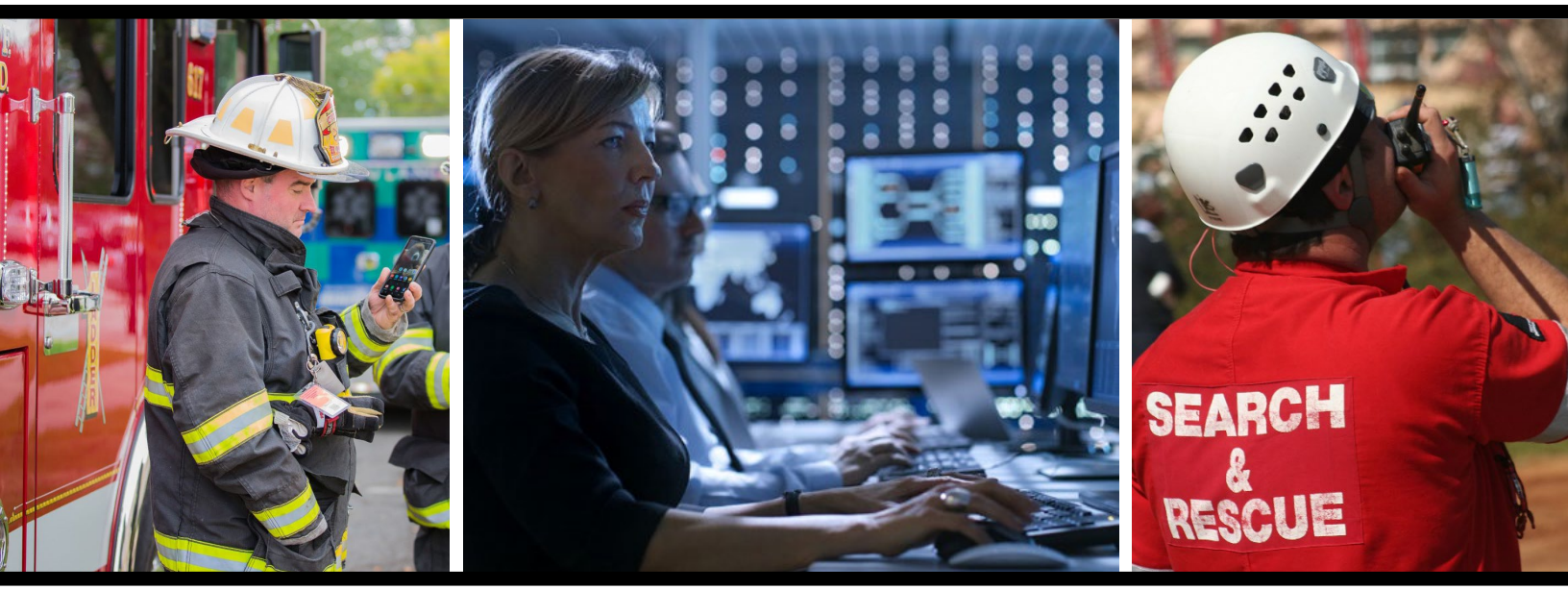


EMERGENCY COMMUNICATIONS TECHNICAL ASSISTANCE AND PLANNING GUIDE

FY2021 Highlights and Offerings

TA/SCIP Guide Version 6.1

January 2021

Cybersecurity and Infrastructure Security Agency

Table of Contents

FOREWORD 1
Communications Unit Virtual Training Student Requirements 2
TA Request Process 4
New and Updated CISA Technical Assistance Offerings for FY2021 5
CISA EMERGENCY COMMUNICATIONS COORDINATION SUPPORT 7
GOVERNANCE 8
Statewide Communication Interoperability Plan (SCIP) Workshop 8
Governance Documentation Review, Assessment, and Development (GOV-DOC) 9
Communications Unit Planning and Policies (COMUPLAN) 10
Communications Unit Assistance under Emergency Management Assistance Compact (EMAC) 11
Grant Funding for Emergency Communications Webinar 12
STANDARD OPERATING PROCEDURES 13
Standard Operating Procedures (SOP)/Standard Operating Guides (SOG)/Communications Plan Review and Development 13
Tactical Interoperable Communication Plan (TICP) Development/ Implementation Workshop 14
Tactical Interoperable Communications Field Operations Guide (TIC-FOG) Development/Update 15
Electronic Field Operations Guide (eFOG) Development 16
TECHNOLOGY 17
Broadband Strategic Planning Support and Education (BRBNDLTE) 17
Mobile and Fixed Site Data Use Assessment for Incidents and Planned Events (BRBEVNTASMT) 18
Broadband Technologies and Data Operability/Interoperability in Support of Public Safety (BRBDATA) 19
Next Generation 9-1-1/Strategic Planning Support (NG9-1-1STRATPLAN) 20
9-1-1/PSAP/LMR Cyber Awareness (9-1-1PSAPCYBRAWR) 21
9-1-1/PSAP/LMR Cyber Assessment (9-1-1PSAPCYBRASMT) 22
Alerts and Warnings (ALERTS) 24
LMR/LTE Coverage Testing & Simulation (LMR/LTE) 25
TRAINING & EXERCISES 26
Communications Unit Exercise (COMMEX) for Communications Unit Trainees 26
Communications-Focused Exercises (TTX, FE, FSE) 27
Communications Focused Drill/Activities (COMMDRILL) 28
Communications-Focused Exercise Design and Planning (EXDESIGN) 29
Communications Unit Leader (COML) Training Course 30
Communications Unit Technician (COMT) Training Course 32
Incident Tactical Dispatcher (INTD) Training Course 33
Information Technology Service Unit Leader (ITSL) Training Course 34
Incident Communications Center Manager (INCM) Training Course 35
All-Hazards Incident Communications Center Manager (INCM)/Incident Tactical Dispatcher (INTD) Awareness Overview (TRG-OVERVW) 36
Radio Operator (RADO) Training Course 37

Auxiliary Communications (AUXCOMM/AUXC) Training Course 38
All-Hazards Incident Communications Awareness Overview (TRG-COMUAWR) 39
Auxiliary Communications Train-the-Trainer (AUXCOMM/AUXC TtT) Course 40
Communications Unit Leader Train-the-Trainer (COMLTtT) Course 42
Communications Unit Technician Train-the-Trainer (COMTTtT) Courses 44
State-Sponsored CISA Recognized Communications Unit Instruction (SS-COMT, SS-COML, SS-AUXCOMM/AUXC) 46
Audio Gateway Information and Training (AG) 49
USAGE 50
Operational Communications Assessment (OP-ASMT), Regional Communications Enhancement Support – Strategic Communications Migration Plan (RCES-SCMP), and Special Event Planning (OP-SPEV) 50
Communication Assets Survey and Mapping (CASM) Tool 51
Encryption Planning and Usage (ENCRYPT) 52
Priority Telecommunications Services (PTS) 53
APPENDIX A: SCIP GUIDE 54
APPENDIX B: SAFECOM RESOURCES 60
APPENDIX C: TA REQUEST FORM 61
APPENDIX D: ADDITIONAL TA RESOURCES 64
APPENDIX E: ACRONYMS 65

Foreword

In a year of a global pandemic, the Cybersecurity and Infrastructure Security Agency (CISA) remained resilient in providing coordination support to the national security and emergency response community to ensure the resiliency and security of our Nation. A key part of this was transitioning in-person technical assistance engagements to the virtual environment.

Since the beginning of the pandemic, CISA's Interoperable Communications Technical Assistance Program (ICTAP) has delivered more than 100 virtual Technical Assistance (TA) engagements in 39 states and territories. This included 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.

With the everchanging emergency communications environment in mind, I am pleased to present the *FY2021 Emergency Communications Technical Assistance/Statewide Communication Interoperability Plan (SCIP) Guide*. This year's Guide includes several new or enhanced virtual TA and SCIP workshop options to accommodate the current social distancing requirements.

CISA TA offerings are provided to all 56 states and territories and Native American and Alaska Native tribes at no cost and may be requested at any time throughout the year. The offerings can be utilized to address a variety of communications interoperability issues, to remain current in the understanding of new and emerging technologies, to revitalize and enhance governance policies and procedures, and to enrich the integrity of Communications Unit personnel training and resource management.

CISA Emergency Communications Coordinators (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. CISA will continue to partner with the public safety community and provide the tools and resources needed to promote communications used by emergency responders and government officials to 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

Virtual TA Services and Priorities for FY2021

Cybersecurity and Infrastructure Security Agency (CISA) continues to offer a portfolio of no-cost virtual technical assistance services during this unprecedented time using a variety of web-based platforms and remote instruction methodologies. Since the beginning of the global pandemic, Interoperable Communications Technical Assistance Program (ICTAP) has delivered more than 100 virtual Technical Assistance (TA) engagements in 39 states and territories. CISA is in the process of revising some of the Communications Unit training courses suitable for a virtual classroom and CISA continues to support interoperable communications capabilities and stakeholder readiness using a variety of remote learning options that support the following TA services:

- Statewide Communication Interoperability Plan (SCIP) Workshop
- Governance Documentation Review and Development
- Communications Unit Planning and Policy Development
- Grant Funding for Emergency Communications
- Standard Operating Procedures (SOP) Review and Development
- Alerts and Warnings
- Tactical Interoperable Communications Plan
- Tactical Interoperable Field Operations Guide
- Electronic Field Operations Guide
- Next Generation 9-1-1 Strategic Planning
- Public Safety Answering Point (PSAP)/9-1-1 Cybersecurity Awareness
- Communication Assets and Survey Mapping (CASM) Tool
- Encryption Planning and Usage

Virtual Communications Unit Training: (available Spring 2021)

- Communications Unit Leader Course (COML)
- Auxiliary Communications Course (AUXCOMM)
- Incident Tactical Dispatcher (INTD)
- Incident Communications Center Manager (INCM)
- INTD & INCM Awareness Overview (TRG-OVERVW)
- All-Hazards Incident Communications Awareness Overview (TRG-COMUAWR)

Throughout 2020 CISA supported states and territories by prioritizing strategic TA support that promoted the National Council of Statewide Interoperability Coordinators (NCSWIC) State Interoperability Markers program, which consists of 25 baseline State Performance Markers. These markers describe a state or territory's level of interoperability "health" and are aligned with state and territory SCIP goals and initiatives. For more information on the program, contact your respective CISA Emergency Communications Coordinator (ECC) referenced on page 6 of this document.

Virtual TA Approach: Nearly all technical assistance offerings can be customized and delivered virtually through a variety of media and web-based platforms. New requests will continue to be coordinated through the respective CISA ECCs and through the SWIC or point of contact requesting the TA in FY2021.

Communications Unit Virtual Training Student Requirements

- CISA has expanded its use of the virtual training platform to include Communications Unit Awareness, Communications Unit Leader (COML), Auxiliary Communications (AUXCOMM), Incident Communications Center Manager (INCM) and Incident Tactical Dispatcher (INTD) training courses. In preparation for attending a virtual training course, the following guidance is provided:

CISA Technical Assistance

- All virtual training courses are limited to a maximum of 15 students.

  Students registered for virtual courses will be required to attend a one-hour technical check and overview of the Webex Training platform prior to the course start date.

- Equipment requirements include:
  - Computer (Students cannot use tablets or smartphones for virtual courses. Many tablets and smartphones will not support the test taking function of Webex Training.)
  - Headsets with a microphone, or earbuds with built-in microphone
  - Web Camera a left on during the entire class
  - A reliable Internet connection (1.544mbps or faster)
- Students will be expected to download a .zip file during the Webex Training technical check that contains the electronic course materials they will need during the training sessions.
- Students will be expected to download a separate .zip file during the Webex Training technical check that contains a few pages they will need to print and have on hand for the course.

CISA Technical Assistance

TA Request Process

This year there are three enhanced categories of TA requests:

Strategic: Support that can be leveraged to directly support advancement of state performance markers, SCIP Goals and Initiatives and the implementation of the National Emergency Communications Plan (NECP).

State, Local, Tribal, and Territorial (SLTT) Requested: Support for the state or territory's normal, interoperable communications capabilities and policies for day-to-day operations and outreach activities related to emergency communications.

Significant Event Support: Support for planned events and unplanned after-action assessments that are designated as National Special Security Event (NSSE)/Special Event Assessment Rating (SEAR) or are the result of a natural or manmade disaster.

TA Request Form: To request TA, the SWIC or other designated SLTT point of contact needs to complete the fillable TA/SCIP request form on the SAFECOM website at: cisa.gov/publication/ictapscip-resources. Please be advised that the form needs to include what TAs the SLTT is requesting and if it is strategic, which guiding document it aligns to (Example: Supports Marker #8). The "Continuation Sheet" at the end of the form should be used to provide these additional details. Once completed, click "Submit" at the bottom of the form or email it directly to TARequest@cisa.dhs.gov.

TA Evaluation Form: At the conclusion of a TA, the SWIC or designated 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.

