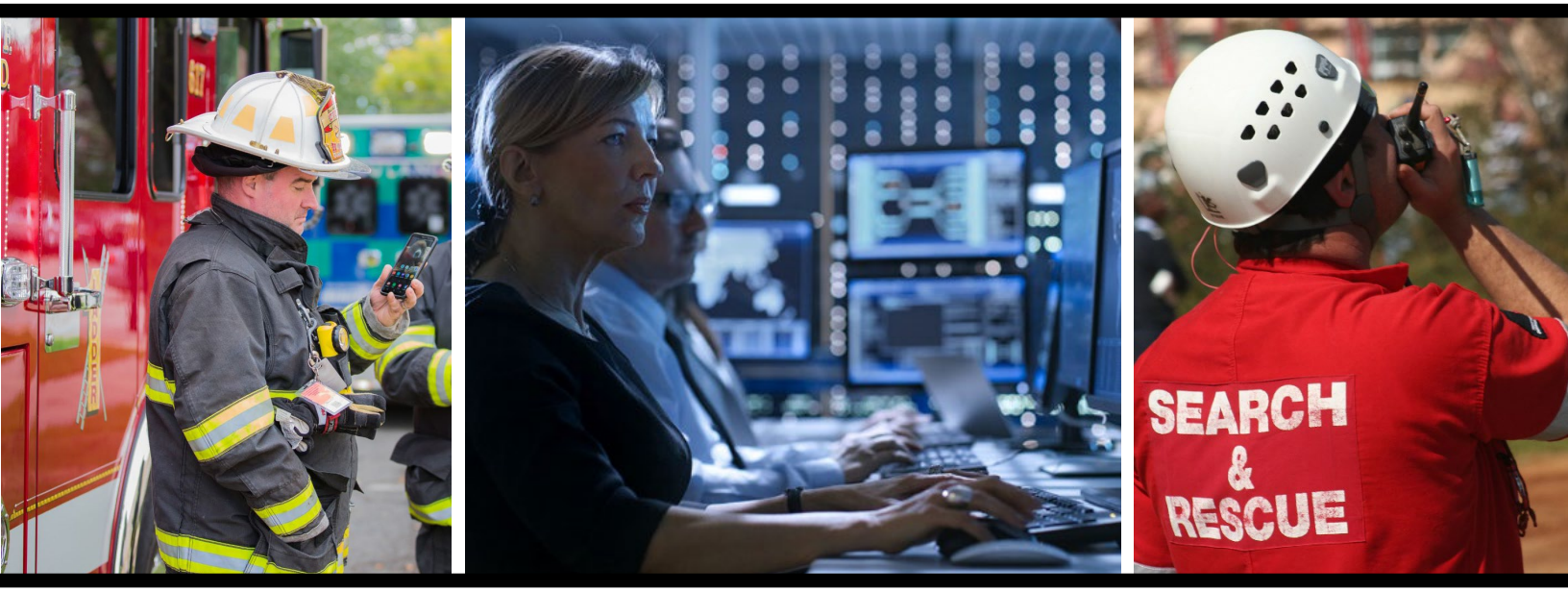


INTEROPERABLE COMMUNICATIONS TECHNICAL ASSISTANCE PROGRAM

Service Offerings Guide

Version 7.1

April 2023

Cybersecurity and Infrastructure Security Agency

Table of Contents

Foreword

Effective interoperability begins with people, partnerships, and practices. To address current and future threats to operable and interoperable communications, the Cybersecurity and Infrastructure Security Agency (CISA) partners with national security and emergency preparedness stakeholders to develop technical assistance (TA) offerings that meet their evolving needs.

COLLABORATION

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

INNOVATION

Thanks to the collaborative process, we glean feedback and adapt and develop new TA. The range of assistance available spans from TA engagements to educational offerings such as Communications Unit Leader (COML) training. 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. TA offerings can be customized and delivered virtually through a variety of media and web-based platforms.

SERVICE

CISA TA offerings are provided to all states and territories and Native American and Alaska Native tribes at no cost. There are no submission deadlines that must be met. When a TA need is identified, a TA request may be submitted at any time throughout the year to meet interoperability requirements.

ACCOUNTABILITY

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

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

Best Regards,

Billy Bob Brown, Jr.

Executive Assistant Director for Emergency Communications

Cybersecurity and Infrastructure Security Agency

CISA Technical Assistance

New and Updated CISA Technical Assistance Offerings

Governance

- Tribal Strategic Communication Interoperability Plan (TSCIP) Workshop

Standard Operating Procedures

- Effective Communications During Active Shooter Incidents
- Primary, Alternate, Contingency, and Emergency (PACE) Plan Development

Technology

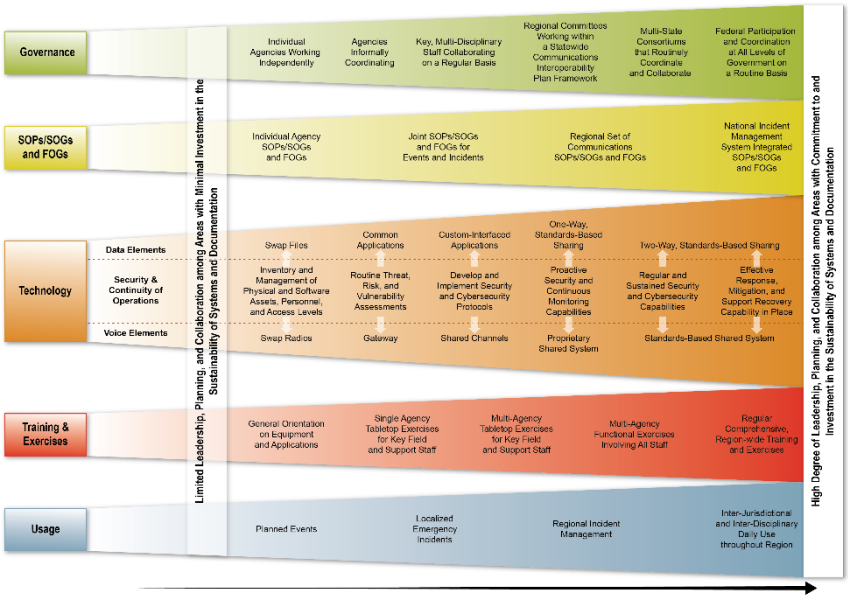
- 9-1-1/PSAP Cyber Awareness Webinar
- LMR Cyber Awareness Webinar
- One-Day Cyber Awareness Workshop
- Two-Day Threat Assessment and Response Workshop
- Full Cyber Assessment
- Rapid Cyber Assessment
- Post Assessment Workshop
- CISA now offers customized Telephony Denial of Service (TDoS) posters upon request. See Appendix C: Additional TA Resources for information on how to request.

