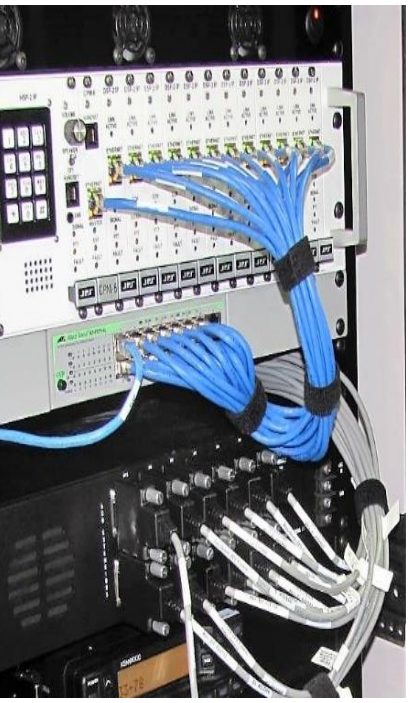
CISA
CYBER+INFRASTRUCTURE



EMERGENCY COMMUNICATIONS TECHNICAL ASSISTANCE AND PLANNING GUIDE

FY2020 Highlights and Offerings

TA/SCIP Guide Version 5.1

OCTOBER 2019

Cybersecurity and Infrastructure Security Agency

Table of Contents

Foreword

The Cybersecurity and Infrastructure Security Agency (CISA) is pleased to publish the FY2020 Emergency Communications Technical Assistance (TA) / Statewide Communication Interoperability Plan (SCIP) Guide. This year's Guide includes a number of new or enhanced offerings to help public safety and government officials meet the challenges in the rapidly changing ecosystem of voice and data interoperable communications.

The release of this Guide also coincides with the release of the 2019 update to the National Emergency Communications Plan (NECP).The 2019 NECP puts forth a vision for strengthening and enhancing emergency communications capabilities nationwide and a strategic plan for driving towards interoperability in this evolving emergency communications ecosystem. The NECP establishes six strategic goals focused on the following: Governance and Leadership; Planning and Procedures; Training, Exercises, and Evaluation; Communications Coordination; Technology and Infrastructure; and Cybersecurity.

During FY2020, CISA will continue to expand and, if needed, customize service offerings with a focus on supporting states and territories to address the following:

- Coordinated statewide governance (e.g. State Mapping Tool, Interoperable Communications Reference Guides, etc.)
- Comprehensive emergency communications planning (e.g. SCIPs, Tactical Interoperable Communications Plan [TICPs], and Field Operations Guides [FOGs])
- Next Generation 9-1-1 (NG9-1-1) planning and implementation
- Data operability and interoperability
- Alerts and warnings
- Broadband deployment
- Cybersecurity education and awareness
- Communications unit planning and procedures

CISA Emergency Communications TA offerings support all 56 states and territories and federally recognized Tribal Nations in helping solve a variety of communications interoperability issues, keeping up to date with new technologies, and enhancing governance policies and the management of Communications Unit (COMU) resources. In addition, while integrating public safety communications with the Nationwide Public Safety Broadband Network (NPSBN) is underway, sustaining mission critical voice communications capabilities for public safety also remains a critical challenge.

CISA Emergency Communications Sector Coordinators are available to answer questions about this Guide and CISA services. CISA looks forward to supporting public safety stakeholders this year and in the future.

Best Regards,

Vincent D. DeLaurentis
Acting Assistant Director for Emergency Communications
Cybersecurity and Infrastructure Security Agency

CISA Technical Assistance

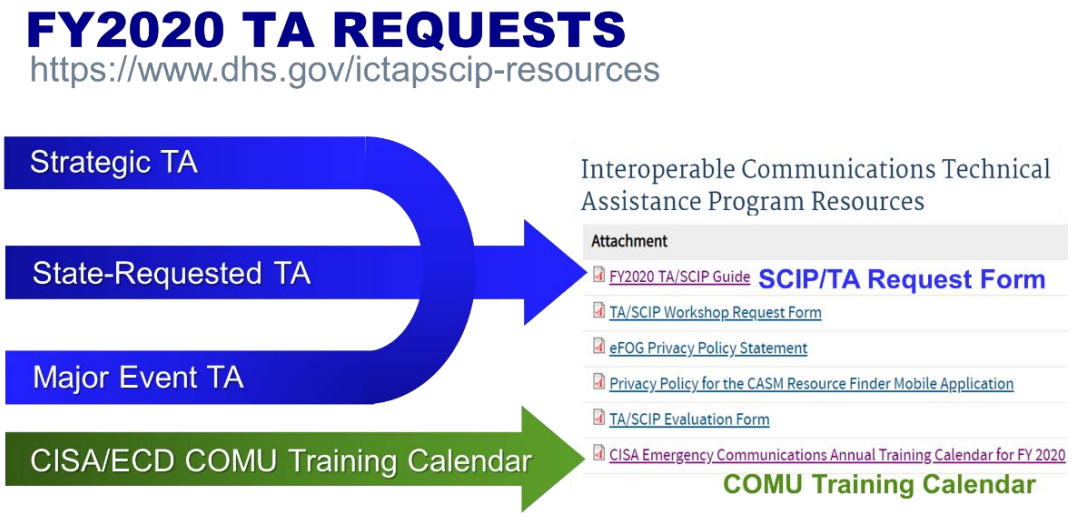
TA Request Process

CISA provides a portfolio of no-cost technical assistance services and will prioritize supporting strategic initiatives through efforts such as the National Governors Association (NGA) workshop goals and State Interoperability Markers. In 2018, CISA and the NGA partnered to conduct governance workshops across the nation that supported each state/territory in collaborating to identify goals to address challenges related to governance. Additionally, in 2019 CISA supported states and territories in establishing an interoperability baseline assessment by measuring progress against 25 markers. These markers describe a state or territory's level of interoperability "health".

New TA Approach: Requests for assistance are coordinated through the SWIC from each state and territory. This year there are three different categories of TAs:

- **Strategic**: Support that can be leveraged to directly support the implementation of the 2019 NECP, most recent SCIP, NGA workshop goals, and/or State Interoperability Markers
- **State-Requested**: Support for the state or territory's normal, day-to-day operations and activities related to emergency communications
- **Major Event Support**: Support for planned and unplanned events that are designated as National Special Security Event (NSSE)/Special Event Assessment Rating (SEAR), or are the result of a natural or manmade disaster

CISA COMU Training Calendar: The COMU Training Calendar was established as an alternative to individual TA requests for COMU courses. The calendar includes pre-planned, regional COMU courses that are being offered and open to any state/territory to send students. Space is on a first come, first served basis. A complete list of all available, CISA-delivered COMU courses and how to register for a course is available at https://www.dhs.gov/publication/ictapscip-resources.



TA Request Form: To request TA, the SWIC or other designated state/territory point of contact completes the fillable TA/SCIP request form on the SAFECOM website: https://www.dhs.gov/ictapscip-resources. The form should indicate which TAs the state/territory is requesting and if it is strategic, which goal or objective it aligns too. The "Continuation Sheet" can be used to provide additional details. Once completed, the form can be submitted by clicking the "Submit" bottom at the bottom or by scanning pages 3-5 and emailing it to TARequest@cisa.dhs.gov.

New and Updated for FY2020: CISA Technical Assistance Offerings

In FY2020, CISA will provide an opportunity for all 56 states and territories to receive TA services at no cost. In preparation for the request process, this Guide lists available TA service offerings. The process for SWICs to request TA services has been updated and is described on page 2. CISA TA services are also available for all federally recognized Tribal Nations. Tribal representatives may submit TA requests via the fillable TA request form on the SAFECOM website (https://www.dhs.gov/publication/ictapscip-resources) and emailed to TARequest@cisa.dhs.gov.

