SAFECOM® NATIONWIDE SURVEY

Paperwork Reduction Act Statement

The public reporting burden to complete this information collection is estimated at 30 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and the completing and reviewing the collected information. The collection of information is voluntary. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information, unless it displays a currently valid Office of Management and Budget (OMB) control number and expiration date. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to sns@cisa.dhs.gov or

ECD – ATTN: Mark Carmel Rm 967
CISA NGR STOP 0645
Cybersecurity and Infrastructure Security Agency
1110 N. Glebe Road
Arlington, VA 20598-0645

Confidentiality Statement

The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) will track responses and participation; however, CISA will not collect personally identifiable information and only aggregated survey data will be made publicly available so that individual responses will not be distinguishable.

SAFECOM Nationwide Survey

SAFECOM in partnership with the U.S Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency is conducting the SAFECOM Nationwide Survey (SNS). The SNS focuses on public safety organizations and their emergency communications capability needs and gaps. The SNS aims to achieve the following objectives:

- ***Raise national awareness*** by reiterating how the role of emergency communications operability, interoperability, and continuity helps keep America safe, secure, and resilient;
- ***Build industry knowledge*** by providing stakeholders with statistically valid data and findings on the current and future state of emergency communications;
- ***Influence public policy*** by informing decision-makers and officials at all government levels about needed support for emergency communications, programs, and services; and
- ***Drive capability improvements*** by identifying nationwide progress, best practices, and gaps, and by formulating data-driven, evidence-based guidance and resources.

Taking the Survey:

- **Plan:** The estimated time to complete the SNS is 30 minutes; however, it does not need to be completed in one session.
- **Coordinate:** SNS results will represent organizational-level responses. An organizational representative should coordinate with colleagues having the knowledge to help answer questions on technical and operational subject matter.
- **Review:** Respondents are encouraged to review the entire survey prior to starting to determine which questions may require collaboration will colleagues across the organization.

Submissions:

- SNS submissions are due by **XXX**.
- For questions or technical help, e-mail sns@cisa.dhs.gov, or call XXX.

Completed surveys can be returned via:

- U.S. Postal Service to:

  ECD – ATTN: Mark Carmel Rm 967
  CISA NGR STOP 0645
  Cybersecurity and Infrastructure Security Agency
  1110 N. Glebe Road
  Arlington, VA 20598-0645
- A scanned copy e-mailed to: sns@cisa.dhs.gov; or
- A faxed copy transmitted to: DHS – CISA, ATTN: Mark Carmel at XXX.

Question and Response Example

Format: The question below illustrates one of the survey's matrix formats with hypothetical responses.

Guidance: Tips on how to answer matrix question types are listed below:

- Read the question prompt and pay close attention to any underlined terms.
- From top to bottom, read the descriptions in the first column on the left.
- From left to right, read the descriptions in the first row across the top.
- Select <u>one</u> response <u>per</u> row (not by column) that best reflects your organization.
- Definitions of key terms ("Capital Investments") are listed below the answer options.

Select the responses that best characterize the funding of the following items related to the <u>network/system(s)</u> used by your organization: (For <u>each row</u>, select <u>one</u> response)

Funding Items	There is no funding for this item	There is funding, but it is insufficient to meet needs	There is funding, and it is sufficient for all needs	Funding is sufficient and has been identified to address needs beyond the current budget cycle	Don't know	Not applicable
Network/system(s) – capital investments	□	☑	□	□	□	□
Network/system(s) – operating costs	□	☑	□	□	□	□
Network/system(s) – Maintenance	□	□	☑	□	□	□
Network/system(s) upgrade(s)	□	□	□	☑	□	□
Network decommissioning	☑	□	□	□	□	□
Applications and services development and implementation	□	□	☑	□	□	□
Telecommunications Service Priority (TSP)	□	□	□	☑	□	□

Capital Investments: Equipment and other one-time costs.

Network Decommissioning: The process of removing systems and equipment from active service.

Telecommunications Service Priority: A CISA program that authorizes National Security and Emergency Preparedness organizations to receive priority treatment for vital voice and data circuits or other telecommunications services. See https://www.cisa.gov/about-pts

Reminder: The completed matrix above is only one example of SNS question types and responses. Throughout the SNS, question formats change and present other instructions. For example, other instructions include the following prompts:

- For <u>each column</u>, select <u>one</u> response;
- For <u>each column</u>, select <u>all</u> that apply; and,
- For <u>each row</u>, select <u>one</u> response <u>per column</u>.
- Please remember to closely read all questions, underlined terms, and definitions. For any questions or technical help, e-mail sns@cisa.dhs.gov or call **XXX**. Thank you for your participation!

Demographic Questions

1. **List your organization's location:** (For each line, enter one response; no acronyms)
   - State/Territory/Tribe ____
   - County ____
   - Locality (e.g., city, town, district) ____
   - Zip Code ____

2. **Enter your organization's formal name (no acronyms)**

   ____

3. **Select the response that best characterizes your organization's public safety discipline:** (Select one response)
   - Fire
   - Law Enforcement
   - Emergency Medical Services
   - Emergency Management
   - Emergency Communications Center (ECC)/Public Safety Answering Point (PSAP)
   - Other Emergency Response Discipline

- **If your organization is classified as "fire or emergency medical services," answer Question 3a.**
- **Otherwise, answer Question 4.**

3a. **Select the response that best characterizes the staffing structure of your organization**: (Select one response)

- Career
- Volunteer
- Hybrid

4. **Select the response that best characterizes the role of the individual coordinating the survey response for your organization:** (Select one response)
   - Executive Leadership
   - Senior Leadership
   - Supervisory Personnel
   - Investigative Personnel
   - Line and Support Personnel

5. **Estimate the number of personnel in your organization who use emergency communications:** (Select one response)
   - Fewer than 50
   - 51 – 250
   - 251 – 500
   - 501 – 1,000
   - 1,001 – 5,000
   - 5,001 – 10,000
   - More than 10,000

Emergency Communications: The means and methods for exchanging communications and information necessary for successful incident management

6. **Estimate the population size that your organization serves:** (Select one response)

- Fewer than 2,500
- 2,501 – 4,999
- 5,000 – 9,999
- 10,000 – 24,999
- 25,000 – 249,999
- 250,000 – 1 million
- More than 1 million

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Governance — the following questions address your organization’s involvement in decision-making groups.

1) My organization participates in informal decision-making groups that address emergency communications that include representatives from: (Select all that apply)

- Within my organization
- Other public safety organizations in the same jurisdiction
- Other government organizations in the same jurisdiction that support public safety
- Other local governments
- State/territorial governments
- Tribal nations
- Federal departments/agencies
- NGOs/private sector
- International/cross-border entities
- My organization does not participate in informal decision-making groups

2) My organization participates in formal decision-making groups that address emergency communications that include representatives from: (Select all that apply)

- Within my organization
- Other public safety organizations in the same jurisdiction
- Other government organizations in the same jurisdiction that support public safety
- Other local governments
- State/territorial governments
- Tribal nations
- Federal departments/agencies
- NGOs/private sector
- International/cross-border entities
- My organization does not participate in formal decision-making groups

Decision-Making Groups: A group or governing body with a published agreement that designates its authority, mission, and responsibilities.

Other Public Safety Organizations in the Same Jurisdiction: Other government agencies outside your own department (e.g., police department or sheriff’s office, fire department, ECCs/PSAPs, emergency management, emergency medical service agency).

Other Government Organizations in the Same Jurisdiction That Support Public Safety: Other government agencies (e.g., public health, public works, transportation, information technology).

Nongovernmental Organizations (NGO)/Private Sector: Non-profit or for-profit organizations participating in public safety/emergency communications planning, use or reconstitution (e.g., nongovernmental organizations, utilities, auxiliary communications, communication service providers, equipment operators, transportation, food distribution, Volunteer Organizations Active in Disasters).

International/Cross-Border Entities: Foreign organizations (e.g., Canadian or Mexican organizations).

Governance — the following questions address your organization's involvement in decision-making groups.

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Question

3) My organization's formal decision-making groups that address emergency communications and <u>proactively recruit participants beyond first responders</u> include representatives from: (Select <u>all</u> that apply)

- Within my organization
- Other public safety organizations in the same jurisdiction
- Other government organizations in the same jurisdiction that support public safety
- Other local governments
- State/territorial governments
- Tribal nations
- Federal departments/agencies
- NGOs/private sector
- International/cross-border entities
- My organization's formal decision-making groups do not proactively recruit participants beyond first responders

Decision-Making Groups: A group or governing body with a published agreement that designates its authority, mission, and responsibilities.

Other Public Safety Organizations in the Same Jurisdiction: Other government agencies outside your own department (e.g., police department or sheriff's office, fire department, ECCs/PSAPs, emergency management, emergency medical service agency).