Training and Exercises

- Resilient Communications Awareness Training Webinar
- Resilient Communications Incident Communications Management Training Course

Usage

- Communication Assets Survey and Mapping (CASM) Tool
- Priority Telecommunications Services (PTS)



SAFECOM Interoperability Continuum

CISA Technical Assistance

Virtual TA Service Offerings

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.

CISA offers a portfolio of no-cost virtual technical assistance services on web-based platforms using remote instruction methodologies. 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
- Primary, Alternate, Contingency, and Emergency (PACE) Plan Development
- Standard Operating Procedures (SOP) Review and Development
- Tactical Interoperable Communications Plan
- Tactical Interoperable Field Operations Guide
- Electronic Field Operations Guide
- Alerts and Warnings
- Next Generation 9-1-1 Strategic Planning
- 9-1-1/PSAP Cyber Awareness Webinar
- LMR Cyber Awareness Webinar
- Full Cyber Assessment
- Post Assessment Workshop
- Rapid Cyber Assessment
- Resilient Communications Awareness Training Webinar
- Encryption Planning and Usage

Virtual Communications Unit Training*:

- Communications Unit Leader (COML)
- Communications Unit Leader Train-the-Trainer (COML TtT)
- Auxiliary Communications (AUXCOMM)
- Auxiliary Communications Train-the-Trainer (AUXCOMM TtT)
- Incident Tactical Dispatcher (INTD)
- Incident Communications Center Manager (INCM)
- INTD/INCM Awareness Overview (TRG-OVERVW)

*For planning purposes, virtual courses are one-day longer than in-person courses due to the additional logistics required.

CISA supports states and territories by prioritizing strategic TA support that promotes the 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).

CISA Technical Assistance

Communications Unit Virtual Training Student Requirements

Students registered for virtual courses will be required to attend a one-hour technical check and overview of the Webex Training platform the week prior to the course start date. Only after completing this technical check, will a student be accepted into the course.

- 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.)
  - Headset with a microphone, or earbuds with built-in microphone
  - Web Camera must be available and left on at all times during the entire course
  - A reliable Internet connection
- 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. One of the folders in the .zip file contains a few pages INTD students are expected to print and have on hand for the course
- Virtual training course capacities are limited to the following:
  - COML has a maximum of 15 students
  - INCM has a maximum of 15 students
  - AUXCOMM has a maximum of 15 students
  - INTD has a maximum of 16 students
  - All Train-the-Trainer courses have a minimum of 8 students and a maximum of 10

CISA Technical Assistance

TA Request Process

- **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:** Pre-event planning support and after-action assessments for National Special Security Events (NSSE)/Special Event Assessment Rating (SEAR) or natural or manmade disasters.
  - **TA Request Form:** To request TA, the SWIC or other designated SLTT point of contact needs to complete the fillable TA request form on the SAFECOM website at: cisa.gov/safecom/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 by E-mail" 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.

CISA Technical Assistance

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 Sector.

East Sector (Regions I, II, III)

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

- **ECC** – Tom Gagnon Thomas.Gagnon@cisa.dhs.gov
- **ECC** – Melissa Nazzaro Melissa.Nazzaro@cisa.dhs.gov
- **ECC** – Steve Singer Steven.Singer@cisa.dhs.gov
- **ECC** – Chris Tuttle Christopher.Tuttle@cisa.dhs.gov

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

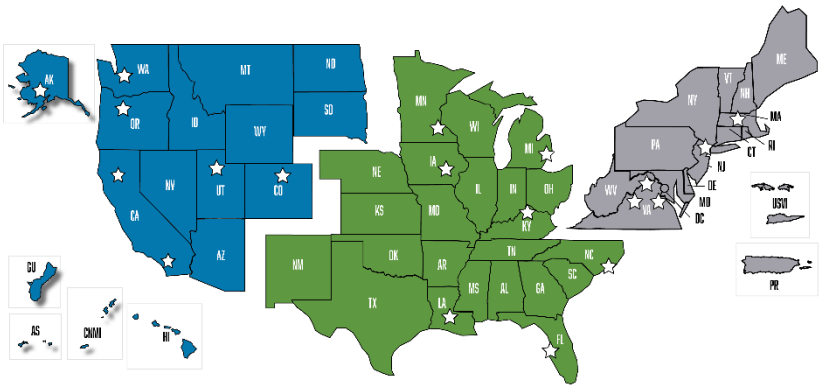
Sector Chief – Chris Essid Chris.Essid@cisa.dhs.gov

- **ECC** – Jim Jarvis James.Jarvis@cisa.dhs.gov
- **ECC** – Travis Johnson Travis.Johnson@cisa.dhs.gov
- **ECC** – Chris Maiers Christopher.Maiers@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 Sector (Regions VIII, IX, X)

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

- **ECC** – Gordy Coles Gordon.Coles@cisa.dhs.gov
- **ECC –** Jeremy Johnson Jeremy.Johnson@cisa.dhs.gov
- **ECC** – Tom Lawless Thomas.Lawless@cisa.dhs.gov
- **ECC** – Artena Moon Artena.Moon@cisa.dhs.gov
- **ECC** – Bruce Richter Bruce.Richter@cisa.dhs.gov
- **ECC –** Brandon Smith Brandon.Smith@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, Virtual or Hybrid Workshop
Recommended Participants:	State Interoperability Executive Committee (SIEC)/Statewide Interoperability Governance Board (SIGB) Members, SWICs, State, Local, Federal, Tribal Stakeholders/Police, Fire and Emergency Medical Services (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 National Governors Association recommendations, consideration of data gathered through the State Performance Markers baseline and NECP goals and objectives
- One or more focused engagements:
    - Governance focused engagement to establish a governance body or strengthening existing governance and building consensus and goals
    - Technology and Cybersecurity focused engagement to review and leverage survey results to develop land mobile radio (LMR), broadband (BRBND), 9-1-1, Alerts and Warnings and Cybersecurity goals
    - Funding sustainability focused engagement on reviewing the FY21 HSGP criteria to develop funding goals
- Customized evaluation and action plan for implementation of the SCIP goals
- Evaluation and progress assessment of goals
- Strategic goals and implementation plan
- Evaluation/progress management

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

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

Governance

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

Offering Overview

The TSCIP is a partner-driven and multi-disciplinary Tribal strategic plan designed to enhance interoperable emergency communications. TSCIPs serve as a single document for partners throughout a Tribe's communications ecosystem to prioritize resources, strengthen administration, identify future investments, and address interoperability gaps. It also serves to complement other plans such as Homeland Security or Disaster Preparedness Plans. A current TSCIP (within 36 months) can help support the need for grant funding of the Tribal Homeland Security Grant Program (THSGP).[2]

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

- Draft TSCIP performance goals baseline against NECP goals and objectives
- A three to five-year roadmap
- One or more focused engagements:
    - Communications Administration focused engagement to establish an administrative body or strengthen the existing administration structure
    - Technology and cybersecurity-focused engagement to review and leverage survey results to develop land mobile radio (LMR), broadband (BRBND), 9-1-1, alerts and warnings, and cybersecurity goals
    - Funding sustainability engagement focused on reviewing the THSGP criteria to develop funding goals
- Customized evaluation and action plan for implementation of the TSCIP goals
- Evaluation and progress assessment of goals
- Strategic goals and implementation plan

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

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

Governance

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 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.[3]

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 a governance group
- Best practices for establishing governance group operating norms
- Assessment of governance group representation and customized approach for improvements
- Evaluation and analysis of SCIP, progress towards stated goals and objectives, and recommendations for SCIP refresh/update

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

Governance

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 to take a more holistic approach in helping states, territories, and tribes formally establish Communications Units. 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 Communications Unit positions.