FY2021 TA/SCIP Resources

cisa.gov/publication/ictapscip-resources

CISA Technical Assistance

New and Updated CISA Technical Assistance Offerings for FY2021

Cybersecurity Assessment and Awareness

- The Cybersecurity Assessment employs the National Institute of Standards and Technology (NIST) Special Publication 800-53, Rev 5, "Security and Privacy Controls for Information Systems and Organizations," as a framework. CISA SMEs collaborate with the requestor on the security and privacy controls from the 800-53 framework to be used during the review.
- Cybersecurity Awareness Webinar: This offering introduces public safety personnel to common cybersecurity threats and vulnerabilities affecting 9-1-1/PSAP/ Land Mobile Radio (LMR) environments. Topics include ransomware attacks and their impact on PSAPs, recent telephony denial of service (TDoS) attacks against administrative lines and 9-1-1 directly, exposed networks and devices, shared passwords, cryptojacking and email phishing.
- CISA now offers customized PSAP Ransomware posters upon request. See Appendix D: Additional TA Resources for information on how to request.

Communications Unit Planning and Policies

- CISA now has a more holistic approach for providing communications unit planning and policy development that looks at the entire lifecycle for the state/territories communications professionals. The new Communications Unit Planning and Policies TA service now includes needs assessment, recruitment, training, qualifications, credentialing, certification, sustainability and succession planning, tracking, reporting and program maintenance.

INCM/INTD Awareness

- The Incident Communications Center Manager (INCM) and Incident Tactical Dispatcher (INTD) roles are critical aspects to managing communications in large-scale incidents or planned events (including NSSE/SEAR). For some incidents, the COML establishes an Incident Communications Center (ICC) staffed with Radio Operators (RADOs) to provide communications support for operations, an INCM for addressing coordination and avoid span-of-control issues, and INTDs for handling event- or incident-specific communications while the Emergency Communications Center/Public Safety Answering Point (PSAP) continues to handle normal call volume. This can be particularly helpful prior to large scale planned events or seasonal weather hazards where an ICC may be activated.

All-Hazards Incident Communications Awareness Overview

- This briefing provides an overview of All-Hazards Incident Communications and focuses on it's relationship to the National Incident Management System (NIMS) Incident Command System (ICS) structure and the skills and expertise of its personnel.
- It is intended for officials and responders who serve in any incident command and coordination role, and especially those who plan and provide emergency communications during planned events and emergent incidents.

Statewide Communication Interoperability Plan (SCIP) Workshop

The SCIP is a stakeholder-driven, multi-jurisdictional, and multi-disciplinary statewide strategic plan to enhance interoperable emergency communications. SCIPs serve as a single document for stakeholders throughout a SLTT communications ecosystem to prioritize resources, strengthen governance, identify future investments and address interoperability gaps.

CISA Technical Assistance

In 2019, CISA partnered with the NCSWIC and identified twenty-five State/Territory Interoperability Markers as a nationwide framework to describe interoperability maturity at the state/territory level. CISA subsequently conducted six Regional Workshops to collect baseline self-assessments for all 56 states and territories, which are updated on an annual basis.

SWICs use this information to update their SCIPs and request relevant technical assistance offerings to address current state/territory needs. SCIP should be updated on an annual basis and SCIP status information is maintained by CISA and is verified by the Federal Emergency Management Agency (FEMA) Grants Program Directorate through programmatic monitoring activities.

The Interoperability Markers also serve as a tool to support NECP implementation and to help States/Territories progress towards interoperability optimization. *(For a more detailed description see pg. 7)*

CISA Emergency Communications Coordination Support

CISA's Emergency Communications Coordinators (ECCs) assist SWICs and regional stakeholders with subject matter expertise, communications strategic planning, planning for day-to-day operations, special events, crisis communications coordination, and customized support that addresses local requirements/policies. They also coordinate the delivery of these services with the SWIC and/or local point of contact. Questions about CISA technical assistance services should be directed to the CISA ECCs assigned to each Branch.

East Branch (Regions I, II, III)

Branch Chief – Marty McLain Marty.Mclain@cisa.dhs.gov

- **ECC** – Bruce Belt Bruce.Belt@cisa.dhs.gov
- **ECC** – Chris Tuttle Christopher.Tuttle@cisa.dhs.gov
- **ECC** – Tom Gagnon Thomas.Gagnon@cisa.dhs.gov

Central Branch (Regions IV, V, VI, VII)

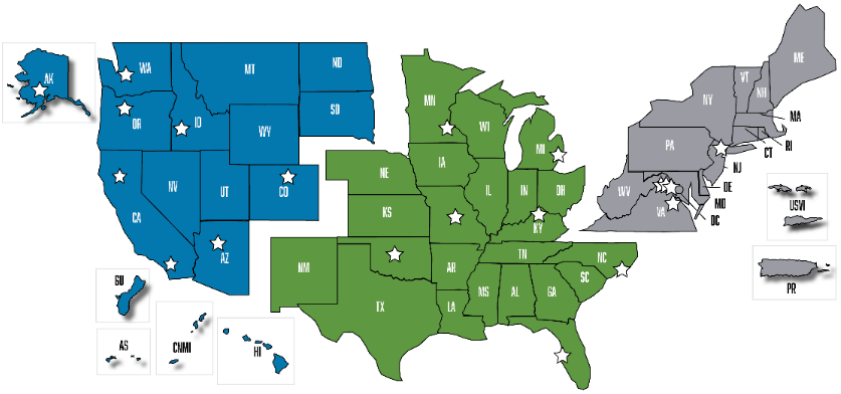
Branch Chief – Chris Essid Chris.Essid@cisa.dhs.gov

- **ECC** – Jim Jarvis James.Jarvis@cisa.dhs.gov
- **ECC** – Jim Lundsted James.Lundsted@cisa.dhs.gov
- **ECC** – Pam Montanari Pam.Montanari@cisa.dhs.gov
- **ECC** – Derek Nesselrode Derek.Nesselrode@cisa.dhs.gov
- **ECC** – James Stromberg James.Stromberg@cisa.dhs.gov

West Branch (Regions VIII, IX, X)

Branch Chief – Steve Noel Steven.Noel@cisa.dhs.gov

- **ECC** – Artena Moon Artena.Moon@cisa.dhs.gov
- **ECC** – Brandon Smith Brandon.Smith@cisa.dhs.gov
- **ECC** – Bruce Richter Bruce.Richter@cisa.dhs.gov
- **ECC** – Tom Lawless Thomas.Lawless@cisa.dhs.gov
- **ECC –** Jeremy Johnson Jeremy.Johnson@cisa.dhs.gov



*Stars on the map depict the geographic dispersion of ECCs across the country.

Governance

Statewide Communication Interoperability Plan (SCIP) Workshop	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	State Interoperability Executive Committee (SIEC)/Statewide Interoperability Governance Board (SIGB) Members: SWICs, State, Local, Federal, Tribal Stakeholders/Police, Fire and EMS Personnel, State 9-1-1 Administrators, FirstNet Representatives, State Information/Technology Officers

Offering Overview

The SCIP is a stakeholder-driven, multi-jurisdictional, and multi-disciplinary statewide strategic plan to enhance interoperable emergency communications. SCIPs serve as a single document for 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 (within 36 months) is a requirement of the Homeland Security Grant Program (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 look different to meet each state's unique needs. Potential design outcomes and deliverables may include:

- Draft SCIP that incorporates NGA recommendations, consideration of data gathered through the State Performance Markers baseline, and NECP goals and objectives
- Focused engagement to establish a governance body or strengthening existing governance, and building consensus
- Technology focused engagement for land mobile radio (LMR), broadband (BRBND), NG9-1-1, and Alerts and Warnings
- LMR sustainment and use of Alerts and Warnings
- Customized evaluation and action plan for implementation of the SCIP goals
- Evaluation and progress assessment of goals
- Governance
- Technology
- Funding sustainability
- Strategic goals and implementation plan
- Evaluation/progress management

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

Governance

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

Offering Overview

The SAFECOM/ NCSWIC 2018 Governance Guide for State, Local, Tribal, and Territorial (SLTT) Officials highlights the need for a formalized statewide governance body (e.g., SIGB, SIEC) or equivalent, that provides a unified approach across multiple disciplines and jurisdictions to address system implementation and upgrades, funding, and overall support for communications interoperability. [2]

CISA assists requestors creating, reviewing, and evaluating existing governance structures and providing recommendations for establishing new governance bodies or structures.

CISA TA support for governance may be applied to strengthening existing governing bodies [for example, SIECs, SIGBs; or assisting 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 look different to meet each state's unique needs. Potential design outcomes and deliverables may include:

- Existing interoperability and emergency communications-focused governance group
- Formal governance documentation (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 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

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

Governance

Communications Unit Planning and Policies (COMUPLAN)	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	SIEC/SIGB; SWICs, Executive, Statutory, and Legislative Personnel

Offering Overview

This TA offering has been updated is to take a more holistic approach in helping states, territories, and tribes formally establish COMUs. This new approach, modeled after the current SCIP Update process, will begin by assisting the SWIC and stakeholders with a needs and geographic location assessment for each of the COMU positions.

The process will include the establishment and documentation of credentialing/recognition requirements, discussions on how to support and maintain the COMU program, and long-term succession planning for COMU positions.

- To help stakeholders create a successful program, the following elements may include but are not limited to:
  - Follow up support from CISA to help identify needed training and exercise opportunities
  - Adjusted credentialing/recognition processes
  - General, on-going support efforts to address administrative challenges
- The TA delivery will consist of three primary phases:
  - **Scoping Call:** The Scoping Call will provide the SWIC with an overview of the TA and allow the Subject Matter Expert(s) to gain insight into the state's needs in formalizing the state's COMU program and get a general idea for the TA delivery timeline.
  - **Planning Webinar:** The two-hour Planning Webinar will map out the state's current COMU efforts and help identify what their desired COMU program would look like. There will be discussions on how to achieve the desired outcome as well as identifying potential participants in the workshop. The workshop dates and location will also be discussed.
  - **One/Two-Day Workshop:** The COMU Workshop will be conducted with key stakeholders to discuss the desired COMU format. These discussions will include COMU position needs assessments and a conversation on where the positions should ideally be geographically located. A draft credentialing/recognition requirements document will be crafted during the workshop along with application and currency processes. Obstacles in obtaining the COMU goals should be identified and ideas for overcoming those obstacles discussed.
- **Potential Follow-up:** For those states, territories and tribes desiring additional formalized processes for the COMU program, a Governance Documentation Review, Assessment, and Development (GOV-DOC) TA could be provided to help establish a charter and by-laws for the group.

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

- Formal COML, COMT, and AUXCOMM recognition or certification/recertification processes
- Review of state Qualifications Review Board COMU Position process or other equivalent programs
- Strategic Plan and/or guiding principles for a Communications Unit Program
- Methods to track and report Communications Unit assets
- Introduction to systems that track COMU personnel qualifications along with recognition/certifications and renewal certifications
- Opportunities to provide training and exercises that develop trainee qualifications and Position Task Book (PTB) completion
- Key performance measures of a Communications Unit program
- CISA provides ongoing, sustained support to help established COMU planning bodies to maintain credentialing quality assurance and candidate vetting as well as formal relationships with state training officers (STO)

Governance

Communications Unit Assistance under Emergency Management Assistance Compact (EMAC)	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	SWICs, Emergency Managers and Administrators, ESF #2 Coordinators, and State Warning Officers

Offering Overview

This CISA service offering is designed to familiarize states/jurisdictions with EMAC, which 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 (EMAs) and has been passed into law in all 50 states and four U.S. territories. However, EMAC is greatly under-utilized for deployment of Communications Unit 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 process for requesting assistance to share resources within their state and with other EMAC members; how to handle similar requests for Communications Unit 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.

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

- Overview of EMAC functions and benefits
- Information regarding in-state procedures/legislation
- Listing of participating in-state agencies and available resources
- Interstate agreements and resources
- Assistance with developing EMAC policies/procedures and building Mission Ready Packages (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)
- Definition of MRPs
- Building and Formatting MRPs
- Overview of the Mutual Aid Support System (MASS)
- Reimbursement procedures
- EMAC training and exercises

Governance

Grant Funding for Emergency Communications Webinar	
TA Delivery Method:	Webinar
Recommended Participants:	SLTT/SIEC/SIGB Members

Offering Overview

Public safety agencies should consider all available funding sources, including traditional grants to help fund initial capital investments or improvements to communications systems, as well as other sources of funding that may partially fund emergency communications projects. CISA, in coordination with SAFECOM and the NCSWIC, publishes numerous resources for state, local, tribal, and territorial governments and their public safety agencies to identify funding mechanisms and plan for emergency communications projects. This offering conducts a review of federal financial assistance opportunities, recommended activities during the grant's lifecycle (e.g., pre-award, award, post award, and closeout), and resources to help agencies apply for and manage federal grants. [3]

This offering is applicable to states 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 fund various emergency communications activities
- *Funding Mechanisms for Public Safety Communications Systems* 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; 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
- *2018 Emergency Communications System Lifecycle Planning Guide* and *Planning Tool* aid 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
- *Interoperability Business Case: An Introduction to Ongoing Local Funding* advises the community on the elements needed to build a strong business case for funding interoperable communications

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

Standard Operating Procedures

Standard Operating Procedures (SOP)/Standard Operating Guides (SOG)/Communications Plan Review and Development	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	SWICs, Public Safety Stakeholders/ Mid-Senior Level Managers

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 a state's unique needs. Potential design options, outcomes and deliverables may include:

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

Standard Operating Procedures

Tactical Interoperable Communication Plan (TICP) Development/ Implementation Workshop	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	SWICs, Communications Unit Managers and Personnel

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. First responders 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 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 each state's 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
- CASM entry/update

Standard Operating Procedures

Tactical Interoperable Communications Field Operations Guide (TIC-FOG) Development/Update	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	SWICs, Communications Unit Managers and Personnel

Offering Overview

Based on the CISA National Interoperability Field Operations Guide (NIFOG), a state/territory-specific TIC-FOG is a compendium of interoperable communications, 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.

