishing awareness and dedicated offerings available through CISA Assessments[8]

[7] Additional information related to ransomware can be located at: cisa.gov/stopransomware.
[8] Additional information regarding CISA Assessments is available at: cisa.gov/cyber-resource-hub.
Further information regarding CISA Cyber Hygiene Services is available at: cisa.gov/cyber-hygiene-services.

# Technology

| *Next Generation 911 and Cybersecurity Overview* | |
|---|---|
| TA Delivery Method: | In-Person Workshop or Webinar |
| Recommended Participants: | ECC/PSAP Staff and Leadership, IT Staff, Other Personnel (internal and/or contracted vendors) tasked with supporting ECC/PSAP Systems |
| Catalog Item Description | CYB-AWRNG911_OVRW |

## Offering Overview

This offering introduces participants to the architecture of NG911, including core services (NGCS) and supporting functional elements. During this discussion, participants will be introduced to the service areas in delivery of a 911 call through NGCS. An overview of cybersecurity risk and impact, as well as identification of security demarcation points within Next Generation systems, will be introduced.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

Topics of cybersecurity, including threats and exploits, preparedness, and mitigation are introduced. In addition, the concepts of risk assessment and defense in-depth will be introduced, as well as how to apply existing security controls (e.g., NIST SP 800-53, NIST Cybersecurity Framework [CSF]) in conjunction with an overview of the National Emergency Number Association (NENA) Security for Next-Generation 911 Standard.

# Technology

| *Next Generation 911 Security Operations and Administration* | |
|---|---|
| TA Delivery Method: | In-Person Workshop or Webinar |
| Recommended Participants: | ECC/PSAP Leadership, IT Staff, Other Personnel (internal and/or contracted vendors) tasked with supporting ECC/PSAP Systems |
| Catalog Item Description | CYB-AWRNG911_ADV |

## Offering Overview

This offering is recommended as a secondary webinar, following "Next Generation 911 and Cybersecurity Overview" (CYB-AWRNG911_OVRW), as topics are more related to technical aspects of policymaking and implementation.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**
This offering provides a high-level review of the architecture of NG911 systems, service delivery, security demarcation points, and potential risks and impacts of security incidents within a NG911 system. Management of cybersecurity challenges are addressed to participants through a high-level risk management process overview with its foundations in the NIST Risk Management Framework (NIST SP 800-37 Rev. 2). The concept of defense in-depth is reintroduced to participants through identification and discussion of security responsibility within the layers of an organization's structure.

The offering continues with high-level recommended best practices for implementation, a discussion of security assessment and audit, vulnerability assessment, and penetration testing. The discussion then begins to form the previously introduced topics into security planning and the formation of a security posture for the organization. This posture is then overlayed across existing security controls, including NIST SP 800-53, NIST CSF, and the NENA Security for Next Generation 911 Standard, and how these individual security functions interconnect to form a comprehensive security plan for the organization.

# Technology

| *Next Generation 911 Cybersecurity Plan Workshop* | |
|---|---|
| TA Delivery Method: | In-Person or Hybrid Workshop |
| Recommended Participants: | ECC/PSAP Leadership, IT Staff, Other Personnel (internal and/or contracted vendors) tasked with supporting ECC/PSAP Systems |
| Catalog Item Description | CYB-NG911CYBPLAN |

## Offering Overview

This offering is presented as a multi-month, multimodal series of workshops that culminate in a comprehensive NG911 Cybersecurity Plan for the organization based on the NENA Security for Next Generation 911 Standard (NG-SEC). Initially, a facilitated discussion with organizational leadership and other stakeholders will identify plans, policies, and procedures that are currently implemented, and any currently known gaps or weaknesses in current cybersecurity strategy to guide the development of the plan during this offering.

**NG-SEC identifies three primary security domains within the NG911 environment:**

- Policy Management
- Operations Management
- Security and Risk Management

Each domain has multiple sub-domains that interconnect to form the comprehensive, multi-layered approach to system security required to ensure uninterrupted delivery of emergency call processing services.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

Continuing through an ongoing series of shorter engagements, facilitators will collaborate with organizational leaders and stakeholders in small, manageable pieces to develop a completed, comprehensive security plan for their organization.

# Technology

| *Two-Day Threat Assessment and Response Planning Workshop* | |
|---|---|
| TA Delivery Method: | In-Person Workshop |
| Recommended Participants: | SWICs, Tribal Communications Coordinators, State/Tribal 911 Coordinators, 911 Operators/ECC/PSAP/LMR Managers, and System Operators |
| Catalog Item Description | CYB-WKSTHRTASMTRSP |

## Offering Overview

This workshop is focused on helping PSAP leadership and emergency managers learn how to develop a Cyber Incident Response Process and a Cybersecurity Incident Response Plan (CSIRP). To help the participants understand the nature of these incidents, the instructors will conduct several live demonstrations of different cyber-attacks including phishing/credential harvesting, ransomware, business email compromise, etc.

The second day of the workshop will begin with an overview of a typical CSIRP. This will be followed by a discussion regarding the CSIRP and COOP Planning. The remainder of the day will be used to help participants use the template to build a response plan for a ransomware attack.

**Workshop Objectives:**

- Build awareness about the different attack vectors common to public safety and their associated indicators of compromise
- Provide examples of response plans and how they are developed
- Demonstrate the connection between the Cyber Incident Response Process and the COOP Plan

***NOTE:*** The session is not meant to be technical. IT personnel are welcome; however, they may find the content to be remedial.

# Technology

| *Cybersecurity Kickstart Workshop* | |
|---|---|
| TA Delivery Method: | In-Person Workshop |
| Recommended Participants: | SWICs, State 911 Coordinators, ECC/PSAP Managers, ECC/PSAP System Operators, Jurisdiction IT Staff, State/Local CIO, State/Local CISO |
| Catalog Item Description | CYB-WKSPKICKSTRT |

## Offering Overview

The Cybersecurity Kickstart Workshop is designed to educate and assist PSAP/ECC Managers who want to mature their cybersecurity program by partnering with their IT department and other key stakeholders to create a multi-year improvement plan and cybersecurity risk management program. Kickstart leverages a benchmarking tool to help identify risks to their organization, document PSAP/ECC current cybersecurity policies and practices and any gaps, then builds a customized cybersecurity roadmap that assists jurisdictions with prioritizing and implementing cybersecurity improvements over time. The Kickstart workshop involves the coordination and engagement of managers, support personnel, and external partners, such as service providers.

The purpose of Kickstart is to coach participants through developing a balanced approach to improving cybersecurity that considers risk and protective measures in context with their current capabilities and daily operations.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

At the conclusion of Kickstart, the host agency/tribe receives their customized roadmap, along with recommendations on assistance from CISA and other federal agencies.

# Technology

| *Next Generation 911 Cybersecurity Event Tabletop Exercise* | |
|---|---|
| TA Delivery Method: | In-Person or Virtual Exercise |
| Recommended Participants: | ECC Staff, IT Staff, ECC Leadership & Managers |
| Catalog Item Description | CYB-NG911_TTX |

## Offering Overview

The Next Generation 911 Cybersecurity Event Tabletop Exercises (TTX) are customized and developed specifically for ECCs and other supporting agencies to improve preparedness for the most common cyber threats to ECCs and 911. Topics that can be covered include, but are not limited to, awareness of roles and responsibilities, ransomware situations, virus attacks in a PSAP/911 Center or on a radio system, unprotected accounts, etc.

Exercises and operational assessments are important tools to assess, train for, and practice mitigation, prevention, response, and recovery capabilities. CISA provides exercise assistance and expertise focused on cyber resilient communications for Tabletop Exercises.

**Customized support for this offering may vary to meet SLTT needs. Potential design options, outcomes, and deliverables may include:**

- Designing, conducting, and evaluating cyber event focused public safety/service exercises
- Preparing cyber event-focused scenarios and injects (both voice and data) for exercises
- Assessing Communications Unit trained personnel
- Initial, mid, and final planning meetings (can be in-person or virtual)
- Logistics checklist
- Exercise Plan (EXPLAN)
- Master Scenario Events List (MSEL)
- After Action Report/Improvement Plan (AAR/IP)

This exercise is structured under Homeland Security Exercise Evaluation Program (HSEEP) Guidelines.

# Technology

| *Emergency Communications Center Cybersecurity Readiness Assessment* | |
|---|---|
| TA Delivery Method: | In-Person Assessment with Facilitated Virtual Discussion |
| Recommended Participants: | ECC/PSAP Leadership, IT Staff, Other Personnel (internal and/or contracted vendors) tasked with supporting ECC/PSAP Systems |
| Catalog Item Description | CYB-ASMTCRA |

## Offering Overview

The Emergency Communication Center (ECC) Cybersecurity Readiness Assessment (CRA) technical assistance offering provides organizations with a high-level understanding of their current cybersecurity posture through a review and discussion of currently implemented policy, process, and procedure. The CRA may be considered as a first step from the available assessment offerings and should be considered by agencies who are unsure of their current posture or are taking steps toward creation or revision of an organizational cybersecurity program.

**The CRA (average one to two-week effort) is intended to identify and/or provide the requesting agency the following:**

- Currently implemented cybersecurity mechanisms in defense of the environment
- High-level gap analysis between current and recommended practice
- Recommendations to fill any identified gaps
- Identify timing for re-assessment or expanded assessment (rapid or full)

The assessment consists of a review of PSAP/ECC systems, policies, processes, and procedures as well as security mechanisms deployed within the organization's purview in protection of mission-critical systems. The assessment is based on the Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1[9], commonly referred to as the CSF from NIST. Assessment questions were crafted within the 23 categories contained in the five functional areas of the CSF to be relatable to PSAP/ECC personnel of technical and non-technical backgrounds while providing a thorough assessment of an organization's cybersecurity posture.

**The cyber assessment engages subject matter experts with PSAP/ECC administration and other system stakeholders to cover:**

- **Kickoff**
  - Work with the requesting agency to explain the process, gather preliminary information (e.g., organizational systems and system architecture information, security related policy, and procedures), identify participants, interviewees, potential sites for review, and timeframes for the assessment.
- **Review**
  - Review the system as it currently exists using various onsite/offsite techniques, including:
    - Documentation and project artifacts (e.g., plans, policies, procedures, network architectures)

***(Continued on next page)***

[9] The Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1is available at: nist.gov/cyberframework

        - Personnel interviews regarding processes and procedures (e.g., system operations, administration, management, use)
        - Site surveys for physical security (e.g., access and environmental controls)
- **Analysis**
    - Analyze review findings to determine implementation status of assessed items
- **Report**
    - Report finding in a Security Assessment Report (SAR), with recommended actions based on assessment findings

This technical assistance provides PSAP/ECC leadership and other system stakeholders with information for improving the cybersecurity posture of their systems. The resulting report can serve as a resource in developing action plans, budgets, staffing requirements, refinement of strategic plans, and as a baseline for future cybersecurity assessments.