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

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

- Formal recognition or certification/recertification processes for identified Communications Unit positions
- Establishment of a Qualifications Review Board (QRB)
- Comprehensive plan and/or guiding principles for a Communications Unit Program
- Methods to track and report Communications Unit human resource assets
- Introduction to systems that track Communications Unit personnel qualifications along with recognition/certifications and renewal certifications
- Discuss opportunities that provide training and exercises to develop and or maintain qualifications and experience
- Assist in developing performance measures of a Communications Unit Program
- CISA provides ongoing, sustained support to help maintain Communications Unit planning bodies for credentialing quality assurance and candidate vetting as well as encouraging relationships with state training officers (STO)

Potential Follow-up: For those states, territories and tribes desiring additional formalized processes for the Communications Unit 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.

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, COMLs, Agency Radio Officers, 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 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 advantages the state/jurisdiction gains by having predetermined Mission Ready Packages (MRP's); 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 via the Mutual Aid Support System (MASS) and predetermined MRP's.

This offering can be delivered in-person or virtually, and can be a one or two-day offering depending on the desires of the State/jurisdiction. The one-day version provides basic familiarity with EMAC, and provides training in creating MRP's. The two-day version allows for completion of a specific MRP which will serve as the first Communications Unit MRP, and be a standard for any additional MRP's that are created by the State/jurisdiction.

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

This offering is applicable to states 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 Guide for Public Safety Communications* provides an overview of various methods of funding emergency communications systems (e.g., bonds, special tax, surcharges), and specific examples of where these methods have been used to fund state and local systems
- *Land Mobile Radio Trio*; *Brochure*; and *Action Memorandum* provide stakeholders with basic information they can give to state and local decision-makers and elected officials on why it is important to fund and sustain public safety radio systems
- *Emergency Communications System Lifecycle Planning Guide* aids stakeholders in their efforts to fund, plan, procure, implement, support, and maintain public safety communications systems, and eventually to replace and dispose of system components
- *Contingency Considerations When Facing Reductions in Emergency Communications Budgets* and *Contingency Planning Guide for Emergency Communications Funding* help state, local, tribal, and territorial government agencies maintain or adjust their budgets in a time of constrained funding

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

Standard Operating Procedures

Effective Communications During Active Shooter Incidents (COMMS-ASI)	
TA Delivery Method:	In-Person Workshop
Recommended Participants:	Communications supervisors and dispatchers; law enforcement, fire and EMS supervisors; radio technicians and PSAP IT support; emergency management; hospital personnel; mutual aid partners; and Public Information Officers

Offering Overview

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

The workshop has three objectives:

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

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

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

Expected Outcomes:

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

Prerequisites for Attendance:

- None

Standard Operating Procedures

Primary, Alternate, Contingency, and Emergency (PACE) Plan Development	
TA Delivery Method:	In-Person Workshop or Webinar
Recommended Participants:	Public safety personnel including PSAP/9-1-1, law enforcement, fire and emergency medical services, emergency management, and any persons responsible for critical government services.

Offering Overview

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

The workshop covers the following topics:

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

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

- Facilitated PACE plan development
- Pre-workshop review of existing plans and SME recommendation on PACE strategies

Standard Operating Procedures

Standard Operating Procedures (SOP)/Standard Operating Guidelines (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
- 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 shall be prioritized, and the steps individual agencies should follow to request, activate, use, and deactivate each asset.

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

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

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

Customized support for this offering may vary to meet 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 that may include information such as frequencies, Government Emergency Telecommunications Service (GETS)/Wireless Priority Service (WPS) information, radio caches, alerts and warning message formats, among others. In addition, reference material for use by emergency response and communications personnel responsible for establishing and maintaining interoperable communications during events or incidents may also be included. A printed copy TIC-FOG is designed as a pocket-sized quick reference guide that can be carried by radio operators and technicians at all times.

Customized support for this offering may vary to meet 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

Standard Operating Procedures

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

Offering Overview

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

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

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

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

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

- Off-line mobile app Field Operations Guide information for state or region
- Live links to reference websites, emails, 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
- A single portal for all eFOGs developed by CISA

Technology

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

Offering Overview

CISA can assist 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.

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
- Long Term Evolution (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 (AAR) that includes an improvement plan (IP) 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/IP

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 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 (Urban Area Security Initiative (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
- Public safety broadband 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/ECC/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
- Computer-Aided Dispatch (CAD) to CAD transition support
- CAD to Records Management System (RMS) transition support
- Automated Security Alarm Protocol (ASAP) to PSAP

Technology

9-1-1/PSAP Cyber Awareness Webinar (CYB-AWR911PSAP)	
TA Delivery Method:	In-Person, Workshop or Webinar
Recommended Participants:	SWICs, State 9-1-1 Coordinators, Dispatchers, Call Takers, 9-1-1 Operators/ECC/PSAP Managers and System Operators

Offering Overview

While the evolution of public safety communications (including the ongoing transition to Next Generation 9-1-1) has dramatically improved voice and data communications, both Legacy 9-1-1 and NG9-1-1 systems are vulnerable to cybersecurity attacks. 9-1-1/PSAP/ECC functions are considered high-value cyber targets to those looking to disrupt public safety services, extort local governments through ransomware[5], or create mischief. Also, ECCs are sometimes an unintended target, becoming 'collateral damage' when a municipality or a supporting managed service provider is attacked. The critical nature of 9-1-1/PSAP/ECC operations means cyberattacks against them can result in a large-scale impact on public safety operations, impacting the public's ability to obtain assistance.

This offering introduces public safety communications stakeholders to common cybersecurity threats and vulnerabilities affecting 9-1-1/PSAP/ECC environments. Topics include ransomware attacks and their impact, Telephony Denial of Service (TDoS) attacks against administrative lines and 9-1-1, exposed networks and devices, why individual logons and password protection is critical, cryptojacking and email phishing. The 9-1-1/PSAP Cybersecurity Awareness Webinar also discusses basic best practices to improve the secure use of emergency communications technologies in daily operations. In addition, guidance is provided on responding to and reporting cyber incidents.