CISA will scope with the requestor state-desired content and format for their TIC-FOG. If the state would like the information contained in the TIC-FOG to be current with their TICP, an update workshop can be scheduled to update and to verify the information in it. Once the site has completed its review, CISA will reformat and condense the operationally relevant information from the TICP to develop the TIC-FOG.

Customized support for this offering may vary to meet each state's unique needs. Potential design options, and contents 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
- EMAC references and procedures

Standard Operating Procedures

Electronic Field Operations Guide (eFOG) Development	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	SWICs, Communications Unit Managers and Personnel

Offering Overview

CISA offers public safety eFOG mobile apps through ICTAP. 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. The first step in developing an eFOG is that the state must have a current word version of their FOG that CISA can convert. 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. 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 a pre-scoping call and the review of legal documents between the state and CISA. This review informs the requestor of the necessary legal documentation which is required before CISA begins actual development on the app being requested. This phase takes at least two weeks and must be completed and agreed to by both parties prior to starting work on the three remaining phases.
- **Configuration Phase:** Configuration Phase: This phase involves CISA's receipt of the required inputs from the state that are necessary for the development of the mobile apps. The state provides CISA with a current word version of its FOG: (see TIC-FOG on page 10) and selects offered mobile app options. This phase takes two weeks on average.
- **Build and Beta Test Phase:** This phase completes CISA's build of the mobile app and the state's live testing of mobile app beta versions, providing feedback to CISA. This phase takes at least two months.
- **Release Phase:** This phase completes CISA's update of the mobile app based on beta test feedback and public release of the mobile apps to the Google Play Store and Apple's App Store. This phase takes at least one month. CISA provides guidance on how authorized responders in the state can download and use the eFOG app on iOS and Android devices.

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

- Off-line mobile app Field Operations Guide information for state or region
- Live links to reference websites, e-mails, and phone number (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

Technology

Broadband Strategic Planning Support and Education (BRBNDLTE)	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	SWICs and Mid – Senior Public Safety Personnel

Offering Overview

Over the past five years, CISA has been assisting states with planning efforts related to the use of broadband mobile data for public safety. In developing strategies for broadband, CISA has encouraged states to consider both the existing use of commercial networks as well as the implementation of FirstNet services. This offering is a half day presentation for mid- to senior-level officials about the policy and operational implications of public safety wireless broadband. It is designed to help state/local and tribal officials understand the current capabilities of mobile data to improve incident response using examples of operational best practices and lessons learned.

This offering may be conducted jointly with the First Responder Network Authority Products and Services Division.

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

- Locality specific data requirements
- Undefined multi-state regional requirements
- LTE technology awareness

Technology

Mobile and Fixed Site Data Use Assessment for Incidents and Planned Events (BRBEVNTASMT)	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	SWICs and Public Safety Personnel

Offering Overview

In this service offering, CISA will conduct an analysis of a state, local area, or individual agency's use of mobile data devices and applications during a planned event or following a real-world incident. This information is critical to understanding the current requirements for use of commercial mobile data networks and technologies during incident response and may assist the state in implementing FirstNet. The requesting agency will receive an after action report that includes an improvement plan with technical and operational recommendations.

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

- Accountability for participating agencies and number/types of devices
- Procedures for data coordination and prioritization
- Undetermined peak and total data usage requirements
- After Action Report
- Analysis and interpretation of data results
- Geographic Information System (GIS)
- GIS mapping of mobile data usage
- Recommendations/Improvement Plan

Technology

Broadband Technologies and Data Operability/Interoperability in Support of Public Safety (BRBDATA)	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	SWICs and Public Safety Personnel

Offering Overview

This offering assists public safety professionals in identifying requirements associated with the selection and implementation of broadband related technologies into the public safety communications architecture for agencies in a specific jurisdiction or geographic area. The blended seminar and workshop stresses how various factors influence technology selection and provides participants the tools and opportunity to create agency specific templates and matrices.

This offering can accommodate an audience of any size, subject to space and seating availability. It focuses on personnel who are tasked with identifying, purchasing, or implementing public safety related broadband technologies. Both public safety and public service agencies including law enforcement, fire, hospitals, public works and emergency services within an urban area, county or other geographic area are welcome. Communications personnel will gain a deeper perspective on how broadband technologies may be selected and adapted into existing and future public safety architectures.

This offering has grown out of the Interoperable Communications Capabilities Assessment Program (ICCAP) observations and technical assistance provided to major urban areas. This offering can also serve as an assessment among the four key disciplines in major urban areas and other locations (UASI/non-UASI; law enforcement, fire, EMS, and public works) to assess how they use both non-mobile and mobile wireless data.

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

- Governance and standard operating procedures
- Information and data requirements
- Transport and network needs
- Information sharing/awareness technologies and systems
- Subscriber devices
- Personnel and security considerations
- Interoperability
- Cybersecurity considerations for data at rest and in transit

Technology

Next Generation 9-1-1/Strategic Planning Support (NG9-1-1STRATPLAN)	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	SWICs, 9-1-1 Operators/PSAP and State Officials

Offering Overview

This service offering is intended for 9-1-1 operators, communications personnel, and state officials who are interested in learning about NG9-1-1, technical and procedural challenges associated with integrating digital communications into their day-to-day operations, and in strategic planning for implementing NG9-1-1.

NG9-1-1 is a system comprised of hardware, software, data and operational capabilities and procedures which continue to evolve. As NG9-1-1 networks replace circuit switched 9-1-1 networks, PSAPs/9-1-1 centers need to be prepared to incorporate technologies such as voice over internet protocol (VoIP) 9-1-1 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 9-1-1.

Customized support for this offering may vary to meet each state's 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
- 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 NG9-1-1 Transition Plan
- CAD to CAD transition support
- CAD to RMS transition support

Technology

9-1-1/PSAP/LMR Cyber Awareness (9-1-1PSAPCYBRAWR)	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	SWICs, State 9-1-1 Coordinators, 9-1-1 Operators/PSAP/LMR Managers and System Operators

Offering Overview

9-1-1/PSAP/LMR functions are considered high-value cyber targets to those looking to disrupt public safety services, extort local governments through ransomware [4], or simply create mischief. The critical nature of 9-1-1/PSAP/LMR functions means cyberattacks against them can result in large-scale impacts on public safety operations.

This offering introduces public safety personnel to common cybersecurity threats and vulnerabilities affecting 9-1-1/PSAP/LMR environments. Topics include ransomware attacks and their impact on PSAPs, recent TDoS attacks against administrative lines and 9-1-1 directly, exposed networks and devices, shared passwords, cryptojacking and email phishing.

The 9-1-1/PSAP/LMR cybersecurity awareness webinar also discusses basic best practices to improve the secure use of emergency communications technologies in daily operations. In collaboration with the CISA Cyber Security 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 approximately 90 minutes long and is focused on non-technical audiences at the local or regional level and may be customized to stakeholder needs. This allows for discussion around specifics that pertain to the attendees' environment and helps managers decide whether a cybersecurity planning workshop is a needed follow-on. The webinar is typically given to participants statewide through a one-time, secure URL and can be provided to participants on a regional or local level.

Customized support for this offering may vary to meet each state's 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 9-1-1, PSAP and LMR operations
- Tailoring to emphasize specific topics or audiences
- Sessions recorded for later re-use
- In-person or webinar delivery using a unique URL provided to attendees identified by the SWIC
- Introduction to CISA phishing awareness and dedicated offerings available through CISA Assessments [5]

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

[5] Additional information regarding CISA Assessments is available at cisa.gov/cybersecurity-assessments.

Technology

9-1-1/PSAP/LMR Cyber Assessment (9-1-1PSAPCYBRASMT)	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	SWICs, 9-1-1/PSAP Managers and LMR System Owners

Offering Overview

The cybersecurity risk assessment technical assistance offering provides organizations with a review of their cyber posture in accordance with nationally recognized best practices guidelines. CISA employs the NIST Special Publication 800-53, Rev 5, "Security and Privacy Controls for Information Systems and Organizations," as a framework [6]. CISA SMEs collaborate with the requestor on the security and privacy controls from the 800-53 framework to be used during the review. The assessment seeks to provide customers with an understanding of their current cyber security risk posture through a representative sampling process (e.g., sites, personnel, systems) to aid in planning risk management efforts, and it can be tailored to focus on various aspects of the organization's operations. The risk assessment process involves:

Kickoff

- Work with the requesting agency to explain the process, gather preliminary information (e.g., system architecture information, security related policy and procedures etc.), identify participants, interviewees, potential sites for review, and timeframes for the assessment.

Categorization

- Categorize the information system and the information processed, stored, and transmitted in the 9-1-1/PSAP/LMT environment based on impact levels related to confidentiality, integrity, and availability.

Control Selection

- Select a set of baseline security controls for the information system based on the security categorization; tailor and supplement the security control baseline as needed based on an organizational assessment of risk and local conditions.

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

Analysis

- Analyze review findings to determine compliance or non-compliance with baseline controls.

Assessment [7]

- Perform a qualitative risk assessment of non-compliant controls, based on vulnerability, threats, potential impact, and likelihood of occurrence.

Report

- Report findings with recommended mitigation strategies in a prioritized format based on potential risk to the organization or its mission.

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

[7] CISA conducts the risk assessment in collaboration with subject matters across the agency to include CSAs and PSAs with in the region.

Technology

(Continued on next page)

This technical assistance can provide 9-1-1/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, developing staffing requirements, etc.

Customized support for this offering may vary 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 Emergency Communications Coordinators can assist stakeholders in identifying additional CISA cybersecurity resources and assistance that may be needed.

Technology

Alerts and Warnings (ALERTS)	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	SWICs, Emergency Management, Public Safety Command/Leadership, and Communications Personnel

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 Warning training is designed to assist emergency managers, public safety command/leadership, communications center/dispatch supervisory personnel (9-1-1), 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 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 Integrated Public Alert and Warning Systems (IPAWS), Wireless Emergency Alerts (WEA), the Emergency Alert System (EAS), and the National Oceanic and Atmospheric Administration (NOAA) Weather Radio and other public alerting systems.

Customized support for this offering may vary to meet each state's 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

Technology

LMR/LTE Coverage Testing & Simulation (LMR/LTE)	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	SWICs and RF Communications System Management Agencies

Offering Overview

Technical assistance support provided by CISA will assist by evaluating the requesting agency's LMR systems in VHF high band (136-174 MHz), 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 GIS overlay to 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 each state's 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

Training & Exercises

Communications Unit Exercise (COMMEX) for Communications Unit Trainees[8]	
TA Delivery Method:	In-Person Workshop and Webinar
Recommended Participants:	AUXCOMM/AUXC, COML, COMT, INCM, INTD, ITSL, and RADO Trainees

Offering Overview

The COMMEX is a follow-on to the AUXCOMM/AUXC, COML, COMT, INCM, INTD, RADO and ITSL) training courses.[9] It provides an opportunity for AUXCOMM/AUXC, COML, COMT, INCM, INTD, RADO and ITSL trainees to demonstrate proficiency and complete requirements in the respective Position Task Books (PTB).

Public safety professionals who have completed an AUXCOMM/AUXC, COML, COMT, INCM, INTD, RADO or ITSL course must complete a series of competency tasks in their PTB as the next step in becoming a certified AUXCOMM/AUXC, COML, COMT, INCM, INTD, RADO, or ITSL for their agency. In this one-day exercise, tasks are designed to simulate challenges Communications Unit trainees will encounter during an incident. The exercise can be repeated on a second day to double the number of trainees that are afforded an opportunity to complete their PTB. The number of Communications Unit trainees will be customized to meet the state's needs during the scoping call and Initial Planning Meeting (IPM).

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

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

- Provide opportunities for testing AUXCOMM/AUXC, COML, COMT, INCM, INTD, RADO, and/or ITSL 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

[8] This exercise is structured under HSEEP guidelines.
[9] Participants must have successfully completed the appropriate Communications Unit training.