Other Government Organizations in the same Jurisdiction That Support Public Safety: Other government agencies (e.g., public health, public works, transportation, information technology).

Nongovernmental Organizations (NGO)/Private Sector: Non-profit or for-profit organizations participating in public safety/emergency communications planning, use or redistribution (e.g., nongovernmental organizations, utilities, auxiliary communications, communication service providers, equipment operators, transportation, food distribution, Volunteer Organizations Active in Disasters).

International/Cross-Border Entities: Foreign organizations (e.g., Canadian or Mexican organizations).

Operability: Ability to provide and maintain reliable communications functionality throughout the area of responsibility.

Interoperability: Ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as authorized.

Continuity: Ability to provide and maintain acceptable levels of communications during disruptions in operations.

Day-to-Day Situations: Situations within the general normal structure for an organization, including routine operations.

Out-of-the-Ordinary Situations: Situations that may stretch and/or overwhelm the abilities of an organization.

4) Do the decision-making groups in which your organization participates sufficiently support your organization's need for communications: (For <u>each row</u>, select <u>one</u> response <u>per column</u>)

	For "day-to-day" situations?	For "out-of-the-ordinary" situations?
Operability	o Yes o No	o Yes o No
Interoperability	o Yes o No	o Yes o No
Continuity	o Yes o No	o Yes o No

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Governance — the following questions address your organization's agreements.

5) **Select the responses that best characterize the agreements your organization has made to enable emergency communications <u>interoperability</u>:** (For <u>each row</u>, select <u>one</u> response) Note: Reading from left to right, the first four responses are progressive (i.e., to select the fourth response, an organization must have surpassed <u>all</u> of the first three response criteria)

	There are informal, undocumented agreements in practice with	There are published and active agreements <u>with some</u>	There are published and active agreements <u>with most</u>	Agreements are reviewed every 3-5 years, after system upgrades, or incidents that test capabilities with	Not Applicable
Other public safety organizations in the same jurisdiction	□	□	□	□	□
Other government organizations in the same jurisdiction that support public safety	□	□	□	□	□
Other local governments	□	□	□	□	□
State/territorial governments	□	□	□	□	□
Tribal nations	□	□	□	□	□
Federal departments/ agencies	□	□	□	□	□
NGOs/private sector	□	□	□	□	□
International/cross-border entities	□	□	□	□	□

Agreements: Formal mechanisms to govern interagency coordination and the use of interoperable emergency communications solutions.

Interoperability: Ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as authorized.

Other Public Safety Organizations in the Same Jurisdiction: Other government agencies outside your own department (e.g., police department or sheriff's office, fire department, ECCs/PSAPs, emergency management, emergency medical service agency).

Other Government Organizations in the Same Jurisdiction That Support Public Safety: Other government agencies (e.g., public health, public works, transportation, information technology).

Published and Active Agreements: Memoranda of Understanding (MOU), Executive Orders, legislation, Intergovernmental agreements, etc.

Nongovernmental Organizations (NGO)/Private Sector: Non-profit or for-profit organizations participating in public safety/emergency communications planning, use or reconstitution (e.g., nongovernmental organizations, utilities, auxiliary communications, communication service providers, equipment operators, transportation, food distribution, Volunteer Organizations Active in Disasters).

International/Cross-Border Entities: Foreign organizations (e.g., Canadian or Mexican organizations).

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Governance — the following questions address your organization's agreements and funding of your organization's communications capabilities, regardless of whether the items it uses are owned, shared, or subscription-based.

6) Do your organization's agreements meet its needs to achieve: (For each row, select one response per column)

	For "day-to-day" situations?	For "out-of-the-ordinary" situations?
Operability	o Yes o No	o Yes o No
Interoperability	o Yes o No	o Yes o No
Continuity	o Yes o No	o Yes o No

7) Select the responses that best characterize the funding of the following items related to the network/system(s) used by your organization: (For each row, select one response)

Funding Items	There is no funding for this item	There is funding, but it is insufficient to meet needs	There is funding, and it is sufficient for all needs	Funding is sufficient and has been identified to address needs beyond the current budget cycle	Don't know	Not applicable
Network/system(s) – capital investments	☐	☐	☐	☐	☐	☐
Network/system(s) – operating costs	☐	☐	☐	☐	☐	☐
Network/system(s) – maintenance	☐	☐	☐	☐	☐	☐
Network/system(s) upgrade(s)	☐	☐	☐	☐	☐	☐
Network decommissioning	☐	☐	☐	☐	☐	☐
Applications and services development and	☐	☐	☐	☐	☐	☐

Agreements: Formal mechanisms to govern interagency coordination and the use of interoperable emergency communications solutions.

Operability: Ability to provide and maintain reliable communications functionality throughout the area of responsibility.

Interoperability: Ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as authorized.

Continuity: Ability to provide and maintain acceptable levels of communications during disruptions in operations.

Day-to-Day Situations: Situations within the general normal structure for an organization, including routine operations.

Out-of-the-Ordinary Situations: Situations that may stretch and/or overwhelm the abilities of an organization.

Capital Investments: Equipment and other one-time costs.

Network Decommissioning: The process of removing systems and equipment from active service.

Telecommunications Service Priority: A CISA program that authorizes National Security and Emergency Preparedness organizations to receive priority treatment for vital voice and data circuits or other telecommunications services. See https://www.cisa.gov/about-pts

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Governance — the following questions address the funding of your organization's communications capabilities, regardless of whether the items it uses are owned, shared, or subscription-based.

8) Select the responses that best characterize the funding for the following items related to the <u>equipment</u> used by your organization: (For <u>each row</u>, select <u>one</u> response)

Funding Items	There is no funding for this item	There is funding, but it is insufficient to meet needs	There is funding, and it is sufficient for all needs	Funding is sufficient and has been identified to address needs beyond the current budget cycle	Don't know	Not applicable
Equipment management	☐	☐	☐	☐	☐	☐
Equipment upgrades	☐	☐	☐	☐	☐	☐
Equipment disposal	☐	☐	☐	☐	☐	☐

9) Select the responses that best characterize the funding of the following related to the <u>interoperability solutions</u> used by your organization: (For <u>each row</u>, select <u>one</u> response)

Funding Items	There is no funding for this item	There is funding, but it is insufficient to meet needs	There is funding, and it is sufficient for all needs	Funding is sufficient and has been identified to address needs beyond the current budget cycle	Don't know	Not applicable
Interoperability solutions – capital investments	☐	☐	☐	☐	☐	☐
Interoperability solutions – operating costs	☐	☐	☐	☐	☐	☐
Interoperability solutions – maintenance costs	☐	☐	☐	☐	☐	☐
Interoperability solutions – research and development	☐	☐	☐	☐	☐	☐

10) Select the responses that best characterize the funding of the following items related to <u>cybersecurity</u> within your organization: (For <u>each row</u>, select <u>one</u> response)

Items	There is no funding for this item	There is funding, but it is insufficient to meet needs	There is funding, and it is sufficient for all needs	Funding is sufficient and has been identified to address needs beyond the current budget cycle	Don't know	Not applicable
Cybersecurity – capital investments	☐	☐	☐	☐	☐	☐
Cybersecurity – operating costs	☐	☐	☐	☐	☐	☐
Cybersecurity – maintenance costs	☐	☐	☐	☐	☐	☐

Interoperability Solution: Any method, process, or system used to enable interoperability (e.g., radio swaps, channel or console cross-patching, shared system or channels).

Governance — the following questions address the funding of your organization's emergency communications capabilities.

11) Select the sources used by your organization to fund emergency communications: (Select all that apply)

- Discretionary funding
- Appropriated/dedicated funding (e.g., operational and/or capital budgets)
- Grants
- Bonds
- Specialized taxes
- Fees
- Shared resources (e.g., operations and maintenance, systems, equipment, real estate)
- Private individuals or organizations
- Personally-supplied communications equipment (e.g., bring-your-own device)
- Don't know

12) Select all organizations with whom your organization shares: (For each column, select all that apply)

	Costs	Resources
Other public safety organizations in the same jurisdiction	□	□
Other government organizations in the same jurisdiction that support public safety	□	□
Other local governments	□	□

Resources: Communications personnel, equipment, supplies, and facilities available or potentially available for assignment to incident operations and for which status is maintained.

Costs: Sharing the responsibility to pay, allocate budgeted funds, or contribute fiscal support for acquisition, operations, and maintenance expenses associated with emergency communications capabilities.

Resources: Communications personnel, equipment, supplies, and facilities available (or potentially available) for assignment to incident operations or planned events.