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

Customized support for this offering may vary to meet 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 ECC operations
- Tailoring to emphasize specific topics or audiences such as managed services providers
- 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[6]

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

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

Technology

LMR Cyber Awareness Webinar (CYB-AWRLMR)	
TA Delivery Method:	In-Person, Workshop, or Online Webinar
Recommended Participants:	SWICs, ECC/LMR Managers and System Operators

Offering Overview

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

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

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

Customized support for this offering may vary to meet 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 LMR and ECC operations
- Tailoring to emphasize specific topics or audiences such as managed services providers
- 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[8]

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

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

Technology

One-Day Cyber Threat Awareness Workshop (CYB-WKSTHRTAWR)	
TA Delivery Method:	In-Person, Instructor Led Training
Recommended Participants:	SWICs, State 9-1-1 Coordinators, 9-1-1 Operators/ECC/PSAP/LMR Managers and System Operators

Offering Overview

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

Workshop Objectives:

- Build awareness about the threats and vulnerabilities common to public safety
- Provide an overview of cyber hygiene best practices
- Develop an understanding of how to identify and manage cyber-risks
- Establishing adequate third-party governance and risk management
- Promote the other offerings available through Interoperable Communications Technical Assistance Program (ICTAP)/Cybersecurity Division (CSD)

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

Technology

Two-Day Threat Assessment and Response Planning Workshop (CYB-WKSTHRTASMTRSP)	
TA Delivery Method:	In-Person, Instructor Led Training
Recommended Participants:	SWICs, State 9-1-1 Coordinators, 9-1-1 Operators/ECC/PSAP/LMR Managers and System Operators

Offering Overview

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

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

Workshop Objectives:

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

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

Technology

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

Offering Overview

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

The Full Assessment (average 6-8 week effort) is intended to identify or provide the following:

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

The assessment consists of a review of a state, territory, tribal nation, region, county, or urban area Land Mobile Radio (LMR) network or Public Safety Answering Point (PSAP) target systems' security mechanisms against the complete LOW Baseline security control set using the nationally-recognized best practice guidelines National Institute of Science and Technology (NIST) Special Publication (SP) 800-53 revision 5, Security and Privacy Controls for Information Systems and Organizations.[9] The control set will be tailored up or down depending on the needs of the agency and system being assessed. Additional controls may be added to support systems that store, transmit or process sensitive data or privacy information, or state/county regulations. Federal government-specific controls will be removed from the baseline.

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

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

(Continued on next page)

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

- **Analysis**
  - Analyze review findings to determine compliance or non-compliance with baseline controls.
- **Assessment**[10]
  - Perform a qualitative assessment of non-compliant controls, based on vulnerability, threats, potential impact, and likelihood of occurrence.
- **Report**
  - Report findings in a Security Assessment Report (SAR) including recommended mitigation strategies in a prioritized format based on potential risk to the organization or its mission.

This technical assistance provides 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, and developing staffing requirements.

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

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

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

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

Technology

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

Offering Overview

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

The Rapid Assessment (average 2-3 week effort) is intended to identify or provide the following Cybersecurity mechanisms in place to defend the environment

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

The assessment consists of a review of a state, territory, tribal nation, region, county, or urban area Land Mobile Radio (LMR) network or Public Safety Answering Point (PSAP) target systems' security mechanisms against a subset of critical or key security controls selected to assess the overall security posture of the 9-1-1/PSAP/LMR environment. The control set consists of 69 NIST separate controls from the National Institute of Science and Technology (NIST) Special Publication (SP) 800-53 revision 5, Security and Privacy Controls for Information Systems and Organizations[11]. This control set was selected after conducting research on critical areas of cybersecurity concern within the PSAP community and provides a cybersecurity snapshot and insight into areas of immediate concern.

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

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

(Continued on next page)

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

Technology

- **Analysis**
  - Analyze review findings to determine compliance or non-compliance with baseline controls.
- **Assessment**[12]
  - Perform a qualitative assessment of non-compliant controls, based on vulnerability, threats, potential impact, and likelihood of occurrence.
- **Report**
  - Report findings in a Security Assessment Report (SAR) with recommended mitigation strategies in a prioritized format based on potential risk to the organization or its mission.

This technical assistance provides 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 for engaging CISA in a Full Assessment of their system(s), developing action plans, refining strategic plans, developing budgets, and developing staffing requirements.

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

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

Technology

Post Assessment Workshop (CYB-WKSPOSTASMT)	
TA Delivery Method:	In Person Workshop and Virtual Meetings
Recommended Participants:	PSAP Managers or LMR System Owners

Offering Overview

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

The workshop will begin with a review of the findings from an assessment completed within the last calendar year. The facilitator will guide the state, territory, tribal nation, region, county, or urban area through the process of prioritizing the recommendations from the assessment to develop potential improvement plans. The session will conclude with development of a multi-year improvement roadmap, sharing of common continuous improvement program measures, and delivery of repeatable self-assessment processes to measure progress.

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

Technology

Alerts and Warnings (ALERTS)	
TA Delivery Method:	In-Person Workshop or Webinar (half day)
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 Warnings 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/webinar provides stakeholders an awareness of the alerts and warning systems available to local, state, federal, tribal, and territorial authorities; to include an overview of FEMA's 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

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

Offering Overview

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

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

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

Customized support for this offering may vary to meet 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[13]	
TA Delivery Method:	In-Person Exercise
Recommended Communications Unit Trainees:	COML, COMT, INCM, INTD, and RADO Trainees

Offering Overview

The COMMEX is a follow-on to the COML, COMT, INCM, INTD, and RADO training courses.[14] It provides an opportunity for COML, COMT, INCM, INTD, and RADO trainees to demonstrate proficiency and complete requirements in the respective Position Task Books (PTB).

Public safety professionals who have completed a COML, COMT, INCM, INTD, or RADO course must complete a series of competency tasks in their PTB as the next step in becoming a certified COML, COMT, INCM, INTD, or RADO 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.

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

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

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

[13] This exercise is structured under HSEEP guidelines.

[14] Participants must have successfully completed the appropriate Communications Unit training.

Training & Exercises

Communications-Focused Exercises (TTX, FE, FSE)[15]	
TA Delivery Method:	Facilitated In-Person and Virtual Exercise
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) (In-person/Virtual)
- Functional Exercises (FE) (In-person)
- Full Scale Exercises (FSE) (In-person)

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 **(can be in-person or virtual)**
- Logistics checklist
- Exercise Plan (EXPLAN)
- Master Scenario Events List (MSEL)
- After Action Report/Improvement Plan (AAR/IP)

[15] 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 (MCU), communications support equipment, audio gateways, digital network communications equipment, and unique modes of communication such as High Frequency (HF), satellite, air-to-ground and marine communications. Drills may consist of actual and/or simulated activities, which can be customized to meet the specific requirements of the requesting site/entity.

Participants will be presented with tasks at individual stations and asked to provide technical solutions to address specific incident needs or challenges. Participants will also be required to resolve communications-related issues and problems that arise during the drill.