Training & Exercises

Communications-Focused Exercises (TTX, FE, FSE)[10]	
TA Delivery Method:	In-Person Exercise and Webinar Planning Meetings
Recommended Participants:	Public Safety Professionals

Offering Overview

Exercises and operational assessments are important tools to assess, train for, and practice mitigation, prevention, response, and recovery capabilities. Frequently, communications are either omitted from or only notionally included in exercises or in operational assessments. To best approximate a real operational environment, exercises should thoroughly incorporate and evaluate available voice and data communications resources, procedures, tools, and personnel in each multi-agency, multi-discipline, and multi-jurisdictional training/testing opportunity.

CISA provides exercise assistance and expertise focused on communications for:

- Tabletop Exercises (TTX)
- Functional Exercises (FE)
- Full Scale Exercises (FSE)

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

- Designing, conducting, and evaluating communications-focused public safety/service discussion-based and functional exercises
- Evaluating communications capabilities at full scale exercises
- Preparing communications-focused scenarios and injects (both voice and data) for exercises
- Pre-planning for interoperable, emergency communications for special events
- Assessing Communications Unit trained personnel on-site operational procedures relating to communications tasks in their respective position task books
- Initial, mid, and final planning meetings
- Logistics checklist
- Exercise Plan (EXPLAN)
- Master Scenario Events List (MSEL)
- After Action Report/Improvement Plan (AAR/IP)

[10] This exercise is structured under HSEEP guidelines.

Training & Exercises

Communications Focused Drill/Activities (COMMDRILL)	
TA Delivery Method:	In-Person Drill and Webinar Planning Meetings
Recommended Participants:	Key Public Safety Communications Personnel

Offering Overview

This service offering provides exercise planning and evaluation support for emergency communications drills to requesting sites/entities. Upon request, CISA evaluators and observers can supplement on-site staff to support and assist in evaluation of Communications Unit personnel on mobile communications units, 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 a Mobile Communications Unit "rodeo" or "rally" during which multiple vehicles and teams assemble from across a region or state. Mobile Communications Unit 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 Communications Unit positions.

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

- Maintaining proficiency with specific communications equipment
- Incorporating new technology for public safety personnel
- Maintaining readiness and interoperable communications
- National Security and Emergency Preparedness (NS/EP) awareness
- Multi-agency/jurisdiction communications interoperability
- Public safety response level emergency communication

Training & Exercises

Communications-Focused Exercise Design and Planning (EXDESIGN)	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	Key Public Safety Communications Personnel

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 Homeland Security Exercise and Evaluation Program (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 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 each state's 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 After Action Reports/Improvement Plans (AARs/IPs)

Training & Exercises

Communications Unit Leader (COML) Training Course	
TA Delivery Method:	Four-Day In-Person Course or Five-Day Webex (see pg. 4 for additional information on virtual training courses)
Recommended Participants:	Emergency Response Personnel with a Technical Communications Background

Offering Overview

This service offering is designed for all state/territory, tribal, regional, and local emergency response professionals and for support personnel with a communications background. It is designed to familiarize these professionals with the role and responsibilities of a COML under NIMS ICS and to provide hands-on exercises that reinforce the lecture materials. CISA and FEMA Emergency Management Institute (EMI) offer this course jointly as "L0969, NIMS ICS All-Hazards Communications Unit Leader Course" for in-person courses and "K0969, NIMS ICS All-Hazards Communications Unit Leader Course" for virtual courses [11]

Under the NIMS ICS structure, a COML is the focal point within the Communications Unit. This course provides U.S. Department of Homeland Security (DHS) approved and NIMS-compliant instruction to ensure that every state/territory has trained personnel capable of coordinating on-scene emergency communications during a multi-jurisdictional response or planned event. CISA instructors are approved by DHS and have had extensive experience as COMLs.

The course is presented with facilitated lectures, hands-on activities, and extensive interactive discussions. CISA 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 Capacity:

- **In person:** minimum of 15 or a maximum of 30 vetted/qualified students
- **Webex:** maximum of 15 vetted/qualified students

Prerequisites for Attendance: ***(prerequisites must be verified 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
  - IS-700: An Introduction to the National Incident Management System
  - IS-800: National Response Framework, An Introduction
- In-person classroom instruction:
  - ICS-300: Intermediate Incident Command System for Expanding Incidents, is required
- Additional recommended training:
  - ICS-400: Advanced Incident Command System for Complex Incidents, is recommended, but not required

(Continued on next page)

[11] For any training courses (COML, COML TtT, ITSL, COMT, AUXCOMM/AUXC, AUXCOMM TtT/AUXC TtT, INCM, INTD, RADO), 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 point of contact [POC]) actions:
  - Provide course dates and location to the CISA Communications Unit Training Coordinator at least 45 days before the course.
  - Designate a recipient of the FEMA student course evaluation forms and provide their name, mailing address, e-mail address and phone number to the CISA Communications Unit Training Coordinator at least 45 days before the course. This person must be available to deliver the packet of forms to the Lead Instructor on the first day of the course.
  - Require each student to submit a FEMA Form 119-25-0-1 General Admissions Application signed by the student and their supervisor with proof of prerequisite completion.
  - Obtain the STO's signature on the FEMA Form 119-25-0-1 General Admissions Application. Scan and e-mail the completed forms to the CISA Communications Unit Training Coordinator 2 weeks in advance of the course.
- CISA Actions:
  - Determine instructor assignments.
  - 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.
  - Fill out the Student Verification form based on the information contained in the FEMA Form 119-25-0-1s, check the agency affiliations against CASM, and provide the file to the Lead Instructor as a start on the typed roster.
  - Receive the final roster, FEMA student course evaluation forms, CISA student course evaluation forms, and Score Capture Sheet from the Lead Instructor.
  - Submit the COML Course Completion Package to FEMA EMI after the course.

Training & Exercises

Communications Unit Technician (COMT) Training Course	
TA Delivery Method:	Five-Day In-Person Course
Recommended Participants:	Emergency Response Personnel with a Technical Communications Background

Offering Overview

This class 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.

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 provides a realistic, hands-on approach to mastering the tasks and skills of a COMT. Each attendee receives a Position Task Book.

This class is taught by CISA instructors who have both practitioner and Communications Unit experience. Prior to the on-site class, CISA staff will work with the requesting site to incorporate communications technologies in use by the participants' agencies. SWICs are encouraged to notify the STO prior to its start to ensure the course is documented.

There must be a minimum of 8 or a maximum 16 vetted/qualified students two weeks in advance of the course in order for CISA to conduct the course.

Prerequisites for Attendance

- 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
  - 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:
  - Submit a completed student verification form to CISA at least 14 days prior to the class.

Training & Exercises

Incident Tactical Dispatcher (INTD) Training Course	
TA Delivery Method:	Four-Day In-Person Course or Five-Day Webex (see pg. 4 for additional information on virtual training courses)
Recommended Participants:	Experienced Dispatchers who are familiar with the Incident Command System

Offering Overview

The course provides a realistic, hands-on approach to mastering the tasks and skills of an Incident Tactical Dispatcher. An Incident Tactical Dispatcher is a specially trained individual qualified to operate in a command post, base camp or at the incident scene in support of a specific incident or tactical operation. Incident Tactical Dispatchers leverage the multi-tasking, communication, accountability and documentation skills of successful telecommunicators to provide public safety communications expertise and support at planned events and extended incidents such as hostage situations, multi-alarm fires, search and rescue operations, bombings, and active shooter incidents in accordance with FEMA National Qualifications Standards. Incident Tactical Dispatchers may support the Communications Unit as a single resource or as part of an incident tactical dispatch team. This course provides a basic understanding for the roles and responsibilities of an incident tactical dispatcher working in a tactical environment.

This course is designed for experienced dispatchers who are familiar with the Incident Command System and dispatch operations. This course is four days long with an end of course INTD exercise on the fourth day. It is limited to 20 students. Each attendee participates in hands-on training exercises and receives a Position Task Book.

Course Capacity:

- **In person:** minimum of 10 or a maximum of 20 vetted/qualified students
- **Webex:** maximum of 15 vetted/qualified students

Prerequisites for Attendance: ***(prerequisites must be verified two weeks in advance of the 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
  - IS-700: An Introduction to the National Incident Management System
  - IS-800: National Response Framework, An Introduction
- Additional recommended training:
  - ICS-300: Intermediate Incident Command System for Expanding Incidents, is recommended, but not required

Course Registration Process

- SWIC (or designated POC) Action:
  - Submit a completed student verification form to CISA at least 14 days prior to the class

Training & Exercises

Information Technology Service Unit Leader (ITSL) Training Course	
TA Delivery Method:	Four-Day In-Person Course
Recommended Participants:	Emergency Response Personnel with a Technical Communications Background
Note: The ITSL curriculum is currently under review and is expected to be available by spring 2021.	

Offering Overview

The requirement to access broadband data during incidents or events has increased exponentially in recent years. This has spurred the need for personnel with highly specialized knowledge and expertise to be included in the ICS during planned events and incidents. In 2018 and 2019, CISA introduced the ITSL course, and SAFECOM and NCSWIC have coordinated with FEMA NIC and other organizations focused on public safety communications to establish the best way to integrate the ITSL into the ICS.[12] The ITSL is needed to provide information management, cybersecurity, and application management for the many critical incident/event related functions, to include: Incident/Unified Command Post, Incident Communications Centers, and various tactical operations centers, joint information center (JIC), staging areas, and field locations. However, the coordinated sharing of this data across agencies and jurisdictions is significantly less mature than radio communication and poses a significant interoperability challenge.

To meet this need, CISA has developed the ITSL course. The ITSL course targets Federal, state/territory, tribal, urban, local, and emergency response professionals, and supports personnel in all disciplines with a communications background and an aptitude for and extensive experience in information technology. The training course provides an overview of the ITSL components including the Unified Help Desk (inclusive of both communications and IT support), IT Infrastructure Manager, Network Manager, and specialist roles. 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.

There must be a minimum of 10 or a maximum 20 qualified students two weeks in advance of the course in order for CISA to conduct the course.

Prerequisites for Attendance

- 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 on-line 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
  - IS-700: An Introduction to the National Incident Management System
  - IS-800: National Response Framework, An Introduction
- Completion of the following in-person classroom instruction:
  - ICS-300: Intermediate Incident Command System for Expanding Incidents
- Additional recommended training:
  - ICS-400: Advanced Incident Command System for Complex Incidents, is recommended but not required

Course Registration Process

- SWIC (or designated POC) Action:
  - Submit student verification form to CISA at least 14 days prior to the class

[12] CISA is currently coordinating with FEMA NIC and EMI on re-defining the ICS COMU to include an Information Technology function.

Training & Exercises

Incident Communications Center Manager (INCM) Training Course	
TA Delivery Method:	Three-Day In-Person Course or Four-Day Webex (see pg. 4 for additional information on virtual training courses)
Recommended Participants:	COMLs, Dispatch Supervisors, Public Safety Communications Professionals

Offering Overview

COMLs and COMTs are not the only communications professionals who manage the communications requirements during an incident or planned event. For some incidents, the COML establishes an Incident Communications Center staffed with Radio Operators and/or Incident Tactical Dispatchers to provide communications support for operations. Once radio personnel and/or telecommunicators are on scene, it becomes important for an Incident Communications Center Manager (INCM) to be assigned for coordination purposes and to avoid span-of-control issues.

The All-Hazards Incident Communications Center Manager course is designed to prepare Communication Unit Leaders, dispatch supervisors and public safety communication professionals for managing all functions in an Incident Communications Center. The course is taught by instructors with experience in dispatch operations, COML and INCM. This three-day course is limited to 20 students. Each attendee participates in hands-on training exercises and receives a Position Task Book.

Course Capacity:

- **In person:** minimum of 10 or a maximum of 20 vetted/qualified students
- **Webex:** maximum of 15 vetted/qualified students

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

- Personal experience:
  - 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
  - IS-700: An Introduction to the National Incident Management System
  - IS-800: National Response Framework, An Introduction
- Additional recommended training:
  - ICS-300: Intermediate Incident Command System for Expanding Incidents, is recommended, but not required

Course Registration Process

- SWIC (or designated POC) Action:
  - Submit a completed student verification form to CISA at least 14 days prior to the class.

Training & Exercises

All-Hazards Incident Communications Center Manager (INCM)/Incident Tactical Dispatcher (INTD) Awareness Overview (TRG-OVERVW)	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	Command & General (C&G) Staff, COMLs, Dispatch Supervisors, Public Safety Communications Professionals, Dispatchers

Offering Overview

The INCM and INTD roles are critical aspects to managing communications in large-scale incidents or planned events (including NSSE/SEAR). For some incidents, the COML establishes an ICC staffed with RADOs to provide communications support for operations, an INCM for addressing coordination and avoid span-of-control issues, and INTDs for handling event- or incident-specific communications while the ECC/PSAP continues to handle normal call volume.