The following highlights our new or updated FY2020 TA offerings:

9-1-1/PSAP Cyber Awareness

The critical nature of 9-1-1/PSAP functions (including computer aided dispatch and LMR) means cyberattacks could result in large-scale impact, making them a high-value target to those looking to disrupt public safety services, extort local governments, or simply create mischief. The 9-1-1 PSAP & Land Mobile Radio Cybersecurity Awareness Webinar also provides basic best practices to improve the secure use of emergency communications technologies in day-to-day operations.
(***For a more detailed description see pg. 19)***

Broadband Technologies and Data Operability/Interoperability in Support of Public Safety

This service offering assists public safety professionals in identifying communication specific requirements associated with the selection and implementation of broadband related technologies into the public safety architecture. 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 seminar runs for one full day and will include lecture material and break-out work groups.
(For a more detailed description see pg. 17)

Communications Unit Leader Train-the-Trainer

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 Position Task Book (PTB). This course helps attendees develop essential core competencies required for teaching the COML course in their own state.
(***For a more detailed description see pg. 37-38)***

Electronic Tactical Interoperable Communications Field Operations Guide Development

This service offering enables emergency communicators to access Field Operations Guide (FOG) information from their mobile devices without an internet connection. CISA works closely with the State to transform their existing FOG Word document into a mobile app available for download from both the Apple Store and Google Play.
(***For a more detailed description see pg. 14)***

CISA Technical Assistance

Encryption Planning and Usage

Understanding the technical aspects of encryption can be very complex and confusing. Whether it's a single community, regional, statewide or an intrastate issue, laying a solid foundation for the use of encryption is essential to developing an interoperable, successful and lasting encryption program.
(***For a more detailed description see pg. 47)***

Grant Funding for Emergency Communications

Public safety agencies should consider all available funding sources, including traditional grants to help fund initial capital investments or improvements to communications systems, as well as other sources of funding that may partially fund emergency communications projects. CISA, in coordination with SAFECOM and the National Council of Statewide Interoperability Coordinators, publishes numerous resources for state, local, tribal, and territorial governments and their public safety agencies to identify funding mechanisms and plan for emergency communications projects.
(***For a more detailed description see pg. 10)***

Information Technology Service Unit Leader

In 2018 and 2019, ICTAP introduced the Information Technology Service Unit Leader (ITSL) course, and SAFECOM/NCSWIC have coordinated with FEMA NIC and other organizations focused on public safety communications to establish the best way to integrate the ITSL into the ICS. The ITSL is needed to provide information management, cybersecurity, and application management for the many critical incident/event related functions, to include: Incident / Unified Command Post, Incident Communications Centers, and various tactical operations centers, joint information center (JIC), staging areas, and field locations.
(***For a more detailed description see pg. 30-31)***

LMR/LTE Coverage Testing

ICTAP's LMR/LTE coverage testing and analysis provides real-world data from wireless RF and cellular networks for indoor and outdoor coverage. This offering can be customized for socio/demographic heat maps to provide a GIS overlay to coverage data.
(***For a more detailed description see pg. 21)***

Next Generation 9-1-1/Strategic Planning Support

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.
(***For a more detailed description see pg. 18)***

Statewide Communication Interoperability Plan Workshop

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.
(***For a more detailed description see pg. 6)***

CISA Sector Chiefs & Coordinators

CISA's Emergency Communications Sector Chiefs and Coordinators 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 Emergency Communications Coordinators assigned to each Sector.

Eastern Sector (Regions I, II, III)

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

- **Coordinator** – Bruce Belt Bruce.Belt@hq.dhs.gov
- **Coordinator** – Chris Tuttle Christopher.Tuttle@hq.dhs.gov
- **Coordinator** – Tom Gagnon Thomas.Gagnon@hq.dhs.gov

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

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

- **Coordinator** – Jim Jarvis James.Jarvis@hq.dhs.gov
- **Coordinator** – Jim Lundsted James.Lundsted@hq.dhs.gov
- **Coordinator** – Pam Montanari Pam.Montanari@hq.dhs.gov
- **Coordinator** – Colleen Wright colleen.wright@hq.dhs.gov

Western Sector (Regions VIII, IX, X)

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

- **Coordinator** – Artena Moon Artena.Moon@hq.dhs.gov
- **Coordinator** – Brandon Smith Brandon.Smith@hq.dhs.gov
- **Coordinator** – Bruce Richter Bruce.Richter@hq.dhs.gov
- **Coordinator** – Dan Hawkins Daniel.Hawkins@hq.dhs.gov
- **Coordinator** – Tom Lawless Thomas.Lawless@hq.dhs.gov

- **COMU Specialist** – Dan Wills Dan.Wills@hq.dhs.gov
- **COMU Specialist** – Robert Hugi Robert.Hugi@hq.dhs.gov

Governance

Statewide Communication Interoperability Plan (SCIP) Workshop	
Type of TA Offering:	Planning Meetings/Webinars/Facilitated Workshop
Stakeholders/Audience:	SIEC/SIGB Members; SWICs, State, Local, Federal, Tribal Stakeholders / Police, Fire and EMS Personnel, State 9-1-1Administrators, FirstNet Representatives, State Information/Technology Officers

Offering Overview

In 2016 CISA partnered with the NGA, to focus on enhancing interoperable communications governance. In 2018 NGA conducted four workshops attended by officials from 47 states and territories to assist in implementing the recommendations from 2016, resulting in specific goals. 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]

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

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

Planning for a SCIP workshop involves several pre-workshop planning calls, webinars, and stakeholder engagement. Appendix A describes the SCIP process in detail.

[1] Additional information regarding the HSGP is available here: https://www.fema.gov/homeland-security-grant-program.

Governance

Governance Documentation Review, Assessment, and Development (GOV-DOC)	
Type of TA Offering:	Workshop
Stakeholders/Audience:	SIEC/SIGB; SWICs, Executive, Statutory, and Legislative Personnel

Offering Overview

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

CISA assists requestors in 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, State Interoperability Executive Councils (SIECs), Statewide Interoperability Governance Boards (SIGBs)]; or assisting with the development of documentation (working group charters) for establishing governance bodies for communications-focused entities such as LMR systems, municipal agencies, and councils of government.

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

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

[2] The 2018 Emergency Communications Governance Guide for SLTT Officials is available here: https://www.dhs.gov/safecom/blog/2018/04/04/2018-sltt-governance-guide.

Governance

Communications Unit Planning and Policies (COMUPLAN)	
Type of TA Offering:	Workshop
Stakeholders/Audience:	SIEC/SIGB; SWICs, Executive, Statutory, and Legislative Personnel

Offering Overview

This workshop provides attendees with tools and best practices to develop a strategic plan to implement state/territory, local and regional level initiatives which improve policies and procedures for managing on-going development of Incident Command System (ICS) Communications Unit personnel and Communications Unit assets.

More than 13,000All Hazards ICS Communications Unit personnel have been trained and every state/territory now has a pool of COMLs, COMTs, and AUXCOMM.[3] Not every state has a program with policies and procedures to track, maintain and utilize ICS Communications Unit resources.

This offer is aimed at mid to senior level managers across all public safety disciplines to increase awareness and understanding of the Communications Unit functions and develop a strategic plan to improve utilization and management of Communications Unit personnel and equipment. The offering can be customized to fit a state's needs to also include tracking and managing other Communications Unit trainees.

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

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

[3] This figure reflects all the state sponsored Communications Unit trainings, drills, and exercises conducted between 2007 and 2017.

Governance

Communications Unit Assistance under Emergency Management Assistance Compact (EMAC)	
Type of TA Offering:	Type of TA Offering:
Stakeholders/Audience:	Stakeholders/Audience:

Offering Overview

This CISA course is designed to familiarize states/jurisdictions with EMAC, which is the Nation's preeminent state-to-state mutual aid system for facilitating the exchange of services, personnel, and equipment during incidents/emergencies.

EMAC is implemented through state Emergency Management Agencies (EMAs) and has been passed into law in all 50 states and four U.S. territories. However, EMAC is greatly under- utilized for deployment of Communications Unit resources due to a lack of awareness of the resources available and how to utilize the process.

This training provides states/jurisdictions an awareness of how EMAC functions; the process for requesting assistance to share resources within their state and with other EMAC members; how to handle similar requests for Communications Unit assets; the preparations required to ensure personnel resources are deployable under EMAC; and guidance on how to streamline the internal EMAC request process and expedite the procurement and deployment of communications resources.

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

- Overview of EMAC functions and benefits
- Information regarding in-state procedures/legislation
- Listing of participating in-state agencies and available resources
- Interstate agreements and resources
- Assistance with developing EMAC policies/procedures and building 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 Mission Ready Packages (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	
Type of TA Offering:	Webinar
Stakeholders/Audience:	SIEC/SIGB Members

Offering Overview

Public safety agencies should consider all available funding sources, including traditional grants to help fund initial capital investments or improvements to communications systems, as well as other sources of funding that may partially fund emergency communications projects. CISA, in coordination with SAFECOM and the National Council of Statewide Interoperability Coordinators, publishes numerous resources for state, local, tribal, and territorial governments and their public safety agencies to identify funding mechanisms and plan for emergency communications projects. This offering conducts a review of federal financial assistance opportunities, recommended activities during the grants lifecycle (e.g., pre-award, award, post award, and closeout), and resources to help agencies apply for and manage federal grants.[4]

This offering is applicable to states or localities with some or all of the following challenges:

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

This offering covers the following resources:

- *SAFECOM Guidance on Emergency Communications Grants* includes typical activities that can be funded through federal grants; best practices, policies, and technical standards that help improve interoperability; and resources to help agencies comply with grant requirements
- *List of Federal Financial Assistance Programs that Fund Emergency Communications* includes available grants, loans, and cooperative agreements that fund various emergency communications activities
- *Funding Mechanisms for Public Safety Communications Systems* provides an overview of various methods of funding emergency communications systems (e.g., bonds, special tax, surcharges), and specific examples of where these methods have been used to fund state and local systems
- *Land Mobile Radio Trio; Brochure; and Action Memorandum* provide stakeholders with basic information they can give to state and local decision-makers and elected officials on why it is important to fund and sustain public safety radio systems
- *2018 Emergency Communications System Lifecycle Planning Guide* and *Planning Tool* aid stakeholders in their efforts to fund, plan, procure, implement, support, and maintain public safety communications systems, and eventually to replace and dispose of system components
- *Interoperability Business Case: An Introduction to Ongoing Local Funding* advises the community on the elements needed to build a strong business case for funding interoperable communications

[4] Additional information regarding SAFECOM funding resources is available here: https://www.dhs.gov/safecom/funding.