# Technology

| *Rapid Cybersecurity Assessment* | |
|---|---|
| TA Delivery Method: | In-Person Assessment and/or Webinar |
| Recommended Participants: | SWICs, Tribal Communications Coordinators, 911/ECC, and PSAP Managers or LMR System Owners |
| Catalog Item Description | CYB-ASMTRAPID |

## Offering Overview

The Rapid Cybersecurity Assessment technical assistance offering provides organizations with a high level understanding of their cybersecurity posture through a representative sampling process (e.g., sites, personnel, systems, and documentation) to aid in planning security management efforts.

**The Rapid Assessment (average two to three-week effort) is intended to identify or provide the following cybersecurity mechanisms in place to defend the environment:**

- Cybersecurity mechanisms in place to defend the environment
- High level gap analysis to determine what may be "wide-open"
- Remediation roadmap
- Determine the need to expand to a full assessment of the environment

The assessment consists of a review of a state, territory, tribal nation, region, county, or urban area LMR network or PSAP target systems' security mechanisms against a subset of critical or key security controls selected to assess the overall security posture of the 911/PSAP/LMR environment. The control set consists of 69 NIST separate controls from the NIST Special Publication (SP) 800-53 revision 5, Security and Privacy Controls for Information Systems and Organizations[10]. This control set was selected after conducting research on critical areas of cybersecurity concern within the PSAP community and provides a cybersecurity snapshot and insight into areas of immediate concern.

**The cyber assessment process involves a facilitator, cybersecurity specialist, or subject matter expert and the collaborative efforts and inputs of the organization's owners, administrators, and operators of the system to cover:**

- **Kickoff**
  - Work with the requesting agency to explain the process, gather preliminary information (e.g., system architecture information, security related policy and procedures), identify participants, interviewees, potential sites for review, and timeframes for the assessment
  - In order to document the posture of the target systems in the most efficient and effective manner, CISA will request a list of the assets and information to be included in the Security Assessment Plan (SAP) prior to starting the assessment
- **Review**
  - Review the system as it currently exists using various onsite/offsite techniques, including:
    - Documentation and project artifacts (e.g., policies, plans, procedures, system requirements, and architecture designs)
    - Personnel interviews regarding processes and procedures (e.g., system operations, administration, management, users)
    - Site surveys for physical security (e.g., access and environmental controls)

***(Continued on next page)***

[10] The NIST Special Publication 800-53 is available at csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

# Technology

- **Analysis**
  - Analyze review findings to determine compliance or non-compliance with baseline controls
- **Assessment**[11]
  - Perform a qualitative assessment of non-compliant controls, based on vulnerability, threats, potential impact, and likelihood of occurrence
- **Report**
  - Report findings in a SAR, with recommended mitigation strategies in a prioritized format based on potential risk to the organization or its mission

This technical assistance provides 911/PSAP managers and LMR system owners with critical information for improving the cyber security posture of their systems. The resulting report can also serve as a foundation for engaging CISA in a Full Assessment of their system(s), developing action plans, refining strategic plans, developing budgets, and developing staffing requirements.

CISA's Emergency Communications Coordinators (ECCs) can assist stakeholders in identifying additional CISA cybersecurity resources and assistance that may be needed.

[11] CISA conducts the cybersecurity assessment in collaboration with subject matter experts across the agency to include CSAs and PSAs within the region.

# Technology

| *Full Cybersecurity Assessment* | |
|---|---|
| TA Delivery Method: | In-Person Assessment and/or Webinar |
| Recommended Participants: | SWICs, Tribal Communications Coordinators, 911/ECC, and PSAP Managers or LMR System Owners |
| Catalog Item Description | CYB-ASMTFULL |

## Offering Overview

The Full Cybersecurity Assessment technical assistance offering provides organizations with an in-depth understanding of their cyber security posture through a representative sampling process (e.g., sites, personnel, systems, and documentation) to aid in planning security management efforts.

**The Full Cybersecurity Assessment (average six to eight-week effort) is intended to identify or provide the following:**

- Cybersecurity mechanisms in place to defend the environment
- Gap analysis to determine what may be "wide-open"
- Remediation roadmap

The assessment consists of a review of a state, territory, tribal nation, region, county, or urban area LMR network or PSAP target systems' security mechanisms against the complete low baseline security control set using the nationally-recognized best practice guidelines NIST Special Publication (SP) 800-53 revision 5, Security and Privacy Controls for Information Systems and Organizations.[12] The control set will be tailored up or down depending on the needs of the agency and system being assessed. Additional controls may be added to support systems that store, transmit or process sensitive data or privacy information, or state/county regulations. Federal government-specific controls will be removed from the baseline.

**The cyber assessment process involves a facilitator, cybersecurity specialist, or subject matter expert and the collaborative efforts and inputs of the organization's owners, administrators, and operators of the system to cover:**

- **Kickoff**
  - Work with the requesting agency to explain the process, gather preliminary information (e.g., system architecture information, security related policy and procedures), identify participants, interviewees, potential sites for review, and timeframes for the assessment
  - To document the posture of the target systems in the most efficient and effective manner, CISA will request a list of the assets and information to be included in the SAP prior to starting the assessment
- **Security Controls Selection**
  - Tailor and supplement the security controls baseline as needed, based on organizational needs and local conditions
- **Review**
  - Review the system as it currently exists using various onsite/offsite techniques, including:

***(Continued on next page)***

[12] The NIST Special Publication 800-53 is available at: csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

  - Documentation and project artifacts (e.g., policies, plans, procedures, system requirements, and architecture designs)
  - Personnel interviews regarding processes and procedures (e.g., system operations, administration, management, and users)
  - Site surveys for physical security (e.g., access and environmental controls)

- **Analysis**
  - Analyze review findings to determine compliance or non-compliance with baseline controls
- **Assessment**[13]
  - Perform a qualitative assessment of non-compliant controls, based on vulnerability, threats, potential impact, and likelihood of occurrence
- **Report**
  - Report findings in a SAR, including recommended mitigation strategies in a prioritized format based on potential risk to the organization or its mission

This technical assistance provides 911/PSAP managers and LMR system owners with critical information for improving the cyber security posture of their systems. The resulting report can also serve as a foundation to assist in developing action plans, refining strategic plans, developing budgets, and developing staffing requirements.

**Support will be customized to meet each state's unique needs. Potential design options, outcomes, and deliverables may include:**

- Customized number of interviews and site visits
- Action plan development

CISA's ECCs can assist stakeholders in identifying additional CISA cybersecurity resources and assistance that may be needed.

[13] CISA conducts the cybersecurity assessment in collaboration with subject matter experts across the agency to include CSAs and PSAs within the region.

# Technology

| *Post Cyber Incident Root Cause Analysis & After-Action Report Workshop* | |
|---|---|
| TA Delivery Method: | In-Person Workshop |
| Recommended Participants: | SWICs, State 911 Coordinators, ECC/PSAP Managers, ECC/PSAP System Operators, Jurisdiction IT Staff, State/Local CIO, State/Local CISO |
| Catalog Item Description | CYB-INCDNTAAR |

## Offering Overview

The Post Cyber Incident Root Cause Analysis (RCA) & AAR/Corrective Action Planning technical assistance offering provides a collaborative, in depth review of a cybersecurity incident that has impacted a jurisdiction. As part of data collection and review, participants, including ECC/PSAP managers, IT personnel, jurisdiction administration and other relevant stakeholders, come together and provide their perspectives on the incident, impacts, response, and recovery. The facilitator will use these to conduct a holistic review of the event to identify unmitigated risks, strengths to build upon, areas for improvement, and steps for preventing future incidents.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

Following the RCA, the team will develop an AAR that outlines key findings, lessons learned and additional measures to enhance the jurisdiction's overall cybersecurity and resilience. This AAR serves as a guide for the jurisdiction during future cybersecurity planning and incident response activities.

# Technology

| *Post Assessment Workshop* | |
|---|---|
| TA Delivery Method: | In-Person Workshop and Virtual Meetings |
| Recommended Participants: | PSAP Managers or LMR System Owners |
| Catalog Item Description | CYB-WKSPOSTASMT |

## Offering Overview

This offering is designed to help a recent recipient of a Cybersecurity Assessment (either CYB-ASMTRAPID or CYB-ASMTFULL) develop a plan of action to address any findings which require attention. Delivery begins with an in-person workshop and is followed by up to 12 weeks of mentoring conducted remotely over phone/video conference.

**Workshop Objectives:**

1) A review of the existing findings from an assessment completed **within the last calendar year**
2) The process of prioritizing the recommendations from the assessment to develop potential improvement plans customized on the opportunity and availability of the site
3) The development of a multi-year improvement roadmap
4) A session on the sharing of common continuous improvement program measures
5) A session on the delivery of repeatable self-assessment processes to measure progress

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

Post-workshop, the remainder of the TA includes mentoring via regularly scheduled meetings between the SMEs and the organization's owners, administrators, and system operators. These calls will be used to discuss progress and provide support to help continue with the implementation of the improvement plan. The cadence and topics for these sessions will be developed during the on-site workshop.

# Technology

| *Next Generation 911/Strategic Planning Support* | |
|---|---|
| TA Delivery Method: | In-Person Workshop or Webinar |
| Recommended Participants: | SWICs, Tribal Communications Coordinators, 911 Operators/ECC/PSAP and State Officials |
| Catalog Item Description | ENG-NG911_STRATPLAN |

## Offering Overview

This service offering is intended for 911 operators, communications personnel, and state/tribal officials who are interested in learning about NG911, technical and procedural challenges associated with integrating digital communications into their day-to-day operations, and in strategic planning for implementing NG911.

NG911 is a system comprised of hardware, software, data, and operational capabilities and procedures which continue to evolve. As NG911 networks replace circuit switched 911 networks, PSAPs/911 centers need to be prepared to incorporate technologies such as voice over internet protocol (VoIP) 911 calls, text messages, images and video, telematics data, and other data such as building plans and medical information over a common data network. PSAP call takers and dispatch personnel will have to move from a business process of handling incoming calls channeled through a single mode to processing and disseminating multi-media inputs received in multiple modes, and support communications and data transfer across county, state, and national borders as well as various emergency response disciplines and agencies. In addition, government officials, managers, and senior public safety personnel need to be familiar with the rapidly evolving technologies to keep the nation's public apprised of rapid changes to 911.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Standardized interfaces from call and message services
- Processing non-voice (multi-media) messages
- Integrating data useful for call routing and handling
- Delivery of calls/messages and data to appropriate PSAPs/ECCs
- Supporting data and communications needs for coordinated incident response and management
- Technology transition, integration, and deployment
- Technology assessments for call handling and processing
- Regulatory legislative issues, funding, and planning
- Draft Strategic NG911 Transition Plan
- Computer-Aided Dispatch (CAD) to CAD transition support
- CAD to Records Management System (RMS) transition support
- Automated Security Alarm Protocol (ASAP) to PSAP

# Technology

| *Land Mobile Radio/Long Term Evolution Coverage Testing & Simulation* | |
|---|---|
| TA Delivery Method: | In-Person Workshop or Webinar |
| Recommended Participants: | SWICs and Radio Frequency (RF) Communications System Management Agencies |
| Catalog Item Description | ENG-LMR_LTE |

## Offering Overview

Technical assistance support provided by CISA will assist by evaluating the requesting agency's LMR systems in Very High Frequency (VHF) high band (136-174 Megahertz [MHz]), Ultra High Frequency (UHF) (400-470 MHz), 700/800 MHz, and cellular (LTE) bands. On-site measurements can include received signals strength, analog audio quality, bit error rate, push to talk, and/or signal coverage measurements.