The All-Hazards INCM/INTD Awareness Overview is designed to prepare C&G Staff, Communication Unit Leaders, dispatch supervisors and public safety communication professionals for managing all functions in an Incident Communications Center. This overview is particularly useful for those staff that are preparing for a large planned event, such as a National Special Security Event (NSSE) or Special Event Assessment Rating (SEAR). This awareness session provides a refresher of INCM/INTD courses as well as awareness and lessons learned regarding ICC operations during a NSSE/SEAR. This three to four hour overview is presented by instructors with experience in dispatch operations, COML, INCM and INTD. This is an awareness session only; no course completion certificate or position task book will be issued.

Targeted Audience

- Public safety communications practitioners

Recommend completion of the following online courses from the FEMA EMI website:

- IS-100, Introduction to the ICS
- IS-200, ICS for Single Resources and Initial Incidents
- IS-700, National Incident Management System (NIMS), an Introduction
- IS-800, National Response Framework (NRF)

This offering can be customized a number of ways, to include:

- In-person delivery in your ICC or training facility
- Virtual / webinar delivery
- Additional information on your specific procedures and plans
- An additional discussion-based (tabletop) exercise

Training & Exercises

Radio Operator (RADO) Training Course	
TA Delivery Method:	Two-Day In-Person Course
Recommended Participants:	Emergency Response Personnel who are familiar with the Incident Command System

Offering Overview

This class provides hands-on and lecture-based training for the All-Hazards ICS RADO position. It is designed for emergency response professionals and support personnel in all disciplines who have a basic understanding of the All-Hazard ICS Communications Unit. It introduces public safety professionals and support personnel to various Radio Operator concepts including radio etiquette, interoperable communications, dispatch operations and emergency communications procedures. Participants develop the essential core competencies used during incident response and planned events to perform the duties of the RADO in an All-Hazards environment including communications support for public safety, wildfire, marine, aviation and HF radio communications. The responsibilities of an All-Hazards RADO can include staffing the Incident Communications Center, monitoring radio traffic, and base station operations for emergency operations centers, hospitals, dispatch centers and non-governmental organizations supporting civil emergency response at the state, local or regional level.

The course provides a realistic, hands-on approach to mastering the tasks and skills of an All- Hazards RADO. This course is two days long and is limited to 20 students. Each attendee participates in hands-on training exercises and receives a Position Task Book.

There must be a minimum of 10 or a maximum 20 qualified students two weeks in advance of the course in order for CISA to conduct the course.

Prerequisites for Attendance

- Personal experience:
  - 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-200: Basic Incident Command System for Initial Response
  - IS-700: An Introduction to the National Incident Management System
  - IS-800: National Response Framework, An Introduction
- Additional recommended training:
  - ICS-300: Intermediate Incident Command System for Expanding Incidents, is recommended, but not required

Course Registration Process

- SWIC (or designated POC) Action:
  - Submit a completed student verification form to CISA at least 14 days prior to the class.

Training & Exercises

Auxiliary Communications (AUXCOMM/AUXC) Training Course[13]	
TA Delivery Method:	Two to Three-Day In-Person Course or Three-Day Webex (see pg. 4 for additional information on virtual training courses)
Recommended Participants:	Licensed Amateur Radio Operators

Offering Overview

This class is designed for amateur radio operators who volunteer to provide backup radio communications support to public safety agencies. Volunteer communications operators/groups, using amateur radio, have been providing backup communications to public safety for nearly 100 years. Event planners, public safety officials, and emergency managers at all levels of government utilize their services. Often, amateur radio services have been used when other forms of communications have failed or have been disrupted. Today, nearly all of the states/territories have incorporated some level of participation by amateur radio auxiliary communication operators into their TICPs and SCIPs.

This course focuses on auxiliary communications interoperability, the relationship between the COML and AUXCOMM/AUXC volunteers, emergency operations center (EOC) etiquette, on-the-air etiquette, Federal Communications Commission (FCC) rules and regulations, auxiliary communications training and planning, and emergency communications deployment. The course is intended to supplement and standardize a volunteer operator's experience and knowledge of emergency amateur radio communications in a public safety context.

Course Capacity:

- **In person:** minimum of 15 or a maximum of 30 vetted/qualified students
- **Webex:** maximum of 15 vetted/qualified students

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

- Personal experience:
  - An active FCC amateur radio license
  - Experience in auxiliary communications
  - An affiliation with a public safety agency
  - A desire to work with COMLs in a 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
  - IS-700: An Introduction to the National Incident Management System
  - IS-800: National Response Framework, An Introduction
- Additional recommended training:
  - ICS-300: Intermediate Incident Command System for Expanding Incidents is recommended, but not required

Course Registration Process

- SWIC (or designated POC) Action:
  - Submit a completed student verification form to CISA at least 14 days prior to the class.

[13] CISA is currently coordinating with FEMA NIC and EMI on re-defining the ICS COMU to include an AUXC position.

Training & Exercises

All-Hazards Incident Communications Awareness Overview (TRG-COMUAWR)	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	Public Safety Stakeholders

Offering Overview

The All-Hazards Incident Communications Awareness service provides a complete overview for the ICS and roles and responsibilities for Communications Unit personnel staffing it. It explains the organizational structure and the staffing of the logistics section service branch component. It reviews the COML responsibilities and supervision of the INCM, COMT, RADO, INTD, AUXC and other technical specialists.

The All-Hazards Incident Communications Awareness Overview is designed to inform and advertise the roles, responsibilities, and services that are provided with a fully-staffed ICS during all-hazards response efforts. This half-day briefing is limited to 20 students. This is an awareness session only, no course completion certificate or position task book will be issued.

There must be a minimum of 10 or a maximum 20 qualified students two weeks in advance of the course in order for CISA to conduct the course.

Prerequisites for Attendance

- Personal experience:
    - Awareness of fundamental public safety communications technology

Recommend completion of the following online courses from the FEMA EMI website:

- IS-100, Introduction to the ICS
- IS-200, ICS for Single Resources and Initial Incidents
- IS-700, National Incident Management System (NIMS), an Introduction
- IS-800, National Response Framework (NRF)

Additional recommended training:

- ICS-300, ICS for Expanding Incidents, is recommended, but not required

This offering can be customized a number of ways, to include:

- In-person delivery in your ICC or training facility
- Virtual / webinar delivery
- Additional information on your specific procedures and plans
- An additional discussion-based (tabletop) exercise

Training & Exercises

Auxiliary Communications Train-the-Trainer (AUXCOMM/AUXC TtT) Course	
TA Delivery Method:	Two-Day In-Person Course
Recommended Participants:	Licensed/Experienced Amateur Radio Operators

Offering Overview

This service offering helps states/territories create a self-sustaining AUXCOMM/AUXC training program by providing instructor training to individuals who have completed the CISA AUXCOMM/AUXC course, the COML course, the COML Position Task Book (PTB) and the AUXCOMM/AUXC PTB, and have held a current valid General Class FCC (or higher) amateur radio operator license for at least the past three years. This course helps attendees develop essential core competencies required for teaching the AUXCOMM/AUXC course within their own state. This course supports learning through discussion, lecture, participation in multiple activities and students teaching portions of the approved basic curriculum. This methodology provides a realistic, hands-on approach to mastering the skills of instructing the AUXCOMM/AUXC course.

The AUXCOMM TtT/AUXC TtT course should be completed by personnel with a volunteer communicator affiliation with a public safety agency and are interested in teaching the AUXCOMM/AUXC course. Through experience and training, participants must demonstrate a working knowledge of ICS and duties associated with the various Communications Unit positions. Students must already be experienced in delivering adult education.

There must be a minimum of eight or a maximum 10 qualified students identified in order for CISA to schedule and conduct the course.

Prerequisites for Attendance

- Personal experience:
  - Experience in auxiliary communications
  - An affiliation with a public safety agency
  - A desire to work with COMLs and Auxiliary Communicators in a NIMS ICS environment
- Completed formal adult education through one of the following fields:
  - National Fire Academy's Educational Methodology Course
  - National Wildfire Coordinating Groups Facilitative Instructor (M-410) Course
  - Center for Domestic Preparedness Instructor Training Certification Course
  - Equivalents (i.e. FEMA E/L0141, Instructional Presentation and Evaluation Skills, Total Army Instructor Training Course; Small Group Instructor Training Course; G265 Basic Instructional Skills Course, etc.)
  - State Certified Level II or higher Fire, Rescue, and/or EMS Instruction (10341)
  - State Certified Teaching Certificate
  - Advanced degree in education, educational psychology, technical education, or related program
- Completion of the most current version 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
  - IS-700: An Introduction to the National Incident Management System
  - IS-800: National Response Framework, An Introduction

(Continued on next page)

- Completion of the most current version of the following courses:
  - ICS-300: Intermediate Incident Command System for Expanding Incidents
  - ICS-400: Advanced Incident Command System for Complex Incidents

Documentation:

- Official, signed copy of an active FCC amateur radio license, General Class or higher, valid for at least the past three years
- CISA AUXCOMM/AUXC course completion certificate
- FEMA EMI COML course completion certificate from the three or four-day COML course
- Signature page from the COML PTB and the AUXCOMM/AUXC PTB dated within three years of initiating the PTB
- SWIC and STO endorsement as a future AUXCOMM/AUXC instructor in the state of residence

Course Registration Process

- SWIC (or designated POC) Actions:
  - Identify students for the course and have them submit proof of prerequisite completion for review. Once satisfied all prerequisites have been met by an individual student, send the prerequisite documentation with a SWIC and STO endorsement of the individual as a future instructor in the state to the CISA Communications Unit Training Coordinator
  - Once at least 8 qualified students have been identified, set the course dates to start at least 30 days later. Provide the course dates and location to the CISA Communications Unit Training Coordinator
  - Submit a completed student verification form to CISA at least 14 days prior to the class
- CISA Actions:
  - Review the prerequisite documentation for sufficiency, build instructor profiles in the COMU Repository and upload prerequisite documentation

Training & Exercises

Communications Unit Leader Train-the-Trainer (COMLTtT) Course	
TA Delivery Method:	Four-Day In-Person Course or Five-Day Webex
Recommended Participants:	COMLs with Completed Position Task Books

Offering Overview

This service offering helps states/territories create a self-sustaining COML training program by providing instructor training to individuals who have completed the basic COML course and the PTB. This course helps attendees develop essential core competencies required for teaching the COML course in their own state. This course supports learning through discussion, lecture, participation in multiple activities and students teaching portions of the basic curriculum. This methodology provides a realistic, hands-on approach to mastering the skills of instructing the COML course.

The COML TtT course should be completed by personnel who are assigned to a COML position and are interested in teaching the COML course. Through experience and training, participants must demonstrate a working knowledge of ICS and duties associated with the various Communications Unit positions. Students must already be experienced in delivering adult education.

There must be a minimum of 8 or a maximum 10 qualified students identified in order for CISA to schedule and conduct the course.

Prerequisites for Attendance

- Completion of formal adult education in one of the following fields:
  - National Fire Academy's Educational Methodology Course
  - National Wildfire Coordinating Groups Facilitative Instructor (M-410) Course
  - Center for Domestic Preparedness Instructor Training Certification Course
  - Equivalents (i.e. FEMA E/L0141, Instructional Presentation and Evaluation Skills, Total Army Instructor Training Course; Small Group Instructor Training Course; G265 Basic Instructional Skills Course, etc.)
  - State Certified Level II or higher Fire, Rescue, and/or EMS Instruction (10341)
  - State Certified Teaching Certificate
  - Advanced degree in education, educational psychology, technical education, or related program
- Completion of the most current version 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
  - IS-700: An Introduction to the National Incident Management System
  - IS-800: National Response Framework, An Introduction
- Completion of the most current version of the following courses:
  - ICS-300: Intermediate Incident Command System for Expanding Incidents
  - ICS-400: Advanced Incident Command System for Complex Incidents

Documentation

- A completed FEMA Form 119-25-0-1, General Admissions Application
- FEMA EMI COML course completion certificate from the three or four-day COML course
- Signature page from the COML PTB dated within three years of initiating the PTB
- SWIC and STO endorsement as a future COML instructor in the state of residence

(Continued on next page)

Training & Exercises

Course Registration Process

- SWIC (or designated POC) Actions:
  - Identify students for the course and have them submit proof of prerequisite completion for review. Once satisfied all prerequisites have been met by an individual student, send the prerequisite documentation with a SWIC and STO endorsement of the individual as a future instructor in the state to the CISA Communications Unit Training Coordinator
  - Once at least 8 qualified students have been identified, set the course dates to start at least 45 days later. Provide the course dates and location to the CISA Communications Unit Training Coordinator
  - Designate a recipient of the FEMA student course evaluation forms and provide their name, mailing address, e-mail address and phone number to the CISA Communications Unit Training Coordinator at least 45 days before the course. This person must be available to deliver the packet of forms to the Lead Instructor on the first day of the course
  - Require each vetted student to submit a FEMA Form 119-25-0-1 General Admissions Application signed by the student and their supervisor
  - Obtain the STO's signature on the FEMA Form 119-25-0-1 General Admissions Application. Scan and e-mail the completed forms to the CISA Communications Unit Training Coordinator at least 2 weeks in advance of 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
  - Review the prerequisite documentation for sufficiency, build instructor profiles in the COMU Repository and upload prerequisite documentation
  - Fill out the Student Verification form based on the information contained in the FEMA Form 119-25-0-1s, check the agency affiliations against CASM, and provide the file to the Lead Instructor as a start on the typed roster
  - Receive the final roster, FEMA student course evaluation forms, and CISA student course evaluation forms from the Lead Instructor
  - Submit the COML Course Completion Package to FEMA EMI after the course

Training & Exercises

Communications Unit Technician Train-the-Trainer (COMTTtT) Courses	
TA Delivery Method:	Five-Day In-Person Course
Recommended Participants:	COMTs with Completed Position Task Books

Offering Overview

This service offering helps states/territories create a self-sustaining COMT training program by providing instructor training to individuals who have completed the basic COMT course and the PTB. This course helps attendees develop essential core competencies required for teaching the COMT course within their own state. This course supports learning through discussion, lecture, participation in multiple activities and students teaching portions of the approved basic curriculum. This methodology provides a realistic, hands-on approach to mastering the skills of instructing the COMT course.