Standard Operating Procedures

Standard Operating Procedures (SOP) / Standard Operating Guides (SOG) / Communications Plan Review and Development	
Type of TA Offering:	Assessment of SOPs and Communications Plans/Workshop
Stakeholders/Audience:	SWICs, Public Safety Stakeholders/ Mid-Senior Level Managers

Offering Overview

Standard Operating Procedures (SOPs) and Standard Operating Guides (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 SOPs/SOGs, various state/territory, urban area, regional, and/or tribal planning documents include specific communications components.

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

- Emergency Operations Plans (EOPs)
- Outdated Continuity of Government (COG) and Continuity of Operations (COOPs)
- Capabilities assessment planning
- Public Safety Communications Center (PSCC) operational plans
- Incident Communications Planning

Standard Operating Procedures

Tactical Interoperable Communication Plan (TICP) Development/ Implementation Workshop	
Type of TA Offering:	Review / Development Workshop / Data Collection
Stakeholders/Audience:	SWICs, Communications Unit Managers and Personnel

Offering Overview

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

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

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

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

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

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

Standard Operating Procedures

Tactical Interoperable Communications Field Operations Guide (TIC-FOG) Development	
Type of TA Offering:	Review / Development Workshop / Data Collection
Stakeholders/Audience:	SWICs, Communications Unit Managers and Personnel

Offering Overview

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

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

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

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

Standard Operating Procedures

Electronic Field Operations Guide (eFOG) Development	
Type of TA Offering:	Review / Development Workshop / Data Collection
Stakeholders/Audience:	SWICs, Communications Unit Managers and Personnel

Offering Overview

CISA offers public safety eFOG mobile apps through ICTAP. These radio frequency interoperability field guides are the go-to reference for emergency communications planning and for radio technicians responsible for radios that will be used during disaster response. The first step in developing an eFOG is that the state must have a current word version of their FOG that CISA can convert. This technical assistance delivers eFOG mobile apps for both Apple and Android mobile devices. The eNIFOG or eAUXFOG mobile apps can be downloaded from either app store as an example of eFOG capabilities. The process involves four distinct phases, each of which involves significant, though remote, interaction between CISA and the state:

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

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

- Quick electronic reference for regional channel and encryption data
- Electronic listing of mutual aid channels
- Electronic situational area maps
- Electronic listing of technical support contacts and Communications Unit personnel
- Electronic formal procedures for interoperable communications equipment requests
- TIC-FOG update
- High resolution imagery or tables included in eFOG
- "Listing" the eFOG in the FirstNet mobile app catalog

Technology

Broadband Strategic Planning Support and Education (BRBNDLTE)	
Type of TA Offering:	Workshop
Stakeholders/Audience:	SWICs and Mid – Senior Public Safety Personnel

Offering Overview

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

This offering may be conducted jointly with the FirstNet Products and Services Division.

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

- Locality specific data requirements
- Undefined multi-state regional requirements
- Long Term Evolution (LTE) technology awareness
- Multi-state regional requirements
- Increased LTE awareness

Technology

Mobile and Fixed Site Data Use Assessment for Planned and Unplanned Events (BRBEVNTASMT)	
Type of TA Offering:	Data Coverage Analysis / Interviews / Data Collection
Stakeholders/Audience:	SWICs and Public Safety Personnel

Offering Overview

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

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

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

Technology

Broadband Technologies and Data Operability/Interoperability in Support of Public Safety (BRBDATA)	
Type of TA Offering:	Workshop / Seminar
Stakeholders/Audience:	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, emergency medical services, within an urban area, county or other geographic area are welcome. Communications personnel will gain a deeper perspective on how broadband technologies may be selected and adapted into existing and future public safety architectures.

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

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

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

Technology

Next Generation 9-1-1 / Strategic Planning Support (NG9-1-1STRATPLAN)	
Type of TA Offering:	Education, Awareness / Data Collection / Draft Plan
Stakeholders/Audience:	SWICs, 9-1-1 Operators / Public Safety Answering Point (PSAP) Personnel 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 international borders as well as various emergency response disciplines and agencies. In addition, government officials, managers, and senior public safety personnel need to be familiar with the rapidly evolving technologies to keep the nation's public apprised of rapid changes to 9-1-1.

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

- Standardized interfaces from call and message services
- Processing non-voice (multi-media) messages
- Integrating data useful for call routing and handling
- Delivery of calls/messages and data to appropriate PSAPs
- Supporting data and communications needs for coordinated incident response and management
- Technology transition, integration, and deployment
- Technology assessments for call handling and processing
- Regulatory legislative issues, funding and planning
- Draft Strategic NG9-1-1 Transition Plan
- CAD to CAD transition support
- CAD to RMS transition support

Technology

9-1-1/PSAP Cyber Awareness (9-1-1PSAPCYBR)	
Type of TA Offering:	Webinar and/or Workshop
Stakeholders/Audience:	SWICs, 9-1-1 Operators / Public Safety Answering Point (PSAP) Personnel and State Officials

Offering Overview

This course introduces public safety personnel to common cybersecurity threats and vulnerabilities affecting the PSAP environment, including exposed networks and devices, shared passwords, and email phishing. The critical nature of 9-1-1/PSAP functions (including computer aided dispatch and LMR) means cyberattacks could result in large-scale impact, making them a high-value target to those looking to disrupt public safety services, extort local governments, or simply create mischief. The 9-1-1 PSAP & Land Mobile Radio Cybersecurity Awareness Webinar also provides basic best practices to improve the secure use of emergency communications technologies in day-to-day operations.

In collaboration with CISA Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR), ICTAP offers a customizable cyber awareness service to inform public safety officials, managers, and technical staff involved with 9-1-1 dispatch/PSAP operations, and present individuals associated with 9-1-1 and PSAPs about the numerous, critical aspects of cyber security and how they relate to those functions.

Introductory webinars are approximately 90 minutes long and may be customized to the stakeholder needs but are focused at the local or regional level. This allows for discussion around specifics that pertain to attendees' environment and determines whether a Cybersecurity Planning Workshop is the next logical step.

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 attacked effecting public safety communications, especially PSAP and 9-1-1 operations
- Phishing Campaign – a service available through the CISA National Cyber Assistance and Technical Services (NCATS)[5] Program

[5] Additional information regarding the NCATS program is available here: https://www.us-cert.gov/resources/ncats.

Technology

Alerts and Warnings (ALERTS)	
Type of TA Offering:	Workshop
Stakeholders/Audience:	SWICs, Emergency Management, Public Safety Command/Leadership, and Communications Personnel

Offering Overview

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

This four-hour introductory Alerts and Warning training is designed to assist emergency managers, public safety command/leadership, communications center/dispatch supervisory personnel (9-1-1), and other authorized operations centers responsible for providing timely emergency and life-safety information (both internally and to the public) to fulfill this critical function.

This Alerts and Warnings workshop provides stakeholders an awareness of the alerts and warning systems available to local, state, federal, tribal, and territorial authorities; to include an overview of Federal Emergency Management Agency (FEMA's) Integrated Public Alert and Warning Systems (IPAWS), Wireless Emergency Alerts (WEA), the Emergency Alert System (EAS), and the National Oceanic and Atmospheric Administration (NOAA) Weather Radio and other public alerting systems.

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

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

Technology

LMR/LTE Coverage Testing (LMR/LTE)	
Type of TA Offering:	Radio Frequency (RF) Engineering and Security
Stakeholders/Audience:	SWICs and RF Communications System Management Agencies

Offering Overview

Technical assistance support provided by ICTAP will assist by evaluating the requesting agency's LMR systems in VHF high band (136-174 MHz), UHF (400-470 MHz), and cellular coverage in the 762-870 MHz band. Real-time measurements can include received signals strength, analog audio quality, bit error rate, push to talk, and signal coverage measurements.