CISA's LMR and LTE coverage testing and analysis provides real-world data from wireless RF and cellular networks for indoor and outdoor coverage. This offering can be customized for socio/demographic heat maps to provide a Geographic Information System (GIS) overlay of coverage data.

CISA can also simulate LTE and LMR coverage. This supports exploring coverage across wide areas, simulating failures of towers/systems, analyzing potential tower/system improvements, post-failure analysis and many other applications. The simulation can be combined with coverage testing results to produce more accurate simulations.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Define and refine system coverage requirements
- Supplement baseline coverage studies
- Provide supplemental information related to network operator assurance testing of LTE devices
- Provide in-building and outdoor coverage measurements including assistance in locating interfering signals
- Assist with system optimization as well as maintenance

# Technology

| *Alerts and Warnings* | |
|---|---|
| TA Delivery Method: | In-Person Workshop or Webinar (Half Day) |
| Recommended Participants: | SWICs, Emergency Management, Public Safety Command/Leadership, and Communications Personnel |
| Catalog Item Description | OP-ALERTS |

## Offering Overview

Alerts and warning systems are essential for expeditiously and effectively delivering emergency notifications to a large subset of people. They are critical for jurisdictions/institutions to advise impacted agencies, inform the populace regarding threats, and provide safety protocol/instructions to protect the public and keep them out of harm's way.

This four-hour introductory Alerts and Warnings training is designed to assist emergency managers, public safety command/leadership, communications center/dispatch supervisory personnel (911), and other authorized operations centers responsible for providing timely emergency and life-safety information (both internally and to the public) to fulfill this critical function.

This Alerts and Warnings workshop/webinar provides stakeholders an awareness of the alerts and warning systems available to local, state, federal, tribal, and territorial authorities; to include an overview of FEMA's IPAWS, Wireless Emergency Alerts (WEA), the Emergency Alert System (EAS), the NOAA Weather Radio, and other public alerting systems.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Explaining the need and potential use cases for public and internal agency notifications
- Capability requirements and reviewing the specifications of available systems
- Interfacing and establishing interagency system sharing agreements with regional first responder and emergency management agencies
- Developing an emergency plan/SOP to establish governance and system utilization protocols, and administrative responsibilities
- Establishing criteria and potential use scenarios for activation/sending alert messages
- Identifying internal/external target audience/developing distribution/contact lists
- Preparing and formatting accurate, appropriate, and accessible warning messages
- Selecting the proper communications mode(s) to deliver the message
- Examining factors influencing public and media response to warning messages
- Training personnel and system testing and exercises
- Reviewing on-going system maintenance and database upkeep requirements
- In collaboration with FEMA, advising jurisdictions on IPAWS certification
- Information and compendium of links to IPAWS and other notification systems
- Specific EAS contacts, plans, policies, and procedures

# Training & Exercises

| ***Communications-Focused Exercise for Information and Communications Technology Branch Trainees[14]*** | |
|---|---|
| TA Delivery Method: | In-Person Exercise with predominantly Virtual Planning Activities |
| Recommended Participants: | Information and Communications Technology (ICT) Branch Trainees |
| Catalog Item Description | OP-COMMEX |

## Offering Overview

The Communications-Focused Exercise (COMMEX) is a one-day functional exercise for ICT branch trainees. The exercise is designed to provide trainees an environment to perform the duties of their trainee position as a member of a functional team with a scenario-based operational tempo.

COMMEX participants will experience an opportunity to perform many of the tasks identified in their Position Task Books (PTBs) and receive documented performance feedback from qualified mentors.

In addition to the trainee participants, the COMMEX requires a significant commitment of personnel and resources from the TA recipient. Host agencies need to provide tactical communications equipment to support multiple operational ICT functional teams, corresponding simulation cell personnel to support each team, as well as qualified/recognized mentors to match the participant's positions. It is critical for the TA recipient point of contact (POC) to coordinate the logistical requirements.

To maximize the logistical requirements of the COMMEX, a second-day execution is desired and a maximum third day is possible. The additional days allow additional runs of the exercise with new participants, thereby maximizing the number of participants for the overall TA.

CISA will provide exercise development and planning coordination with the TA recipient POC, and provide exercise execution support and coordination during the event.

At the end of the exercise, recognized Communications Unit Leaders (COMLs) can sign off on COML, INCM, INTD, and RADO tasks within the PTB for trainees who have successfully demonstrated their proficiency at completing the task(s). Recognized Communications Technicians (COMTs) can sign off COMT trainees. If the requesting jurisdiction does not have qualified COMLs/COMTs, CISA will help the requestor identify or can provide qualified personnel to sign off the PTBs.

**Customized support for this offering may vary to meet each SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Provide opportunities for testing COML, COMT, INCM, INTD, and/or RADO trainee proficiency
- Promote state recognition and certification programs
- Increase utilization of recently trained Communications Unit personnel
- Integrate Communications Unit personnel into the Incident Command System (ICS)
- Local mobile communications equipment and resources may be integrated into the COMMEX
- AAR/Improvement Plan (IP)
- Planning Meetings (can be in-person or virtual)

[14] This exercise is structured under HSEEP guidelines.

| ***Communications-Focused Tabletop Exercises[15]*** | |
|---|---|
| TA Delivery Method: | Facilitated In-Person and Virtual Exercise with predominantly Virtual Planning Activities |
| Recommended Participants: | Public Safety Professionals |
| Catalog Item Description | OP-TTX |

## Offering Overview

In this service offering, CISA staff collaborate with public safety and public service professionals from a state/territory, tribe, region, or urban area to design, facilitate, and evaluate a communications-focused TTX. This exercise is aligned with Emergency Support Function (ESF) #2 (Communications) and the DHS guidance on capabilities. The TTX is a discussion-based, one-day event designed to identify gaps in communications plans, policies, procedures, and communications systems needed to prevent, respond to, and recover from an emergency incident scenario.

The TTX provides an opportunity for responders, supervisors, and communications specialists to discuss communications plans, assets, and personnel in a static environment. Players review and discuss their ability to use regional communications assets in response to a large-scale incident scenario. A TTX is an excellent means for initiating multi-agency exercise relationships or reviewing regional policies or procedures.

**CISA provides exercise assistance and expertise focused on emergency communications, and/or the ICT function, through:**

- Providing an exercise facilitator and evaluators. CISA staff partners with the local Exercise Planning Team (EPT) to ensure the TTX meets the specific needs of the requestor
- Facilitating exercise planning meetings
- Providing electronic masters for all exercise documentation (Situation Manual, logistics checklists, and an AAR/IP

CISA briefs the results of the TTX through a QuickLook presentation immediately following the exercise, followed by a detailed, written AAR/IP. This AAR/IP documents best practices and gaps and makes recommendations to resolve gaps.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Designing, conducting, and evaluating results of the discussion-based exercise
- Preparing emergency communications and/or ICT Function-focused scenarios and injects (voice, data and cyber) for exercises
- Initial, midterm, and final planning meetings (can be in-person or virtual)
- Logistics package (invitations, checklists, etc.)
- Situation Manual (SITMAN)
- Exercise presentations and briefings
- QuickLook presentation
- AAR/IP

[15] This exercise is structured under HSEEP guidelines.

# Training & Exercises

| *Communications-Focused Functional Exercises*[16] | |
|---|---|
| TA Delivery Method: | Facilitated In-Person Exercise with predominantly Virtual Planning Activities |
| Recommended Participants: | Public Safety Professionals |
| Catalog Item Description | OP-FE |

## Offering Overview

This service offering provides a CISA Exercise Design Team (EDT) that collaborates with public safety professionals from the requesting area to design, facilitate, and evaluate a communications-focused Functional Exercise (FE). This exercise is aligned with ESF #2 (Communications). Exercise participants demonstrate their ability to use regional communications assets in a large-scale incident scenario, but the movement of personnel and equipment is simulated.

An FE is an excellent follow-on exercise to a TTX and a training lead-in to a Full Scale Exercise (FSE). It is a one day, onsite event with three one day planning sessions. The CISA EDT partners with the local EPT to ensure the exercise is designed to meet the needs of the requestor. CISA also provides controllers and evaluators for the exercise who are trained to identify successes and gaps revealed during the exercise.

CISA compiles the results of the FE through a written AAR/IP. The AAR/IP documents exercise best practices, gaps, and recommendations to resolve those gaps. If the FE follows a CISA TTX, the AAR/IP will also assess progress made on gaps identified during the TTX.

**CISA provides exercise assistance and expertise focused on emergency communications and/or the ICT Function through:**

- Providing an exercise director, controllers, and evaluators. CISA staff partners with the local EPT to ensure the FE meets the specific needs of the requestor
- Facilitating exercise planning meetings
- Providing electronic masters for all exercise documentation (Exercise Plan, Master Scenario Events List [MSEL], logistics checklists, and an AAR/IP

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Designing, conducting, and evaluating the functional exercise
- Preparing emergency communications, and/or ICT Function-focused scenarios and injects for exercises
- Maintaining proficiency with specific communications equipment
- Incorporating/practicing new technology for public safety personnel
- Maintaining readiness and interoperable communications
- Multi-agency/jurisdiction communications interoperability
- Public safety response level emergency communication
- Initial, midterm, and final planning meetings (can be in-person or virtual)
- EXPLAN
- MSEL
- AAR/IP

[16] This exercise is structured under HSEEP guidelines.

| ***Communications-Focused Full Scale Exercises[17]*** | |
|---|---|
| TA Delivery Method: | In-Person Exercise evaluation support with predominantly Virtual Planning Activities |
| Recommended Participants: | Public Safety Professionals |
| Catalog Item Description | OP-FSE |

## Offering Overview

This service offering helps a requestor plan for and assess interoperable emergency communications capabilities during execution of a requestor-sponsored FSE. Although communication is one of several capabilities included in an exercise scenario, interoperable communications are frequently not an evaluation focus, and gaps in this area may be overlooked in exercise reports. FSEs are often large multi-agency, multidiscipline, multi-jurisdictional exercises designed to test many facets of emergency response and recovery operations. CISA staff can assist the local EPT in its planning and development of an annex to the documentation for the FSE to integrate interoperable communications into the exercise.

