Homeland Security

2018 SAFECOM Nationwide Survey Results
National-Level Summary

August 2018

SAFECOM Nationwide Survey

- The *SAFECOM Nationwide Survey* (SNS) was a data collection initiative that the Department of Homeland Security Office of Emergency Communications (OEC) conducted from late 2017 thru March 2018 in order to enable the assessment of federal, state, local, tribal, and territorial governments in regards to emergency communications

- Results from the SNS support OEC's development of the *Nationwide Communications Baseline Assessment* (NCBA) in accordance with the *Homeland Security Act of 2002*, as amended (6 U.S.C. § 573(a))

- The SNS consisted of 38 questions from across the 5 elements of the *SAFECOM Interoperability Continuum,* as well as a Security element that accounted for equipment and cybersecurity

- The SNS results on the following slides are national-level results of a random sample of local-level public safety organizations (law enforcement, fire, EMS, and public safety answering points [PSAPs]) from across the Nation.
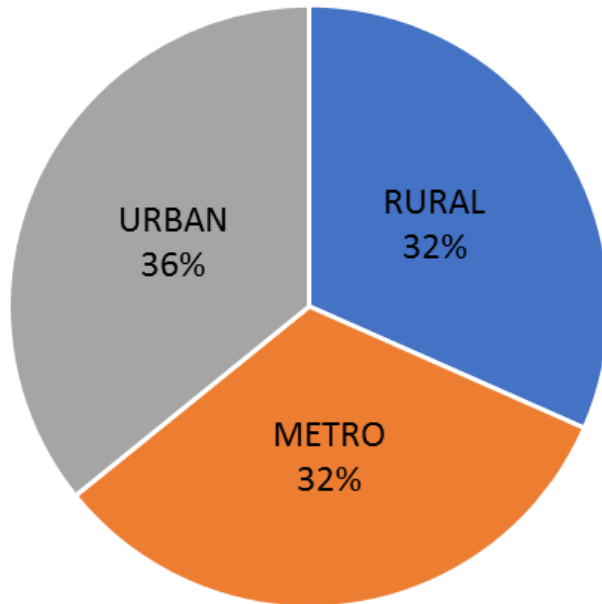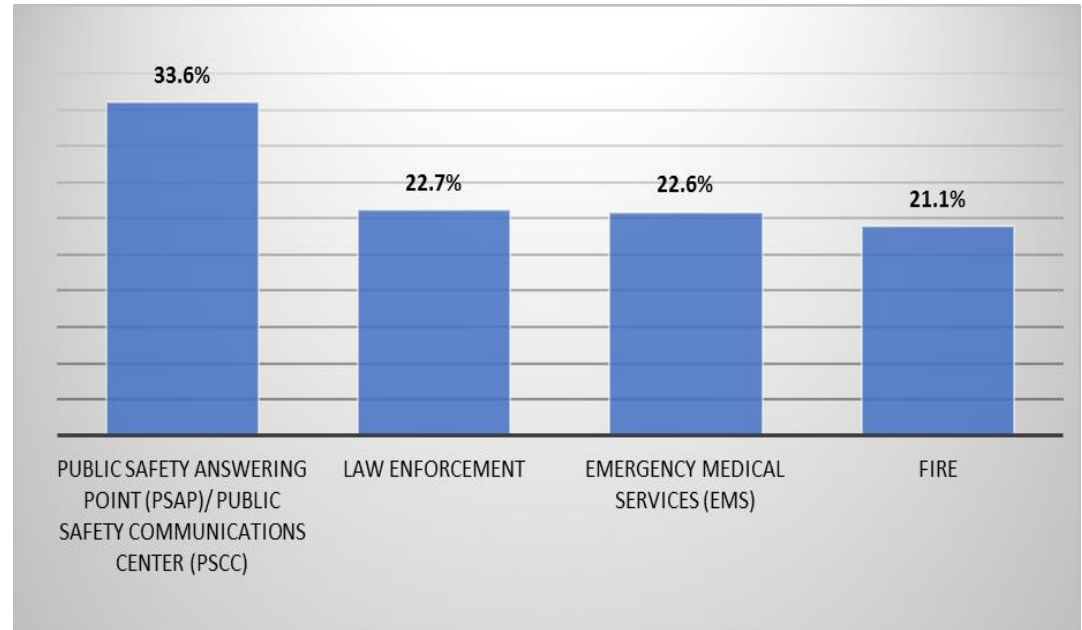
DEMOGRAPHICS

Geographic Environment

Geographic Representation of All Respondents

- URBAN 36%
- RURAL 32%
- METRO 32%

Discipline Representation of All Respondents

- PUBLIC SAFETY ANSWERING POINT (PSAP)/PUBLIC SAFETY COMMUNICATIONS CENTER (PSCC): 33.6%
- LAW ENFORCEMENT: 22.7%
- EMERGENCY MEDICAL SERVICES (EMS): 22.6%
- FIRE: 21.1%

Data Description

- There was a total of 2,738 local-level responses.
- The number of responses in the random sample from urban, metro, and rural areas are nearly equally sized
- All disciplines were well represented, and the majority of responses were from PSAPs/PSCCs
- Responses were weighted to ensure that survey representation from each discipline and geographic environment matched best estimates of their real-life distribution
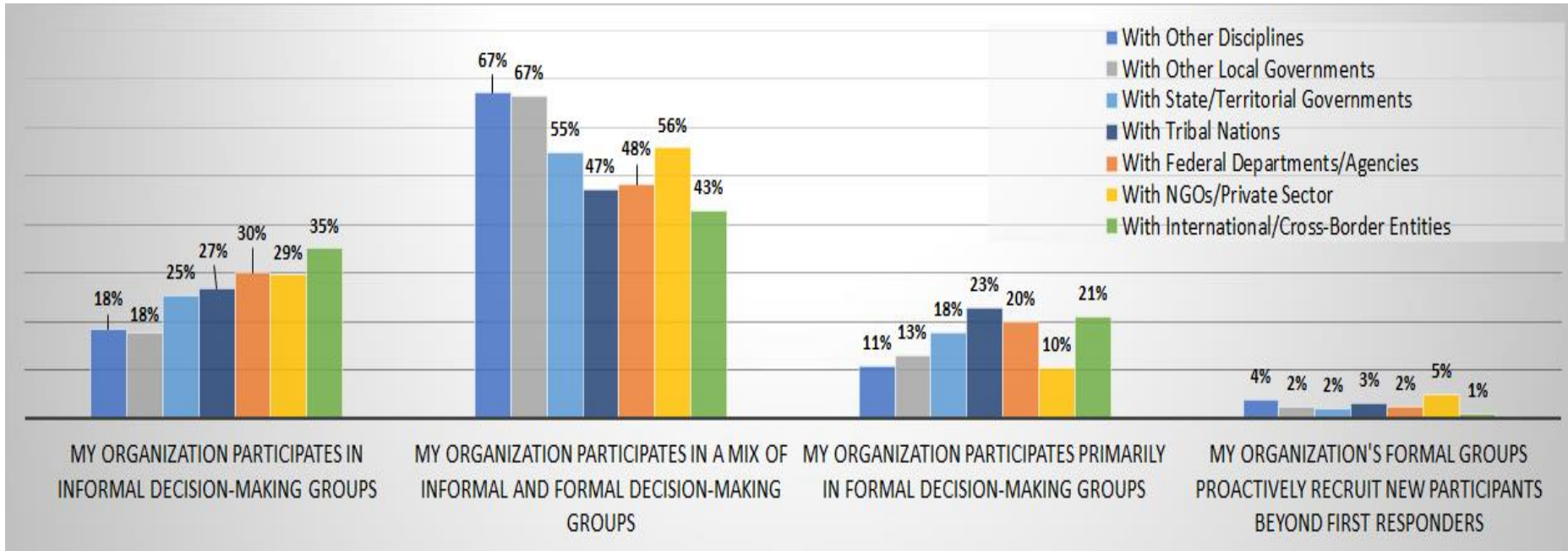
GOVERNANCE