Other Public Safety Organizations in the Same Jurisdiction: Other government agencies outside your own department (e.g., police department or sheriff's office, fire department, ECCs/PSAPs, emergency management, emergency medical service agency).

Other Government Organizations in the Same Jurisdiction That Support Public Safety: Other government agencies (e.g., public health, public works, transportation, information technology).

Nongovernmental Organizations (NGO)/Private Sector: Non-profit or for-profit organizations participating in public safety/emergency communications planning, use or reconstitution (e.g., nongovernmental organizations, utilities, auxiliary communications, communication service providers, equipment operators, transportation, food distribution, Volunteer Organizations Active in Disasters).

International/Cross-Border Entities: Foreign organizations (e.g., Canadian or Mexican organizations).

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Governance — the following questions address your organization's strategic planning for emergency communications.

13) Select the response that best characterizes your organization's <u>strategic planning process</u> for emergency communications: (Select <u>one</u> response) Note: Responses are progressive (i.e., to select the fourth response, an organization must have surpassed all of the first three response criteria)

- No planning process or plan is in place
- A planning process is in place and a plan for addressing emergency communications is under development
- A plan for addressing emergency communications is in place and operationalized by participating organizations
- A plan for addressing emergency communications is in place and is reviewed annually, after system upgrades and incidents/events that test organizational capabilities

- **If your organization has "no planning process or plan in place," <u>skip</u> to Question 14 on the next page.**
- **Otherwise, <u>answer</u> Question 13a.**

13a) Identify organizations included in your strategic planning processes for emergency communications: (Select <u>all</u> that apply)

- Other public safety organizations in the same jurisdiction
- Other government organizations in the same jurisdiction that support public safety
- Other local governments

Other Public Safety Organizations in the Same Jurisdiction: Other government agencies outside your own department (e.g., police department or sheriff's office, fire department, ECCs/PSAPs, emergency management, emergency medical service agency).

Other Government Organizations in the Same Jurisdiction That Support Public Safety: Other government agencies (e.g., public health, public works, transportation, information technology).

Nongovernmental Organizations (NGO)/Private Sector: Non-profit or for-profit organizations participating in public safety/emergency communications planning, use or reconstitution (e.g., nongovernmental organizations, auxiliary communications, utilities, communication service providers, equipment operators, transportation, food distribution, Volunteer Organizations Active in Disasters).

International/Cross-Border Entities: Foreign organizations (e.g., Canadian or Mexican organizations).

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Governance — the following question addresses your organization's strategic planning for emergency communications.

14) Does your organization's strategic planning process sufficiently meet its need for: (For each row, select one response per column)

	For "day-to-day" situations?	For "out-of-the-ordinary" situations?
Operability	o Yes o No	o Yes o No
Interoperability	o Yes o No	o Yes o No
Continuity	o Yes o No	o Yes o No

Strategic Planning: A planning process that establishes organizational goals and identifies, scopes, and establishes requirements for the provisioning of capabilities and resources to achieve them.

Operability: Ability to provide and maintain reliable communications functionality throughout the area of responsibility.

Interoperability: Ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as authorized.

Continuity: Ability to provide and maintain acceptable levels of communications during disruptions in operations.

Day-to-Day Situations: Situations within the general normal structure for an organization, including routine operations.

Out-of-the-Ordinary Situations: Situations that may stretch and/or overwhelm the abilities of an organization.

Standard Operating Procedures (SOP): Generally refers to a reference document or an operations manual that provides the purpose, authorities, duration, and details for the preferred method of performing a single function or a number of interrelated functions in a uniform manner.

Standard Operating Guidelines (SOG): Intended to outline best practice - they are not mandatory, but help personnel follow the rules while allowing for flexibility.

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Standard Operating Procedures/Guidelines (SOPs/SOGs) – the following questions address your organization's SOPs/SOGs.

- **If "no communications SOPs/SOGs current exist" for your organization, skip to Question 16 on page 15.**
- **Otherwise, answer Questions 15a-d.**

15a) Select the responses that best characterize your organization's SOPs/SOGs: (For each row, select one response) Note: Reading from left to right, the first four responses are progressive (i.e., to select the fourth response, an organization must have surpassed all of the first three response criteria)

	Informal practices and procedures are in place	Formal policies/ practices/ procedures enable day-to-day situations' interoperability	Formal policies/ practices/ procedures enable out-of-the-ordinary situations' interoperability	Processes for SOP/SOG development and review exist for consistency across responders	Not Applicable
Within my organization	○	○	○	○	○
With other public safety organizations in the same jurisdiction	○	○	○	○	○
With other government organizations in the same jurisdiction that support public safety	○	○	○	○	○

SOP: Generally refers to a reference document or an operations manual that provides the purpose, authorities, duration, and details for the preferred method of performing a single function or a number of interrelated functions in a uniform manner.

SOG: Intended to outline best practice - they are not mandatory, but help personnel follow the rules while allowing for flexibility.

Other Public Safety Organizations in the Same Jurisdiction: Other government agencies outside your own department (e.g., police department or sheriff's office, fire department, ECCs/PSAPs, emergency management, emergency medical service agency).

Other Government Organizations in the Same Jurisdiction That Support Public Safety: Other government agencies (e.g., public health, public works, transportation, information technology).

Nongovernmental Organizations (NGO)/Private Sector: Non-profit or for-profit organizations participating in public safety/emergency communications planning, use or reconstitution (e.g., nongovernmental organizations, auxiliary communications, utilities, communication service providers, equipment operators, transportation, food distribution, Volunteer Organizations Active in Disasters).

International/Cross-Border Entities: Foreign organizations (e.g., Canadian or Mexican organizations).

Standard Operating Procedures/Guidelines (SOPs/SOGs) – the following questions address your organization's SOPs/SOGs.

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

- **If "no communications SOPs/SOGs currently exist" for your organization, skip to Question 16 on the next page.**
- **If not, answer Questions 15b-d.**

15b) Select the guidelines or standards that have influenced your organization's communications SOPs/SOGs: (Select all that apply)

- Local guidance
- State guidance
- Territorial guidance
- Tribal guidance
- National/federal guidance
- Industry guidance (e.g., vendor, provider, trade organization)
- None of the above

15c) Select the national/federal sources, guidelines, or standards that have influenced your organization's communications SOPs/SOGs: (Select all that apply)

- Communications Security, Reliability, and Interoperability Council's (CSRIC) guidance
- Criminal Justice Information Services (CJIS) guidance
- DHS Communications Sector-Specific Plan (CSSP)
- Federal Partnership for Interoperable Communications (FPIC)
- Federal Plain Language Guidelines
- Information Sharing and Analysis Centers (ISAC)
- Information Sharing and Analysis Organizations (ISAO)
- National Emergency Communications Plan (NECP)
- National Infrastructure Protection Plan (NIPP)
- National Interoperability Field Operations Guide (NIFOG)
- National Incident Management System (NIMS)/Incident Command System (ICS) guidance
- National Information Exchange Model (NIEM) guidance
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- National Response Framework (NRF)
- NIMS/ICS Communications Unit
- SAFECOM Approach for Developing an Interoperable Information Sharing Framework (ISF)
- SAFECOM Guidance on Emergency Communications Grants
- SAFECOM Interoperability Continuum
- Other joint SAFECOM/National Council of Statewide Interoperability Coordinators (NCSWIC) guidance (e.g., Guidelines for Encryption in Land Mobile Radio [LMR] Systems, Next Generation 911 [NG911] Cybersecurity Primer)
- Other
- None of the above

Standard Operating Procedures (SOP): Generally refers to a reference document or an operations manual that provides the purpose, authorities, duration, and details for the preferred method of performing a single function or a number of interrelated functions in a uniform manner.

Standard Operating Guidelines (SOG): Intended to outline best practice - they are not mandatory, but help personnel follow the rules while allowing for flexibility.

Standard Operating Procedures/Guidelines (SOPs/SOGs) – the following question addresses your organization's SOPs/SOGs.

15d) Select the topics that are included in your organization's SOPs/SOGs: (Select all that apply)

- Land Mobile Radio (LMR)
- Broadband
- Project 25 (P25) encryption
- Social media
- Cybersecurity
- Priority services
- Next Generation 911 (NG911)
- Alerts, warnings, and notifications (e.g., Wireless Emergency Alert, Emergency Alert System)
- Continuity of communications (e.g., resiliency, redundancy, primary/secondary/backup)

Standard Operating Procedures (SOP): Generally refers to a reference document or an operations manual that provides the purpose, authorities, duration, and details for the preferred method of performing a single function or a number of interrelated functions in a uniform manner.

Standard Operating Guidelines (SOG): Intended to outline best practice - they are not mandatory, but help personnel follow the rules while allowing for flexibility.