CISA does not independently design or facilitate stand-alone communications-focused FSEs. However, CISA staff can help ensure a local EPT considers all components of interoperable communications. This assistance can include tasks such as developing or enhancing exercise injects to trigger communications events and responses, incorporating applicable communications performance measures, identifying communications assets for exercise play, and documenting known communications challenges that could impact exercise play.

CISA can also provide evaluators at the FSE who focus on assessing communications. CISA provides evaluation results to the local EPT for incorporation into the exercise AAR, and will only comment on communications related issues within the confines of the FSE.

**CISA provides exercise assistance and expertise focused on emergency communications and/or the ICT Function through:**

- Providing exercise design inputs focused on communications issues
- Providing evaluators at the exercise who focus on assessing communications
- Developing and delivering an After-Action Supplemental Report, focused on communications issues identified during the exercise along with recommendations on how to resolve those issues

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Assisting with design of the full-scale exercise
- Evaluating emergency communications and/or ICT functional capabilities, plans, or procedures at full scale exercises
- Preparing emergency communications and/or ICT function-focused scenarios and injects for the exercise
- Participating in initial, midterm, and final planning meetings (can be in-person or virtual)
- AAR Supplemental Report

[17] This exercise is structured under HSEEP guidelines.

# Training & Exercises

| *Communications Focused Drill* | |
|---|---|
| TA Delivery Method: | Facilitated In-Person and Virtual Exercise with predominantly Virtual Planning Activities |
| Recommended Participants: | Public Safety Professionals |
| Catalog Item Description | OP-COMMDRILL |

## Offering Overview

This service offering provides exercise planning and evaluation support for emergency communications drills to requesting sites/entities. The drills are one type of FE. Upon request, CISA evaluators and observers can supplement on-site staff to support and assist in evaluation of ICT personnel expertise on mobile communications units (MCU), communications support equipment, audio gateways, digital network communications equipment, and unique modes of communication such as High Frequency (HF), satellite, air-to-ground, and marine communications. Drills may consist of actual and/or simulated activities, which can be customized to meet the specific requirements of the requesting site/entity.

Participants will be presented with tasks at individual stations and asked to provide technical solutions to address specific incident needs or challenges. Participants will also be required to resolve communications related issues and problems that arise during the drill. A typical venue to conduct communications drills would be in conjunction with events such as an MCU "rodeo" or "rally," during which multiple vehicles and teams assemble from across a region or state. MCU events offer participating agencies an opportunity to test their voice and data equipment and capabilities and to learn more about resources within their region or state. The drills can potentially involve all ICT positions.

**CISA provides exercise assistance and expertise focused on emergency communications and/or the ICT Function through:**

- Providing an exercise director, controllers, and evaluators. CISA staff partners with the local EPT to ensure the drill meets the specific needs of the requestor
- Facilitating exercise planning meetings
- Providing electronic masters for all exercise documentation (Exercise Plan, MSEL, logistics checklists, and an AAR/IP

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Maintaining proficiency with specific communications equipment
- Incorporating new technology for public safety personnel
- Maintaining/practicing readiness and interoperable communications
- Multi-agency/jurisdiction communications interoperability
- Public safety response level emergency communication
- Planning meetings (can be in-person or virtual)
- AAR/IP

# Training & Exercises

| *Communications-Focused Exercise Design and Planning* | |
|---|---|
| TA Delivery Method: | In-Person or Virtual Workshop |
| Recommended Participants: | Key Public Safety Communications Personnel |
| Catalog Item Description | OP-EXDESIGN |

## Offering Overview

This service offering provides public safety communications and exercise specialists an opportunity to incorporate communications into operations-based and discussion-based public safety exercises. The seminar stresses voice and data communications and discusses how best to build these components into exercises to ensure emphasis on interoperable communications. This seminar runs for one full day. All discussions are framed within the guidelines of the HSEEP.

This seminar can accommodate an audience of any size, subject to space and seating availability. It focuses on exercise design and planning personnel who are tasked with executing both operational- and discussion-based exercises and is particularly useful for State Training Officers (STOs). Both public safety and public service agencies including law enforcement, fire, hospitals, public works, emergency medical services, etc. are welcome. Public safety communications personnel will gain a deeper perspective on exercise design and learn how to integrate communications objectives into both communications-focused and operational exercises.

Exercise planners will gain insight into how voice and data communications affect exercise "play." Attendees should be familiar with public safety exercises in their jurisdictions and have roles in the planning and design of exercises. Exercise design training such as HSEEP courses, FEMA on-line independent study courses, or the FEMA Master Exercise Practitioner (MEP) Program are recommended but not required.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Understanding the exercise planning process
- How to incorporate communications elements into exercises
- Identifying the "right" participants
- Developing ideal scenarios (MSELs and injects)
- Developing AARs/IPs
- Planning meetings (can be in-person or virtual)

| ***Communications Unit Leader Training Course*** | |
|---|---|
| TA Delivery Method: | Four-day In-Person Course |
| Recommended Participants: | Emergency Response Personnel with a Technical Communications Background |
| Catalog Item Description | TRG-COML or SS-COML |

## Offering Overview

In 2023 FEMA introduced NIMS Functional Guidance establishing the ICT Branch within the Logistics Section. Within the ICT Branch are the existing Communications Unit and the newly created Information Technology Services Unit and the Cybersecurity Unit. The Communications Unit Leader (COML) leads the Communications Unit and plans and manages the technical and operational aspects of meeting the communications needs of an incident or event.

This service offering is designed for all state/territory, tribal, regional, and local emergency response professionals and for support personnel with a communications background. CISA and FEMA Emergency Management Institute (EMI) offer this course jointly as "L0969, NIMS ICS All-Hazards Communications Unit Leader Course".[18]

The course is presented with facilitated lectures, hands-on activities, and extensive interactive discussions. Instructors work through the discussions and activities to explain in detail the processes used to achieve communication operability, interoperability, and how to incorporate additional communications solutions. Course materials and the COML Position Task Book will be provided to students via digital download prior to the course start date.

**Course Requirements:**

There must be a minimum of six and up to a maximum of 30 vetted students identified two weeks in advance of the course in order for CISA to conduct the Course (TRG-COML). There are no minimum student requirements for the State Sponsored Course (SS-COML) course. The SS-COML requires two state-qualified CISA-recognized instructors to conduct the course.

**Prerequisites for Attendance (prerequisites must be verified two weeks in advance of a course):**

- **Personal experience:**
  - A public safety background with experience in field operations
  - A technical communications background
  - Awareness of fundamental public safety communications technology
  - Basic knowledge of applicable communications plans
- **Completion of the following online courses from the FEMA/EMI website:**
  - IS-100: Introduction to the Incident Command System, ICS 100
  - IS-200: Basic Incident Command System for Initial Response, ICS-200
  - IS-700: An Introduction to the National Incident Management System
  - IS-800: National Response Framework, An Introduction
- **Completion of ICS-300: Intermediate Incident Command System for Expanding Incidents**
- **Additional recommended (not required) training:**
  - ICS-400: Advanced Incident Command System for Complex Incidents

***(Continued on next page)***

[18] For any training courses, SWICs are encouraged to notify the STO prior to its start to ensure the course is documented properly.

# Training & Exercises

**Course Registration Process:**

- **SWIC (or designated POC) actions:**
  - Provide course dates and location to the CISA ICT Training Coordinator at least 45 days before the course
  - Designate a course registrar to review and vet/approve each student's prerequisite documentation for sufficiency and inform the State Training Officer (STO) of the students' names
  - Issue the Coupon Code and Online Application Process Job Aid to qualified students.
  - Obtain the STO's endorsement on each student's electronic application via FEMA's online registration process
  - Submit a completed student verification form to CISA at least 14 days prior to the course
- **CISA actions:**
  - Submit a "Request to Conduct NIMS ICS Training Class" form to FEMA/EMI at least 45 days before the requested course start date to register the course in the FEMA EMI database
  - Make arrangements for the submission of the COML Course Completion Package to FEMA EMI within 10 days after the course

# Training & Exercises

| *Communications Technician Training Course* | |
|---|---|
| TA Delivery Method: | Five-day In-Person Course |
| Recommended Participants: | Emergency Response Personnel with a Technical Communications Background |
| Catalog Item Description | TRG-COMT or SS-COMT |

## Offering Overview

This course provides introductory and refresher training for the NIMS ICS COMT position. It introduces public safety professionals and support staff to various communications concepts and technologies including interoperable communications solutions, LMR communications, satellite, telephone, data, and computer technologies used in incident response and planned events. It is designed for state/territory, tribal, urban, and local emergency response professionals and support personnel in all disciplines who have a technical communications background.

Participants develop the essential core competencies required for performing the duties of the COMT in an all-hazards incident, including responsibilities while operating in a local, regional, or state-level All-Hazards Incident Management Team (IMT).

The course is instructor-led and supports learning through discussion, lecture, and hands-on exercises to explain processes used for establishment and operation of the technical communications resources for an incident or planned event. The course is five days and provides a realistic, hands-on approach to mastering the tasks and skills of a COMT. Prior to the on-site course, CISA staff will work with the requesting site to incorporate communications technologies in use by the participants' agencies. Course materials and the COMT Position Task Book will be provided to attendees via digital download prior to the course start date.

**Course Requirements:**

There must be a minimum of 8 and up to a maximum of 16 vetted students identified two weeks in advance of the course in order for CISA to conduct the Course (TRG-COMT). There are no minimum student requirements for the State Sponsored Course (SS-COMT) course. The SS-COMT requires two state-qualified CISA-recognized instructors to conduct the course.

**Prerequisites for Attendance (prerequisites must be verified by the state two weeks in advance of the course):**

- **Personal experience:**
  - A public safety background with experience in field operations
  - A technical communications background
  - Awareness of fundamental public safety communications technology
  - Basic knowledge of applicable communications plans
- **Completion of the following online courses from the FEMA EMI website:**
  - IS-100: Introduction to the Incident Command System, ICS 100
  - IS-200: Basic Incident Command System for Initial Response, ICS-200
  - IS-700: An Introduction to the National Incident Management System
  - IS-800: National Response Framework, an Introduction
- **Familiarity with the pre-course reading materials**

**Course Registration Process:**

- **SWIC (or designated POC) action:**
  - Review and vet/approve the prerequisite documentation for sufficiency
  - Submit a completed student verification form to CISA 14 days prior to the course

# Training & Exercises

| *Incident Tactical Dispatcher Training Course* | |
|---|---|
| TA Delivery Method: | Four-day In-Person Course |
| Recommended Participants: | Experienced Public Safety Telecommunicators who are familiar with the Incident Command System |
| Catalog Item Description | TRG-INTD or SS-INTD |

## Offering Overview

The Incident Tactical Dispatcher (INTD) course is designed to prepare experienced public safety telecommunicators for operating remote from the ECC/PSAP. These temporary, and sometimes mobile, facilities are usually focused on communications support to a specific event or incident operations, but may be employed as a Continuity of Operations resource. These facilities are likely to contain minimalistic communications, resource tracking, and documentation systems.