Office of Emergency Communications

Decision-Making Groups

Characterization of an Organization's Involvement in Decision-Making Groups

Legend:
- With Other Disciplines
- With Other Local Governments
- With State/Territorial Governments
- With Tribal Nations
- With Federal Departments/Agencies
- With NGOs/Private Sector
- With International/Cross-Border Entities

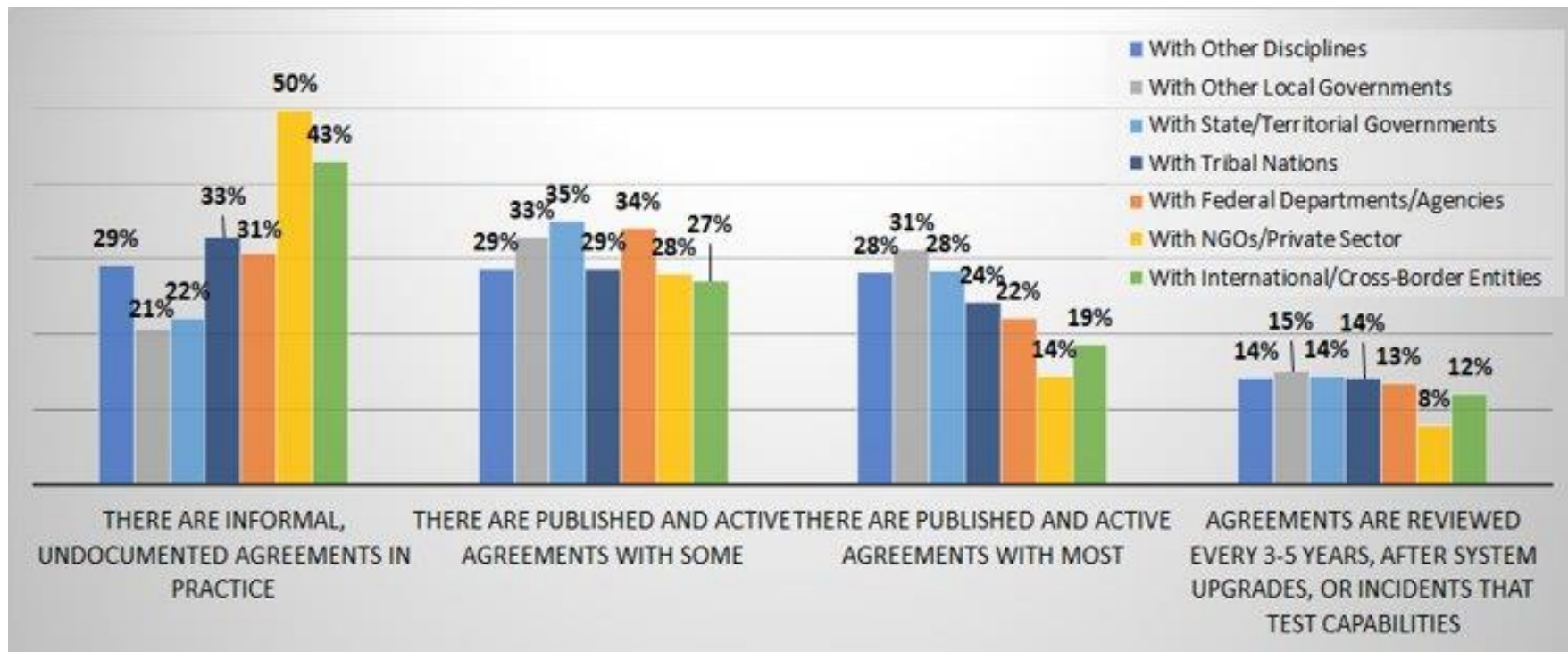|	With Other Disciplines	With Other Local Governments	With State/Territorial Governments	With Tribal Nations	With Federal Departments/Agencies	With NGOs/Private Sector	With International/Cross-Border Entities
MY ORGANIZATION PARTICIPATES IN INFORMAL DECISION-MAKING GROUPS	18%	18%	25%	27%	30%	29%	35%
MY ORGANIZATION PARTICIPATES IN A MIX OF INFORMAL AND FORMAL DECISION-MAKING GROUPS	67%	67%	55%	47%	48%	56%	43%
MY ORGANIZATION PARTICIPATES PRIMARILY IN FORMAL DECISION-MAKING GROUPS	11%	13%	18%	23%	20%	10%	21%
MY ORGANIZATION'S FORMAL GROUPS PROACTIVELY RECRUIT NEW PARTICIPANTS BEYOND FIRST RESPONDERS	4%	2%	2%	3%	2%	5%	1%

Data Description

- Most organizations report that their emergency communications governance structure is comprised of formal and informal decision making groups.
- Very few decision-making groups, in which organizations are involved, are proactively seeking new participants beyond first responders

Agreements[1]

Characterization of Agreements an Organization has Made

Legend:
- With Other Disciplines
- With Other Local Governments
- With State/Territorial Governments
- With Tribal Nations
- With Federal Departments/Agencies
- With NGOs/Private Sector
- With International/Cross-Border Entities