Priority Services: Government Emergency Telecommunications Service (GETS), WPS, TSP.

Continuity of Communications: The ability of emergency response agencies to maintain communications capabilities when primary infrastructure is damaged or destroyed.

Operability: Ability to provide and maintain reliable communications functionality throughout the area of responsibility.

Interoperability: Ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as authorized.

Continuity: Ability to provide and maintain acceptable levels of communications during disruptions in operations.

Day-to-Day Situations: Situations within the general normal structure for an organization, including routine operations.

Out-of-the-Ordinary Situations: Situations that may stretch and/or overwhelm the abilities of an organization.

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Technology — the following question addresses your organization's technology solutions.

17) Select the <u>interoperability solutions</u> your organization employs, regardless of whether the systems in use are owned, shared, or subscription-based: (Select <u>all</u> that apply)

- Base Interface Module solution (BIM-to-BIM)
- Channel/console cross-patching
- Cloud-based environment
- Commercial wireless service (e.g., bring-your-own-device)
- Commercial wireless service (e.g., government furnished equipment)
- Common applications (e.g., use of same or compatible applications to share data)
- Console-to-console intercom interconnections (e.g., center-to-center voice and data)
- Crossband repeaters
- Custom-interfaced applications (e.g., custom linking of proprietary applications or use of middleware to share data)
- Data exchange hubs (e.g., computer-aided dispatch [CAD]-to-CAD, integrated message switching systems [MSS])
- Deployable audio/gateway switch
- Deployable site infrastructure (e.g., cell on wheels [COW]/cell on light truck [COLT])
- Digital system (Internet Protocol-based)
- Established channel sharing agreements
- Fixed audio/gateway switch
- Inter-RF Subsystem Interface (ISSI)/Console Subsystem Interface (CSSI)
- Mobile command post/mobile communications center
- Mutual aid channels/talkgroups (e.g., shared channels/talkgroups)
- Nationwide Public Safety Broadband Network (NPSBN)/FirstNet
- National Information Exchange Model (NIEM)-based data exchange
- National Public Safety Planning Advisory Committee (NPSPAC) channels
- One-way standards-based sharing of data (e.g., applications to "broadcast/push" or "receive/pull" data from systems)
- Radio cache/radio exchange
- Radio reprogramming
- Shared system (conventional or trunked)
- Standards-based shared systems (e.g., Project 25 [P25])
- None of the above

18) Select the <u>types</u> of information that are exchanged between your organization and others: (Select <u>all</u> that apply)

- Voice
- Video
- Geographic Information System (GIS) data
- Evacuee/patient tracking data
- Accident/crash (telematics) data
- Resource data (available equipment, teams, shelter/hospital beds)
- Biometric data
- Computer-Aided Dispatch (CAD) data
- Automatic Vehicle Location (AVL) data
- Common Operating Picture data/Situational awareness
- Records Management System (RMS)
- Threat intelligence data

Interoperability: Ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as authorized.

Technology — the following question addresses your organization's technology solutions, regardless of whether the systems in use are owned, shared, or subscription-based.

19) Select the extent to which the following factors have impacted your organization's ability to communicate: (For each row, select one response)

Factors	None	Little extent	Some extent	Great extent	Not applicable
Unplanned system/equipment failure	☐	☐	☐	☐	☐
Excessive planned downtime	☐	☐	☐	☐	☐
Frequency interference	☐	☐	☐	☐	☐
System congestion (e.g., limited spectrum capacity, insufficient frequencies)	☐	☐	☐	☐	☐
Cybersecurity disruption or breach	☐	☐	☐	☐	☐
Poor coverage (in-building)	☐	☐	☐	☐	☐
Poor coverage (outdoors)	☐	☐	☐	☐	☐
Poor subscriber unit quality	☐	☐	☐	☐	☐
Insufficient site hardening	☐	☐	☐	☐	☐
Insufficient system/equipment redundancy	☐	☐	☐	☐	☐
Insufficient route diversity	☐	☐	☐	☐	☐
Insufficient wireless voice application interoperability	☐	☐	☐	☐	☐
Insufficient wireless data application interoperability	☐	☐	☐	☐	☐
Deferred maintenance	☐	☐	☐	☐	☐
Deferred capital expenditures	☐	☐	☐	☐	☐
Diminished service due to adding users from beyond our organization	☐	☐	☐	☐	☐
System/equipment failure beyond the ownership or control of our organization	☐	☐	☐	☐	☐
Incompatibility of proprietary systems, modes, and algorithms	☐	☐	☐	☐	☐

20) Does your organization have the appropriate infrastructure, systems, equipment, and facilities

Insufficient System/Equipment Redundancy: Inability of additional or duplicate communications assets to share the load or provide backup to the primary asset.

Insufficient Route Diversity: A single point of failure or dependence on a single provider causing diminished ability to communicate (e.g., backhaul servers buried cable and causes outage).

Day-to-Day Situations: Situations within the general normal structure for an organization, including routine operations.

Out-of-the-Ordinary Situations: Situations that may stretch and/or overwhelm the abilities of an organization.

Continuity of Communications: The ability of emergency response agencies to maintain communications capabilities when primary infrastructure is damaged or destroyed.

Technology — the following questions address the sufficiency of your organization's technology solutions.

21) Does your organization have the appropriate fixed, portable, mobile, deployable, and/or temporary solutions to support interoperability? (For each row, select one response)

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
For "day-to-day" situations?	☐	☐	☐	☐	☐
For "out-of-the-ordinary" situations?	☐	☐	☐	☐	☐

22) Select the response that best characterizes how well your organization's communications systems meet its mission requirements: (Select one response)

- Systems do not currently meet mission requirements
- Systems meet only basic mission requirements
- Systems meet mission requirements of day-to-day situations, but not out-of-the-ordinary situations
- Systems meet all mission requirements of day-to-day and most out-of-the-ordinary situations

Cybersecurity — the following questions address your organization's approach to cybersecurity.

23) Has your organization engaged in cybersecurity planning and/or implementation? (Select one

Interoperability: Ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as authorized.

Day-to-Day Situations: Situations within the general normal structure for an organization, including routine operations.

Out-of-the-Ordinary Situations: Situations that may stretch and/or overwhelm the abilities of an organization.

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Cybersecurity — the following questions address your organization's approach to cybersecurity.

- **If your organization "has engaged in cybersecurity planning or implementation," answer Questions 23a-b2.**
- **Otherwise, skip to Question 24 on page 21.**

23a) Select the cybersecurity planning measures your organization uses: (Select all that apply)

- Risk assessment
- Incident response plans/policies
- Vulnerability response plans/policies
- Coordination lead (e.g., incident manager)
- Incident Response Team (IRT)
- Integration of Cyber Threat Intelligence (CTI) sources
- Means for collecting digital forensics and other data or evidence
- Agreement with another entity that provides cybersecurity services (e.g., commercial vendor, internal IT department or function)
- Cybersecurity insurance
- Recovery exercises (e.g., use of failover systems, backup recovery)
- None of the above

23b) Select the cybersecurity measures that your organization has implemented: (Select all that apply)

- Single factor authentication (e.g., passwords)
- Multi-factor authentication (e.g., smart cards, personal identification verification [PIV] cards, tokens)
- Continuous monitoring (e.g., antivirus, intrusion detection)
- Backups
- Automated updates
- Failover system
- Hardened workstations for monitoring and response activities
- Disk and active memory imaging
- Coordinated response and restoration activities with internal and external parties
- Post-incident lessons learned analysis (e.g., hotwash, after-action report)
- None of the above

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Cybersecurity — the following questions address your organization's approach to cybersecurity.

- **If your organization has implemented "continuous monitoring" <u>answer</u> Question 23b1.**
- **Otherwise, <u>skip</u> to Question 23b2.**

23b1) Indicate which <u>continuous monitoring</u> capabilities your organization uses: (Select <u>all</u> that apply)

- Antivirus (AV) software
- Endpoint Detection and Response (EDR) solutions
- Data Loss Prevention (DLP) capabilities
- Intrusion Detection and Prevention Systems (IDPS)
- Authorization, host, application, and cloud logs
- Network flows
- Packet Capture (PCAP)
- Security Information and Event Management (SIEM) systems
- Other

- **If your organization has implemented "backups," <u>answer</u> Question 23b2.**
- **Otherwise, <u>skip</u> to Question 24 on the next page.**

23b2) Indicate which <u>backup</u> capabilities and practices your organization uses: (Select <u>all</u> that apply)

- Manual backups
- Automated backups
- Offline backups
- Frequent training on backups
- Exercises on restoring from backups
- Other

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Cybersecurity — the following questions address your organization's approach to cybersecurity.