The course utilizes classroom learning and hands-on exercises in a simulated tactical environment. Since INTDs may support the ICT function of the ICS as a single resource or as part of an incident tactical dispatch team, the course focuses on an ICS foundation that can expand into applicable support scenarios.

Course materials and the INTD Position Task Book will be provided to attendees via digital download prior to the course start date.

**Course Requirements:**

There must be a minimum of eight and up to a maximum of 20 vetted students identified two weeks in advance of the course in order for CISA to conduct the course (TRG-INTD). There are no minimum student requirements for the State Sponsored course (SS-INTD) course. The SS-INTD requires two state-qualified CISA-recognized instructors to conduct the course.

To facilitate the functional exercise contained in the course, a radio cache with radios for each student/instructor/facilitator, and a minimum of five clear channels/talkgroups must be provided by the state or hosting agency. The exercise requires two separated classrooms, or ideally, one or more mobile command centers or mobile communications vehicles for the students to operate in.

**Prerequisites for Attendance (prerequisites must be verified by the state two weeks in advance of a course):**

- **Personal experience:**
  - A public safety background with three years of experience in dispatch operations
  - Awareness of fundamental public safety communications technology
- **Must have completed the following online courses from the FEMA EMI website:**
  - IS-100: Introduction to the Incident Command System, ICS 100
  - IS-144: Telecommunicators Emergency Response Taskforce (TERT) Basic Course
  - IS-200: Basic Incident Command System for Initial Response, ICS-200
  - IS-700: An Introduction to the National Incident Management System
  - IS-800: National Response Framework, an Introduction
- **Additional recommended (not required) training:**
  - ICS-300: Intermediate Incident Command System for Expanding Incidents

**Course Registration Process:**

- **SWIC (or designated POC) action:**
  - Review and vet/approve the prerequisite documentation for sufficiency
  - Submit a completed student verification form to CISA 14 days prior to the course

| *Information Technology Service Unit Leader Training Course* | |
|---|---|
| TA Delivery Method: | Four-day In-Person Course |
| Recommended Participants: | Emergency Response Personnel with an Information Technology or Technical Communications Background<br>Experienced Information Technology Support Personnel |
| Catalog Item Description | TRG-ITSL or SS-ITSL |

## Offering Overview

In 2023, FEMA introduced NIMS Functional Guidance establishing the ICT Branch within the Logistics Section. Within the ICT Branch are the existing Communications Unit and the newly created Information Technology Services Unit and the Cybersecurity Unit. The Information Technology Unit Leader (ITSL) leads the IT Services Unit, and provides information and application management for the many critical incident/event related functions, to include: Incident/Unified Command Post, Incident Communications Centers, Joint Information Center, staging areas, and field locations.

The ITSL course is instructor-led, and supports learning through discussion, lecture, and hands-on exercises to explain the processes and requirements for information management throughout incident response. The course is designed for personnel in all disciplines with a background and some level of experience in IT. The training course provides an overview of the ICT Branch and the IT Services Unit components including the Unified Help Desk (inclusive of both communications and IT support) and Information Technology Support Specialist. It provides an in-depth overview of their responsibilities and includes exercises for the ITSL's major functions to ensure reliable and timely delivery of IT services to participating agencies and officials. Course materials and the ITSL Position Task Book will be provided to attendees via digital download prior to the course start date.

**Course Requirements:**

There must be a minimum of six and up to a maximum of 20 vetted students identified two weeks in advance of the course in order for CISA to conduct the course (TRG-ITSL). There are no minimum student requirements for the State Sponsored Course (SS-ITSL) course. The SS-ITSL requires two state-qualified CISA-recognized instructors to conduct the course.

**Prerequisites for Attendance (prerequisites must be verified by the state two weeks in advance of a course):**

- **Personal experience:**
  - A public safety background with experience in field operations and/or experience providing information technology solutions to support public safety operations
  - Awareness of fundamental public safety broadband and wireless communications technology
- **Must have completed the following online courses from the FEMA EMI website:**
  - IS-100: Introduction to the Incident Command System, ICS 100
  - IS-200: Basic Incident Command System for Initial Response, ICS-200
  - IS-700: An Introduction to the National Incident Management System
  - IS-800: National Response Framework, an Introduction
- **Must have completed ICS-300: Intermediate Incident Command System for Expanding Incidents**

***(Continued on next page)***

- **Additional recommended (not required) training:**
  - ICS-400: Advanced Incident Command System for Complex Incidents

**Course Registration Process:**

- **SWIC (or designated point of contact [POC]) action:**
  - Review and vet/approve the prerequisite documentation for sufficiency
  - Submit a completed student verification form to CISA at least 14 days prior to the course

# Training & Exercises

| *Incident Communications Center Manager Training Course* | |
|---|---|
| TA Delivery Method: | Three-day In-Person Course |
| Recommended Participants: | Public Safety Communications Professionals with preferred experience as an Incident Tactical Dispatcher<br>ECC/PSAP Supervisor, Team Lead, or aspiring leader |
| Catalog Item Description | TRG-INCM or SS-INCM |

## Offering Overview

The Incident Communications Center Manager (INCM )course is designed to prepare public safety communication professionals for managing all functions in an Incident Command Center (ICC). An ICC is typically established remotely from the ECC/PSAP, is staffed with the appropriate mix of Incident Tactical Dispatchers, Radio Operators, and Auxiliary Communicators, and is focused on communications support to a specific event or incident operations.

Course materials and the INCM Position Task Book will be provided to attendees via digital download prior to the course start date.

**Course Requirements:**

There must be a minimum of six and up to a maximum of 20 vetted students identified two weeks in advance of the course in order for CISA to conduct the Course (TRG-INCM). There are no minimum student requirements for the State Sponsored Course (SS-INCM) course. The SS-INCM requires two state-qualified CISA-recognized instructors to conduct the course.

To facilitate the functional exercise contained in the course, a radio cache with radios for each student/instructor/facilitator, and a minimum of five clear channels/talkgroups must be provided by the state or hosting agency. The exercise requires two separated classrooms, or ideally, one or more mobile command centers or mobile communications vehicles for the students to operate in.

**Prerequisites for Attendance (prerequisites must be verified by the state two weeks in advance of a course):**

- **Personal experience:**
  - Awareness of fundamental public safety communications technology
  - Preferred experience or qualification as an INTD
- **Must have completed the following online courses from the FEMA EMI website:**
  - IS-100: Introduction to the Incident Command System, ICS 100
  - IS-144: Telecommunicators Emergency Response Taskforce (TERT) Basic Course
  - IS-200: Basic Incident Command System for Initial Response, ICS-200
  - IS-700: An Introduction to the National Incident Management System
  - IS-800: National Response Framework, an Introduction
- **Additional recommended (not required) training:**
  - ICS-300: Intermediate Incident Command System for Expanding Incidents

**Course Registration Process:**

- **SWIC (or designated POC) action:**
  - Review and vet/approve the prerequisite documentation for sufficiency
  - Submit a completed student verification form to CISA 14 days prior to the course

# Training & Exercises

| *Auxiliary Communicator Training Course* | |
|---|---|
| TA Delivery Method: | Two to Three-day In-Person Course |
| Recommended Participants: | Radio Operators and those interested in supporting emergency and disaster communications as part of a NIMS organization |
| Catalog Item Description | TRG-AUXC or SS-AUXC |

## Offering Overview

This course is designed for auxiliary communicators who volunteer to provide emergency communications support to public safety or emergency management organizations.

This course focuses on general auxiliary communications interoperability, on-the-air etiquette, Federal Communications Commission (FCC) rules and regulations, with specific emphasis on the NIMS ICT Branch position of Auxiliary Communicator (AUXC). The AUXC position formally brings the auxiliary communicator into the NIMS ICS environment. Course materials and the AUXC Position Task Book will be provided to students via digital download prior to the course start date.

**Course Requirements:**

There must be a minimum of eight and up to a maximum of 20 vetted students identified two weeks in advance of the course in order for CISA to conduct the course (TRG-AUXC). There are no minimum student requirements for the State Sponsored Course (SS-AUXC) course. The SS-AUXC requires two state-qualified CISA-recognized instructors to conduct the course.

**Prerequisites for Attendance (prerequisites must be verified by the state two weeks in advance of a course):**

- **Personal experience:**
  - Experience in auxiliary communications
  - An affiliation with a public safety agency
  - A desire to work within the NIMS ICS environment
- **Must have completed the following online courses from the FEMA EMI website:**
  - IS-100: Introduction to the Incident Command System, ICS 100
  - IS-200: Basic Incident Command System for Initial Response, ICS-200
  - IS-700: An Introduction to the National Incident Management System
  - IS-800: National Response Framework, an Introduction
- **Additional recommended (not required) training:**
  - ICS-300: Intermediate Incident Command System for Expanding Incidents

**Course Registration Process:**

- **SWIC (or designated POC) action:**
  - Review and vet/approve the prerequisite documentation for sufficiency
  - Submit a completed student verification form to CISA at least 14 days prior to the course

| *Audio Gateway Information and Training* | |
|---|---|
| TA Delivery Method: | One-day In-Person Workshop |
| Recommended Participants: | Information and Communications Technology (ICT) Branch Personnel (COMT and Technical Specialists) |
| Catalog Item Description | ENG-AG |

## Offering Overview

This offering provides different levels of understanding on audio gateways (i.e., audio bridge) functionality and operations. Participation in all three modules trains state/territory, tribal, regional, or urban area communications personnel on how to activate and deactivate various gateway devices.