THERE ARE INFORMAL, UNDOCUMENTED AGREEMENTS IN PRACTICE: 29%, 21%, 22%, 33%, 31%, 50%, 43%

THERE ARE PUBLISHED AND ACTIVE AGREEMENTS WITH SOME: 29%, 33%, 35%, 29%, 34%, 28%, 27%

THERE ARE PUBLISHED AND ACTIVE AGREEMENTS WITH MOST: 28%, 31%, 28%, 24%, 22%, 14%, 19%

AGREEMENTS ARE REVIEWED EVERY 3-5 YEARS, AFTER SYSTEM UPGRADES, OR INCIDENTS THAT TEST CAPABILITIES: 14%, 15%, 14%, 14%, 13%, 8%, 12%
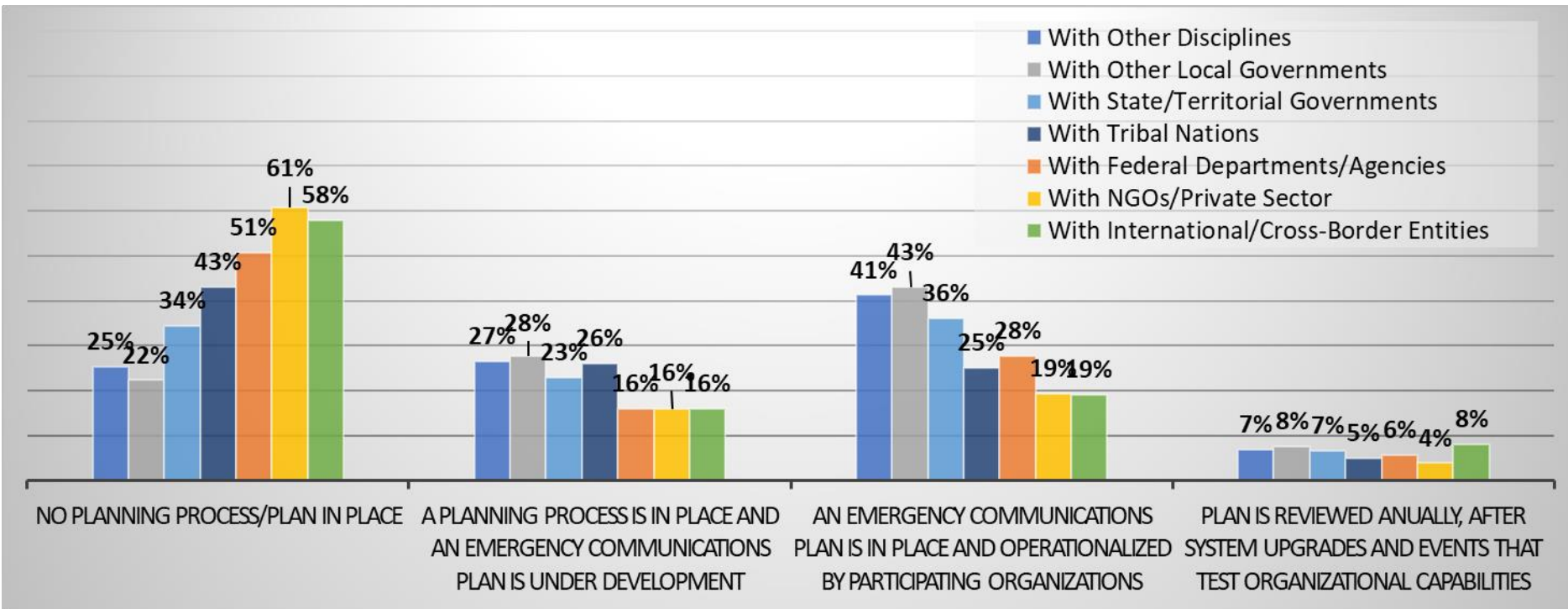
Data Description

- Less than half of organizations indicate they operate with informal, undocumented agreements with other organizations
- The majority of organizations have published and active agreements with some or most of the other organizations with which they interact, though few review them periodically

1 Graph data may not total to 100% due to data rounding or respondents' ability to select more than one answer option.

Homeland Security

Office of Emergency Communications

Strategic Planning Process

Characterization of an Organization's Strategic Planning Process

Legend:
- With Other Disciplines
- With Other Local Governments
- With State/Territorial Governments
- With Tribal Nations
- With Federal Departments/Agencies
- With NGOs/Private Sector
- With International/Cross-Border Entities

NO PLANNING PROCESS/PLAN IN PLACE: 25%, 22%, 34%, 43%, 51%, 61%, 58%

A PLANNING PROCESS IS IN PLACE AND AN EMERGENCY COMMUNICATIONS PLAN IS UNDER DEVELOPMENT: 27%, 28%, 23%, 26%, 16%, 16%, 16%

AN EMERGENCY COMMUNICATIONS PLAN IS IN PLACE AND OPERATIONALIZED BY PARTICIPATING ORGANIZATIONS: 41%, 43%, 36%, 25%, 28%, 19%, 19%

PLAN IS REVIEWED ANUALLY, AFTER SYSTEM UPGRADES AND EVENTS THAT TEST ORGANIZATIONAL CAPABILITIES: 7%, 8%, 7%, 5%, 6%, 4%, 8%

Data Description

- The majority of organizations have established a planning process and/or emergency communications plan with other disciplines and State/territorial/local governments
- Most have no planning process or plan in place with tribal nations or cross-border entities, and many have no planning process or plan in place with federal departments/agencies or non-governmental organizations
- Few organizations are reviewing their strategic planning annually, after upgrades and events that test capabilities
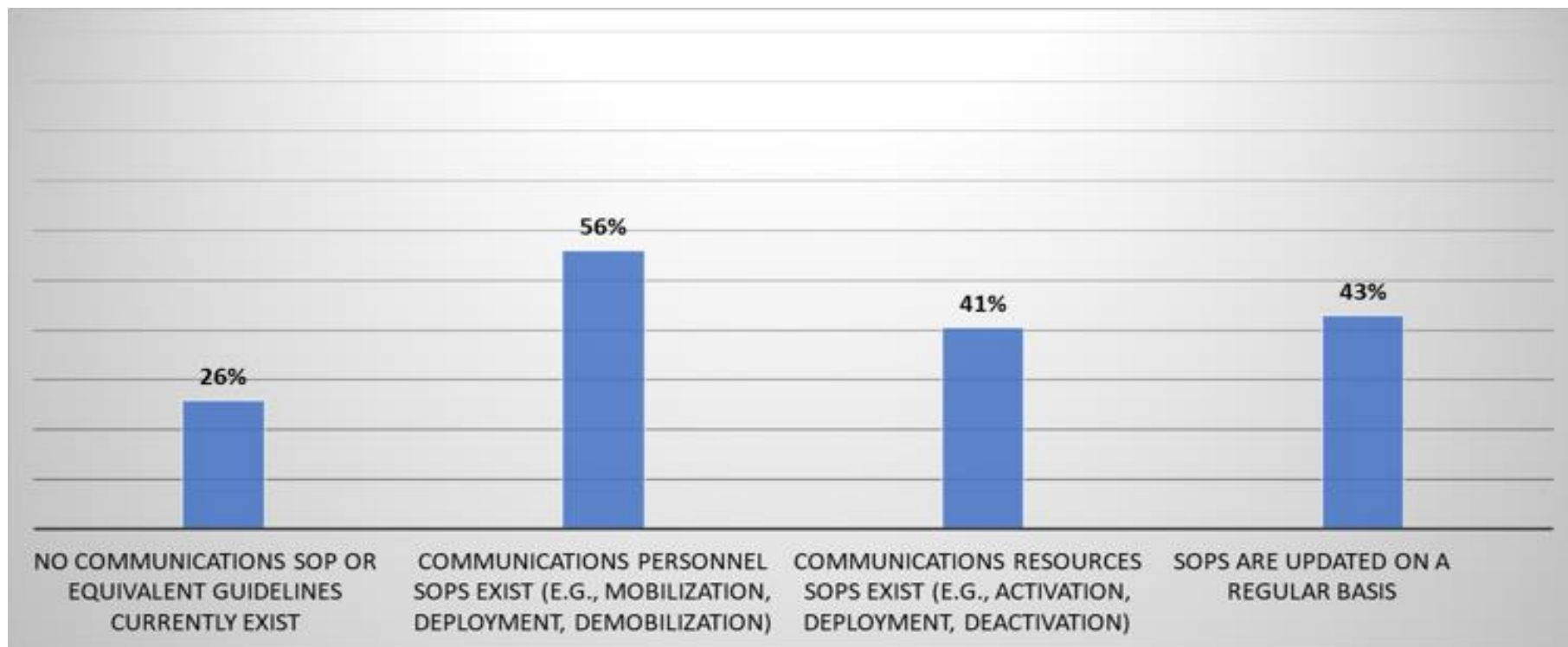
Homeland Security