A typical venue to conduct communications drills would be in conjunction with events such as an MCU "rodeo" or "rally" during which multiple vehicles and teams assemble from across a region or state. MCU events offer participating agencies an opportunity to test their voice and data equipment and capabilities and to learn more about resources within their region or state. The drills can potentially involve all 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 awareness
- Multi-agency/jurisdiction communications interoperability
- Public safety response level emergency communication
- Planning meetings **(can be in-person or virtual)**

Training & Exercises

Communications-Focused Exercise Design and Planning (EXDESIGN)	
TA Delivery Method:	In-Person or Virtual Workshop
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)
- Planning meetings **(can be in-person or virtual)**

Training & Exercises

Communications Unit Leader (COML) Training Course	
TA Delivery Method:	Four-Day In-Person Course or Five-Day Virtual Course (Refer to "Virtual TA Service Offerings" at the beginning of this Guide)
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 National Incident Management System (NIMS) ICS and to provide hands-on activities 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. [16]

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 materials and the COML Position Task Book will be provided to students via digital download prior to the course start date.

Course Capacity:

- **In-person**: minimum of 15 up to a maximum of 30 vetted/qualified students
- **Virtual:** maximum of 15 vetted/qualified students (more information will be made available during the scoping call)

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

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

(Continued on next page)

[16] For any training courses (COML, COML TtT, ITSL, COMT, AUXCOMM, AUXCOMM 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 course registrar to review and vet/approve each student's prerequisite documentation for sufficiency and inform the STO of the students' names.
  - Issue the Coupon Code and Online Application Process Job Aid to qualified students.
  - Obtain the STO's endorsement on each student's electronic application via FEMA's online registration process.
  - Submit a completed student verification form to CISA at least 14 days prior to the course.
- **CISA actions:**
  - Submit a "Request to Conduct NIMS ICS Training Class" form to FEMA/EMI at least 45 days before the requested course start date to register the course in the FEMA EMI database.
  - Make arrangements for the submission of the COML Course Completion Package to FEMA EMI within 10 days after the course.

Training & Exercises

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

Offering Overview

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

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

The course is instructor-led and supports learning through discussion, lecture, and hands-on exercises to explain processes used for establishment and operation of the technical communications resources for an incident or planned event. The course is five-days and provides a realistic, hands-on approach to mastering the tasks and skills of a COMT. Course materials and the COMT Position Task Book will be provided to attendees via digital download prior to the course start date.

This course is taught by CISA instructors who have both practitioner and Communications Unit experience. Prior to the on-site course, 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.

Course Capacity:

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

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

- **Personal experience:**
  - A public safety background with experience in field operations
  - A technical communications background
  - Awareness of fundamental public safety communications technology
  - Basic knowledge of applicable communications plans
- **Completion of the following online courses from the FEMA EMI website:**
  - IS-100: Introduction to the Incident Command System, ICS 100
  - IS-200: Basic Incident Command System for Initial Response
  - 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 point of contact [POC]) action:**
  - Review and vet/approve the prerequisite documentation for sufficiency.
  - Submit a completed student verification form to CISA at least 14 days prior to the course.

Training & Exercises

Incident Tactical Dispatcher (INTD) Training Course	
TA Delivery Method:	Four-Day In-Person Course or Five-Day Virtual Course (Refer to "Virtual TA Service Offerings" at the beginning of this Guide)
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. Each attendee participates with hands-on training activities and in an exercise on the final day of the course. Course materials and the INTD Position Task Book will be provided to attendees via digital download prior to the course start date.

Course Capacity:

- **In-person:** minimum of 10 up to a maximum of 20 vetted/qualified students
- **Virtual:** maximum of 16 vetted/qualified students (additional information will be provided during the scoping call)

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

Personal experience:

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

Course Registration Process:

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

Training & Exercises

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

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 National Integration Center (NIC) and other organizations focused on public safety communications to establish the best way to integrate the ITSL into the ICS. 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, 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 (IT). 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. Course materials and the ITSL Position Task Book will be provided to attendees via digital download prior to the course start date.

There must be a minimum of 10 up to 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 ICS-300: Intermediate Incident Command System for Expanding Incidents**
- **Additional recommended (not required) training:**
  - ICS-400: Advanced Incident Command System for Complex Incidents

Course Registration Process:

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

Training & Exercises

Incident Communications Center Manager (INCM) Training Course	
TA Delivery Method:	Three-Day In-Person Course or Four-Day Virtual Course (Refer to "Virtual TA Service Offerings" at the beginning of this Guide)
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. Course materials and the INCM Position Task Book will be provided to attendees via digital download prior to the course start date.

Course Capacity:

- **In-person:** minimum of 10 up to a maximum of 20 vetted/qualified students
- **Virtual:** maximum of 15 vetted/qualified students (additional information will be provided during the scoping call)

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

- **Personal experience:**
  - Awareness of fundamental public safety communications technology
- **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 (not required) training:**
  - ICS-300: Intermediate Incident Command System for Expanding Incidents

Course Registration Process:

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

Training & Exercises

All-Hazards Incident Communications Awareness Overview (TRG-COMUAWR)	
TA Delivery Method:	In-Person Workshop or Webinar (half day briefing)
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, Auxiliary Communicator (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 is an awareness session only, no course completion certificate or position task book will be issued.

Recommended for Attendance:

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

Recommend (not required) completion of the following training:

- 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
- ICS-300: Intermediate ICS for Expanding Incidents

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

All-Hazards Incident Communications Center Manager (INCM)/Incident Tactical Dispatcher (INTD) Awareness Overview (TRG-OVERVW)	
TA Delivery Method:	In-Person Workshop or Virtual (half day briefing)
Recommended Participants:	Command & General 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 National Special Security Event (NSSE)/Special Event Assessment Rating (SEAR)). For some incidents, the COML establishes an Incident Communications Center (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 Command and General Staff, Communication Unit Leaders, dispatch supervisors and public safety communication professionals for managing all functions in an ICC. This overview is particularly useful for those staff that are preparing for a large planned event, such as an NSSE or SEAR. This awareness session provides a refresher of INCM/INTD courses as well as awareness and lessons learned regarding ICC operations during an NSSE/SEAR. This three 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 (not required) 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

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 familiar with the Incident Command System

Offering Overview

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

Course Capacity:

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

Prerequisites for Attendance: ***(prerequisites must be verified by the state 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-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 (not required) training:**
  - ICS-300: Intermediate Incident Command System for Expanding Incidents

Course Registration Process:

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

Training & Exercises

Auxiliary Communications (AUXCOMM) Training Course	
TA Delivery Method:	Two to Three-Day In-Person Course or Three-Day Virtual Course (Refer to "Virtual TA Service Offerings" at the beginning of this Guide)
Recommended Participants:	Licensed Amateur Radio Operators

Offering Overview

This course is designed for auxiliary communicators who volunteer to provide backup emergency communications support to "public safety" agencies. Volunteer communications operators/groups, using amateur radio, and other communications platforms, have been providing emergency backup communications to the public safety sector for over 100 years. Event planners, public safety officials, and emergency managers at all levels of government utilize their services. Often, AUXCOMM services have been used when other forms of communications have failed or have been significatly disrupted. Today, nearly every state/territory has incorporated some level of participation by AUXCOMM personnel into their TICPs and SCIPs.