**There is a minimum of five or a maximum of 10 students identified for the gateway hands-on configuration module in order for CISA to schedule and conduct the course.**

**Training Modules:**

- **Gateway Overview:** A high-level overview for all personnel requiring a basic understanding of audio gateway capabilities. There is no set maximum capacity for this portion. It can be presented even in a conference setting.
- **Advanced Audio Gateway Operation**: For communication/technical specialists who need a more advanced understanding of gateway operations; for example, the various types of patches and how to establish or disconnect them. Each person (up to 20) needs to have a laptop that simulation software can be uploaded to for this module, which is ideal for dispatchers and gateway technicians.
- **Gateway Hands-on Configuration**: Focused on specific equipment and is for gateway installers, maintenance technicians, and specialists. This module is limited to 10 students. A second instructor can be assigned to double the course capacity if necessary to meet the needs of the site.
- The workshop's lectures, discussions, and practical exercises are focused on the gateways specific to the site and are intended to prepare personnel in a region to quickly activate and deactivate their own equipment. The workshop with all modules is approximately six to eight hours long. Each module builds on previous module(s). The Gateway Hands-on Configuration training session can accommodate up to 10 students.
- Customized support for this offering may vary to meet each state's unique needs. Potential design options, outcomes, and deliverables may include:
    - Basic understanding of audio gateway functionality
    - Advanced audio gateway operations for ICT Branch personnel
    - Limited operator proficiency
    - Identifying LMR communications interoperability issues
    - High level overview for different audio gateways
    - Audio gateway integration into NIMS ICS operations for ICT Branch personnel
    - Hands-on exercise
    - Techniques for mitigating RF interference

# Training & Exercises

| *Resilient Communications Awareness Webinar* | |
|---|---|
| TA Delivery Method: | Four-hour Webinar |
| Recommended Participants: | Emergency Response Personnel to include fire, EMS, law enforcement, emergency management, and telecommunications personnel |
| Catalog Item Description | TRG-RESCOM_AWR |

## Offering Overview

Public safety agencies continue to deal with radio interference from both malicious and non-malicious sources that impacts operational effectiveness. Many operational personnel do not receive training on how to recognize interference or on what steps to take to attempt restoration of their communications when they experience interference in the field.

This webinar provides first responders with the essential knowledge to understand the causes of interference and remedial actions that can be taken to restore communications by first recognizing an occurrence of interference, and then appropriately reacting to and reporting the incident.

**There are no minimum participants for this offering.**

**Prerequisites for Attendance:**

- None

**Course Registration Process:**

- Registration needs will be determined during a scoping call

| *Resilient Incident Communications Management Training Course* | |
|---|---|
| TA Delivery Method: | Two-day In-Person Course |
| Recommended Participants: | Information and Communications Technology Branch personnel, public safety agency communications managers and technical personnel |
| Catalog Item Description | TRG-RESCOM_MGT |

## Offering Overview

Public safety agencies continue to deal with radio interference from both malicious and non-malicious sources that impacts operational effectiveness. Many operational personnel do not receive training on how to recognize interference or on what steps to take to attempt restoration of their communications when they experience interference in the field.

This course provides trained ICT Branch, public safety agency communications managers and communications technical personnel with enhanced communications resiliency planning and RF interference recognition capabilities, enabling better preparedness and rapid mitigation of communications obstacles.

**There must be a minimum of eight and up to a maximum of 20 qualified students for CISA to conduct the course.**

**Prerequisites for Attendance:**

- **Required:**
  - Familiarity developing incident communications plans
  - Demonstrated experience deploying and troubleshooting LMR communications in support of an incident
  - Understanding of RF concepts including propagation, interference, attenuation, etc.
- **Recommended:**
  - RESCOM-AWR Webinar
  - L0969 – All-Hazards COML
  - All-Hazards Incident COMT

**Course Registration Process:**

- **SWIC (or designated POC) action:**
  - Review and approve the student list for appropriate qualification
  - Submit student verification form to CISA at least 14 days prior to the course

**Offering Requirements:**

To facilitate the exercise activities contained in the course, a radio cache with radios for each student and a minimum number of clear channels must be provided by the state or hosting agency. Ideally the channels should be conventional, analog or digital, simplex. These requirements will be discussed in a logistics call prior to course delivery.

# Usage

| *Rural, Tribal, Territorial Emergency Communications Needs Assessment* | |
|---|---|
| TA Delivery Method: | In-Person Workshop |
| Recommended Participants: | Local Public Safety Personnel, Local Emergency Communications Personnel, Tribal Leadership, SWIC |
| Catalog Item Description | OP-ASMTRTTECN |

## Offering Overview

This TA offering will serve as a vital resource for underserved communities to make informed and cost-effective decisions regarding LMR, Alerts and Warnings, and PSAP equipment. The assessment documents the operation, maintenance, and replacement of LMR, Alerts and Warning, and PSAP systems while offering stakeholders valuable insights into best practices throughout the entire equipment lifecycle in a comprehensive report.

To assess the unique needs of the stakeholder's emergency communication system, this TA offering concentrates on several key areas in both operational and functional aspects of the equipment. It evaluates the type and age of the equipment; its potential for reuse; interoperability with neighboring jurisdictions; and the extent of manufacturer support for vital components, such as base stations, portable and mobile radios, and dispatch consoles. As part of this process, a conceptual system design will be developed and guided by propagation analyses and thorough documentation to address any identified technical and functional gaps.

The assessment also identifies the essential features and functions required for a new system to effectively meet operational needs and align with industry best practices, as gathered from user interviews and previous system evaluations. The review includes a summary of current system users across various agencies and disciplines, as well as an evaluation of other technical components and systems, such as in-car repeaters, fire paging systems, and cybersecurity. By integrating these initiatives, the assessment delivers an evaluation of the system's existing capabilities, while also outlining suggested improvements to increase effectiveness and guide the strategic allocation of limited financial resources.

**Customized support for this offering may vary to meet rural, tribal and territorial unique needs. Potential design options, outcomes, and deliverables may include:**

- Assessment of existing system(s), including:
  - User interviews to determine current system challenges
  - Tower locations, antennas, shelter, shelter equipment, and backhaul
  - Frequencies in use – propagation for in building, critical buildings, mobile and portable talk-in and talk-out
  - Equipment type, age and ability to be reused, manufacture support (base stations, portable and mobile radios, dispatch consoles, etc.)
  - Current system design
  - Other technical components or systems (in-car repeaters, fire paging, etc.)
  - Cybersecurity
- Documentation of current system users – agencies and disciplines
- Documentation of interoperability partners

***(Continued on next page)***

# Usage

- Identification of features and functions the new system must have to meet operational needs and existing industry best practices identified in interviews and system evaluation
- Conceptual system design with propagation analyses and documentation of filling technical and functional gaps
- Assessment of usage with other existing regional or state systems

# Usage

| *Operational Communications Assessment* | |
|---|---|
| TA Delivery Method: | In-Person Workshop or Webinar |
| Recommended Participants: | SWICs and Public Safety Professionals |
| Catalog Item Description | OP-ASMT |

## Offering Overview

All operable and interoperable communications must be efficient and intuitive in order to be effective tools for public safety responders and communications specialists. Operational communications assessments, therefore, ensure that proposed or in-place technologies, plans, and procedures enhance and support operations. CISA presents the results of each assessment through an Operational Assessment Report.

**Customized support for this offering may vary to meet each SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Communications Assessment Workshop identifying site-specific strengths and needs
- Site-specific Operational Communications Assessment Report focusing on technological and procedural capabilities and needs
- Operational Communications Assessment Report Review Meeting/Briefing

# Usage

| ***Regional Communications Enhancement Support – Strategic Communications Migration Plan*** | |
|---|---|
| TA Delivery Method: | In-Person Workshop or Webinar |
| Recommended Participants: | SWICs and Public Safety Professionals |
| Catalog Item Description | RCES-SCMP |

## Offering Overview

This TA offering helps stakeholders develop a usable regional Strategic Communications Migration Plan that requires the collaborative efforts and inputs of local public safety professionals. In order to document the input of all stakeholders and develop a plan in the most efficient and effective manner, the workshop provides an opportunity for stakeholders to define their individual and regional operational needs, identify commonalities between the goals and needs of various stakeholder groups, develop regional migration goals and priorities that capitalize on those commonalities, and establish milestones to facilitate achieving each goal and priority.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Regional Strategic Communications Migration Plan Workshop
- Regional Strategic Communications Migration Plan
- Regional Strategic Communications Migration Plan Review Briefing

# Usage

| *Communications Focused Special Event Planning* | |
|---|---|
| TA Delivery Method: | In-Person Workshop/Webinar and/or On-site Support |
| Recommended Participants: | SWICs and Public Safety Professionals |
| Catalog Item Description | OP-SPEV |

## Offering Overview

Large-scale planned events require substantial operational planning and preparation to coordinate all public safety participants to ensure that the event proceeds smoothly, and to prepare to respond to related incidents that may occur during planned events.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Use of NSSE/SEAR. Communications Planning Toolkit[19] and implementation support
- Event-specific Communications Plan(s)/ SOP(s)
- Customized Event Planning "Battle Rhythm"
- Event-specific Concept of Operations (CONOPS)
- Event-specific frequency/channel plan(s)
- Customized event planning briefing tools/kits
- On-site planning and coordination support

[19]The NSSE/SEAR Communications Planning Toolkit provides guidance and helpful tools to assist officials tasked with preparing for and providing communications support during events designated as National Special Security Events, or receiving a Special Event Assessment Rating.

# Usage

| *Communication Assets Survey and Mapping Tool Training* | |
|---|---|
| TA Delivery Method: | In-Person Workshop |
| Recommended Participants: | SWICs, Communications Planners, System Owners, Communications Unit Personnel |
| Catalog Item Description | CASM-TRAIN |

## Offering Overview

CISA provides, at no-cost to authorized requestors, a secure web-based tool for all public safety agencies to maintain, share, and visualize their radio communications asset information for coordination and planning purposes. This offering provides assistance in establishing, maintaining, and sharing communications resource information in the Communication Assets Survey and Mapping (CASM) Tool, as well as training on its operation for interoperability planning.

Currently, CASM stores data regarding over 96,000 agencies nationwide on a secure server with multiple levels of access depending on authorizations. CASM is Federal Information Security Management Act (FISMA)-compliant, with an authority to operate on the DHS secure network. DHS has committed to CASM long term as an officially recognized level 3 system under formal Chief Information Officer management. CASM maintains data about public safety agencies and their radio communications equipment across all public safety disciplines and levels of government. As shared by agencies, CASM provides a standardized nationwide view of agencies, fixed and mobile assets, personnel, and spectrum usage information, as well as coverage plots for radio base stations.

CASM provides a means for agencies working together to plan and improve public safety communications. It is important that data in CASM be as complete and accurate as possible to ensure communications planning is effective. CASM SMEs are available to review an agency's data for errors and consistency.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- CASM training to:
  - Maintain a detailed inventory of communications infrastructure (systems, comm sites, and dispatch centers)
  - Engage with other jurisdictions to do detailed planning
  - Track Communications Unit personnel contact information, deployability, and certifications
  - Initiate or maintain statewide or interstate planning
  - Maintain shared channel or talkgroup, and agency usage information
  - Maintain information about MCU capabilities and deployability
  - Maintain information about mobile assets (caches, gateways, etc.)
  - Manage information access control including delegation of privileges
  - Generate coverage plots
- On-site assistance with data entry and validation supporting any of the above

# Usage

| *Encryption Planning and Usage* | |
|---|---|
| TA Delivery Method: | In-Person Workshop or Webinar |
| Recommended Participants: | SWICs, Regional Emergency Communications Coordination Working Group (RECCWGs), LMR System Operators, Public Safety Command/Leadership, and Communications Personnel |
| Catalog Item Description | ENG-ENCRYPT |

## Offering Overview

Understanding the technical aspects of encryption can be very complex and confusing. Whether it's a single community, regional, or statewide intrastate issue, laying a solid foundation for the use of encryption is essential to developing an interoperable, successful, and lasting encryption program.