24) In the event of a cyber incident, which entities are alerted or engaged by your organization? (Select all that apply)

- Agency's own Information Technology (IT) resources
- Parent organization or agency's IT resources
- IT cybersecurity vendor
- Organizations with interconnected networks (e.g., equipment vendors, partner agencies)
- Cybersecurity and Infrastructure Security Agency (CISA) (e.g., CISA Central, Automated Indicator Sharing [AIS])
- Federal Bureau of Investigation (FBI) (e.g., field offices, Internet Crime Complaint Center [IC3], InfraGard)
- Multi-State Information Sharing and Analysis Center (MS-ISAC)®
- United States Secret Service
- Region-based support
- State-based support (e.g., National Guard, fusion center, state-sponsored cyber unit)
- Local- or tribal-based support beyond the immediate organization
- Other
- None of the above

25) Indicate the types of cyber attacks that your organization has experienced: (Select all that apply)

- Phishing/email spoofing attack
- Ransomware attack
- Password or credential attack (i.e., unauthorized use of password or credential)
- Denial of service attack
- Telephony Denial of Service (TDoS) attack
- Domain Name Service (DNS) tunneling attack
- Doxing attack (i.e., data access with information threatened to be sold or revealed)
- Other malware (e.g., viruses, trojans)
- Internet of Things-based attack (i.e., attacker entered network through "smart" devices or systems)
- Other types of attack (e.g., SQL injection, cross-scripting, eavesdropping)
- Attacks of unknown type
- Our organization has not identified any cyber attacks
- Don't know

Cybersecurity — the following questions address your organization's approach to cybersecurity.

26) Complete this sentence: "Our organization is _______________ in our ability to detect and respond to cybersecurity threats and vulnerabilities." (Select one response)

- Not confident
- Somewhat confident
- Confident
- Very confident

27) Complete this sentence: "Since 2018, cybersecurity incidents have had _______________ on the ability of our organization to communicate." (Select one response)

- Severe impact
- Some impact
- Minimal impact
- No impact
- Don't know

Physical Security — the following question addresses your organization's physical security posture.

28) Select the response that best characterizes your organization's physical security for facilities and communications infrastructure: (For each row, select one response) Note: Reading from left to right, responses are progressive (i.e., to select the third response, an organization must have surpassed both of the first two response criteria)

	Physical security is present only as a consequence of other requirements (e.g., building codes, zoning requirements, architectural recommendations/guidance, SOPs/SOGs) and what may be found in a similar commercial building or facility	Solution sets designed and implemented for the intended occupancy, purpose, and use of the building/facility	Mitigation, response, and recovery procedures identified through the formal risk assessment(s) are regularly trained and exercised, incorporating the physical security

Facilities: Structures and premises staffed on a day-to-day or around-the-clock basis, including Emergency Communications Centers/Public Safety Answering Points, police, fire, and emergency medical stations, and emergency operations centers.

Communications Infrastructure: Fixed structures and deployable platforms that shelter communications equipment, including tower and repeater sites, data centers, network hubs, and console systems.

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Training – the following question addresses your organization's <u>end user</u> training practices for emergency communications.

29) Select the responses that best characterize your organization's emergency communications training: (Select <u>one</u> response)

- No personnel have received training
- Personnel have received, at most, informal training
- Some personnel have received formal training
- Substantially all personnel have received formal and regular training

- **If "no personnel have received training" in your organization, <u>skip</u> to Question 30 on the next page.**
- **Otherwise, <u>answer</u> Questions 29a–c.**

29a) <u>Evaluations</u> of training are documented and assessed along with the changing operational environment, to adapt future training to address gaps and needs. (Select <u>one</u> response)

- Yes
- No

29b) Select the <u>topics</u> that are included in your organization's emergency communications training: (Select <u>all</u> that apply)

- National Incident Management System (NIMS) Incident Command System (ICS)
- Software training/refresher
- Communications Unit (COMU)
- Commonly used frequencies
- Equipment training/refresher
- Backup systems
- Cybersecurity
- Radio/device encryption
- Radio etiquette and terminology
- National Interoperability Field Operations Guide (NIFOG)

End User: Individuals receiving or transmitting information.

Personnel: Individuals responsible for communications installations, operations, and maintenance.

Informal Training: Training with no lesson plans or assessments of student performance; may be on-the-job training or educational materials.

Formal Training: Training that includes a lesson plan and an assessment of student performance, change or behavior; may be in a classroom or on-the-job.

Interoperability: Ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as authorized.

Priority Services: Government Emergency Telecommunications Service (GETS), WPS, TSP.

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Training – the following question addresses your organization's end user training practices for emergency communications.

- **If "no personnel have received training" in your organization, skip to Question 30.**
- **Otherwise, answer Questions 29c.**

29c) Select the external groups that are included in your organization's emergency communications training: (Select all that apply)

- Other public safety organizations in the same jurisdiction
- Other government organizations in the same jurisdiction that support public safety
- Other local governments
- State/territorial governments
- Tribal nations
- Federal departments/agencies
- NGOs/private sector
- International/cross-border entities
- None of the above

30) Are your organization's personnel adequately trained in: (For each row, select one response per column)

	For "day-to-day" situations?	For "out-of-the-ordinary" situations?
Operability	o Yes o No	o Yes o No
Interoperability	o Yes o No	o Yes o No
Continuity	o Yes o No	o Yes o No

Other Public Safety Organizations in the Same Jurisdiction: Other government agencies outside your own department (e.g., police department or sheriff's office, fire department, ECCs/PSAPs, emergency management, emergency medical service agency).

Other Government Organizations in the Same Jurisdiction That Support Public Safety: Other government agencies (e.g., public health, public works, transportation, information technology).

Nongovernmental Organizations (NGO)/Private Sector: Non-profit or for-profit organizations participating in public safety/emergency communications planning, use or reconstitution (e.g., nongovernmental organizations, utilities, auxiliary communications, communication service providers, equipment operators, transportation, food distribution, Volunteer Organizations Active in Disasters).

International/Cross-Border Entities: Foreign organizations (e.g., Canadian or Mexican organizations).

Personnel: Individuals responsible for communications installations, operations, and maintenance.

Operability: Ability to provide and maintain reliable communications functionality throughout the area of responsibility.

Interoperability: Ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as authorized.

Continuity: Ability to provide and maintain acceptable levels of communications during disruptions in operations.

Day-to-Day Situations: Situations within the general normal structure for an organization, including routine operations.

Out-of-the-Ordinary Situations: Situations that may stretch and/or overwhelm the abilities of an organization.

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Exercises – the following questions address your organization's exercises.

31) Does your organization participate in or conduct exercises? (Select one response)

- Yes
- No

- **If your organization DOES "participate in or conduct exercises," answer Questions 31a–c.**
- **If your organization DOES NOT "participate in or conduct exercises," skip to Question 31d on the next page.**

31a) Select the types of capabilities included as part of the exercises in which your organization either participates or conducts: (Select all that apply)

- Communications operability (voice)
- Communications operability (data)
- Communications interoperability (voice)
- Communications interoperability (data)
- Communications continuity (voice)
- Communications continuity (data)
- Cyber incident response and recovery
- Radio/device encrypted interoperability
- Social media
- None of the above

31b) Select the types of roles included as part of the exercises in which your organization either participates or conducts: (Select all that apply)

- Auxiliary Communications (AUXCOMM)
- Incident Tactical Dispatch (INTD)
- Communications Unit Leader (COML)
- Communications Unit Technician (COMT)
- Communications Coordinator (COMC)
- IT Service Unit Leader (ITSL)
- Mobile command post/mobile communications center
- None of the above

31c) Select the statement that best characterizes how your organization evaluates communications as an exercise objective: (Select one response)

- Communications is not an exercise objective
- Communications is not evaluated
- Communications is evaluated but not documented
- Communications is evaluated and documented
- Communications is evaluated and documented in accordance with the Homeland Security Exercise Evaluation Program (HSEEP)

Interoperability: Ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as authorized.

Continuity: Ability to provide and maintain acceptable levels of communications during disruptions in operations.

Auxiliary Communications (AUXCOMM): Backup emergency radio communications provided by volunteers who support public safety and emergency response professionals and their agencies.

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Exercises – the following questions address your organization's exercises.

- **If your organization DOES NOT "participate in or conduct exercises," answer Question 31d.**
- **Otherwise, skip to Question 32.**

31d) My organization does not participate in exercises because it has: (Select all that apply)

- No personnel for exercise coordination
- Chronically low staffing levels
- No funding available to participate in exercises sponsored by other organizations
- No funding available to backfill personnel attending exercises
- Insufficient overtime funding to allow staff to participate in exercises conducted by my organization
- Insufficient overtime funding to allow staff to participate in exercises conducted by other organizations
- Limited exercises opportunities
- Competing organizational priorities
- None of the above

---

32) Complete this sentence: "My organization ___________ emergency communications-focused exercises." (Select one response)

- Does not participate in or conduct
- Participates in
- Conducts
- Participates in and conducts

32a) Select the types of emergency communications-focused exercises your organization participates in or conducts: (Select all that apply)

- Simulations
- Equipment tests and/or drills
- Seminars/workshops
- Tabletops
- Functional
- Full-scale

Personnel: Individuals responsible for communications installations, operations, and maintenance.