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

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[6]	
Type of TA Offering:	Communications-Focused Functional Exercise
Stakeholders/Audience:	AUXCOMM, COML, COMT, INCM, INTD, ITSL, and RADO Trainees

Offering Overview

The COMMEX is a follow on to the Communications Unit Leader (COML), Communications Unit Technician (COMT), Auxiliary Communications (AUXCOMM), Incident Communications Center Manager (INCM), Incident Tactical Dispatcher (INTD), and Radio Operator (RADO) training courses.[7] It provides an opportunity for COML, COMT, AUXCOMM, 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, AUXCOMM, INCM, INTD, ITSL, or RADO course must complete a series of competency tasks in their PTB as the next step in becoming a certified COML, COMT, AUXCOMM, INCM, INTD, ITSL, 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 (IPM).

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

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

- Provide opportunities for testing COML, COMT, AUXCOMM, INCM, INTD, RADO, and/or ITSL trainee proficiency
- Promote state recognition and certification programs
- Increase utilization of recently trained Communications Unit personnel
- Integrate Communications Unit personnel into the Incident Command System (ICS)
- Local mobile communications equipment and resources may be integrated into the COMMEX

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

Training & Exercises

Communications-Focused Exercises (TTX, FE, FSE)[8]	
Type of TA Offering:	Tabletop, Functional, and Full-Scale Exercises
Stakeholders/Audience:	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.

ICTAP provides exercise assistance and expertise focused on communications for:

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

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

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

[8] This exercise is structured under HSEEP guidelines.

Training & Exercises

Communications Focused Drill / Activities (COMMDRILL)	
Type of TA Offering:	Hands on Communications Performance Drill Activities
Stakeholders/Audience:	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, ICTAP evaluators and observers can supplement on-site staff to support and assist in evaluation of Communications Unit personnel on mobile communications units, communications support equipment, audio gateways, digital network communications equipment, and unique modes of communication such as High Frequency (HF), satellite, air-to-ground and marine communications. Drills may consist of actual and/or simulated activities, which can be customized to meet the specific requirements of the requesting site/entity.

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

A typical venue to conduct communications drills would be in conjunction with events such as a Mobile Communications Unit "rodeo" or "rally" during which multiple vehicles and teams assemble from across a region or state. Mobile Communications Unit events offer participating agencies an opportunity to test their voice and data equipment and capabilities and to learn more about resources within their region or state. The drills can potentially involve all Communications Unit positions.

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

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

Training & Exercises

Communications-Focused Exercise Design and Planning (EXDESIGN)	
Type of TA Offering:	Workshop to Develop Communications-Focused Exercises
Stakeholders/Audience:	Key Public Safety Communications Personnel

Offering Overview

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

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

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

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

- Understanding the exercise planning process
- How to incorporate communications elements into exercises
- Identifying the "right" participants
- Developing ideal scenarios (MSELs and injects)
- Developing After Action Reports/Improvement Plans (AARs/IPs)

Training & Exercises

Communications Unit Leader (COML) Training Course	
Type of TA Offering:	Four-Day Course (30 students maximum)
Stakeholders/Audience:	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 the National Incident Management System (NIMS) Incident Command System (ICS) and to provide hands-on exercises that reinforce the lecture materials. CISA and FEMA Emergency Management Institute (EMI) offer this course jointly as "L0969, NIMS ICS All-Hazards Communications Unit Leader Course." [9]

Under the NIMS ICS structure, a COML is the focal point within the Communications Unit.[10] This course provides 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.

There must be a minimum of 15 vetted/qualified students two weeks in advance of the course in order for CISA to conduct the course.

Prerequisites for Attendance

Personal experience:

- A public safety background with experience in field operations
- A technical communication background
- Awareness of fundamental public safety communications technology
- Basic knowledge of applicable communications plan

Completion of the following online courses from the FEMA/EMI website:

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

(Continued on next page)

[9] 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.
[10] CISA is currently coordinating with FEMA NIC and EMI on redesignating the ICS COMU as a branch-level function. This guide will be updated as that change takes place.

Training & Exercises

In-person classroom instruction:

- ICS-300, Intermediate ICS for Expanding Incidents, is required

Additional recommended training:

- ICS-400, Advanced ICS Command and General Staff Complex Incidents, is recommended, but not required

Course Registration Process

SWIC Actions:

- Provide course dates and location to the ICTAP Communications Unit Training Coordinator at least 45 days before the course.
- Designate a recipient of the FEMA student course evaluation forms and provide their name, mailing address, e-mail address and phone number to the ICTAP Communications Unit Training Coordinator at least 45 days before the course. This person must be available to deliver the packet of forms to the Lead Instructor on the first day of the course.
- Require each student to submit a FEMA Form 119-25-1 General Admissions Application signed by the student and their supervisor with proof of prerequisite completion.
- Obtain the STO's signature on the FEMA Form 119-25-1 General Admissions Application. Scan and e-mail the completed forms to the ICTAP Communications Unit Training Coordinator 2 weeks in advance of the course.

ICTAP Actions:

- Determine instructor assignments.
- Submit a "Request to Conduct NIMS ICS Training Class" form to FEMA/EMI at least 45 days before the requested course start date in order to register the course in the FEMA EMI database.
- Fill out the Student Verification form based on the information contained in the FEMA Form 119-25-1s, check the agency affiliations against CASM, and provide the file to the Lead Instructor as a start on the typed roster.
- Fill out the Score Capture Sheet based on the information contained in the FEMA Form 119-25-1 and provide it to the Lead Instructor.
- Submit the COML Course Completion Package to FEMA EMI after the course.

Training & Exercises

Communications Unit Technician (COMT) Training Course	
Type of TA Offering:	Five-Day Course (16 students maximum)
Stakeholders/Audience:	Emergency Response Personnel with a Technical Communications Background

Offering Overview

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

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

The course is instructor-led and supports learning through discussion, lecture, and hands-on exercises to explain processes used for establishment and operation of the technical communications resources for an incident or planned event. The course provides a realistic, hands-on approach to mastering the tasks and skills of a COMT.

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

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

Prerequisites for Attendance

Personal experience:

- A public safety background with experience in field operations
- A technical communication background
- Awareness of fundamental public safety communications technology
- Basic knowledge of applicable Communications Plan

Completion of the following online courses from the FEMA EMI website:

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

SWIC (or designated point of contact [POC]) action:

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

Incident Tactical Dispatcher (INTD) Training Course	
Type of TA Offering:	Four-Day Course (20 students maximum)
Stakeholders/Audience:	Experienced Dispatchers who are familiar with the Incident Command System

Offering Overview

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

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

There must be a minimum of 10 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 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 ICS
- IS-144, Telecommunicators Emergency Response Taskforce (TERT) Basic Course
- IS-200, ICS for Single Resources and Initial Incidents
- IS-700, National Incident Management System (NIMS), an Introduction
- IS-800, National Response Framework (NRF)

Additional recommended training:

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

SWIC (or designated POC) action:

- Submit a completed student verification form to ICTAP at least 14 days prior to the class

Training & Exercises

Information Technology Service Unit Leader (ITSL)Training Course	
Type of TA Offering:	Five-Day Course (20 students maximum)
Stakeholders/Audience:	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, ICTAP introduced the ITSL course, and SAFECOM/NCSWIC have coordinated with FEMA NIC and other organizations focused on public safety communications to establish the best way to integrate the ITSL into the ICS. The ITSL is needed to provide information management, cybersecurity, and application management for the many critical incident/event related functions, to include: Incident/Unified Command Post, Incident Communications Centers, and various tactical operations centers, joint information center (JIC), staging areas, and field locations. The critical need for sufficient access to data, applications, and systems has been reconfirmed during observation of recent ICCAP events which have revealed the widespread and well-established use of a variety of means by individual agencies to access mobile data. However, the coordinated sharing of this data across agencies and jurisdictions is significantly less mature and poses a significant interoperability challenge.

To meet this need, ICTAP has developed the ITSL course. The ITSL course targets Federal, state/territory, tribal, urban, local, and emergency response professionals, and support personnel in all disciplines with a communications background and an aptitude for and extensive experience in information technology.

Specifically, the training course provides an overview of the ITSL components including Communications/IT Help Desk or Unified Help Desk, IT Infrastructure Manager, Network Manager. It covers their roles and responsibilities and provides an in-depth overview with exercises for the ITSL's major functions, to include ensuring reliable and timely delivery of IT services to participating agencies and officials.