In addition to providing a basic overview of encryption and its technical aspects, CISA's encryption workshop will also provide stakeholders an awareness of the encryption support that is available to SLTT authorities.

**Customized support for this offering may vary to meet SLTT unique needs. Potential design options, outcomes, and deliverables may include:**

- Explaining the basics of encryption
- Explaining more technical aspects of encryption
- Establishing criteria and potential use scenarios or use of encryption
- Facilitating discussion amongst users to gauge willingness to participate in a coordinated encryption effort
- Surveying users on multiple factors to determine current capabilities, potential gaps, and future encryption needs
- Identifying the capability requirements and reviewing the specifications of available hardware
- Identifying Memoranda of Agreement (MOAs) or Memoranda of Understanding (MOUs) that are necessary for implementation
- Reviewing on-going system maintenance and database upkeep requirements
- Working with governmental and non-governmental radio shops in the application of encryption programs
- Equipment, encryption basic use analysis
- Encryption system SOP template and full plan assessment and development (minimum equipment for subscriber units and rules of use)

# Usage

| *Priority Telecommunications Services* | |
|---|---|
| TA Delivery Method: | Webinar |
| Recommended Participants: | SWICs and Public Safety Managers and Stakeholders |
| Catalog Item Description | TRG-GETSWPS |

## Offering Overview

Federal, state, local, tribal, and territorial government organizations rely on a mix of communications devices technologies to communicate during an emergency. When communicating by cellular or landline networks, government users share those networks with the public. Should those networks become overloaded due to high call volumes or other impairment, responders may not be able to communicate at a critical moment.

**The Government Emergency Telecommunications Service (GETS)** provides public safety personnel priority access and prioritized processing in the local and long-distance segments of the landline networks, greatly increasing the probability of call completion. Typical GETS users are responsible for the command and control functions critical to management of, and response to, national security and public safety emergencies, particularly during the first 24 to 72 hours following an event.

**Wireless Priority Service (WPS)** provides public safety personnel priority access and prioritized processing in all nationwide and several regional cellular networks, greatly increasing the probability of call completion. WPS is intended to be used when cellular networks are congested and the probability of completing a normal cellular call is reduced.

**Telecommunications Service Priority (TSP)** authorizes public safety organizations to receive priority treatment for vital voice and data circuits. The TSP program provides service vendors an FCC mandate to prioritize requests by identifying those services critical to national security and public safety. A TSP assignment ensures that it will receive priority attention by the service vendor before any non-TSP service.

Tailored support for these services is available through the appropriate CISA Priority Telecommunications Services Area Representative (PAR) and by contacting the CISA Priority Telecommunications Service Center at 1-866-627-2255. Additional information regarding GETS, WPS, and TSP can be found at the following websites:

- Government Emergency Telecommunications Service (GETS) | CISA
- Wireless Priority Service (WPS) | CISA
- Telecommunications Service Priority (TSP) | CISA

**Customized support for this offering may vary to meet each state's unique needs. Potential design options, outcomes, and deliverables may include:**

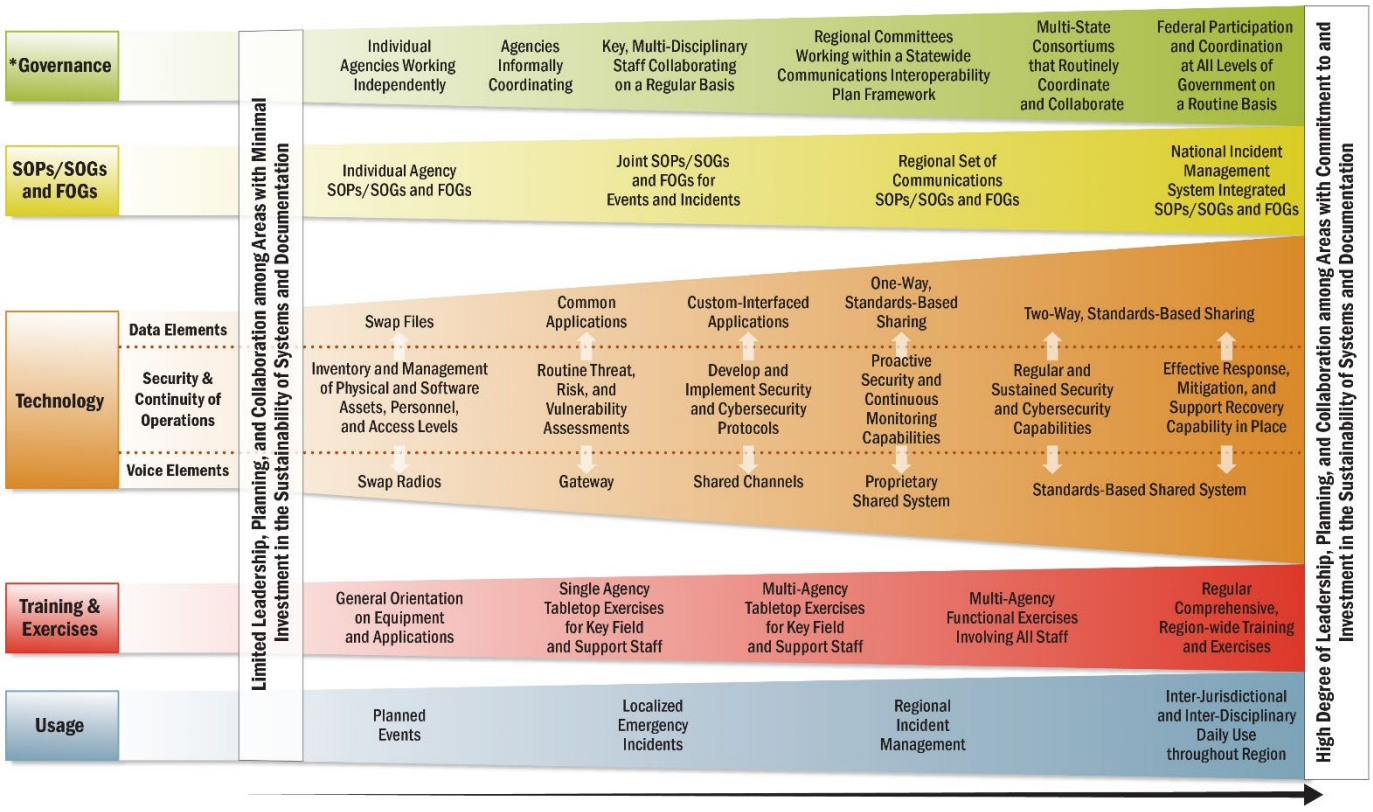
- 30-minute webinar
- Explanation of National Security/Emergency Preparedness Services
- How to request National Security/Emergency Preparedness Services
- Eligibility criteria and costs
- How GETS and WPS operate within the FirstNet environment

# Appendix A: SAFECOM Resources

## SAFECOM Website Resources

SAFECOM's mission is to improve designated emergency response providers' inter-jurisdictional and inter-disciplinary emergency communications interoperability through collaboration with emergency responders across SLTT governments and international borders.[20]

CISA supports emergency communications professionals and responders by providing access to tools, resources, and training for maintaining interoperable emergency communications systems, policies and procedures. The CISA TA Request Form for SWICs' use and the TA Evaluation Form for stakeholders' feedback are posted with instructions for their completion here: [cisa.gov/safecom/ictapscip-resources](cisa.gov/safecom/ictapscip-resources).




SAFECOM Interoperability Continuum

[20]Additional information regarding SAFECOM is available at: [cisa.gov/safecom](cisa.gov/safecom).

# APPENDIX B: ADDITIONAL TA RESOURCES

## National Interoperability Field Operations Guide (NIFOG) 2.01

The NIFOG version 2.01 can be viewed and downloaded by clicking on the link below. New content in 2.01 includes references on Information Technology, Emergency Wireless Carrier Services, Interference Management, Encryption, and Cybersecurity. The NIFOG is a technical reference for emergency communications planning and for radio technicians responsible for radios that will be used in disaster response. The NIFOG includes rules and regulations for use of nationwide and other interoperability channels, tables of frequencies and standard channel names, and other reference material, formatted as a pocket-sized guide for radio technicians to carry with them.

To view and download the PDF version, please visit: cisa.gov/publication/fog-documents.

## National Special Security Events (NSSE)/Special Event Assessment Rating (SEAR) Communications Planning Toolkit

The NSSE/SEAR Communications Planning Toolkit includes the updated NIMS/ICS structure and a standardized approach to the command, control, and coordination for event management. Planning considerations for cybersecurity and information technology have been added to Version 2.0.

CISA has continued to provide communications planning support to the state, local, and federal jurisdictions managing communications for NSSEs such as the Super Bowl and political conventions. This toolkit, which leverages best practices from those events, has been written as a resource guide for state, local, and federal authorities tasked with preparing for and providing communications support for future NSSEs. It also includes tools and templates to support communications planning.

Providing resources like this toolkit is part of our mission to support you and your jurisdictions in strengthening emergency communications capabilities and preparedness nationwide.

To request an electronic copy of the NSSE/SEAR Planning Toolkit, please contact: TARequest@cisa.dhs.gov.

# Appendix B: Additional TA Resources

## Primary, Alternate, Contingency, Emergency (PACE) Planning Toolkit

The PACE Planning Toolkit helps organizations establish options for redundant communications capabilities if primary capabilities are disrupted or degraded. Communications ecosystem failures clearly highlight the need for an agency to have a communications PACE plan. The toolkit includes a PACE card, infographic, checklist, and sample scenarios.

The toolkit leads an agency through the planning effort from identifying points of possible primary system failures, recognizing and cataloging alternate back-up resources, consideration of contingent systems, and last resort emergency options. The toolkit helps an agency decide what the PACE triggers may be. It also reminds the user that training and exercises are necessary for the successful implementation of PACE plans.

Providing resources like this toolkit is part of our mission to support you and your jurisdiction in strengthening emergency communications capabilities and preparedness nationwide.

To request an electronic copy of the PACE Planning Toolkit, please contact: TARequest@cisa.dhs.gov.

## Rural Emergency Medical Communications Demonstration Project (REMCDP) Planning Toolkit

The REMCDP Planning Toolkit is an extensive toolkit that offers a systematic approach for facilitating conversations with local and tribal stakeholders, creating scenarios to improve resilience in emergency communications, and providing resources to help local and tribal entities conduct their own workshops.

The toolkit also includes key materials and templates such as radio training resources, funding information handouts, a facilitator's guide for a COOP, and resources for PACE planning.

Through these resources, we aim to support you and your jurisdictions in strengthening emergency communications capabilities and overall preparedness across the nation.