Exercises – the following questions address your organization's emergency communications-focused exercises.

- o **If your organization does not "participate in or conduct emergency communications-focused exercises," skip to Question 33 on page 30.**
- o **Otherwise, answer Questions 32b-g.**

32b) The emergency communications-focused simulations our organization participates in or conducts include: (Select all that apply)

- Other public safety organizations in the same jurisdiction
- Other government organizations in the same jurisdiction that support public safety
- Other local governments
- State/territorial governments
- Tribal nations
- Federal departments/agencies
- NGOs/private sector
- International/cross-border entities
- My organization does not participate in or conduct simulations

32c) The emergency communications-focused equipment tests and/or drills our organization participates in or conducts include: (Select all that apply)

- Other public safety organizations in the same jurisdiction
- Other government organizations in the same jurisdiction that support public safety
- Other local governments
- State/territorial governments
- Tribal nations
- Federal departments/agencies
- NGOs/private sector
- International/cross-border entities
- My organization does not participate in or conduct equipment tests and/or drills

Other Public Safety Organizations in the Same Jurisdiction: Other government agencies outside your own department (e.g., police department or sheriff's office, fire department, ECCs/PSAPs, emergency management, emergency medical service agency).

Other Government Organizations in the Same Jurisdiction That Support Public Safety: Other government agencies (e.g., public health, public works, transportation, information technology).

Nongovernmental Organizations (NGO)/Private Sector: Non-profit or for-profit organizations participating in public safety/emergency communications planning, use or reconstitution (e.g., nongovernmental organizations, utilities, auxiliary communications, communication service providers, equipment operators, transportation, food distribution, Volunteer Organizations Active in Disasters)

International/Cross-Border Entities: Foreign organizations (e.g., Canadian or Mexican organizations).

Exercises – the following questions address your organization's emergency communications-focused exercises.

- **If your organization does not "participate in or conduct emergency communications-focused exercises," skip to Question 33 on page 30.**
- **Otherwise, answer Questions 32d-g.**

32d) The emergency communications-focused seminars/workshops our organization participates in or conducts include: (Select all that apply)

- Other public safety organizations in the same jurisdiction
- Other government organizations in the same jurisdiction that support public safety
- Other local governments
- State/territorial governments
- Tribal nations
- Federal departments/agencies
- NGOs/private sector
- International/cross-border entities
- My organization does not participate in or conduct seminars/workshops

32e) The emergency communications-focused tabletop exercises our organization participates in or conducts include: (Select all that apply)

- Other public safety organizations in the same jurisdiction
- Other government organizations in the same jurisdiction that support public safety
- Other local governments
- State/territorial governments
- Tribal nations
- Federal departments/agencies
- NGOs/private sector
- International/cross-border entities
- My organization does not participate in or conduct tabletop exercises

Other Public Safety Organizations in the Same Jurisdiction: Other government agencies outside your own department (e.g., police department or sheriff's office, fire department, ECCs/PSAPs, emergency management, emergency medical service agency).

Other Government Organizations in the Same Jurisdiction That Support Public Safety: Other government agencies (e.g., public health, public works, transportation, information technology).

Nongovernmental Organizations (NGO)/Private Sector: Non-profit or for-profit organizations participating in public safety/emergency communications planning, use or reconstitution (e.g., nongovernmental organizations, utilities, auxiliary communications, communication service providers, equipment operators, transportation, food distribution, Volunteer Organizations Active in Disasters)

International/Cross-Border Entities: Foreign organizations (e.g., Canadian or Mexican organizations).

Exercises – the following question addresses your organization's emergency communications-focused exercises.

- o **If your organization does not "participate in or conduct emergency communications-focused exercises," skip to Question 33 on the next page.**
- o **Otherwise, answer Questions 32f-g.**

32f) The emergency communications-focused functional exercises our organization participates in or conducts include: (Select all that apply)

- Other public safety organizations in the same jurisdiction
- Other government organizations in the same jurisdiction that support public safety
- Other local governments
- State/territorial governments
- Tribal nations
- Federal departments/agencies
- NGOs/private sector
- International/cross-border entities
- My organization does not participate in or conduct functional exercises

32g) The emergency communications-focused full-scale exercises our organization participates in or conducts include: (Select all that apply)

- Other public safety organizations in the same jurisdiction
- Other government organizations in the same jurisdiction that support public safety
- Other local governments
- State/territorial governments
- Tribal nations
- Federal departments/agencies
- NGOs/private sector
- International/cross-border entities
- My organization does not participate in or conduct full-scale exercises

Other Public Safety Organizations in the Same Jurisdiction: Other government agencies outside your own department (e.g., police department or sheriff's office, fire department, ECCs/PSAPs, emergency management, emergency medical service agency).

Other Government Organizations in the Same Jurisdiction That Support Public Safety: Other government agencies (e.g., public health, public works, transportation, information technology).

Nongovernmental Organizations (NGO)/Private Sector: Non-profit or for-profit organizations participating in public safety/emergency communications planning, use or reconstitution (e.g., nongovernmental organizations, utilities, auxiliary communications, communication service providers, equipment operators, transportation, food distribution, Volunteer Organizations Active in Disasters)

International/Cross-Border Entities: Foreign organizations (e.g., Canadian or Mexican organizations).

Exercises – the following questions address your organization's exercises.

33) Have exercises adequately prepared your organization's personnel to achieve: (For each row, select one response per column)

	For "day-to-day" situations?	For "out-of-the-ordinary" situations?
Operability	o Yes o No	o Yes o No
Interoperability	o Yes o No	o Yes o No
Continuity	o Yes o No	o Yes o No

Usage — the following questions address the usage of your organization's emergency communications capabilities.

34) Select the emergency communications capabilities that are used or tested: (For each row, select all that apply)

Capabilities	For "day-to-day" situations	For "out-of-the-ordinary" situations	With personnel beyond our organization	In accordance with SOPs/SOGs
Primary voice	□	□	□	□
Primary data	□	□	□	□
Voice interoperability	□	□	□	□
Data interoperability	□	□	□	□
Backup voice	□	□	□	□
Backup data	□	□	□	□
Alerts and warnings	□	□	□	□

Personnel: Individuals responsible for communications installations, operations, and maintenance.

Operability: Ability to provide and maintain reliable communications functionality throughout the area of responsibility.

Interoperability: Ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as authorized.

Continuity: Ability to provide and maintain acceptable levels of communications during disruptions in operations.

Day-to-Day Situations: Situations within the general normal structure for an organization, including routine operations.

Out-of-the-Ordinary Situations: Situations that may stretch and/or overwhelm the abilities of an organization.

Usage — the following questions address the usage of your organization's emergency communications capabilities.

35) Select the response that best characterizes whether your organization uses Telecommunications Service Priority (TSP) for <u>restoration</u> or <u>priority provisioning</u> of critical telecommunications services: (Select <u>one</u> response)

- No policy for use has been established
- No, as our organization is unaware of this program
- No, the fees are cost prohibitive
- No, will only use this service for priority provisioning of new services
- Yes, but only some critical circuits/services are registered for priority restoration
- Yes, all critical voice, video, and data circuits/services are registered for priority restoration
- Yes, all critical voice, video, and data circuits/services are registered for priority restoration and the organization is aware and proficient in priority provisioning
- None of the above

36) Select the responses that best characterize your organization's emergency communications <u>resource capacity</u>: (For <u>each row</u>, select <u>one</u> response)

Communications Resource	Insufficient for day-to-day situations	Sufficient for day-to-day situations but not for out-of-the-ordinary situations	Sufficient for day-to-day and most out-of-the-ordinary situations	Sufficient for almost all situations, including those requiring resources beyond our organization
Primary voice	□	□	□	□
Primary data	□	□	□	□
Voice interoperability	□	□	□	□
Data interoperability	□	□	□	□
Backup voice	□	□	□	□
Backup data	□	□	□	□
Alerts and warnings	□	□	□	□

Telecommunications Service Priority: A CISA program that authorizes National Security and Emergency Preparedness organizations to receive priority treatment for vital voice and data circuits or other telecommunications services. See https://www.cisa.gov/about-pts

Day-to-Day Situations: Situations within the general normal structure for an organization, including routine operations.