Office of Emergency Communications

STANDARD OPERATING PROCEDURES

Homeland Security

Presence of SOPs

Presence and Type of Standard Operating Procedures

No Communications SOP or Equivalent Guidelines Currently Exist: 26%
Communications Personnel SOPs Exist (E.G., Mobilization, Deployment, Demobilization): 56%
Communications Resources SOPs Exist (E.G., Activation, Deployment, Deactivation): 41%
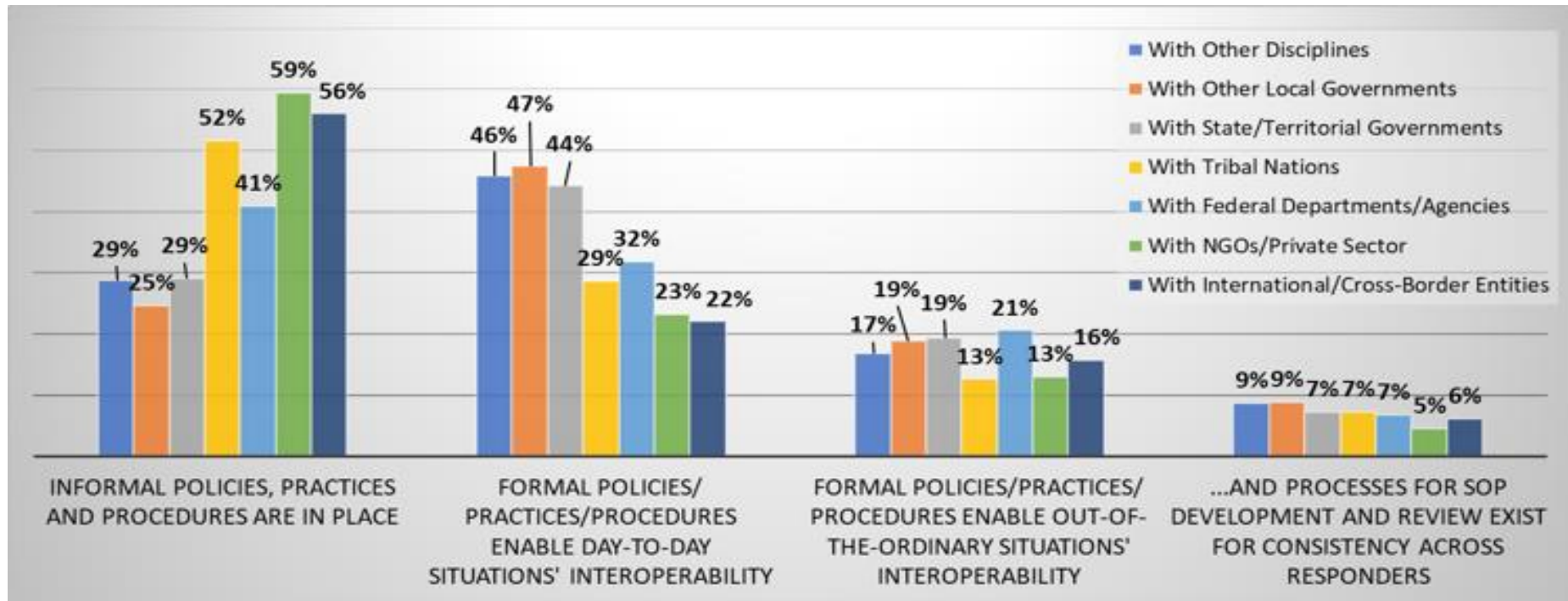**SOPs Are Updated On A Regular Basis:** 43%

Data Description

- Over a quarter of the organizations indicated having no communications SOPs or equivalent guidelines

Characterization of SOPs

Characterization of an Organization's Standard Operating Procedures

	Data Description

- Formal SOPs enable day-to-day or out-of-the-ordinary situations for most organizations' interactions with other disciplines (72%), local governments (75%) and State/territorial governments (70%)
- Many organizations still rely on informal SOPs for interactions with tribal nations, non-governmental organizations/private sector, and international/cross-border entities

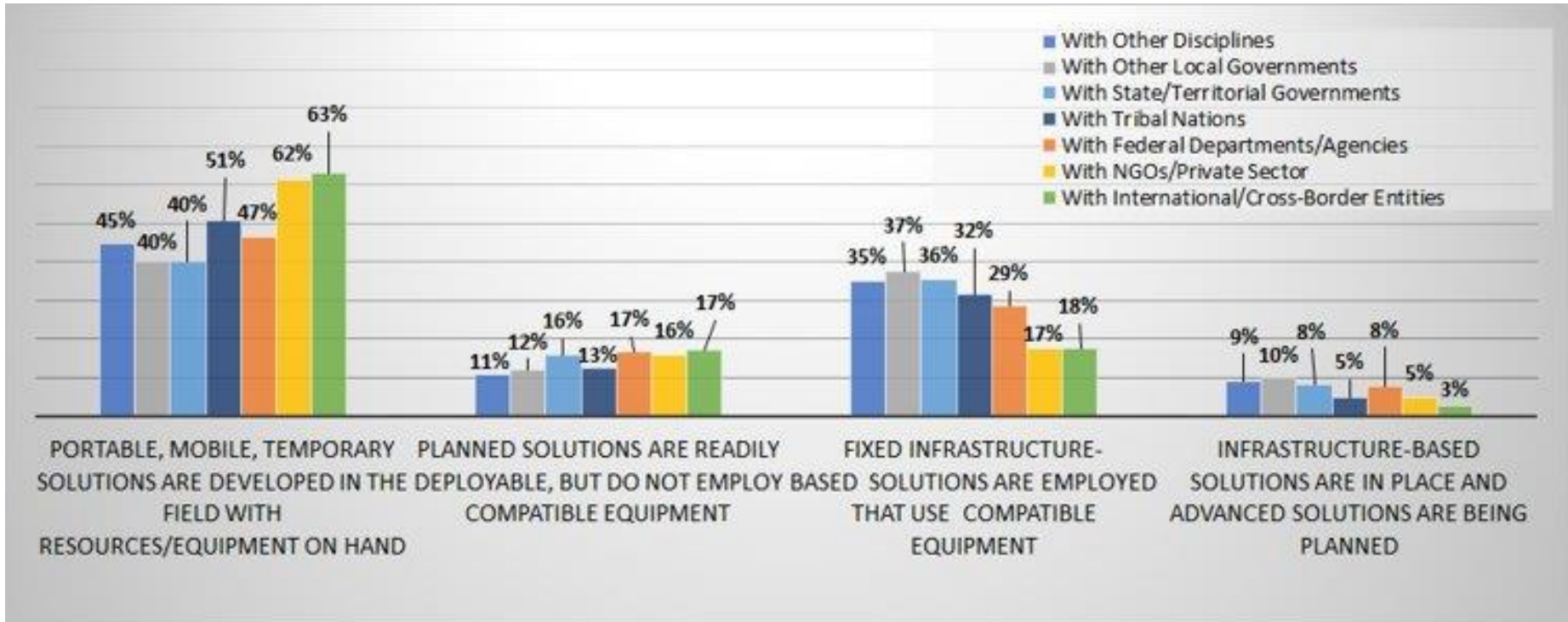Office of Emergency Communications

TECHNOLOGY

Solutions for Interoperability with Other Entities

Characterization of the Technology Systems Used by an Organization

Legend:
- With Other Disciplines
- With Other Local Governments
- With State/Territorial Governments
- With Tribal Nations
- With Federal Departments/Agencies
- With NGOs/Private Sector
- With International/Cross-Border Entities

PORTABLE, MOBILE, TEMPORARY SOLUTIONS ARE DEVELOPED IN THE FIELD WITH RESOURCES/EQUIPMENT ON HAND: 45%, 40%, 40%, 51%, 47%, 62%, 63%