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

<u>Prerequisites for Attendance</u>

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

(Continued on next page)

Training & Exercises

Completion of the following in-person classroom instruction:

- ICS-300, Intermediate ICS for Expanding Incidents

Additional recommended training:

- ICS-400, Advanced ICS Command and General Staff Complex Incidents, is recommended but not required

SWIC (or designated POC) action:

- Submit a completed student verification form to ICTAP at least 14 days prior to the class

Training & Exercises

Incident Communications Center Manager (INCM) Training Course	
Type of TA Offering:	Three Day Course (20 students maximum)
Stakeholders/Audience:	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 to provide communications support for operations. Once radio personnel are on scene, it becomes important for an Incident Communications Center Manager (INCM) to be assigned for coordination purposes and to avoid span-of-control issues.

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

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

Prerequisites for Attendance

Personal experience:

- Awareness of fundamental public safety communications technology

Must have completed the following online courses from the FEMA EMI website:

- IS-100, Introduction to the ICS
- IS-144, Telecommunicators Emergency Response Taskforce (TERT) Basic Course
- IS-200, ICS for Single Resources and Initial Incidents
- IS-700, National Incident Management System (NIMS), an Introduction
- IS-800, National Response Framework (NRF)

Additional recommended training:

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

SWIC (or designated POC) action:

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

Training & Exercises

Radio Operator (RADO) Training Course	
Type of TA Offering:	Two Day Course (20 students maximum)
Stakeholders/Audience:	Emergency Response Personnel who are familiar with the Incident Command System

Offering Overview

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

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

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

Prerequisites for Attendance

Personal experience:

- Awareness of fundamental public safety communications technology

Must have completed the following online courses from the FEMA/EMI website:

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

Additional recommended training:

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

SWIC (or designated POC) action:

Submit a completed student verification form to ICTAP at least 14 days prior to the class.

Training & Exercises

Auxiliary Communications (AUXCOMM) Training Course	
Type of TA Offering:	Two- or Three-Day Workshop (30 students maximum)
Stakeholders/Audience:	Licensed Amateur Radio Operators

Offering Overview

This class is designed for auxiliary communicators and groups who volunteer to provide backup radio communications support to public safety agencies. Typically, this includes amateur radio and Radio Emergency Associated Communications Team (REACT) communicators and other types of volunteer communicators.

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

This course focuses on auxiliary communications interoperability, the relationship between the COML and AUXCOMM 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.

There must be a minimum of 15 qualified students two weeks in advance of the course in order for CISA to conduct the course.

Prerequisites for Attendance

Personal experience:

- An active FCC amateur radio license
- Past experience in auxiliary emergency 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 ICS
- IS-200, ICS for Single Resources and Initial Incidents
- IS-700, National Incident Management System (NIMS), an Introduction
- IS-800, National Response Framework (NRF)

Additional recommended training:

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

SWIC (or designated POC) action:

Submit a completed student verification form to ICTAP at least 14 days prior to the class.

Training & Exercises

Auxiliary Communications Train-the-Trainer (AUXCOMM TtT) Course	
Type of TA Offering:	Two Day Workshop (10 students maximum)
Stakeholders/Audience:	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 ICTAP AUXCOMM course, the COML course, the COML Position Task Book (PTB) or the AUXCOMM 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 who have 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.

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

Prerequisites for Attendance

Personal experience:

- Past experience in auxiliary emergency communications
- An affiliation with a public safety agency
- A desire to work with COMLs and Auxiliary Communicators in a NIMS ICS environment

Documentation:

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

(Continued on next page)

Training & Exercises

Completed formal adult education through one of the following fields:

- National Fire Academy's Educational Methodology Course
- National Wildfire Coordinating Groups Facilitative Instructor (M-410) Course
- Center for Domestic Preparedness Instructor Training Certification Course
- Equivalents (i.e. FEMA E/L0141, Instructional Presentation and Evaluation Skills, Total Army Instructor Training Course; Small Group Instructor Training Course; G265 Basic Instructional Skills Course, etc.)
- State Certified Level II or higher Fire, Rescue, and/or EMS Instruction (10341)
- State Certified Teaching Certificate
- Advanced degree in education, educational psychology, technical education, or related program

Completion of the most current version of the following online courses from the FEMA EMI website:

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

Completion of the most current version of the following courses:

- ICS-300, Intermediate ICS for Expanding Incidents
- ICS-400, Advanced ICS for Command and General Staff

SWIC (or designated POC) action:

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

ICTAP Actions:

- Review the prerequisite documentation for sufficiency, build instructor profiles in the COMU Repository and upload prerequisite documentation

Training & Exercises

Communications Unit Leader Train-the-Trainer (COMLTtT) Course	
Type of TA Offering:	Three Day Course (10 students maximum)
Stakeholders/Audience:	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 Position Task Book (PTB). This course helps attendees develop essential core competencies required for teaching the COML course in their own state. This course supports learning through discussion, lecture, participation in multiple activities and students teaching portions of the basic curriculum. This methodology provides a realistic, hands-on approach to mastering the skills of instructing the COML course.

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

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

Prerequisites for Attendance

Documentation:

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

Completion of formal adult education in one of the following fields:

- National Fire Academy's Educational Methodology Course
- National Wildfire Coordinating Groups Facilitative Instructor (M-410) Course
- Center for Domestic Preparedness Instructor Training Certification Course
- Equivalents (i.e. FEMA E/L0141, Instructional Presentation and Evaluation Skills, Total Army Instructor Training Course; Small Group Instructor Training Course; G265 Basic Instructional Skills Course, etc.)
- State Certified Level II or higher Fire, Rescue, and/or EMS Instruction (10341)
- State Certified Teaching Certificate
- Advanced degree in education, educational psychology, technical education, or related program

(Continued on next page)

Training & Exercises

Completion of the most current version of the following online courses from the FEMA EMI website:

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

Completion of the most current version of the following courses:

- ICS-300, Intermediate ICS for Expanding Incidents
- ICS-400, Advanced ICS for Command and General Staff

Course Registration Process

SWIC (or designated POC) Actions:

- Identify students for the course and have them submit proof of prerequisite completion for review. Once satisfied all prerequisites have been met by an individual student, send the prerequisite documentation with a SWIC and STO endorsement of the individual as a future instructor in the state to the ICTAP 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 ICTAP Communications Unit Training Coordinator
- Designate a recipient of the FEMA student course evaluation forms and provide their name, mailing address, e-mail address and phone number to the ICTAP Communications Unit Training Coordinator at least 45 days before the course. This person must be available to deliver the packet of forms to the Lead Instructor on the first day of the course
- Require each vetted student to submit a FEMA Form 119-25-1 General Admissions Application signed by the student and their supervisor
- Obtain the STO's signature on the FEMA Form 119-25-1 General Admissions Application. Scan and e-mail the completed forms to the ICTAP Communications Unit Training Coordinator at least 2 weeks in advance of the course

ICTAP Actions:

- Submit a "Request to Conduct NIMS ICS Training Class" form to FEMA/EMI at least 45 days before the requested course start date in order to register the course in the FEMA EMI database
- Review the prerequisite documentation for sufficiency, build instructor profiles in the COMU Repository and upload prerequisite documentation
- Fill out the Student Verification form based on the information contained in the FEMA Form 119-25-1s, check the agency affiliations against CASM, and provide the file to the Lead Instructor as a start on the typed roster
- Fill out the Score Capture Sheet based on the information contained in the FEMA Form 119-25-1 and provide it to the Lead Instructor

Training & Exercises

Communications Unit Technician Train-the-Trainer (COMTTtT) Courses	
Type of TA Offering:	Five Day Course (10 students maximum)
Stakeholders/Audience:	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 Position Task Book (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 qualified students identified in order for CISA to schedule and conduct the course.