Out-of-the-Ordinary Situations: Situations that may stretch and/or overwhelm the abilities of an organization.

Capacity: Upper bound on the rate at which information can be reliably transmitted over a communications channel.

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Usage — the following questions address the usage of your organization's emergency communications capabilities.

37) Select the responses that best characterize how often your organization uses or deploys the following: (For each row, select one response)

	Never	As needed	Semi-annually	Quarterly	Monthly	Daily
Interoperability solutions – voice	□	□	□	□	□	□
Interoperability solutions – data	□	□	□	□	□	□
Communications Unit Leader (COML)	□	□	□	□	□	□
Communications Unit Technician (COMT)	□	□	□	□	□	□
IT Service Unit Leader (ITSL)	□	□	□	□	□	□
Incident Tactical Dispatcher (INTD)	□	□	□	□	□	□
Auxiliary Communications (AUXCOMM) Operator (e.g., Amateur Radio Operator, Auxiliary Communications Operator)	□	□	□	□	□	□
Incident Communications Manager (INCM)	□	□	□	□	□	□

38) Are your organization's end users proficient in using emergency communications capabilities to achieve: (For each row, select one response per column)

	For "day-to-day" situations?	For "out-of-the-ordinary" situations?
Operability	o Yes o No	o Yes o No
Interoperability	o Yes o No	o Yes o No
Continuity	o Yes o No	o Yes o No

Auxiliary Communications (AUXCOMM): Backup emergency radio communications provided by volunteers who support public safety and emergency response professionals and their agencies.

End User: Individuals receiving or transmitting information.

Operability: Ability to provide and maintain reliable communications functionality throughout the area of responsibility.

Interoperability: Ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as authorized.

Continuity: Ability to provide and maintain acceptable levels of communications during disruptions in operations.

Day-to-Day Situations: Situations within the general normal structure for an organization, including routine operations

Out-of-the-Ordinary Situations: Situations that may stretch and/or overwhelm the abilities of an organization.

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Equipment — the following questions address the technology systems your organization uses.

39) Select the responses that characterize the technology systems your organization uses, regardless of whether the systems are owned, shared, or subscription-based: (Select all that apply)

- Land Mobile Radio (LMR) system
- 4G/Long-Term Evolution (LTE) system
- 5G system
- Satellite system
- High Frequency (HF) Radio (Auxiliary Communications [AUXCOMM]/SHAred RESources [SHARES]/FEMA National Radio System [FNARS])
- Paging system
- WiFi
- Legacy cellular system (2nd Generation/3rd Generation)
- Wireline/landline (e.g., fiber, copper, cable, optical)
- Microwave backhaul
- 911 telephony (e.g., basic, enhanced, Next Generation 911 [NG911])

- **If your organization uses a Land Mobile Radio (LMR) system, regardless of whether the system is owned, shared, or subscription-based, answer Questions 39a1-9 based on the LMR system your organization uses most often for interoperability.**
- **If not, skip to Question 39b1 on page 36.**

39a1) The primary LMR system used by my organization is: (Select all that apply)

- Used for voice
- Used for video
- Used for data
- Used for voice interoperability
- Used for data interoperability

39a2) The primary LMR system used by my organization supports: (Select all that apply)**:**

- Day-to-day situations with intervention
- Day-to-day situations without intervention
- Out-of-the-ordinary situations with intervention
- Out-of-the-ordinary situations without intervention

Primary: The system your organization uses most often for interoperability.

Intervention: The system requires assistance beyond first responder operating procedures (e.g., must get patch through dispatcher/telecommunicator, must be authorized by a third party).

Day-to-Day Situations: Situations within the general normal structure for an organization, including routine operations

Out-of-the-Ordinary Situations: Situations that may stretch and/or overwhelm the abilities of an organization.

Equipment — the following questions address the technology systems your organization uses.

- **If your organization uses a Land Mobile Radio (LMR) system, regardless of whether the system is owned, shared, or subscription-based, answer Questions 39a3-9 based on the LMR system your organization uses most often for interoperability.**
- **Otherwise, skip to Question 39b1 on page 36.**

39a3) The primary LMR system used by my organization is: (Select one response)

- Independently owned and operated (e.g., single jurisdiction system) and used exclusively by our organization
- Part of a communications system that serves multiple public safety and/or public service organizations in our jurisdiction
- Part of a multi-jurisdictional shared system
- Part of a statewide shared system
- A commercial, subscription-based service

- **If your organization's primary LMR system is "a commercial, subscription-based service," skip to Question 39a6 on the next page.**
- **Otherwise, answer Questions 39a4-5.**

39a4) The primary LMR system used by my organization is: (Select one response)

- 0-1 year old
- 2 – 5 years old
- 6 – 10 years old
- Over 10 years old
- Don't know

39a5) The primary LMR system used by my organization is planned to be replaced or significantly upgraded: (Select one response)

- Within 1 year
- Within 5 years
- Within 6 – 10 years
- In more than 10 years
- Don't know

Primary: The system your organization uses most often for interoperability.

Equipment — the following questions address the technology systems your organization uses.

39a6) Select the response that best characterizes the network architecture of your organization's primary LMR system: (Select one response)

- Conventional (not trunked)
- Trunked
- Both

- **If your organization's primary LMR system network architecture is "conventional (not trunked)," skip to Question 39a8.**
- **Otherwise, answer Question 39a7.**

39a7) Does your organization's primary LMR system comply with Project 25 (P25) standards (i.e., a P25-compliant system)? (Select one response)

- Yes, Phase 1 (frequency division multiple access [FDMA] only) system
- Yes, Phase 2 (time division multiple access [TDMA] only) system
- Yes, both Phase 1 and 2 (FDMA and TDMA)
- No
- Don't know

39a8) Is the primary LMR system used by your organization interoperable with the Long-Term Evolution (LTE) system used by your organization? (Select one response)

- Yes
- No
- My organization does not use LTE

- **If your organization uses an interoperable LTE/LMR system, regardless of whether the system is owned, shared, or subscription-based, answer Question 39a9.**
- **If not, skip to Question 39b1 on the next page.**

39a9) My organization's LTE/LMR system interoperability is enabled by: (Select one response)

- P25 standards-based Inter-RF Subsystem Interface (ISSI)/Console Subsystem Interface (CSSI)
- Applications-based solution
- Proprietary interworking function
- Interworking Function (IWF)
- Don't know

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Equipment — the following questions address the technology systems your organization uses.

39a10) Select the responses that best characterize the current state of your organization's LMR encryption capabilities: (Select all that apply)

- Proprietary/non-standard
- Proprietary/non-standard transitioning to Advanced Encryption Standard (AES)
- Data Encryption Standard (DES) (including all derivatives)
- DES transitioning to AES
- AES
- AES actively expanding the number of encrypted talkgroups and/or channels
- Link Layer Encryption (LLE) (Applies to Trunked Systems Only)
- Over-the-Air Rekeying (OTAR)
- Procuring Multi-Key Subscriber devices
- None
- Don't know

39a11) Select the response that best characterize your organization's timeline for LMR encryption transition to AES only capabilities: (Select one response)

- No plans to transition to AES
- Planning initiated, no specific timeline for implementation
- Within 1 year
- Within 5 years
- Within 6 – 10 years
- In more than 10 years
- Don't know

Proprietary Encryption/Non-Standard: Encryption algorithms that are not publicly known and/or **not** accredited by the National Institute of Standards and Technology Standard Institute (NIST) or other technical Standards Development Organizations

Data Encryption Standard (DES): A deprecated encryption algorithm that was originally developed in 1971 and accepted as the approved Federal Encryption Standard in 1976. NIST withdrew its approval DES in 2005.

Advanced Encryption Standard (AES). The current Federal Standard for encryption as promulgated by NIST. AES is a built-in feature of P25 standards compliant LMR equipment and is considered the de facto standard for encryption.

Link Layer Authentication: P25 that offers additional protection against unauthorized system access. The link layer authentication standard defines a challenge and response protocol, incorporating a 129-bit AES authentication key, that allows the radio system infrastructure and/or subscriber radio to authenticate itself before service is granted.

Over-the-Air-Rekeying (OTAR): OTAR remotely (i.e., over-the-air) updates encryption keys and other key materials and dramatically simplifies the process of rekeying subscriber radios in the field. It removes requirements to physically touch each radio to load keys with a key-loader. Notwithstanding, OTAR still has a degree of administrative overhead to locate and follow-up on subscriber radios that were not successfully rekeyed.

Multikey Subscriber Device: LMR mobile and portable subscriber radios that support more than a single encryption key. Multi-key devices are necessary for OTAR operations.

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Equipment — the following questions address the technology systems your organization uses.