PLANNED SOLUTIONS ARE READILY DEPLOYABLE, BUT DO NOT EMPLOY COMPATIBLE EQUIPMENT: 11%, 12%, 16%, 13%, 17%, 16%, 17%

FIXED INFRASTRUCTURE-BASED SOLUTIONS ARE EMPLOYED THAT USE COMPATIBLE EQUIPMENT: 35%, 37%, 36%, 32%, 29%, 17%, 18%

INFRASTRUCTURE-BASED SOLUTIONS ARE IN PLACE AND ADVANCED SOLUTIONS ARE BEING PLANNED: 9%, 10%, 8%, 5%, 8%, 5%, 3%
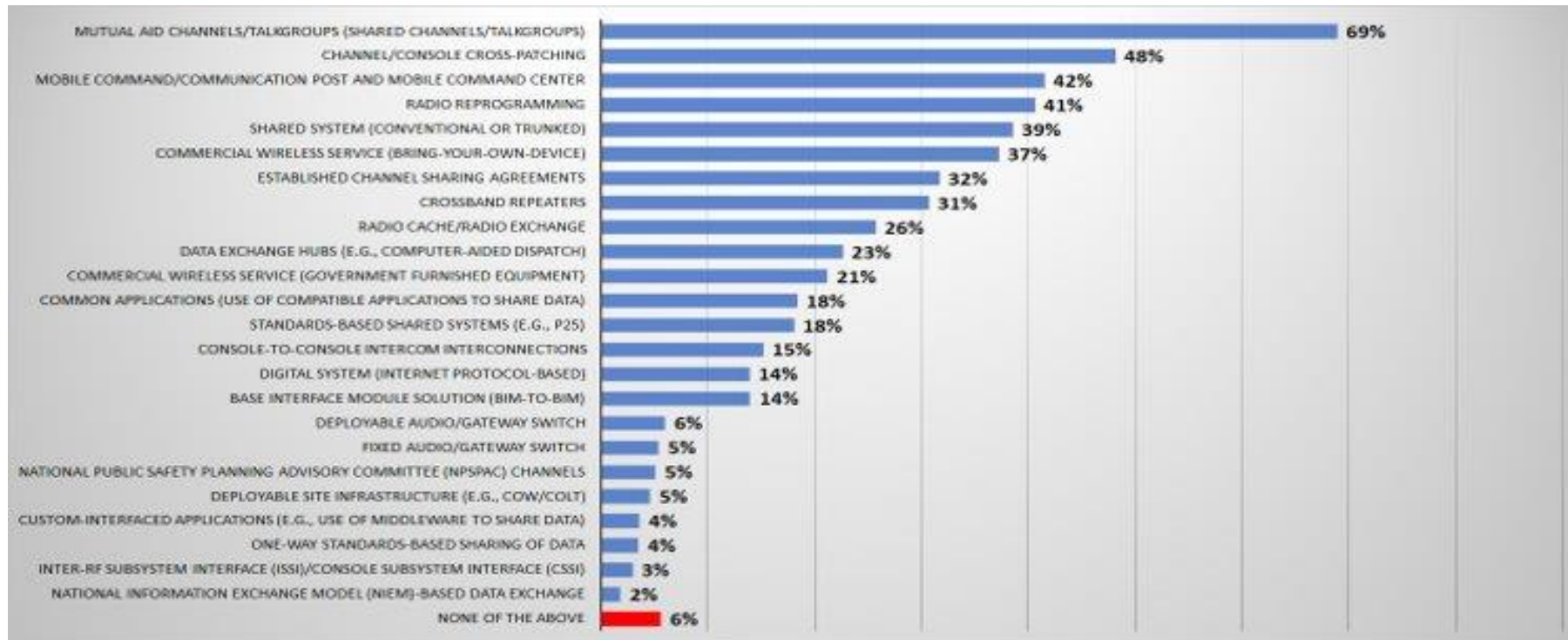
Data Description

- 45% of organizations said they achieve interoperability with other disciplines in the field with the resources/equipment on hand
- 44% of organizations indicate they achieve interoperability with other disciplines with fixed infrastructure-based solutions with compatible equipment

Homeland Security

Interoperability Solutions

Interoperability Solutions in Use by Organizations

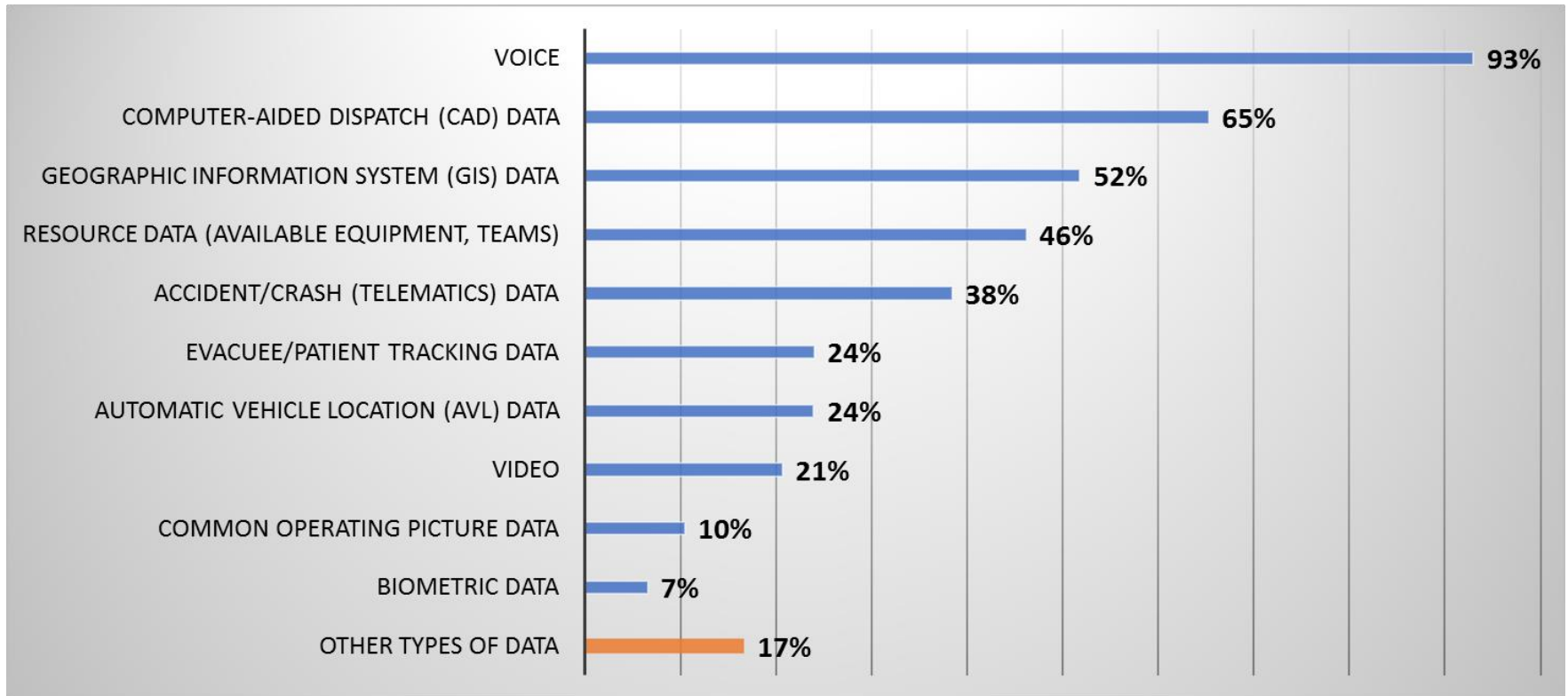| Solution	Percentage
MUTUAL AID CHANNELS/TALKGROUPS (SHARED CHANNELS/TALKGROUPS)	69%
CHANNEL/CONSOLE CROSS-PATCHING	48%
MOBILE COMMAND/COMMUNICATION POST AND MOBILE COMMAND CENTER	42%
RADIO REPROGRAMMING	41%
SHARED SYSTEM (CONVENTIONAL OR TRUNKED)	39%
COMMERCIAL WIRELESS SERVICE (BRING-YOUR-OWN-DEVICE)	37%
ESTABLISHED CHANNEL SHARING AGREEMENTS	32%
CROSSBAND REPEATERS	31%
RADIO CACHE/RADIO EXCHANGE	26%
DATA EXCHANGE HUBS (E.G., COMPUTER-AIDED DISPATCH)	23%
COMMERCIAL WIRELESS SERVICE (GOVERNMENT FURNISHED EQUIPMENT)	21%
COMMON APPLICATIONS (USE OF COMPATIBLE APPLICATIONS TO SHARE DATA)	18%
STANDARDS-BASED SHARED SYSTEMS (E.G., P25)	18%
CONSOLE-TO-CONSOLE INTERCOM INTERCONNECTIONS	15%
DIGITAL SYSTEM (INTERNET PROTOCOL-BASED)	14%
BASE INTERFACE MODULE SOLUTION (BIM-TO-BIM)	14%
DEPLOYABLE AUDIO/GATEWAY SWITCH	6%
FIXED AUDIO/GATEWAY SWITCH	5%
NATIONAL PUBLIC SAFETY PLANNING ADVISORY COMMITTEE (NPSPAC) CHANNELS	5%
DEPLOYABLE SITE INFRASTRUCTURE (E.G., COW/COLT)	5%
CUSTOM-INTERFACED APPLICATIONS (E.G., USE OF MIDDLEWARE TO SHARE DATA)	4%
ONE-WAY STANDARDS-BASED SHARING OF DATA	4%
INTER-RF SUBSYSTEM INTERFACE (ISSI)/CONSOLE SUBSYSTEM INTERFACE (CSSI)	3%
NATIONAL INFORMATION EXCHANGE MODEL (NIEM)-BASED DATA EXCHANGE	2%
NONE OF THE ABOVE	6%