Prerequisites for Attendance

Documentation:

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

Completion of formal adult education in one of the following fields:

- National Fire Academy's Educational Methodology Course
- National Wildfire Coordinating Groups Facilitative Instructor (M-410) Course
- Center for Domestic Preparedness Instructor Training Certification Course
- Equivalents (i.e. FEMA E/L0141, Instructional Presentation and Evaluation Skills, Total Army Instructor Training Course; Small Group Instructor Training Course; G265 Basic Instructional Skills Course, etc.)
- State Certified Level II or higher Fire, Rescue, and/or EMS Instruction (10341)
- State Certified Teaching Certificate
- Advanced degree in education, educational psychology, technical education, or related program

Completion of the most current version of the following online courses from the FEMA/EMI website:

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

(Continued on next page)

Training & Exercises

Completion of the most current version of the following courses:

- ICS-300, Intermediate ICS for Expanding Incidents
- ICS-400, Advanced ICS for Command and General Staff

SWIC (or designated POC) Actions:

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

ICTAP Actions:

- Review the prerequisite documentation for sufficiency, build instructor profiles in the COMU Repository and upload prerequisite documentation

State-Sponsored CISA Recognized Communications Unit Instruction (SSCOMT, SSCOML, SSAUXCOMM)	
Type of TA Offering:	State-Sponsored CISA Recognized Training for COML/COMT/AUXCOMM
Stakeholders/Audience:	Communications Unit Trained Personnel

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 ICTAP. Students receive CISA course completion certificates for COMT and AUXCOMM training, and FEMA EMI course completion certificates for COML training. State-sponsored instructors are required to acquire and maintain the same instructor prerequisites as the ICTAP 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 COMU 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 Communication Assets Survey and Mapping (CASM) database under the Communications Unit Classes section (https://casm.dhs.gov) for their state. This will assist the state in documenting the names and locations of COMLs, COMTs, and AUXCOMM 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 ICTAP contracted instructor requirements for a Communications Unit course:

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

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

(Continued on next page)

Training & Exercises

CISA Instructor Recognition Process

State Actions:

States desiring to use this State-Sponsored/CISA Recognized Communications Unit Instruction Program for students to obtain CISA or FEMA course completion certificates, as applicable to the course, will follow the guidelines below:

- The STO and the SWIC must recommend to CISA individuals from their state who they want to become CISA recognized instructors
- The STO/SWIC will ensure that their recommended instructors submit documentation showing completion of all prerequisites to ICTAP, the final vetting authority, at least 30 days in advance of any COMT or AUXCOMM course and at least 45 days in advance of a COML course

ICTAP Actions:

- Vet the submitted documentation of prerequisite completion for sufficiency.
- Notify the SWIC/STO/applicant of vetting status
- Create an instructor profile in the COMU Repository and upload prerequisite documentation

Process to Conduct a State-Sponsored Communications Unit Course

SWIC/STO Actions:

- The SWIC and/or STO will submit a Technical Assistance request to CISA through their CISA Emergency Communications Coordinator no less than 45 days prior to the start of the state-sponsored COMT or AUXCOMM course or no less than 60 days prior to the start of the state-sponsored COML course. This lead-time gives ICTAP time to approve the TA request and order course materials. The TA request should include:
    - Planned dates for the course
    - The names of the qualified CISA Recognized State-Sponsored Instructors who will teach the course
    - The location of the course
    - The state point of contact (the person responsible for course coordination, receipt of course materials
    - A statement that the state accepts all responsibility and liability for the course, its students and the instructors
    - Participate in a scoping call between ICTAP, the requesting individual, and the instructors involved

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

(Continued on next page)

Training & Exercises

Instructor Actions:

- Participate in a scoping call between ICTAP, the requesting individual, and the instructors involved
- Obtain all logistical support (venue, projector, easels with pads of paper, etc.)
- Ensure all course documentation (student prerequisites validation, attendee sign-in sheets, typed class rosters, student evaluations, and trip report) and processes follow ICTAP course guidelines
- Teach the state-sponsored COML, COMT, or AUXCOMM course without any changes, additions or deletions to the ICTAP core curriculum. Any additional material the state wishes to have taught must be taught either before or after the ICTAP core curriculum
- Send a copy of all student sign-in sheets, the typed class roster, student course evaluations and trip report to ICTAP, the SWIC and STO within five working days after the course
- 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 ICTAP in accordance with state retention policies
- Ensure a CISA TA Evaluation Form is completed and returned to ICTAP

ICTAP Actions:

- Conduct one national COMT TtT annually when at least eight individual students who meet the prerequisites are identified to attend a course
- Conduct one national COML TtT course annually when at least eight individual students who meet the prerequisites are identified to attend the course
- Maintain a file copy of all certifications/qualifications of ICTAP recognized instructors.
- Participate in a scoping call between ICTAP, the requesting individual, and the instructors involved
- Ship course materials approximately one week prior to the start of the course.
- Issue ICTAP course completion certificates via email to the individual students within two weeks of receipt of the certified typed class roster and the CISA TA Evaluation for COMT and AUXCOMM courses
- Add the roster of students that have completed the ICTAP approved state-sponsored Communications Unit course into CASM
- Submit the course completion package to FEMA for COML courses

Training & Exercises

Audio Gateway Information and Training (AG)	
Type of TA Offering:	One Day Workshop (10 students maximum)
Stakeholders/Audience:	Communications Unit Personnel (COMT and Technical Specialists)

Offering Overview

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

Training Modules:

- Gateway Overview. A high-level overview for personnel requiring a basic understanding of audio gateway functionality
- Advanced Audio Gateway Operation. Targeted for personnel such as Communications Unit Leaders (COML), Communications Unit Technicians (COMT), and other communication technical specialists who need a more advanced understanding of gateway operations; for example, specific issues such as co-site RF interference
- Gateway Hands-on Configuration. Focused on specific equipment and is for gateway installers, maintenance technicians, and specialists
- The workshop's lectures, discussions, and practical exercises are focused on the gateways specific to the site and are intended to prepare personnel in a region to quickly activate and deactivate their own equipment. The workshop with all modules is approximately six to eight hours long. Each module builds on previous module(s). The 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 (e.g. ACU 1000, ISSI, and CSSI)
- Audio gateway integration into NIMS ICS operations for Communications Unit personnel
- Hands-on exercise
- Techniques for mitigating RF interference

Operational Communications Assessment (OP-ASMT), Regional Communications Enhancement Support – Strategic Communications Migration Plan (RCES-SCMP), and Special Event Planning (OP-SPEV)	
Type of TA Offering:	On-Site Assessment and Plan Development
Stakeholders/Audience:	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. ICTAP 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[11]

[11] The NSSE toolkit was created by ICTAP 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	
Type of TA Offering:	CASM support both on-site and/or via webinar
Stakeholders/Audience:	SWICs, Communications Planners, System Owners, Communications Unit Personnel

Offering Overview

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

Currently, CASM stores data regarding over 96,000 agencies nationwide on a secure server with multiple levels of access depending on authorizations. CASM is FISMA compliant with an authority to operate on the DHS secure network. DHS has committed to CASM long term as an officially recognized level 3 system under former CIO management. CASM maintains data about public safety agencies and their radio communications equipment across all public safety disciplines. CASM provides a nation-wide Google-maps based view of agencies, fixed and mobile assets, Federal Communications Commission (FCC) information about public safety frequencies and licenses, as well as coverage plots for associated transceivers.

CASM provides a means to maintain, find, report, and share information about agencies, POCs, communication assets (such as COMU personnel, coverage plots, radio systems, dispatch centers, mutual aid channels/sets, gateways, radio caches and mobile communication assets), and agency ownership, sharing, and usage of those assets. It is important that data in CASM be as complete and accurate as possible to ensure communications planning is effective. CASM Subject Matter Experts (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:

- Ability to keep track of communications equipment and have real-time location reporting
- Ability to engage with other jurisdictions to do detailed planning
- Ability to keep track of trained Communications Unit personnel
- Seek to standardize Regional planning
- Desire access to a broad community of expertise
- Access to radio system channels used by an agency or programmed in radio caches
- Standardization of talk groups provided by a trunked radio system, used by an agency, or programmed in a radio cache
- Information about communications sites, i.e., tower, shelter, and associated asset
- Information about dispatch centers and the agencies served
- Information about mobile communication units (MCUs)
- State recognition of trained Communications Unit personnel

Usage

Encryption Planning and Usage (ENCRYPT)	
Type of TA Offering:	Educational Workshop and/or analysis and planning sessions (as needed)
Stakeholders/Audience:	SWICs, RECCWGs, LMR System Operators, Public Safety Command/Leadership, and Communications Personnel

Offering Overview

Understanding the technical aspects of encryption can be very complex and confusing. Whether it's a single community, regional, statewide of an 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 local, state, federal, tribal and territorial authorities.

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

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

Usage

Government Emergency Telephone Service (GETS) / Wireless Priority Service (WPS) and Telecommunications Service Priority (TSP) Support	
Type of TA Offering:	Educational Overview Webinar
Stakeholders/Audience:	SWICs and Public Safety Managers and Stakeholders

Offering Overview

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

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

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

Telecommunications Service Priority (TSP) authorizes public safety organizations to receive priority treatment for vital voice and data circuits. The TSP program provides service vendors a Federal Communications Commission mandate to prioritize requests by identifying those services critical to national security and public safety. A TSP assignment ensures that it will receive priority attention by the service vendor before any non-TSP service. These services are available through the appropriate CISA Priority Telecommunications Services Area Representative (PAR) and by contacting the DHS Priority Telecommunications Service Center at 1-866-627-2255. Additional information regarding GETS, WPS, and TSP can be found at the following websites:

- www.dhs.gov/gets
- www.dhs.gov/wps
- www.dhs.gov/tsp

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

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

Appendix A: SCIP Guide

The Value and Purpose of the SCIP Workshop

The United States Department of Homeland Security (DHS) and Federal Emergency Management Agency (FEMA) released the Fiscal Year (FY) 2018 Homeland Security Grant Program (HSGP) Notice of Funding Opportunity (NOFO) to provide funding to states, territories, urban areas, and other local and tribal governments. These are DHS grants, administered by FEMA with inputs from all elements of the homeland security enterprise. The new guidance addresses several recommendations advocated by the emergency communications community. DHS seeks to enhance the ability of states, local governments, tribes, and territories prevent, protect against, respond to, and recover from potential terrorist acts and other hazards. To meet this requirement, states and territories are required to update their SCIP by FY18.