The COMT TtT course should be completed by personnel who are assigned to function in a COMT position and are interested in teaching the COMT course. Through experience and training, participants must demonstrate a working knowledge of ICS and the Communications Unit position specific duties associated with the COMT position. Students must already be experienced in delivering adult education.

There must be a minimum of eight and maximum 10 qualified students identified in order for CISA to schedule and conduct the course.

Prerequisites for Attendance

- Completion of formal adult education in one of the following fields:
  - National Fire Academy's Educational Methodology Course
  - National Wildfire Coordinating Groups Facilitative Instructor (M-410) Course
  - Center for Domestic Preparedness Instructor Training Certification Course
  - Equivalents (i.e. FEMA E/L0141, Instructional Presentation and Evaluation Skills, Total Army Instructor Training Course; Small Group Instructor Training Course; G265 Basic Instructional Skills Course, etc.)
  - State Certified Level II or higher Fire, Rescue, and/or EMS Instruction (10341)
  - State Certified Teaching Certificate
  - Advanced degree in education, educational psychology, technical education, or related program
- Completion of the most current version 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
  - IS-700: An Introduction to the National Incident Management System
  - IS-800: National Response Framework, An Introduction
- Completion of the most current version of the following courses:
  - ICS-300: Intermediate Incident Command System for Expanding Incidents
  - ICS-400: Advanced Incident Command System for Complex Incidents

Documentation:

- CISA COMT course completion certificate from the five-day CISA COMT course
- Signature page from the COMT PTB dated within three years of initiating the PTB
- SWIC and STO endorsement as a future COMT instructor in the state of residence

(Continued on next page)

Training & Exercises

Course Registration Process

- SWIC (or designated POC) Actions:
  - Identify students for the course and have them submit proof of prerequisite completion for review. Once satisfied all prerequisites have been met by an individual student, send the prerequisite documentation with a SWIC and STO endorsement of the individual as a future instructor in the state to the CISA Communications Unit Training Coordinator
  - Once at least 8 qualified students have been identified, set the course dates to start at least 30 days later. Provide the course dates and location to the CISA Communications Unit Training Coordinator
  - Submit a completed student verification form to CISA at least 14 days prior to the class
- CISA Actions:
  - Review the prerequisite documentation for sufficiency, build instructor profiles in the COMU Repository and upload prerequisite documentation

Training & Exercises

State-Sponsored CISA Recognized Communications Unit Instruction (SS-COMT, SS-COML, SS-AUXCOMM/AUXC)	
TA Delivery Method:	In-Person Workshop
Recommended Participants:	Communications Unit Trained Instructors

Offering Overview

The State-Sponsored CISA Recognized Communications Unit Instruction Program enables a state to use its own CISA recognized instructors to teach CISA curricula utilizing materials provided by CISA. Students receive CISA course completion certificates for COMT and AUXCOMM training, and FEMA EMI course completion certificates for COML training. State-Sponsored instructors are required to acquire and maintain the same instructor prerequisites as the CISA contracted instructors.

States may want to use their own CISA recognized instructors when conducting training. This gives the state control over their own training programs and helps them develop a pool of trained Communications Unit personnel. Students who successfully complete these courses, taught by CISA recognized instructors, receive uniform, nationally recognized instruction and a DHS course completion certificate. These students will be listed in the CASM database under the Communications Unit Classes section (casm.dhs.gov) for their state. This will assist the state in documenting the names and locations of COMLs, COMTs, and AUXCOMM/AUXC personnel across the state. Course completion certificates indicate successful completion of training and do not equate to a certification or credential.

Instructor Requirements to attain CISA Recognition

A "CISA recognized instructor" is defined as an individual who meets, or exceeds, all CISA contracted instructor requirements for a Communications Unit course:

- For COML instructors: An individual must meet all current requirements to attend the CISA COML TtT course, must have completed the CISA COML TtT course after 2011, and be designated as a state recognized instructor for their respective state
- For COMT instructors: An individual must meet all current requirements to attend the CISA COMT TtT course, must have completed the CISA COMT TtT course after 2011, and be designated as a state recognized instructor for their respective state
- For AUXCOMM/AUXC instructors: An individual must meet all current requirements to attend the CISA AUXCOMM/AUXC TtT course, must have either completed the CISA AUXCOMM/AUXC TtT course, and be designated as a state recognized instructor for their respective state, or alternatively, must meet all current requirements to attend the CISA AUXCOMM TtT course, must have completed the CISA COML TtT course and be designated as a state recognized instructor for their respective state

Note: Designation as a state recognized instructor for their respective state means that both the SWIC and the STO have endorsed in writing the individual as an instructor of Communications Unit courses in their state of residence. States may add to the above list of requirements to attain state instructor designation. The requirement to meet all current requirements to attend the applicable TtT course means that in order to maintain their CISA recognition status, instructors must always update their training to the most current versions of the prerequisite courses.

(Continued on next page)

Training & Exercises

CISA Instructor Recognition Process

- State Actions:
  - States desiring to use this State-Sponsored/CISA Recognized Communications Unit Instruction Program for students to obtain CISA or FEMA course completion certificates, as applicable to the course, will follow the guidelines below:
  - The STO and the SWIC must recommend to CISA individuals from their state who they want to become CISA recognized instructors
  - The STO/SWIC will ensure that their recommended instructors submit documentation showing completion of all prerequisites to CISA, the final vetting authority, at least 30 days in advance of any COMT or AUXCOMM/AUXC course and at least 45 days in advance of a COML course
- CISA Actions:
  - Vet the submitted documentation of prerequisite completion for sufficiency.
  - Notify the SWIC/STO/applicant of vetting status
  - Create an instructor profile in the COMU Repository and upload prerequisite documentation

Process to Conduct a State-Sponsored Communications Unit Course

- SWIC/STO Actions
  - The SWIC and/or STO will submit a Technical Assistance request to CISA through their CISA Emergency Communications Coordinator no less than 45 days prior to the start of the state-sponsored COMT or AUXCOMM/AUXC course or no less than 60 days prior to the start of the state-sponsored COML course. This lead-time gives CISA time to approve the TA request and order course materials. The TA request should include:
    - Planned dates for the course
    - The names of the qualified CISA Recognized State-Sponsored Instructors who will teach the course
    - The location of the course
    - The state point of contact (the person responsible for course coordination, receipt of course materials
    - A statement that the state accepts all responsibility and liability for the course, its students, and the instructors
    - Participate in a scoping call between CISA, the requesting individual, and the instructors involved
- Instructor Actions
  - Participate in a scoping call between CISA, the requesting individual, and the instructors involved
  - Obtain all logistical support (venue, projector, easels with pads of paper, etc.)
  - Ensure all course documentation (student prerequisites validation, attendee sign-in sheets, typed class rosters, student evaluations, and trip report) and processes follow CISA course guidelines
  - Teach the state-sponsored COML, COMT, or AUXCOMM/AUXC course without any changes, additions, or deletions to the CISA core curriculum. Any additional material the state wishes to have taught must be taught either before or after the CISA core curriculum
  - Send a copy of all student sign-in sheets, the typed class roster, student course evaluations and trip report to CISA, the SWIC and STO within five working days after the course

(Continued on next page)

  - Certify on the typed class roster by placing an "X" in the daily attendance blocks that the students attended all sessions and successfully completed the course. Do not include student information on the typed roster for students who did not successfully complete the course. Course completion certificates will only be provided to students who attend all sessions and successfully complete the course
  - Maintain copies of all documentation required by the state and CISA in accordance with state retention policies
  - Ensure a CISA TA Evaluation Form is completed and returned to CISA
- CISA Actions:
  - Maintain a file copy of all certifications/qualifications of CISA recognized instructors.
  - Participate in a scoping call between CISA, the requesting individual, and the instructors involved
  - Ship course materials approximately one week prior to the start of the course.
  - Issue CISA course completion certificates via email to the individual students within two weeks of receipt of the certified typed class roster, the Trip Report, the student evaluations and the CISA TA Evaluation for COMT and AUXCOMM courses
  - Add the roster of students that have completed the CISA approved state-sponsored Communications Unit course into CASM
  - Submit the course completion package to FEMA for COML courses

Questions regarding instructor requirements can be emailed to COMU@cisa.dhs.gov.

Training & Exercises

Audio Gateway Information and Training (AG)	
TA Delivery Method:	One-Day In-Person Workshop
Recommended Participants:	Communications Unit Personnel (COMT and Technical Specialists)

Offering Overview

This offering provides different levels of understanding on analog and digital LMR 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 5 or a maximum 10 students identified in order for CISA to schedule and conduct the course.

Training Modules:

- Gateway Overview. A high-level overview for personnel requiring a basic understanding of audio gateway functionality
- Advanced Audio Gateway Operation for communication technical specialists who need a more advanced understanding of gateway operations; for example, specific issues such as co-site RF interference
- Gateway Hands-on Configuration. Focused on specific equipment and is for gateway installers, maintenance technicians, and specialists
- 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 Communications Unit personnel
- Limited operator proficiency
- Identifying LMR communications interoperability issues
- High level overview for different audio gateways
- Audio gateway integration into NIMS ICS operations for Communications Unit personnel
- Hands-on exercise
- Techniques for mitigating RF interference

Usage

Operational Communications Assessment (OP-ASMT), Regional Communications Enhancement Support – Strategic Communications Migration Plan (RCES-SCMP), and Special Event Planning (OP-SPEV)	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	SWICs and Public Safety Professionals

Offering Overview

Operational Communications Assessment

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.

Regional Communications Enhancement Support – Strategic Communications Migration Plan

This TA offering helps stakeholders develop usable regional communications enhancement plans that require 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.

Special Event Planning

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 each state's unique needs. Potential design options, outcomes, and deliverables may include:

- Defined scope and authority in existing SOPs
- Compatibility with other federal, state/territory, tribal, regional, and/or local procedures/plans
- Responsibility and process for maintenance and update of the plan
- Training requirements and pre-event communications drills and exercises
- Understanding of and compliance with NIMS ICS principles
- Defined maintenance process plan
- Established training requirements and schedule
- Use of National Special Security Events (NSSE) Communications Toolkit [14]

[14] The NSSE toolkit was created by CISA and provides guidance information and helpful tools to assist local, state, and federal officials tasked with preparing for and providing communications support during National Special Security Events.

Usage

Communication Assets Survey and Mapping (CASM) Tool	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	SWICs, Communications Planners, System Owners, Communications Unit Personnel

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 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 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 former CIO 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 nation-wide view of agencies, fixed and mobile assets, fixed and mobile asset, personnel, and spectrum usage information, as well as coverage plots for associated transceivers.

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 each state's unique needs. Potential design options, outcomes, and deliverables may include:

- CASM training to:
  - maintain a detailed inventory of communications infrastructure (systems, comm sites, 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 talk group, and agency usage information
  - maintain information about mobile communications unit capabilities and Deployability
  - maintain 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 (ENCRYPT)	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	SWICs, RECCWGs, LMR System Operators, Public Safety Command/Leadership, and Communications Personnel

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 federal, state, local, tribal and territorial (FSLTT) authorities.