Data Description

- The majority of organizations (94%) indicated they are using at least one communications interoperability solution listed
- Mutual aid channels (69%), cross-patching (48%), and mobile command posts (42%) were most popular
- Organizations indicated an emerging use of data interoperability solutions, such as data exchange hubs (23%) and common applications (18%)

Homeland Security

Office of Emergency Communications

Types of Information Exchanged

Types of Information Exchanged between Organizations

Type	Percentage
VOICE	93%
COMPUTER-AIDED DISPATCH (CAD) DATA	65%
GEOGRAPHIC INFORMATION SYSTEM (GIS) DATA	52%
RESOURCE DATA (AVAILABLE EQUIPMENT, TEAMS)	46%
ACCIDENT/CRASH (TELEMATICS) DATA	38%
EVACUEE/PATIENT TRACKING DATA	24%
AUTOMATIC VEHICLE LOCATION (AVL) DATA	24%
VIDEO	21%
COMMON OPERATING PICTURE DATA	10%
BIOMETRIC DATA	7%
OTHER TYPES OF DATA	17%

Data Description

- Almost all (93%) organizations are sharing voice
- Over half of organizations are sharing CAD or GIS data
- Only 21% of organizations are sharing video

Factors that Affect Ability to Communicate

Factors that Affect an Organizations Ability to Communicate

Legend: ■ Great Extent ■ Some Extent ■ Little Extent ■ None

Factor	Great Extent	Some Extent	Little Extent	None
POOR COVERAGE (IN-BUILDING)	30%	35%	26%	9%
UNPLANNED SYSTEM/EQUIPMENT FAILURE	30%	36%	28%	6%
POOR COVERAGE (OUTDOORS)	24%	34%	30%	12%
DEFERRED CAPITAL EXPENDITURES	20%	26%	24%	30%
EQUIPMENT FAILURE BEYOND THE CONTROL OF OUR ORG	15%	20%	33%	31%
INSUFFICIENT SYSTEM/EQUIPMENT REDUNDANCY	14%	23%	31%	32%
EXCESSIVE PLANNED DOWNTIME	14%	25%	40%	21%
INCOMPATIBILITY OF PROPRIETARY SYSTEMS/MODES/ALGORITHMS	13%	15%	28%	43%
SYSTEM CONGESTION (E.G., LIMITED SPECTRUM CAPACITY)	13%	25%	37%	26%
POOR SUBSCRIBER UNIT QUALITY	12%	19%	32%	38%
FREQUENCY INTERFERENCE	11%	25%	38%	25%
INSUFFICIENT ROUTE DIVERSITY	11%	16%	28%	45%
CYBERSECURITY DISRUPTION OR BREACH	10%	9%	25%	57%
DEFERRED MAINTENANCE	10%	21%	32%	38%
INSUFFICIENT SITE HARDENING	10%	16%	27%	48%
DIMINISHED SERVICE DUE TO ADDING USERS BEYOND OUR ORG	9%	13%	26%	53%

Data Description

- The majority of organizations (91%) report poor in-building coverage impacting to some extent their ability to communicate, and 88% report poor outdoor coverage impacting to some extent their ability to communicate
- Over 30% of organizations reported unplanned system failures greatly affect their organization's ability to communicate
- Over 44% of organizations identify a cybersecurity disruption/breach as impacting their ability to communicate