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

Throughout 2018, CISA partnered with the NGA in four regional policy academies to provide states and territories with the opportunity to create interoperability goals with high level stakeholders present. States and territories that participated have since worked towards either carrying out those goals or incorporating them into the SCIP goals and objectives. These academies were meant to bring a wider number of stakeholders together to discuss needed action within the realm of emergency communications.[12]

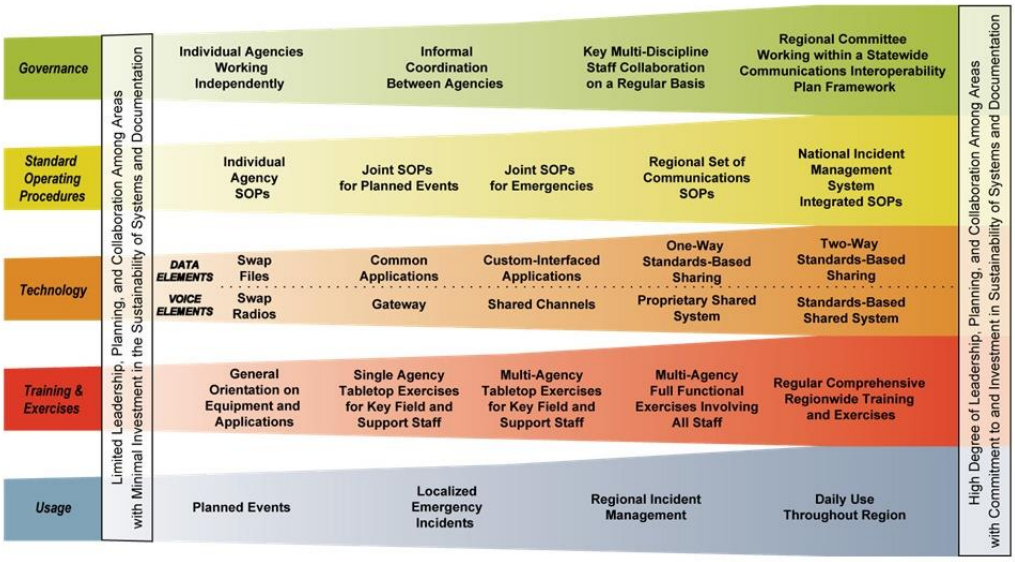


Figure 1: SAFECOM Interoperability Continuum

[12] The SAFECOM Continuum is available here: https://www.dhs.gov/sites/default/files/publications/interoperability_continuum_brochure_2.pdf.

Appendix A: SCIP Guide

Emergency Communications Planning Framework

The interoperable communications ecosystem provides a framework for reviewing the various methods of communications with and among public safety agencies. Various communications systems impact interoperable communications between first responders, the delivery of alerts and warnings to the public, requests for assistance from the public, and the information exchange between public safety responders and the communities they serve. During the SCIP development, stakeholders review the effectiveness of communication interactions that take place in the delivery of their emergency services.

The ecosystem is a framework through which state goals within the SCIP can take form through the various lanes of the SAFECOM Interoperability Continuum with five lanes: Governance, Standard Operating Procedures, Technology, Training & Exercises, and Usage. The five lanes of the continuum are used to create a framework for stakeholders to view how their emergency communications are thriving and direction to take in their efforts to improve or maintain their current systems.

Additionally, states can align the SCIP with the 2019 National Emergency Communications Plan (NECP) which provides information and guidance to those that plan for, coordinate, invest in, and use operable and interoperable communications for response and recovery operations. States are also encouraged to use State Performance Markers rated as "initial", "defined", or "optimized", as well as any remaining 2018 NGA workshop goals as strategic goals and objectives in their SCIPs.

Land Mobile Radio (LMR)

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

Broadband

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

9-1-1

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

Alerts and Warnings

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

Appendix A: SCIP Guide

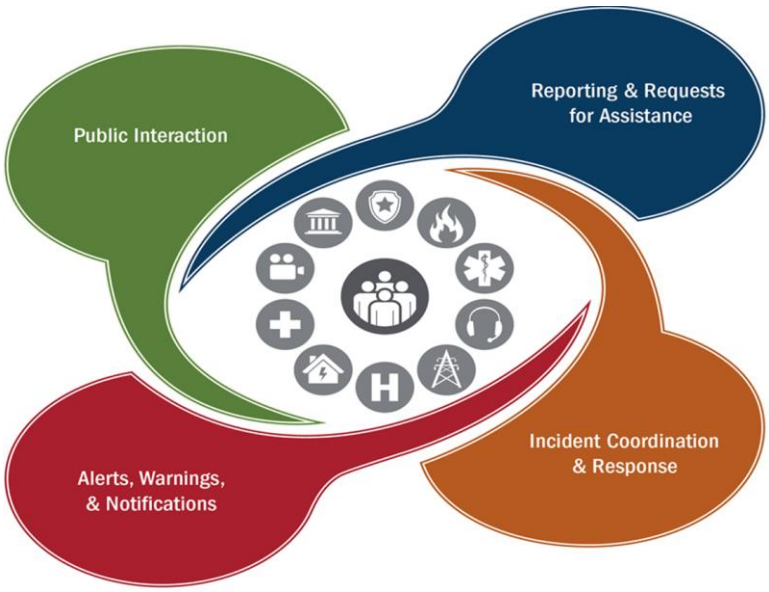


Figure 2: Emergency Communications Ecosystem

Central Focus Areas of the SCIP Workshop

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

Governance

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

Technology

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

Funding Sustainability

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

Appendix A: SCIP Guide

SCIP Process and Timeline

Overview of the SCIP Process

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

SCIP Planning Timeline

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

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

Figure 3: SCIP Process Timeline

Appendix A: SCIP Guide

Who Should Attend a SCIP Workshop?

The SCIP Workshop presents a unique opportunity to bring together a variety of stakeholders from across the state or territory for a two-day intensive strategic planning workshop. When a diverse group collaborates to develop the SCIP, the result is a high-quality, executable plan with stakeholder ownership. Identifying key stakeholders that are relevant to the state or territory's interoperable and public safety communications efforts fosters strong working relationships while ensuring full representation in supporting the vision and mission of the SCIP. Subject matter experts and decision makers, including representation from all jurisdictions, disciplines, and levels of government (federal, regional, state, county, local, and tribal), as well as representation from emerging technologies (broadband, NG 9-1-1, and alerts and warnings) should be included. Past experience has shown that having 40 public safety stakeholders in attendance at a SCIP workshop represents an optimal number of participants. During the workshop planning, the SCIP team will work with the SWIC to discuss the best approach, to include leveraging CISA leadership and their sphere of influence to ensure the broad attendance. CISA can also provide support with drafting invitation language that highlights state-specific information or issues and creating background or reference materials for stakeholders to review prior to the workshop. CISA can disseminate workshop invitation and track RSVPs.