This course focuses on auxiliary communications interoperability, the relationship between the COML and 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 materials and the AUXC Position Task Book will be provided to students via digital download prior to the course start date.

Course Capacity:

- **In-person:** minimum of 15 up to a maximum of 30 vetted/qualified students
- **Virtual:** maximum of 15 vetted/qualified students (additional information will be provided during the scoping call)

Prerequisites for Attendance: ***(prerequisites must be verified by the state two weeks in advance of a 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 (not required) training:**
  - ICS-300: Intermediate Incident Command System for Expanding Incidents

Course Registration Process:

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

Training & Exercises

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

Offering Overview

This service offering helps states/territories create a self-sustaining AUXCOMM training program by providing instructor training to individuals who have completed the CISA AUXCOMM course, and the 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 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 course.

The AUXCOMM TtT course should be completed by personnel with a volunteer communicator affiliation with a public safety agency and are interested in teaching the AUXCOMM 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.

Course Capacity:

There must be a minimum of eight up to a maximum of 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.)
  - Federal or State Law Enforcement Instructor Certificate
  - 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 <u>most current version</u> 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:

- Copy of an active FCC amateur radio license, General Class or higher, valid for at least the past three years.
- CISA AUXCOMM course completion certificate.
- Signature page from the AUXC PTB dated within three years of initiating the PTB.
- SWIC or STO endorsement as a future AUXCOMM instructor in the state of residence.

Course Registration Process:

- **SWIC (or designated point of contact [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 or 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, submit a completed student verification form to the CISA Communications Unit Training Coordinator and set the course dates to start at least 35 days later. Provide the course dates and location to the CISA Communications Unit Training Coordinator.
- **CISA actions:**
  - Review and vet/approve the prerequisite documentation for sufficiency. (CISA has final approval for Train-the-Trainer course attendees.)
  - Provide course materials to attendees via digital download prior to the course.

Training & Exercises

Communications Unit Leader Train-the-Trainer (COML TtT) Course	
TA Delivery Method:	Four-Day In-Person Course or Five-Day Virtual Course (Refer to "Virtual TA Service Offerings" at the beginning of this Guide)
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 COML PTB. This course helps attendees develop essential core competencies required for teaching the COML course within 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 up to a maximum of 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.)
  - Federal or State Law Enforcement Instructor Certificate
  - 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 <u>most current version</u> 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:

- 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 or STO endorsement as a future COML instructor in the state of residence

(Continued on next page)

Training & Exercises

Course Registration Process:

- **SWIC (or designated point of contact [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 or 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 course registrar to review and vet/approve each student's prerequisite documentation for sufficiency and inform the STO of the students' names.
  - Issue the Coupon Code and Online Application Process Job Aid to qualified students.
  - Obtain the STO's endorsement on each student's electronic application via FEMA's online registration process.
  - Submit a completed student verification form to CISA at least 14 days prior to the course.
- **CISA actions:**
  - Submit a "Request to Conduct NIMS ICS Training Class" form to FEMA/EMI at least 45 days before the requested course start date to register the course in the FEMA EMI database.
  - Review and vet/approve the prerequisite documentation for sufficiency. (CISA has final approval for Train-the-Trainer course attendees.)
  - Provide the course materials to attendees via digital download prior to the course.
  - Submit the COML TtT Course Completion Package to FEMA EMI within 10 days after the course.

Training & Exercises

Communications Technician Train-the-Trainer (COMT TtT) 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 COMT 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 or up to a maximum of 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.)
  - Federal or State Law Enforcement Instructor Certificate
  - 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 <u>most current version</u> 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 <u>most current version</u> 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 or STO endorsement as a future COMT instructor in the state of residence

(Continued on next page)

Training & Exercises

Course Registration Process:

- **SWIC (or designated point of contact [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 or 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 35 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 course.
- **CISA actions:**
  - Review and vet/approve the prerequisite documentation for sufficiency. (CISA has final approval for Train-the-Trainer course attendees.)
  - Provide the course materials to attendees via digital download prior to the course.

Training & Exercises

CISA's Communications Unit State-Sponsored Instructor Program (SS-COMT, SS-COML, SS-AUXCOMM, SS-INCM, SS-INTD, SS-RADO)	
TA Delivery Method:	In-Person Course
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, INTD, INCM, RADO 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, INTDs, INCMs, RADOs and 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 or FEMA COML TtT course, and be designated as a state recognized instructor for their respective state.
- **For COMT, INCM, INTD and RADO instructors:** An individual must have completed the basic course they want to teach, have completed the corresponding Position Task Book, meet all current requirements to attend any one of the CISA TtT courses, must have completed any one of the CISA TtT courses, and be designated as a state recognized instructor for their respective state.
- **For AUXCOMM instructors:** An individual must have completed the AUXCOMM course, have completed the AUXC Position Task Book, meet all current requirements to attend any one of the CISA TtT courses, must have completed any one of the CISA TtT courses, been a licensed amateur radio operator at the general class or higher level for at least three years, 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 either the SWIC or the STO have endorsed in writing the individual as an instructor of Communications Unit course(s) in their state of residence. States may add to the above list of requirements to attain state instructor designation. The requirement to continue to meet all current requirements to attend a CISA 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:**
  - The STO or the SWIC must recommend to CISA a minimum of two 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, as the final vetting authority, at least 30 days in advance of any COMT, INCM, INTD, RADO or AUXCOMM course and at least 60 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 Communications Unit 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, INCM, INTD, RADO or AUXCOMM 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
  - Identification of a state representative to 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 (e.g., student prerequisite validation, attendee sign-in sheets, typed class rosters, student evaluations, event report, etc.) and processes follow CISA course guidelines.
  - Teach the state-sponsored COML, COMT, INCM, INTD, RADO or AUXCOMM course without any changes, or deletions to the CISA core curriculum.
  - Send a copy of all student sign-in sheets, the typed class roster, student course evaluations and event 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 Technical Assistance (TA) Evaluation Form is completed and returned to CISA.
- **CISA actions:**
  - Maintain a file copy of all certifications/qualifications of CISA-recognized instructors.
  - Schedule and lead a scoping call with the requesting individual, and the instructors involved.
  - Ship printed course materials to the state-requested public safety agency and provide electronic downloadable course materials to each registered student 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, event report, and the student evaluations for COMT, INCM, INTD, RADO, 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 audio gateways (i.e., audio bridge) functionality and operations. Participation in all three modules trains state/territory, tribal, regional, or urban area communications personnel on how to activate and deactivate various gateway devices.

There is a minimum of 5 or a maximum of 10 students identified for the gateway hands-on configuration module in order for CISA to schedule and conduct the course.