Customized support for this offering may vary to meet each state's 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 to 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 MOAs or 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 (PTS)	
TA Delivery Method:	Webinar
Recommended Participants:	SWICs and Public Safety Managers and Stakeholders

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 in an emergency or crisis situation 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 a 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. These services are 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:

- cisa.gov/gets
- cisa.gov/wps
- cisa.gov/tsp

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

- Thirty-minute webinar
- Explanation of NS/EP Telecommunications Services
- How to request NS/EP Services
- Eligibility criteria and costs
- How GETS and WPS operate within the FirstNet environment

Appendix A: SCIP Guide

The Value and Purpose of the SCIP Workshop

Every year the Department of Homeland Security (DHS) releases the Homeland Security Grant Program (HSGP) Notice of Funding Opportunity (NOFO) through the Federal Emergency Management Agency (FEMA) to announce funding opportunities that are available to states, territories, urban areas, and other local and tribal governments. These are DHS grants administered by FEMA with inputs from all elements of the homeland security enterprise. The new guidance addresses several recommendations advocated by the emergency communications community. DHS seeks to enhance the ability of states, local governments, tribes, and territories to prevent, protect against, respond to, and recover from potential terrorist acts and other hazards. To meet this requirement, states and territories are required to have an approved Statewide Communications Interoperability Plan (SCIP).

A SCIP defines the strategic direction for interoperable and emergency communications within a state. It outlines interoperability goals with specific steps for action (including action owners and completion timeframes) and defined mechanisms to measure achievements. The state may use the SCIP to demonstrate to leadership and elected officials' statewide successes, outline obstacles or challenges, and report on progress. The SCIP provides structure and focus through strategic planning for a one to three-year timeframe. It supports states and territories in developing their vision of future capabilities by incorporating all elements across the Emergency Communications Ecosystem.

In June 2019, Cybersecurity and Infrastructure Security Agency (CISA) began self-assessment workshops, which allowed states to collaborate regionally while assessing their individual status against newly developed State Interoperability Markers. The information collected will enable CISA to tailor support through technical assistance (TA) to states and territories, enhancing their interoperable communications capabilities. This has allowed states to continue the discussion of needed action within the realm of emergency communications, and ensure they plan and successfully implement interoperability solutions.

Emergency Communications Planning Framework

There are several different emergency communications frameworks states and territories can use to outline their goals and objectives. The Interoperability Continuum [15] has five lanes: Governance, Standard Operating Procedures, Technology, Training & Exercises, and Usage.

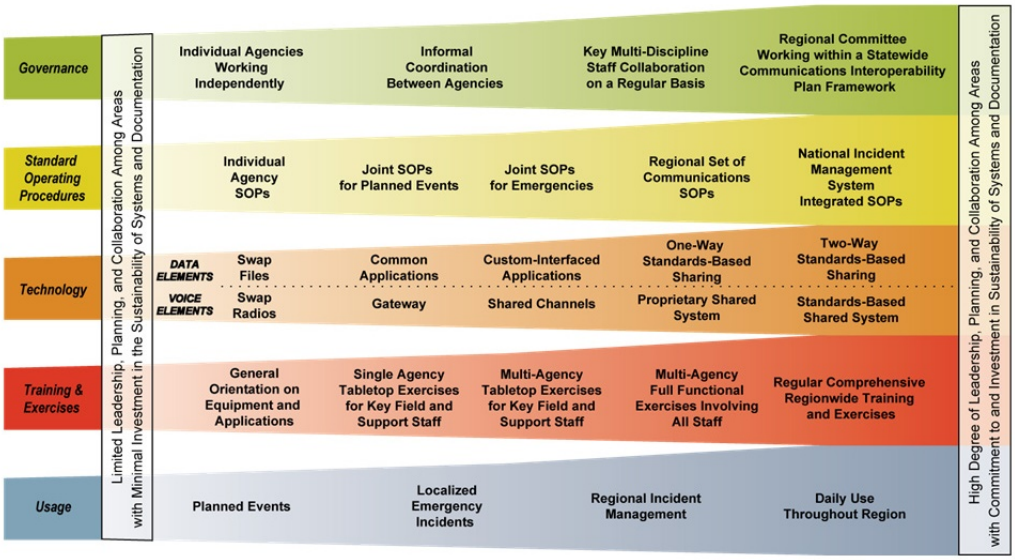


Figure 1: Interoperability Continuum

[15] The Interoperability Continuum is available here: cisa.gov/publication/interoperability.

Appendix A: SCIP Guide

States can also structure their SCIP to align with the National Emergency Communications Plan (NECP) [16], which provides guidance to drive enhancements of the Nation's emergency communications capabilities, by developing 6 goals: Governance & Leadership; Planning & Procedures, Training, Exercise, & Evaluation; Communications Coordination; Technology & Infrastucture; and Cybersecurity. The Emergency Communications Ecosystem, depcited in the NECP, is comprised of the various functions and people that exchange information prior to, during, and after incidents. Key functions necessary to achieve reliable, secure, and interoperable emergency communications include: Reporting and Requests for Assistance, Incident Coordination and Response; Alerts, Warnings, and Notifications, and Public Interaction.

Figure 2: Emergency Communications Ecosystem

CISA partnered with the National Council of Statewide Interoperability Coordinators (NCSWIC) to develop the State Interoperability Markers, which are 25 indicators of interoperable communications maturity aligned with the Interoperability Continuum, used to identify interoperability strengths and gaps, and then leveraging that information to set strategic goals in their SCIPs, and inform TA requests.

Central Focus Areas of the SCIP Workshop

Feedback from states and territories over the last few years has led CISA to focus on the central areas of governance, technology, and funding sustainability as the framework for development of goals and objectives within the SCIP. However, states and territories may also choose to use one of the above-mentioned emergency communications frameworks (e.g., the Interoperability Continuum, the NECP and/or the State Interoperability Markers) instead to outline goals and objectives.

Governance

These workshops focus on enhancing statewide governance and public safety communications planning. In working with all 56 states and territories, CISA learned that states with the most effective governance typically have the highest levels of interoperability among the stakeholders. A strong governance structure allows for all lanes of the Interoperability Continuum to receive consideration and for implementation. The SCIP process will review in detail the state's current governance structure, to include capabilities and identified gaps. CISA facilitators will lead discussions on the key elements of effective governance to identify best practices that can be implemented in the state.

[16] The NECP is available here: cisa.gov/necp.

Appendix A: SCIP Guide

Technology

The technology section of the workshop focuses on technology's current state and ideal future state based on technological needs across all emergency communications technologies and capabilities. Stakeholders outline the SCIP to maintain and upgrade existing technology while developing a roadmap to identify and implement new and emerging technology solutions with a focus on the following:

Land Mobile Radio (LMR)

LMR has been the foundational public safety communications mechanism for half a century and is the primary lifeline of two-way, push-to-talk mission critical communications among public safety agencies. Participants discuss, plan, and develop goals critical to maintaining and modernizing LMR systems to ensure uninterrupted availability.

Broadband

Emerging broadband technologies promise to enhance all aspects of public safety communications. These technologies will augment the transport and sharing of voice, data, and video communications. Participants will discuss strategies for incorporating the broader use of broadband during day-to-day events and the planning for broadband data integration in large-scale public safety mutual-aid responses.

9-1-1

The use of 9-1-1 continues to be the public's lifeline to request help from public safety agencies; however, the migration from wired landline to cellular service has required operational changes within Public Safety Answering Points (PSAPS) and dispatch functions nationwide. Participants discuss the integration of modern technologies, strategies and associated challenges, and the transition from legacy 9-1-1 to Next Generation 9-1-1.

Alerts and Warnings

Another key system serving the public is the use of emergency alerting and warning systems. Examples of these systems would include Integrated Public Alerts & Warning System (IPAWS), National Weather Service alerts, reverse 9-1-1 and warning sirens. Participants may discuss and plan for how these systems will work in conjunction with other communications systems.

Funding Sustainability

SCIP workshop attendees also discuss strategies to fund existing and future interoperable and emergency communications priorities. States and territories seek to identify alternative sources of funding to maintain existing systems and capabilities, and to assist with the integration of new technologies to keep pace with the ever-changing emergency communications landscape.

SCIP Process and Timeline

Overview of the SCIP Process

Developing a strategic plan provides direction and focus for the entire state, including all agencies and jurisdictions, on the primary interoperable and emergency communications goals and initiatives. CISA's collaborative process gives agencies and jurisdictions an opportunity to be involved in shaping and defining statewide goals and initiatives to improve the likelihood of success for the development and implementation of a SCIP. To complete a SCIP, CISA developed a five-phased process for a recommended duration of eight to ten weeks to develop and conduct a workshop and deliver a completed SCIP to the Statewide Interoperability Coordinator (SWIC).

SCIP Planning Timeline

When a state or territory requests a SCIP workshop, there are a variety of planning milestones associated with ensuring the SWIC has all the materials, stakeholder commitments, and federal resources necessary to create a productive workshop. As an overall planning strategy, the desired course of action to provide an effective workshop is reflected in Figure 2 below.

Appendix A: SCIP Guide

Approximately eight to ten weeks prior to a desired on-site workshop, CISA and the SWIC will coordinate with stakeholders to develop the desired outcomes and participant list. During the planning process, the SWIC may utilize a survey to increase SCIP awareness, bring light to any new concerns, and gauge stakeholders' priorities related to emergency communications in their state. Following the pre-workshop planning process, CISA, in coordination with the SWIC, will develop all supporting materials necessary to ensure a successful meeting and an all-encompassing SCIP document. A draft SCIP will be delivered by CISA a few weeks following the workshop. Note, the planning process can be customized to meet the state's own completion date. The notional timeline below reflects the milestones and key steps in CISA's collaboration with states/territories in building a successful SCIP workshop and resulting plan.

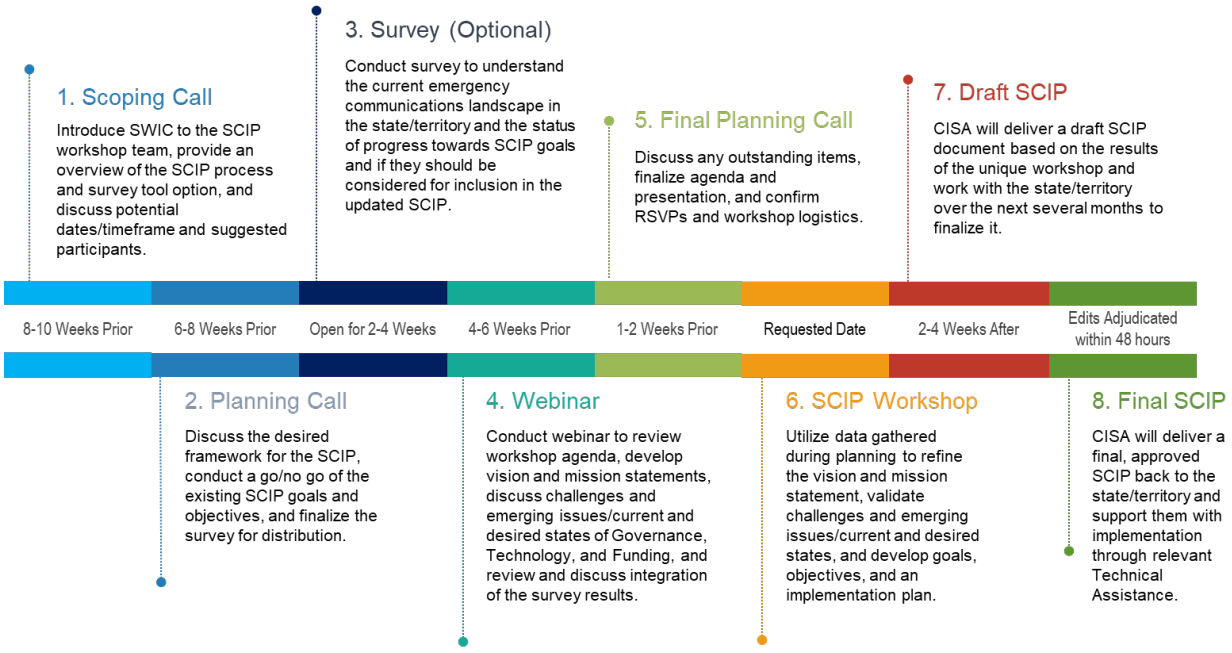


Figure 3: SCIP Process Timeline

Who Should Attend a SCIP Workshop?

The SCIP Workshop presents a unique opportunity to bring together a variety of stakeholders from across the state/territory for an intensive strategic planning workshop. When a diverse group collaborates to develop the SCIP, the result is a high-quality, executable plan with stakeholder ownership. Identifying key stakeholders that are relevant to the state/territory's interoperable and public safety communications efforts fosters strong working relationships while ensuring full representation in supporting the vision and mission of the SCIP. Subject matter experts and decision makers as well as representation from emerging technologies (broadband, NG 9-1-1, and alerts and warnings) should be included. During the planning phase, the SCIP team works with the SWIC to discuss the best approach to include leveraging CISA leadership and their sphere of influence to ensure broad attendance. CISA can also provide support with drafting invitation language that highlights state-specific information and create background materials for stakeholders to review prior to the workshop. CISA can disseminate workshop invitation and track RSVPs.