State Communications Leaders

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

State Government Leadership/Designee

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

Public Safety/Public Service Entities

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

Associations

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

Other Entities

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

Appendix A: SCIP Guide

SWIC Checklist

Scoping Call

- ✓ Discuss variety of services ICTAP can provide throughout process
- ✓ Engage SWIC on use of State Survey
- ✓ Integration of NGA Goals into SCIP Workshop

Survey Design

- ✓ Survey review
- ✓ Provide stakeholder emails
- ✓ Disseminate

Planning Call

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

Webinar

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

Final Planning Call

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

SCIP Workshop

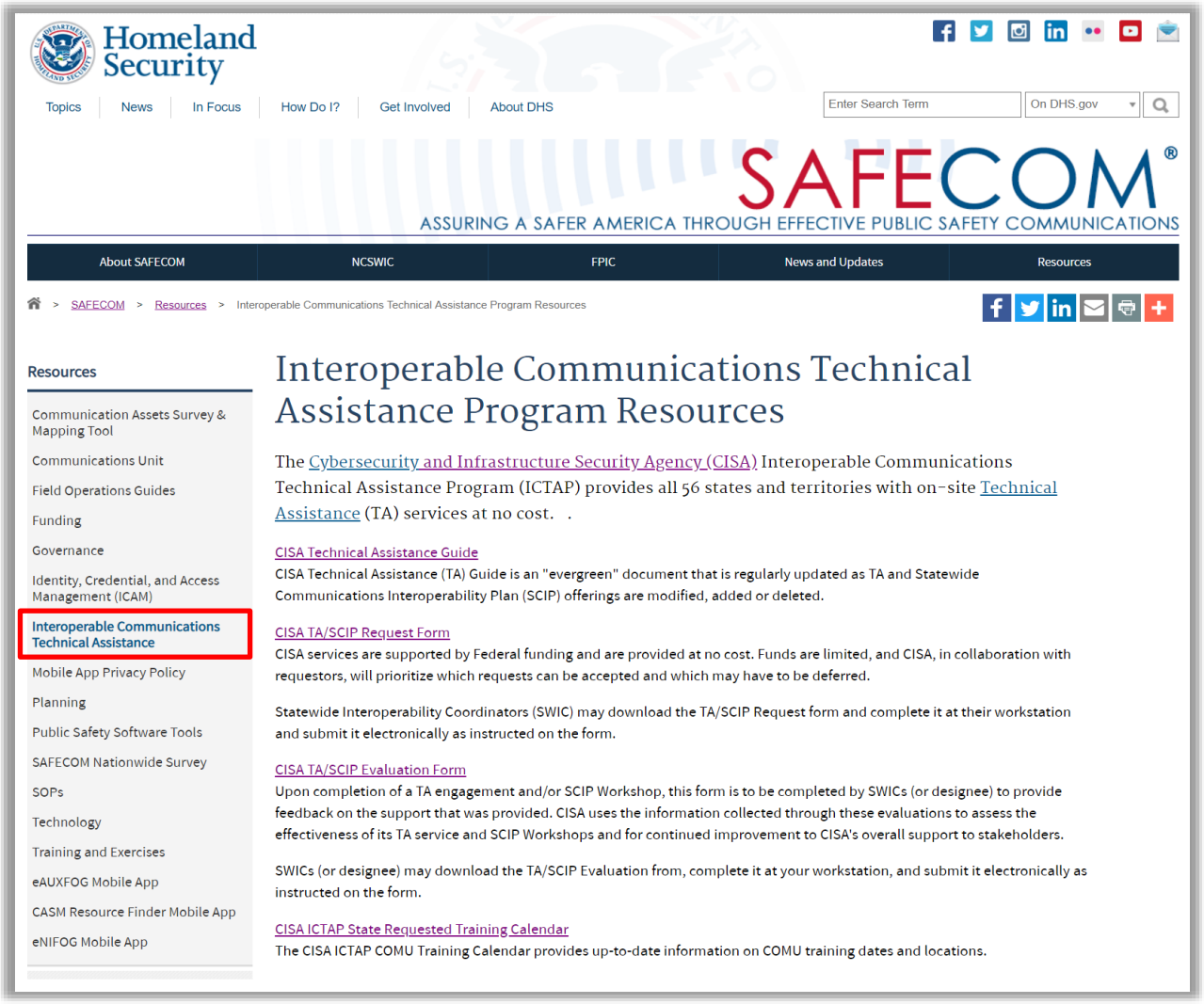
- ✓ Review live capture document with goals, objectives, and an implementation and provide any feedback

Appendix B: SAFECOM Resources

SAFECOM Website Resources

SAFECOM's mission is to improve designated emergency response providers' inter-jurisdictional and inter-disciplinary emergency communications interoperability through collaboration with emergency responders across Federal, State, local, tribal, and territorial governments, and international borders.[13]

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



[13] Additional information regarding SAFECOM is available here: https://www.dhs.gov/safecom.

Appendix C: TA Request Form

OMB No. 1670-0023
Expiration Date: 6/30/2019

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: https://www.dhs.gov/ictapscip-resources.
Email the completed PDF to: TARequest@cisa.dhs.gov.

(Requestor) Contact Information:

State:
Name:
Phone:
Email:

Sector Coordinator:

☐ **SCIP Workshop:**	**Requester's Target Date Range for Workshop:**
To request a SCIP workshop: • Check the box above and insert the desired target date(s) for the workshop in the space provided	**From:** ____ **To:** ____

Appendix C: TA Request Form

OMB No. 1670-0023
Expiration Date: 6/30/2019

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

CISA/ICTAP is Providing These New and Improved TA Service Offerings	
✓ SCIP Workshop ✓ Grant Funding for Emergency Communications ✓ Electronic Field Operations Guide ✓ Broadband Technologies/Interoperability ✓ Next Generation 9-1-1/Strategic Planning Support	✓ 9-1-1/PSAP Cyber Awareness ✓ LMR/LTE, Systems Engineering ✓ Information Technology Service Unit Leader ✓ Communications Unit Leader Train-the-Trainer ✓ Encryption Planning and Usage

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, NGA, 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
Date of Concurrence

SIEC/SIGB/Chair

Submission Date

Notification may be given verbally or by email

Appendix C: TA Request Form

OMB No. 1670-0023
Expiration Date: 6/30/2019

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 D: Acronyms

Acronym	Definition
AAR / IP	After Action Report / Improvement Plan
AG	Audio Gateway
ACU 1000	Intelligent Audio Communication Gateway
AUXCOMM	Auxiliary Communications
BRBND	Broadband
CAD	Computer-Aided Dispatch
CASM	Communication Assets Survey and Mapping Tool
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
COG	Continuity of Government
COML	Communications Unit Leader
COMMDRILL	Communications Drill
COMMEX	Communications Unit Exercise
COMT	Communications Unit Technician
COMU	Communications Unit
COMUPLAN	Communications Unit Planning and Policies
COOP	Continuity of Operations Plan
CSSI	Console Subsystem Interface
CYBR	Cyber
DHS	Department of Homeland Security
EAS	Emergency Alert System
eAUXFOG	Electronic Auxiliary Communications Field Operations Guide
eFOG	Electronic Field Operations Guide
eNIFOG	Electronic National Interoperability Field Operations Guide
EMA	Emergency Management Agency
EMAC	Emergency Management Assistance Compact
EMS	Emergency Medical Services
ENCRYPT	Encryption
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
ESF	Emergency Support Function
EXDESIGN	Exercise Design
EXPLAN	Exercise Plan
FCC	Federal Communications Commission
FEMA EMI	Federal Emergency Management Agency Emergency Management Institute

Appendix D: Acronyms

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

Appendix D: Acronyms

Acronym	Definition
NG9-1-1	Next Generation 9-1-1
NGA	National Governors Association
NIFOG	National Interoperability Field Operations Guide
NIMS	National Incident Management System
NOAA	National Oceanic and Atmospheric Administration
NOFO	Notice of Funding Opportunity
NPSBN	Nationwide Public Safety Broadband Network
NRF	National Response Framework
NS/EP	National Security and Emergency Preparedness
NSSE	National Special Security Events
OP-ASMT	Operational Assessment
PAR	Priority Telecommunications Service Area Representative
POC	Point of Contact
PSAP	Public Safety Answering Point
PSCC	Public Safety Communications Center
PTB	Position Task Book
RADO	Radio Operator
RCES	Regional Communications Enhancement Support
REACT	Radio Emergency Associated Communications Team
RECCWG	Regional Emergency Communications Coordination Working Group
RF	Radio Frequency
RMS	Records Management System
SCMP	Strategic Communications Migration Plan
SCIP	Statewide Communication Interoperability Plan
SEAR	Special Event Assessment Rating
SECIR	Stakeholder Engagement and Cyber Infrastructure Resilience
SIEC	Statewide Interoperability Executive Council
SIGB	Statewide Interoperability Governance Board
SLTT	State, Local, Tribal, and Territorial
SME	Subject Matter Expert
SOG	Standard Operating Guide
SOP	Standard Operating Procedure
SPEV	Special Event
SPOC	Single Point of Contact
SSCOMT	State-Sponsored Communications Unit Technician
SSCOML	State-Sponsored Communications Unit Leader
SSAUXCOMM	State-Sponsored Auxiliary Communications

Appendix D: Acronyms

Acronym	Definition
STO	State Training Officer
STRATPLAN	Strategic Planning
SWIC	Statewide Interoperability Coordinator
TA	Technical Assistance
TBD	To Be Determined
TERT	Telecommunicator Emergency Response Taskforce
TICFOG	Tactical Interoperable Communications Field Operations Guide
TICP	Tactical Interoperable Communications Plan
TSP	Telecommunications Service Priority
TtT	Train-the-Trainer
TTX	Tabletop Exercise
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