Training Modules:

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

Training & Exercises

Resilient Communications Awareness Training Webinar (RESCOM-AWR)	
TA Delivery Method:	Webinar
Recommended Participants:	Emergency Response Personnel to include fire, emergency medical services (EMS), law enforcement, emergency management, and telecommunications personnel

Offering Overview

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

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

There must be a minimum of 10 registered participants two weeks in advance of the offering in order for CISA to conduct the webinar.

Prerequisites for Attendance:

- None

Course Registration Process:

- **SWIC (or designated point of contact [POC]) action:**
  - Review and approve the attendees

Training & Exercises

Resilient Communications Incident Communications Management Training Course (RESCOM-MGT)	
TA Delivery Method:	In-Person Course
Recommended Participants:	Communications Unit personnel including COML, COMT Public safety agency communications technical personnel

Offering Overview

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

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

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

Prerequisites for Attendance:

- **Required:**
  - Familiarity developing incident communications plans
  - Demonstrated experience deploying and troubleshooting LMR communications in support of an incident
  - Understanding of RF concepts including propagation, interference, attenuation, etc.
- **Recommended:**
  - L0969 – All-Hazards Communications Unit Leader (COML)
  - All-Hazards Communications Technician (COMT)

Course Registration Process:

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

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 [17]

[17] 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
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 Federal Information Security Management Act (FISMA) compliant with an authority to operate on the DHS secure network. DHS has committed to CASM long term as an officially recognized level 3 system under formal Chief Information Officer management. CASM maintains data about public safety agencies and their radio communications equipment across all public safety disciplines and levels of government. As shared by agencies, CASM provides a standardized nation-wide view of agencies, fixed and mobile assets, personnel, and spectrum usage information, as well as coverage plots for radio base stations.

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

Customized support for this offering may vary to meet 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 MCU capabilities and Deployability
  - maintain information about mobile assets (caches, gateways, etc.)
  - manage information access control including delegation of privileges
  - generate coverage plots
- On-site assistance with data entry and validation supporting any of the above

Usage

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

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 state, local, tribal, and territorial (SLTT) 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 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 Memorandum of Agreements (MOAs) or Memorandum of Understanding (MOUs) that are necessary for implementation
- Reviewing on-going system maintenance and database upkeep requirements
- Working with governmental and non-governmental radio shops in the application of encryption programs
- Equipment, encryption basic use analysis
- Encryption system SOP template and full plan assessment and development (minimum equipment for subscriber units and rules of use)

Usage

Priority Telecommunications Services (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 when cellular networks are congested and the probability of completing a normal cellular call is reduced.

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

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

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

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

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

Appendix A: SAFECOM Resources

SAFECOM Website Resources

SAFECOM's mission is to improve designated emergency response providers' inter-jurisdictional and inter-disciplinary emergency communications interoperability through collaboration with emergency responders across state, local, tribal, and territorial governments (SLTT), and international borders. [18]

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 Technical Assistance (TA) Request Form for SWICs' use and the TA Evaluation Form for stakeholders' feedback are posted with instructions for their completion here: cisa.gov/safecom/ictapscip-resources.

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

Appendix B: 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/safecom/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 workshop please check the box above and insert the desired target date(s) for the workshop in the space provided	From: ____ To: ____

Appendix B: 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

Examples of CISA Technical Assistance (TA) Service Offerings Include:	
✓ Statewide Communication Interoperability Plan (SCIP) Workshop ✓ Tactical Interoperable Communications Field Operations Guide (TIC-FOG) ✓ Standard Operating Procedures (SOP) Development ✓ Priority Telecommunications Services (GETS, WPS, TSP) ✓ Communications Unit Planning and Policy Development	✓ Communication Assets Survey and Mapping (CASM) Tool ✓ Communications Unit Planning and Policy ✓ Alerts and Warnings ✓ Cybersecurity Awareness and Assessment ✓ One-Day Cyber Awareness Workshop ✓ Rapid Cyber Assessment ✓ NIMS ICS Communications Unit Personnel Training ✓ Next Generation 9-1-1/Strategic Planning Support

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

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

CONTINUATION SHEET – TA REQUEST

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

Appendix C: Additional TA Resources

National Interoperability Field Operations Guide (NIFOG) 2.01

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

To view and download the PDF version, please visit 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 Events (NSSE)/Special Event Assessment Rating (SEAR) Communications Planning Toolkit

The Cybersecurity and Infrastructure Security Agency (CISA) has released an updated version of the National Special Security Events (NSSE)/Special Event Assessment Rating (SEAR) Communications Planning Toolkit. This toolkit includes the updated National Incident Management System (NIMS)/Incident Command System (ICS) structure and a standardized approach to the command, control, and coordination for event management. Planning considerations for cybersecurity and information technology have been added to Version 2.0.

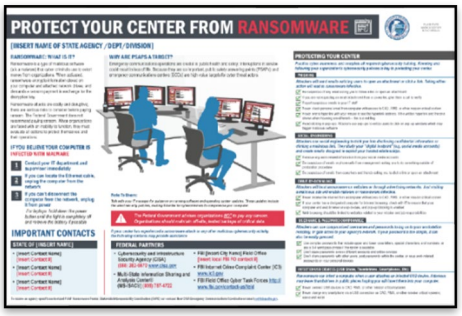
CISA has continued to provide communications planning support to the state, local, and federal jurisdictions managing communications for NSSEs such as the Super Bowl and political conventions. This toolkit, which leverages best practices from those events, has been written as a resource guide for state,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

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

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

Appendix C: Additional TA Resources

Cybersecurity PSAP Ransomware Poster



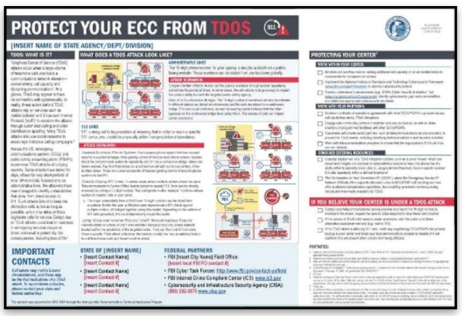
The ransomware poster can be placed in an Emergency Communications Center/Public Safety Answering Point (PSAP), 9-1-1 Call or Dispatch Centers. The poster provides information about what ECC staff can do to reduce the risk of ransomware. Although the poster's focus is on ransomware, its recommendations 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 posterrequests@commscollabcenter.com.

SWICs, state, local, territory, and tribal points of contact may request up to 2 printed 20"x 30" copies of the poster and an 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.