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

- **If your organization uses a 4G/Long-Term Evolution (LTE) system, regardless of whether the system is owned, shared, or subscription-based, answer Questions 39b1-2.**
- **Otherwise, skip to Question 39c1.**

39b1) The 4G/LTE system used by my organization is: (Select all that apply)

- Used for voice
- Used for video
- Used for data
- Used for voice interoperability
- Used for data interoperability

39b2) The 4G/LTE system used by my organization is: (Select one response)

- Independently owned and operated (e.g., single jurisdiction system) and used exclusively by our organization
- Part of a communications system that serves multiple public safety and/or public service organizations in our jurisdiction
- Part of a multi-jurisdictional shared system
- Part of a statewide shared system
- A commercial, subscription-based service

- **If your organization uses a 5G system, regardless of whether the system is owned, shared, or subscription-based, answer Questions 39c1-2.**
- **Otherwise, skip to Question 39d1 on the next page.**

39c1) The 5G system used by my organization is: (Select all that apply)

- Used for voice
- Used for video
- Used for data
- Used for voice interoperability
- Used for data interoperability

39c2) The 5G system used by my organization is: (Select one response)

- Independently owned and operated (e.g., single jurisdiction system) and used exclusively by our organization
- Part of a communications system that serves multiple public safety and/or public service organizations in our jurisdiction
- Part of a multi-jurisdictional shared system
- Part of a statewide shared system
- A commercial, subscription-based service

Equipment — the following questions address the technology systems your organization uses.

- If your organization uses a High Frequency (HF) radio system, regardless of whether the system is owned, shared, or subscription-based, answer Questions 39d1-2.
- Otherwise, skip to Question 39e1 below.

39d1) The HF radio system used by my organization is: (Select one response)

- 0-1 year old
- 2 – 5 years old
- 6 – 10 years old
- Over 10 years old
- Don't know

39d2) The HF radio system used by my organization is planned to be replaced or significantly upgraded: (Select one response)

- Within 1 year
- Within 5 years
- Within 6 – 10 years
- In more than 10 years
- Don't know

- If your organization uses a 911 telephony system, regardless of whether the system is owned, shared, or subscription-based, answer Questions 39e1-4.
- Otherwise, skip to Question 40 on page 39.

39e1) The 911 system used by my organization is: (Select one response)

- 0-1 year
- 2 – 5 years
- 6 – 10 years
- Over 10 years old
- Don't know

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Equipment — the following questions address the technology systems your organization uses.

- **If your organization uses a 911 telephony system, regardless of whether the system is owned, shared, or subscription-based, answer Questions 39e2-4.**
- **Otherwise, skip to Question 40 on the next page.**

39e2) The 911 system used by my organization is planned to be replaced or significantly upgraded: (Select one response)

- Within 1 year
- Within 5 years
- Within 6 – 10 years
- In more than 10 years
- Don't know

39e3) The 911 system used by my organization accepts: (Select all that apply)

- Voice
- Texts
- Video
- Other data

39e4) Select the responses that best characterize the current state of your organization's 911 architecture: (Select all that apply)

- Basic
- Transitioning to Enhanced 911 (E911)
- E911
- Transitioning to Next Generation 911 (NG911)
- NG911: Emergency Services IP Network (ESInet) ready to receive 911 calls from the originating service providers via a Legacy Network Gateway
- NG911: ESInet ready to receive 911 calls in SIP (Session Initiation Protocol) format
- NG911: ESInet ready to receive 911 calls in NG911 format

Basic 911: Allows callers to reach the universal emergency telephone number; relies on caller and call taker communications with one another to identify the telephone and location from which caller is dialing.

Enhanced 911 (E911): Allows automatic number and location indications of caller delivered to call taker; enables call taker to send help even when caller is unable to communicate.

Next Generation 911 (NG911): Allows same information-sharing opportunities as E911, and enables caller the ability to use commercial communication devices to send voice, data, and video to Public Safety Answering Points (PSAPs).

Emergency Services IP Network (ESInet): A managed internet protocol (IP) network that is used for emergency services communications, and which can be shared by public safety agencies.

Session Initiation Protocol (SIP): An application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Equipment — the following questions address the capabilities your organization uses.

40) Select the responses that indicate the capabilities your organization currently uses, regardless of whether the capability is owned, shared, or subscription-based: (Select all that apply)

- Integrated Public Alert & Warning System (IPAWS)
- Emergency Alert System (EAS)
- Wireless Emergency Alerts (WEA)
- National Oceanic and Atmospheric Administration (NOAA) National Weather Service (NWS)
- Regional, state, local, tribal, and/or territorial alert, warning, and notification systems (e.g., reverse 911 systems, outdoor sirens, digital signs, short message service/mass email)
- Sensor-based alert systems (e.g., gunshot detection, flooding, earthquake, hurricane, volcano)
- Internet of Things devices (e.g., smart clothing, smartphones, smart watches)
- Unmanned aerial systems (e.g., drones)
- Mission critical push-to-talk applications
- Cloud computing
- Artificial intelligence
- Nationwide Public Safety Broadband Network (NPSBN)/FirstNet
- Other broadband service provider
- Citizens Broadband Radio Service (CBRS)
- File download/upload from/to servers
- Web sessions to organization/public sites
- Third-party texting/chat applications
- Software-as-a-service
- CISA cybersecurity resources
- None of the above

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions

Equipment — the following question addresses the CISA cybersecurity resources your organization uses.

- **If your organization uses "CISA cybersecurity resources," answer Question 40a.**
- **Otherwise, skip to Question 41 on the next page.**

40a) Select the CISA cybersecurity resources your organization uses in its cybersecurity planning and implementation: (Select all that apply)

- Advanced Malware Analysis Center (AMAC) Services
- Assessment Evaluation and Standardization Program (AES)
- CISA Central
- Cyber Essentials
- Cyber Infrastructure Survey
- Cyber Resiliency Review (CRR)
- Cybersecurity Advisory (CSA) Program
- Cybersecurity Assessment and Risk Management Approach
- Cybersecurity Evaluation Tool (CSET®)
- Continuous Diagnostics and Mitigation (CDM)
- Continuous Phishing Campaign Assessment (CON-PCA)
- Enhanced Cybersecurity Services (ECS)
- External Dependencies Management (EDM) Assessment
- Federal Virtual Training Environment (FedVTE)
- Hunt and Incident Response Team (HIRT) Services
- ICTAP 9-1-1/PSAP/LMR Cyber Assessment
- ICTAP 9-1-1/PSAP/LMR Cyber Awareness Course
- Joint Cyber Defense Collaborative (JCDC)
- Public Safety Communications and Cyber Resiliency Toolkit
- Remote Penetration Testing (RPT)
- Vulnerability/Cyber Hygiene Scanning
- Web Application Scanning
- Other CISA resources
- Other CISA-advertised public and private sector resources
- None of the above

Last Questions

41) My organization experienced the following emergency communications impacts as a result of the COVID-19 pandemic: (Select all that apply)

- Expanded/implemented remote work and telework options
- Expanded or opened backup facilities
- Established communications redundancy with neighboring jurisdictions
- Created non-emergency lines or hotlines to help divert COVID-19 related calls from 911 services
- Implemented operational changes based on federal, state, and/or local guidance
- Drafted new policies and procedures related to pandemic planning and response
- Updated existing policies and procedures related to pandemic planning and response
- Diverted funds to cover pandemic-related expenses (e.g., personal protective equipment, cleaning supplies)
- Adjusted budgets due to decreased funding from state and local revenues
- Delayed systems/network construction, maintenance, and/or upgrade projects
- Established/maintained communications capabilities for alternate care sites
- Increased cybersecurity posture and promoted cyber hygiene practices
- Ceased operations temporarily
- Experienced staffing below established minimum levels
- None of the above

42) Between 2018 and present, what was your organization's level of improvement in strengthening emergency communications: (For each row, select one response per column)

	For "day-to-day" situations?				For "out-of-the-ordinary" situations?			
	Regressed	None	Some	Significant	Regressed	None	Some	Significant
Operability	○	○	○	○	○	○	○	○
Interoperability	○	○	○	○	○	○	○	○
Continuity	○	○	○	○	○	○	○	○

Operability: Ability to provide and maintain reliable communications functionality throughout the area of responsibility.

Interoperability: Ability of emergency response providers and relevant government officials to communicate across jurisdictions, disciplines, and levels of government as needed and as authorized.

Continuity: Ability to provide and maintain acceptable levels of communications during disruptions in operations.

Day-to-Day Situations: Situations within the general normal structure for an organization, including routine operations.

Out-of-the-Ordinary Situations: Situations that may stretch and/or overwhelm the abilities of an organization.

Governance
SOPs/SOGs
Technology
Security
Training
Usage
Equipment
Last Questions