Homeland Security

Office of Emergency Communications

TRAINING & EXERCISES

Homeland
Security

Training

Characterization of an Organization's Emergency Communications Training

Training Evaluations

- Evaluations are documented and assessed along with the changing operational environment, to adapt future training to address gaps and needs
- Evaluations are NOT documented and assessed along with the changing operational environment, to adapt future training to address gaps and needs
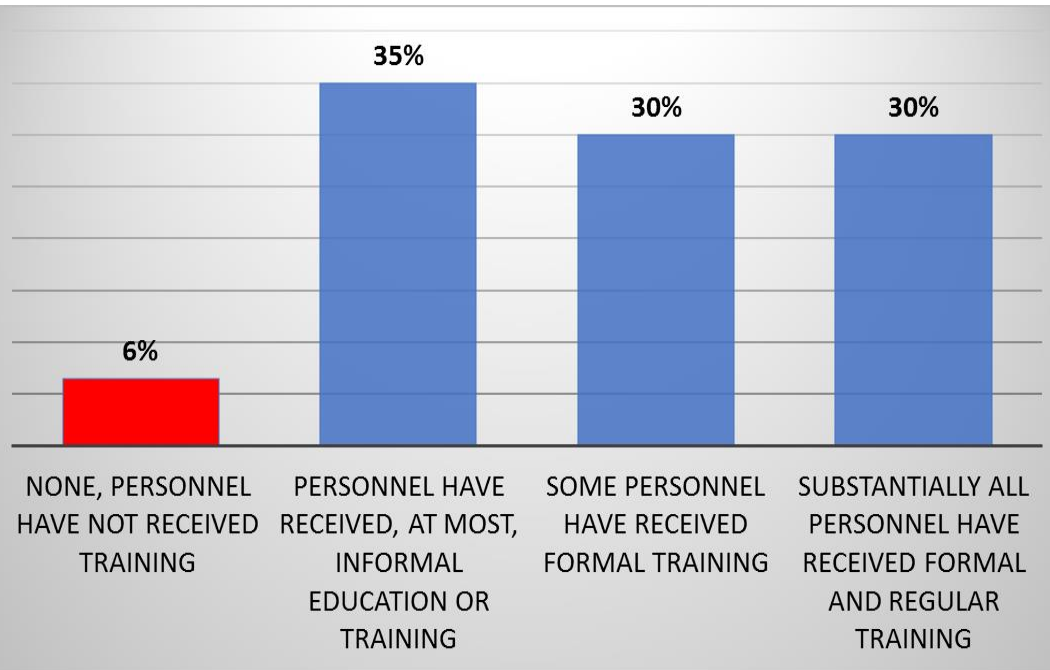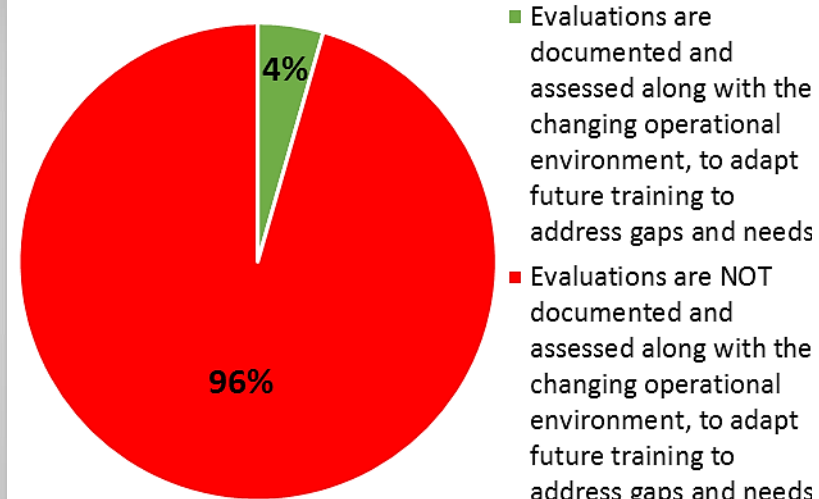
Data Description

- The majority of organizations (95%) indicate that their personnel have received formal or informal training
- Very few organizations are using their communications exercise evaluations to adapt future training to address gaps and needs

Office of Emergency Communications

Training Topics

Topics Included in an Organizations Emergency Communications Training
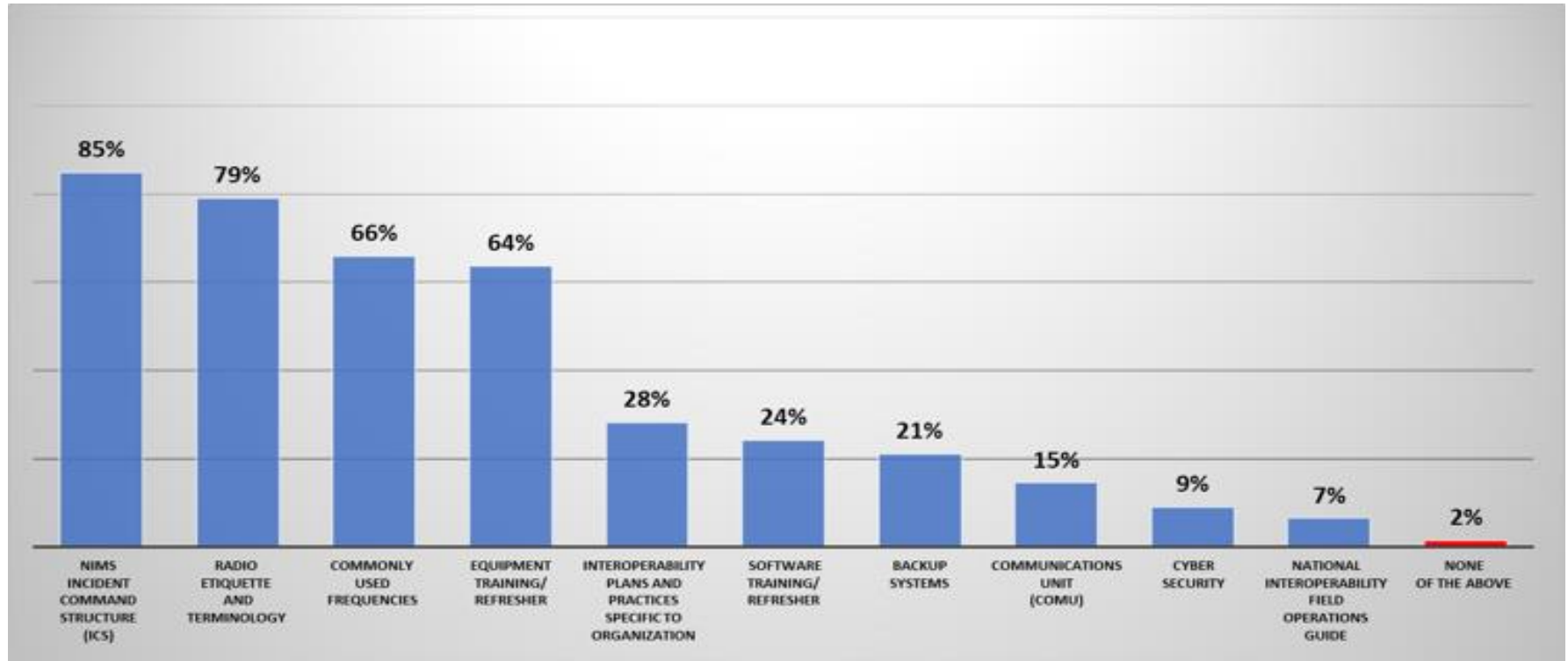
Data Description	

- *Of the 95% of organizations that train*, the majority of organizations (85%) reported including NIMS ICS in their training; and
- Over three-quarters (79%) of organizations reported training on radio etiquette and terminology; and
- Two-thirds of organizations reported training on commonly used frequencies (66%)