Cybersecurity Telephony Denial of Service (TDoS) Poster



The TDoS poster can be placed in an Emergency Communications Center/Public Safety Answering Point (PSAP), 9-1-1 Call or Dispatch Centers. The poster provides information about what ECC staff can do to reduce the risk of TDoS attacks. The poster reviews TDoS attack vectors and provides examples of TDoS attacks targeting administrative and 911 lines, specific best practices and recommendations on how to mitigate TDoS attacks, and contact information for federal partners and customizable space for additional resources. To request an agency or state-specific poster, Statewide Interoperability Coordinators (SWICs) may contact their CISA Emergency Communications Coordinator and/or email the request to posterrequests@commscollabcenter.com.

SWICs, state, local, territory, and tribal points of contact may request up to 2 printed 20" x 30" copies of the poster and an electronic file will be provided for printing additional copies.

To view, download and request printed copies of the TDoS please visit this site:

cisa.gov/publication/next-generation-911.

Appendix D: Acronyms

Acronym	Definition
AAR/IP	After Action Report/Improvement Plan
AG	Audio Gateway
ASAP	Automated Security Alarm Protocol
AUXC	Auxiliary Communicator
AUXCOMM	Auxiliary Communications
AUXCOMM TtT	Auxiliary Communications Train-the-Trainer
AUXFOG	Auxiliary Communications Field Operations Guide
BRBND	Broadband
BRBNDLTE	Broadband Strategic Planning Support and Education
BRBEVNTASMT	Mobile and Fixed Site Data Use Assessment for Incidents and Planned Events
BRBDATA	Broadband Technologies and Data Operability/Interoperability in Support of Public Safety
CAD	Computer-Aided Dispatch
CASM	Communication Assets Survey and Mapping
CISA	Cybersecurity and Infrastructure Security Agency
COG	Continuity of Government
COML	Communications Unit Leader
COML TtT	Communications Unit Leader Train-the-Trainer
COMMDRILL	Communications Drill
COMMEX	Communications Exercise
COMMS-ASI	Communications During Active Shooter Incidents
COMT	Communications Technician
COMUAWR	All-Hazards Incident Communications Unit Awareness
COMUPLAN	Communications Unit Planning and Policies
COOP	Continuity of Operations Plan
CSA	Cybersecurity Advisor
CSD	Cybersecurity Division
CYBR	Cyber
CYB-ASMTFULL	Full Cyber Assessment
CYB-ASMTRAPID	Rapid Cyber Assessment
CYB-WKSPOSTASMT	Post Assessment Workshop
CYB-WKSTHRTASMTRSP	Threat Assessment and Response Workshop
CYB-WKSTHRTAWR	Cyber Threat Awareness Workshop
DHS	U.S. Department of Homeland Security
EAS	Emergency Alert System
ECC	Emergency Communications Coordinator
ECC	Emergency Communications Center
ECD	Emergency Communications Division

Appendix D: Acronyms

Acronym	Definition
eAUXFOG	Electronic Auxiliary Communications Field Operations Guide
eFOG	Electronic Field Operations Guide
eNIFOG	Electronic National Interoperability Field Operations Guide
EMAC	Emergency Management Assistance Compact
EMI	Emergency Management Institute
EMS	Emergency Medical Services
ENCRYPT	Encryption
EOC	Emergency Operations Center
ESF	Emergency Support Function
EXDESIGN	Exercise Design
EXPLAN	Exercise Plan
FE	Functional Exercise
FCC	Federal Communications Commission
FEMA EMI	Federal Emergency Management Agency Emergency Management Institute
FEMA NIC	Federal Emergency Management Agency National Integration Center
FirstNet	First Responder Network Authority
FISMA	Federal Information Security Management Act
FOG	Field Operations Guide
FSE	Full Scale Exercise
GETS	Government Emergency Telecommunications Service
GIS	Geographic Information System
GOV-DOC	Governance Document
HF	High Frequency
HSGP	Homeland Security Grant Program
HSEEP	Homeland Security Exercise and Evaluation Program
ICC	Incident Command Center
ICS	Incident Command System
ICTAP	Interoperable Communications Technical Assistance Program
IP	Improvement Plan
IPAWS	Integrated Public Alert and Warning Systems
INCM	Incident Communications Center Manager
INTD	Incident Tactical Dispatcher
IT	Information Technology
ITSL	Information Technology Service Unit Leader
LMR	Land Mobile Radio
LTE	Long Term Evolution
MASS	Mutual Aid Support System
MEP	Master Exercise Practitioner
MCI	Mass Casualty Incident
MCU	Mobile Communications Unit

Appendix D: Acronyms

Acronym	Definition
MHz	Megahertz
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MRP	Mission Ready Package
MSEL	Master Scenario Events List
NCSWIC	National Council of Statewide Interoperability Coordinators
NECP	National Emergency Communications Plan
NG9-1-1	Next Generation 9-1-1
NIFOG	National Interoperability Field Operations Guide
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NSSE	National Special Security Events
OP-ASMT	Operational Assessment
OP-SPEV	Special Event Planning
PAR	Priority Telecommunications Services Area Representative
PACE	Primary, Alternate, Contingency, and Emergency
POC	Point of Contact
PSA	Protective Security Advisor
PSAP	Public Safety Answering Point
PTB	Position Task Book
PTS	Priority Telecommunications Services
QRB	Qualifications Review Board
RADO	Radio Operator
RCES	Regional Communications Enhancement Support
RECCWG	Regional Emergency Communications Coordination Working Group
RESCOM-AWR	Resilient Communications Awareness Training Webinar
RESCOM-MGT	Resilient Communications Incident Communications Management
RF	Radio Frequency
RMS	Records Management System
SAP	Security Assessment Plan
SAR	Security Assessment Report
SCMP	Strategic Communications Migration Plan
SCIP	Statewide Communication Interoperability Plan
SEAR	Special Event Assessment Rating
SIEC	State Interoperability Executive Committee
SIGB	Statewide Interoperability Governance Board
SLTT	State, Local, Tribal, and Territorial
SME	Subject Matter Expert
SOG	Standard Operating Guidelines
SOP	Standard Operating Procedure

Appendix D: Acronyms

Acronym	Definition
SP	Special Publication
SPEV	Special Event
SS-AUXCOMM	State-Sponsored Auxiliary Communications Course
SS-COML	State-Sponsored Communications Unit Leader Course
SS-COMT	State-Sponsored Communications Technician Course
STO	State Training Officer
STRATPLAN	Strategic Planning
SWIC	Statewide Interoperability Coordinator
TA	Technical Assistance
TDoS	Telephony Denial of Service
TERT	Telecommunicator Emergency Response Taskforce
THSGP	Tribal Homeland Security Grant Program
TICFOG	Tactical Interoperable Communications Field Operations Guide
TICP	Tactical Interoperable Communications Plan
TSCIP	Tribal Strategic Communication Interoperability Plan
TSP	Telecommunications Service Priority
TtT	Train-the-Trainer
TTX	Tabletop Exercise
UASI	Urban Area Security Initiative
UHF	Ultra-High Frequency
VHF	Very High Frequency
VoIP	Voice over Internet Protocol
WEA	Wireless Emergency Alerts
WPS	Wireless Priority Service