Appendix A: SCIP Guide

State Communications Leaders

- Statewide Interoperability Governing Body / Executive Committee
- Statewide Interoperability Coordinator
- Working Group Chairs
- FirstNet Single Point of Contact (SPOC)
- State Broadband Office / Committee Members
- 9-1-1 Board Members

State Government Leadership/Designee

- Executive and Legislative Leaders
- Governor's Office
- State Adjutant General
- Public Utility Commission
- Utility Regulation Authority
- Grants Coordinator
- State Chief Financial Officer
- State Chief Information Officer
- State Chief IT Security Officer
- State Chief Technology Officer
- Department of Emergency Management
- ESF-2 Coordinator
- State Director of Homeland Security
- State 9-1-1 Administrator
- Emergency Communications Office
- Incident Management Teams
- State EMAC Coordinator
- State Training Officer
- Regional Exercise Officer
- Public Safety Academy/Dispatch Training

Public Safety/Public Service Entities

- FirstNet Regional Representatives
- 9-1-1/PSAP Officials
- Corrections
- Emergency Management
- Emergency Medical Services
- Fire Departments
- Law Enforcement
- Public Health
- Public Safety Communications Network Operators
- Public Works
- Department of Transportation
- Department of Health
- Maritime/Port Authorities

Associations

- Association of Chiefs of Police
- State Sheriff's Association
- National Emergency Number Association
- National Association of State 9-1-1 Administrators
- National Association of CIOs
- Association of Counties
- Association of EMS Administrators
- Association of Public-Safety Communications Officials
- Emergency Management Associations
- Fire Chiefs' Association
- State Fire Fighters' Associations
- Hospital and Public Health Associations
- Public Works Associations
- Other associations of elected leaders (County Commissioners, Judges, etc.)
- State-level Amateur Radio Organizations

Other Entities

- Board of Regents
- College and University Public Safety
- Bordering State SWICs
- Communications Industry
- Rail Industry
- Non-Governmental Organizations
- Regional Councils of Government
- Municipal Government Leadership
- Private Public Safety Entities
- Tribal Nation Representation

SWIC Checklist

Scoping Call

- ✓ Discuss desired planning framework/approach
- ✓ Engage SWIC on use of State Survey
- ✓ Discuss variety of services CISA can provide throughout process

Survey Design

- ✓ Provide feedback on templated survey questions and customize it to meet state-specific outcomes

Planning Call

- ✓ Review survey questions and provide any feedback as well as a list of potential survey respondents
- ✓ Review Scoping Call Summary and Read Ahead Package
- ✓ Invite suggested participants to join Webinar

Appendix A: SCIP Guide

Webinar

- ✓ Review Planning Call Summary and provide any feedback
- ✓ Invite suggested participants to the in-person SCIP workshop on [insert date]
- ✓ Review live capture document with current and desired state / successes, challenges, and emerging issues and provide any feedback

Final Planning Call

- ✓ Provide any final edits to the workshop agenda, updated list of RSVPs, and any outstanding items
- ✓ Schedule Walkthrough of venue

SCIP Workshop

- ✓ Review live capture document with goals, objectives, and an implementation and provide any feedback

Appendix B: 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 federal, state, local, tribal, and territorial governments (FSLTT), and international borders. [17]

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 and SCIP Workshop 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

[17] Additional information regarding SAFECOM is available at cisa.gov/safecom.

Appendix C: TA Request Form

OMB No. 1670-0023
Expiration Date: 7/31/2023

DEPARTMENT OF HOMELAND SECURITY
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)
TECHNICAL ASSISTANCE (TA) REQUEST FORM

TA Service Offerings and SCIP Workshop requests can be submitted by completing the fillable form located on the SAFECOM website: cisa.gov/publication/ictapscip-resources.
Email the completed PDF to: TARequest@cisa.dhs.gov.

(Requestor) Contact Information:

State:
Name:
Phone:
Email:

Sector Coordinator:

☐ SCIP Workshop	Requester's Targeted Date Range for Workshop:
To request a SCIP wokrshop please check the box above and insert the desired target date(s) for the workshop in the space provided	From: ____ To: ____

Appendix C: TA Request Form

OMB No. 1670-0023
Expiration Date: 7/31/2023

DEPARTMENT OF HOMELAND SECURITY
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)
TECHNICAL ASSISTANCE (TA) REQUEST FORM

CISA is providing these new and improved TA service offerings	
✓ Virtual SCIP Workshop ✓ Virtual Communications Unit Training ✓ Incident Communications Awareness Overview ✓ Incident Tactical Dispatcher / Communications Center Manager Awareness Overview	✓ 9-1-1/PSAP Cyber Assessment ✓ 9-1-1/PSAP Cyber Awareness ✓ Communications Unit Planning and Policy ✓ Alerts and Warnings ✓ Tactical Field Operations Guide ✓ Electronic Field Operations Guide ✓ Tactical Interoperable Communications Plan

Note: If the Requested TA is Strategic, please check the box in the "Priority" column and describe what Goal or Objective it aligns with (i.e., SCIP, NECP, or State Markers) in the corresponding block on the Continuation Sheet (page 5) of this form.

TA Guide Service Offering Selections			
Priority	**CISA TA Offering**	**Timeframe From/To**	**Primary Point of Contact (Name, Phone, Email)**
1 ☐			
2 ☐			
3 ☐			
4 ☐			
5 ☐			

SWIC/SCIP POC

SIEC/SIGB/Chair Date of Concurrence

Submission Date

Notification may be given verbally or by email

OMB No. 1670-0023
Expiration Date: 7/31/2023

DEPARTMENT OF HOMELAND SECURITY
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)
TECHNICAL ASSISTANCE (TA) REQUEST FORM

CONTINUATION SHEET – TA REQUEST

Priority	TA Requrements/Description of Assistance
1	
2	
3	
4	
5	

Appendix D: Additional TA Resources

National Interoperability Field Operations Guide (NIFOG)

The National Interoperability Field Operations Guide (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, download and request printed copies of the NIFOG please visit this site: cisa.gov/publication/fog-documents.

Auxiliary Communications Field Operations Guide (AUXFOG)

The Auxiliary Communications Field Operations Guide (AUXFOG) is a reference for auxiliary communicators who directly support backup emergency communications for State/local public safety entities or for an amateur radio organization supporting public safety.

To view or download the AUXFOG, please visit this site: cisa.gov/publication/fog-documents.

National Special Security Event (NSSE) Special Event Assessment Rating (SEAR) Toolkit

This toolkit is designed for all persons involved in the communications planning and operations process. It provides guidance information and helpful tools to assist local, state, and federal officials tasked with preparing for and providing communications support during NSSE/SEAR events. The information provided is not all inclusive and not all information may be applicable during all events or in all jurisdictions.

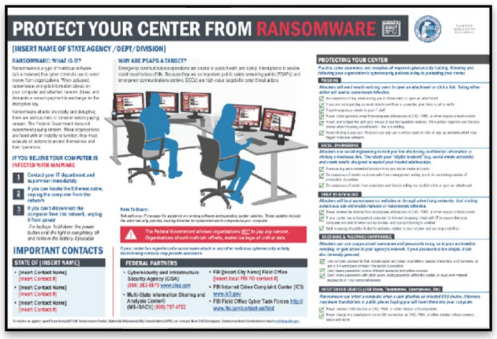
To request a printed copy please contact your CISA Emergency Communications Coordinator listed on page 6 of this guide or send an email request to ECD@cisa.dhs.gov.

Cybersecurity Ransomware Poster

The ransomware poster can be placed in an Emergency Communications Center/ Public Safety Answering Point (PSAP), 911 Call or 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 poster, Statewide Interoperability Coordinators (SWICs) may contact their CISA Emergency Communications Coordinator and/or email the request to ECD@cisa.dhs.gov.

SWICs may request two printed 20" x 30" copies of the poster and a customized electronic file will be provided for printing additional copies.

To view, download and request printed copies of the Ransomware Poster please visit this site: cisa.gov/publication/next-generation-911.



Appendix E: Acronyms

Acronym	Definition
AAR/IP	After Action Report/Improvement Plan
AG	Audio Gateway
ACU 1000	Intelligent Audio Communication Gateway
AUXCOMM/AUXC	Auxiliary Communications
BRBND	Broadband
CAD	Computer-Aided Dispatch
CASM	Communication Assets Survey and Mapping Tool
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
COG	Continuity of Government
COML	Communications Unit Leader
COMMDRILL	Communications Drill
COMMEX	Communications Unit Exercise
COMT	Communications Unit Technician
COMU	Communications Unit
COMUAWR	All Hazards Incident Communications Unit Awareness
COMUPLAN	Communications Unit Planning and Policies
COOP	Continuity of Operations Plan
COVID-19	Coronavirus Disease 2019
CSA	Cybersecurity Advisor
CYBR	Cyber
DHS	U.S. Department of Homeland Security
DSL	Digital Subscriber Line
ECC	Emergency Communications Coordinator
ECC/PSAP	Emergency Communications Center/
ECD	Emergency Communications Division
EAS	Emergency Alert System
eAUXFOG	Electronic Auxiliary Communications Field Operations Guide
eFOG	Electronic Field Operations Guide
eNIFOG	Electronic National Interoperability Field Operations Guide
EMA	Emergency Management Agency
EMAC	Emergency Management Assistance Compact
EMS	Emergency Medical Services
ENCRYPT	Encryption
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
ESF	Emergency Support Function
EXDESIGN	Exercise Design
EXPLAN	Exercise Plan
FCC	Federal Communications Commission
FEMA EMI	Federal Emergency Management Agency Emergency Management Institute

Appendix E: Acronyms

Acronym	Definition
FEMA NIC	Federal Emergency Management Agency National Integration Center
FCC	Federal Communications Commission
FirstNet	First Responder Network Authority
FE	Function Exercise
FY	Fiscal Year
FISMA	Federal Information Security Management Act
FSE	Full Scale Exercise
FSLTT	Federal, State, Local, Territorial, Tribal
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
ICCAP	Interoperable Communications Capabilities Assessment Program
ICS	Incident Command System
ICTAP	Interoperable Communications Technical Assistance Program
IPAWS	Integrated Public Alert and Warning Systems
IPM	Initial Planning Meeting
INCM	Incident Communications Center Manager
INTD	Incident Tactical Dispatcher
ISSI	Inter Radio Frequency (RF) Subsystem Interface
IT	Information Technology
ITSL	Information Technology Service Unit Leader
JIC	Joint Information Center
LMR	Land Mobile Radio
LTE	Long Term Evolution
MASS	Mutual Aid Support System
MEP	Master Exercise Practitioner
MCU	Mobile Communications Unit
MHz	Megahertz
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MRP	Mission Ready Package
MSEL	Master Scenario Events List
NCATS	National Cyber Assistance and Technical Services
NCSWIC	National Council of Statewide Interoperability Coordinators
NECP	National Emergency Communications Plan
NG9-1-1	Next Generation 9-1-1
NGA	National Governors Association
NIFOG	National Interoperability Field Operations Guide
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration

Appendix E: Acronyms

Acronym	Definition
NOFO	Notice of Funding Opportunity
NPSBN	Nationwide Public Safety Broadband Network
NRF	National Response Framework
NS/EP	National Security and Emergency Preparedness
NSSE	National Special Security Events
OP-ASMT	Operational Assessment
PAR	Priority Telecommunications Service Area Representative
POC	Point of Contact
PSA	Protective Security Advisor
PSAP	Public Safety Answering Point
PSCC	Public Safety Communications Center
PTB	Position Task Book
RADO	Radio Operator
RCES	Regional Communications Enhancement Support
REACT	Radio Emergency Associated Communications Team
RECCWG	Regional Emergency Communications Coordination Working Group
RF	Radio Frequency
RMS	Records Management System
SCMP	Strategic Communications Migration Plan
SCIP	Statewide Communication Interoperability Plan
SEAR	Special Event Assessment Rating
SECIR	Stakeholder Engagement and Cyber Infrastructure Resilience
SIEC	State Interoperability Executive Council
SIGB	Statewide Interoperability Governance Board
SLTT	State, Local, Tribal, and Territorial
SME	Subject Matter Expert
SOG	Standard Operating Guide
SOP	Standard Operating Procedure
SPEV	Special Event
SPOC	Single Point of Contact
SSCOMT	State-Sponsored Communications Unit Technician
SSCOML	State-Sponsored Communications Unit Leader
SSAUXCOMM/AUXC	State-Sponsored Auxiliary Communications
STO	State Training Officer
STRATPLAN	Strategic Planning
SWIC	Statewide Interoperability Coordinator
TA	Technical Assistance
TBD	To Be Determined
TDoS	Telephony Denial of Service
TERT	Telecommunicator Emergency Response Taskforce
TICFOG	Tactical Interoperable Communications Field Operations Guide
TICP	Tactical Interoperable Communications Plan
TSP	Telecommunications Service Priority
TtT	Train-the-Trainer
TTX	Tabletop Exercise

Appendix E: Acronyms

Acronym	Definition
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