To request an electronic copy of the REMCDP Planning Toolkit, please contact: TARequest@cisa.dhs.gov.

# Appendix B: Additional TA Resources

## Cybersecurity PSAP Ransomware Poster

The ransomware poster can be placed in an ECC/PSAP, 911 Call Centers, or 911 Dispatch Centers. The poster provides information about what ECC staff can do to reduce the risk of ransomware. Although the poster's focus is on ransomware, its recommendations are applicable across a range of cyber threats like phishing, social engineering, and password management. To request an agency or state-specific customized electronic PDF version of the poster suitable for printing, SWICs may contact their CISA Emergency Communications Coordinator and/or email the request to: posterrequests@ntat.us.

To view and download the PDF version, please visit: Cybersecurity PSAP Ransomware Poster

## Cybersecurity Telephony Denial of Service (TDoS) Poster

The TDoS poster can be placed in an ECC/PSAP, 911 Call Centers, or 911 Dispatch Centers. The poster provides information about what ECC staff can do to reduce the risk of TDoS attacks. The poster reviews TDoS attack vectors and provides examples of TDoS attacks targeting administrative and 911 lines, specific best practices, recommendations on how to mitigate TDoS attacks, and contact information for federal partners and customizable space for additional resources. To request an agency or state-specific customized electronic PDF version of the poster suitable for printing, SWICs may contact their CISA Emergency Communications Coordinator and/or email the request to: posterrequests@ntat.us.

To view and download the PDF version, please visit: Cybersecurity TDoS Poster

## Cybersecurity PSAP Swatting Poster

The PSAP Swatting poster can be placed in an ECC/PSAP, 911 Call Centers, or 911 Dispatch Centers. The poster provides information about what Swatting is and what ECC staff can do to recognize and reduce the impact of Swatting attacks. The poster reviews characteristics of an attack, key points to consider during an event, planning and considerations, and contact information for federal partners and customizable space for additional resources. SWICs and/or SLTT POCs may request a digital copy of the poster (sized at 24"x 36") for printing. To request an agency or state-specific poster, SWICs may contact their CISA Emergency Communications Coordinator and/or email the request to posterrequests@ntat.us.

To view additional resources, please visit: cisa.gov/publication/next-generation-911.

# Appendix C: Acronyms

| Acronym | Definition |
|---|---|
| **AAR/IP** | After-Action Report/Improvement Plan |
| **AG** | Audio Gateway |
| **ASAP** | Automated Security Alarm Protocol |
| **ASI** | Active Shooter Incident |
| **AUXC** | Auxiliary Communicator |
| **AUXCOMM** | Auxiliary Communications |
| **AUXFOG** | Auxiliary Communications Field Operations Guide |
| **AWN** | Alerts, Warnings, and Notifications |
| **BRBND** | Broadband |
| **BRBNDLTE** | Broadband Strategic Planning Support and Education |
| **BRBEVNTASMT** | Mobile and Fixed Site Data Use Assessment for Incidents and Planned Events |
| **BRBDATA** | Broadband Technologies and Data Operability/Interoperability in Support of Public Safety |
| **CAD** | Computer-Aided Dispatch |
| **CASM** | Communication Assets Survey and Mapping |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **COG** | Continuity of Government |
| **COML** | Communications Unit Leader |
| **COMMDRILL** | Communications Drill |
| **COMMEX** | Communications Exercise |
| **COMMS-ASI** | Communications During Active Shooter Incidents |
| **COMT** | Communications Technician |
| **COMUAWR** | All-Hazards Incident Communications Unit Awareness |
| **COMUPLAN** | Communications Unit Planning and Policies |
| **COOP** | Continuity of Operations Plan |
| **CR911** | Cyber Resilient 911 |
| **CRA** | Cybersecurity Readiness Assessment |
| **CSA** | Cybersecurity Advisor |
| **CSD** | Cybersecurity Division |
| **CSF** | Cybersecurity Framework |
| **CYBR** | Cyber |
| **CYB-ASMTFULL** | Full Cyber Assessment |
| **CYB-ASMTRAPID** | Rapid Cyber Assessment |
| **CYB-WKSPOSTASMT** | Post Assessment Workshop |
| **CYB-WKSTHRTASMTRSP** | Threat Assessment and Response Workshop |
| **CYB-WKSTHRTAWR** | Cyber Threat Awareness Workshop |

# Appendix C: Acronyms

| Acronym | Definition |
|---|---|
| **DHS** | U.S. Department of Homeland Security |
| **EAS** | Emergency Alert System |
| **ECC** | Emergency Communications Coordinator |
| **ECC** | Emergency Communications Center |
| **ECD** | Emergency Communications Division |
| **EDT** | Exercise Design Team |
| **eAUXFOG** | Electronic Auxiliary Communications Field Operations Guide |
| **eFOG** | Electronic Field Operations Guide |
| **eNIFOG** | Electronic National Interoperability Field Operations Guide |
| **EMAC** | Emergency Management Assistance Compact |
| **EMI** | Emergency Management Institute |
| **EMS** | Emergency Medical Services |
| **ENCRYPT** | Encryption |
| **EOC** | Emergency Operations Center |
| **EPT** | Exercise Planning Team |
| **ESF** | Emergency Support Function |
| **EXDESIGN** | Exercise Design |
| **EXPLAN** | Exercise Plan |
| **FCC** | Federal Communications Commission |
| **FE** | Functional Exercise |
| **FEMA** | Federal Emergency Management Agency |
| **FEMA EMI** | Federal Emergency Management Agency Emergency Management Institute |
| **FEMA NIC** | Federal Emergency Management Agency National Integration Center |
| **FirstNet** | First Responder Network Authority |
| **FISMA** | Federal Information Security Management Act |
| **FOG** | Field Operations Guide |
| **FSE** | Full Scale Exercise |
| **FSLTT** | Federal, State, Local, Tribal, and Territorial |
| **FY** | Fiscal Year |
| **GETS** | Government Emergency Telecommunications Service |
| **GIS** | Geographic Information System |
| **GOV-DOC** | Governance Document |
| **HF** | High Frequency |
| **HSGP** | Homeland Security Grant Program |
| **HSEEP** | Homeland Security Exercise and Evaluation Program |
| **ICC** | Incident Command Center |
| **ICS** | Incident Command System |
| **ICT** | Information Communications and Technology |
| **ICTAP** | Interoperable Communications Technical Assistance Program |
| **IP** | Improvement Plan |
| **IPAWS** | Integrated Public Alert and Warning Systems |

# Appendix C: Acronyms

| Acronym | Definition |
|---|---|
| **INCM** | Incident Communications Center Manager |
| **INTD** | Incident Tactical Dispatcher |
| **IT** | Information Technology |
| **ITSL** | Information Technology Service Unit Leader |
| **LMR** | Land Mobile Radio |
| **LTE** | Long Term Evolution |
| **MASS** | Mutual Aid Support System |
| **MEP** | Master Exercise Practitioner |
| **MCI** | Mass Casualty Incident |
| **MCU** | Mobile Communications Unit |
| **MHz** | Megahertz |
| **MOA** | Memorandum of Agreement |
| **MOU** | Memorandum of Understanding |
| **MRP** | Mission Ready Package |
| **MSEL** | Master Scenario Events List |
| **NCSWIC** | National Council of Statewide Interoperability Coordinators |
| **NECP** | National Emergency Communications Plan |
| **NENA** | National Emergency Number Association |
| **NG911** | Next Generation 911 |
| **NGCS** | Next Generation 911 including Core Services |
| **NG-SEC** | Security for Next Generation 911 Standard |
| **NIFOG** | National Interoperability Field Operations Guide |
| **NIMS** | National Incident Management System |
| **NIST** | National Institute of Standards and Technology |
| **NOAA** | National Oceanic and Atmospheric Administration |
| **NSSE** | National Special Security Events |
| **OP-ASMT** | Operational Assessment |
| **OP-SPEV** | Special Event Planning |
| **ORAP** | Operational Rapid Assistance Package |
| **PAR** | Priority Telecommunications Services Area Representative |
| **PACE** | Primary, Alternate, Contingency, and Emergency |
| **POC** | Point of Contact |
| **PSA** | Protective Security Advisor |
| **PSAP** | Public Safety Answering Point |
| **PTB** | Position Task Book |
| **PTS** | Priority Telecommunications Services |
| **QRB** | Qualifications Review Board |
| **RADO** | Radio Operator |
| **RCA** | Root Cause Analysis |
| **RCES** | Regional Communications Enhancement Support |
| **RECCWG** | Regional Emergency Communications Coordination Working Group |
| **REMCDP** | Rural Emergency Medical Communications Program |

# Appendix C: Acronyms

| Acronym | Definition |
|---|---|
| **RESCOM-AWR** | Resilient Communications Awareness Training Webinar |
| **RESCOM-MGT** | Resilient Communications Incident Communications Management |
| **RF** | Radio Frequency |
| **RMS** | Records Management System |
| **SAFECOM** | Safety Communications |
| **SAP** | Security Assessment Plan |
| **SAR** | Security Assessment Report |
| **SCMP** | Strategic Communications Migration Plan |
| **SCIP** | Statewide Communication Interoperability Plan |
| **SEAR** | Special Event Assessment Rating |
| **SIEC** | State Interoperability Executive Committee |
| **SIGB** | Statewide Interoperability Governance Board |
| **SITMAN** | Situation Manual |
| **SLTT** | State, Local, Tribal, and Territorial |
| **SME** | Subject Matter Expert |
| **SOG** | Standard Operating Guidelines |
| **SOP** | Standard Operating Procedure |
| **SP** | Special Publication |
| **SPEV** | Special Event |
| **SS-AUXCOMM** | State-Sponsored Auxiliary Communications Course |
| **SS-COML** | State-Sponsored Communications Unit Leader Course |
| **SS-COMT** | State-Sponsored Communications Technician Course |
| **STO** | State Training Officer |
| **STRATPLAN** | Strategic Planning |
| **SWIC** | Statewide Interoperability Coordinator |
| **TA** | Technical Assistance |
| **TDoS** | Telephony Denial of Service |
| **TERT** | Telecommunicator Emergency Response Taskforce |
| **THSGP** | Tribal Homeland Security Grant Program |
| **TICFOG** | Tactical Interoperable Communications Field Operations Guide |
| **TICP** | Tactical Interoperable Communications Plan |
| **TSCIP** | Tribal Strategic Communication Interoperability Plan |
| **TSP** | Telecommunications Service Priority |
| **TtT** | Train-the-Trainer |
| **TTX** | Tabletop Exercise |
| **UASI** | Urban Area Security Initiative |
| **UHF** | Ultra-High Frequency |
| **VHF** | Very High Frequency |
| **VoIP** | Voice over Internet Protocol |
| **WEA** | Wireless Emergency Alerts |
| **WPS** | Wireless Priority Service |