Homeland Security

Training with Other Organizations

Groups Included in an Organizations Emergency Communications Training
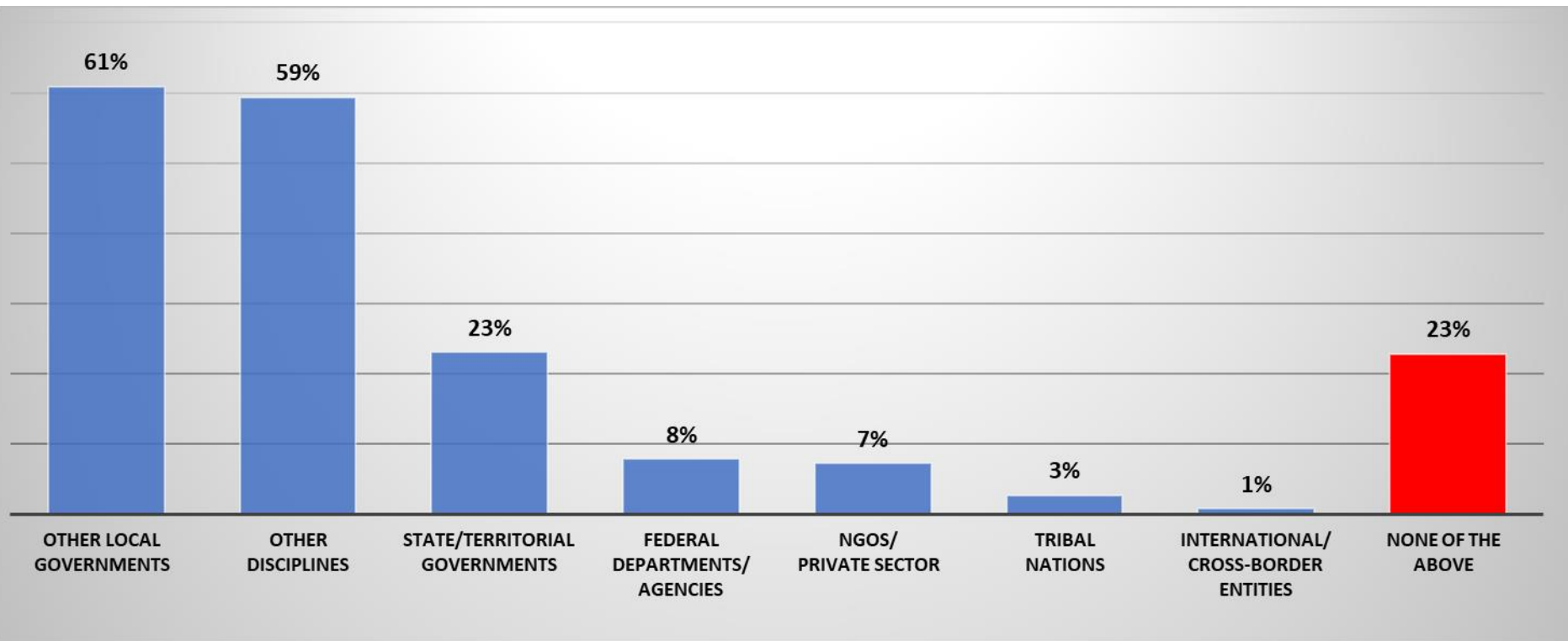
Data Description

- *Of the 95% of organizations that train,* most organizations (roughly 60%) train with other disciplines or other local governments; and
- Nearly a quarter (23%) train with state/territorial governments; and
- Nearly a quarter (23%) do not train with other organizations

Exercises

Exercise Practices of an Organization

26%

74%
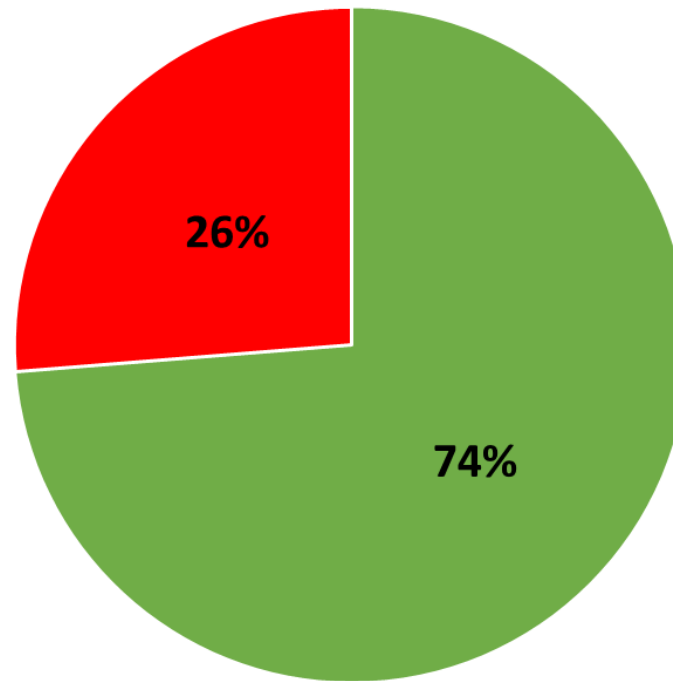
■ Participates in Exercises   ■ Does Not Participate in Exercises

Data Description
▪ Almost three-quarters of organizations (74%) indicated that they participate in exercises

Homeland Security

Office of Emergency Communications

Communications as an Exercise Objective

**An Organizations Evaluation of Communications as an Exercise Objective**
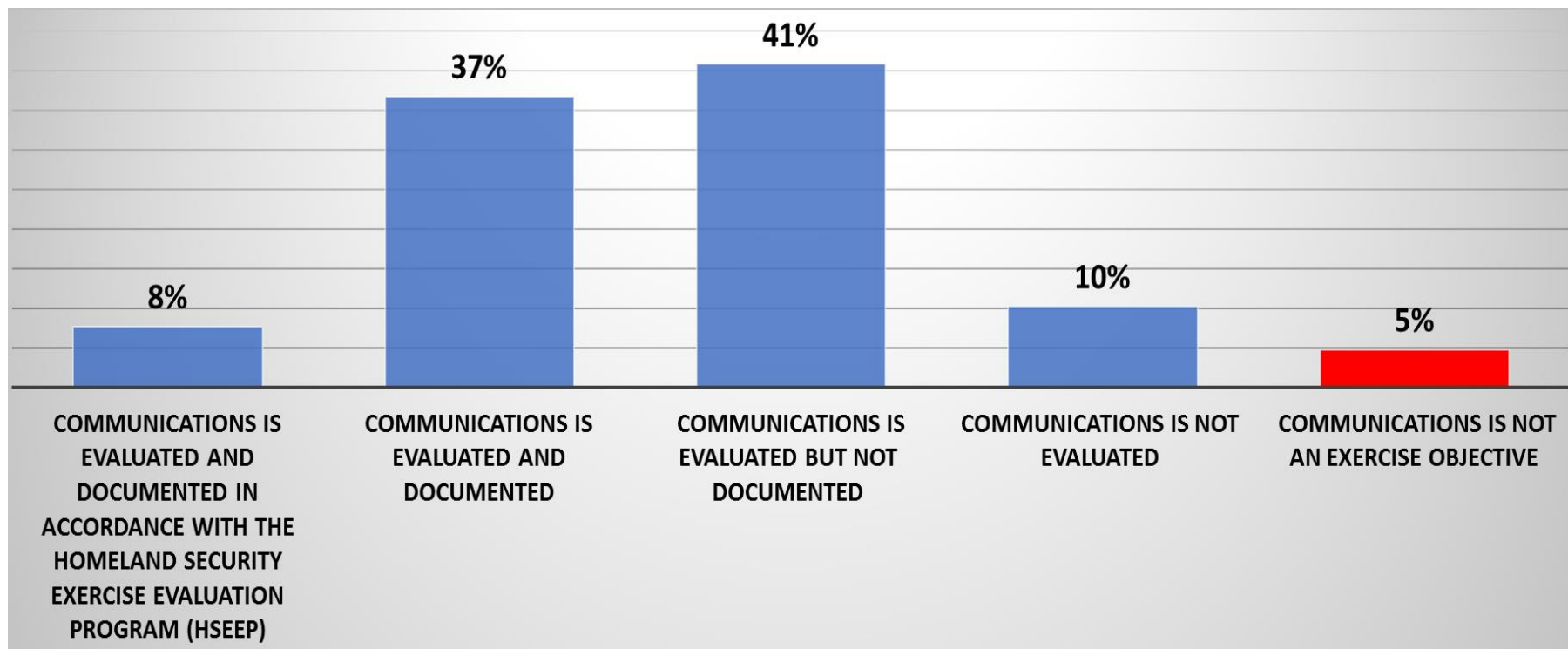
Data Description

- *Of the 74% of organizations that exercise*, the majority of respondents (86%) evaluate communications as an exercise objective; and
- Only 5% of organizations indicated that communications is not an exercise objective

Emergency Communications-Focused Exercises

**Emergency Communications-Focused Exercise
Practices of an Organization**

60%

20%

15%

5%
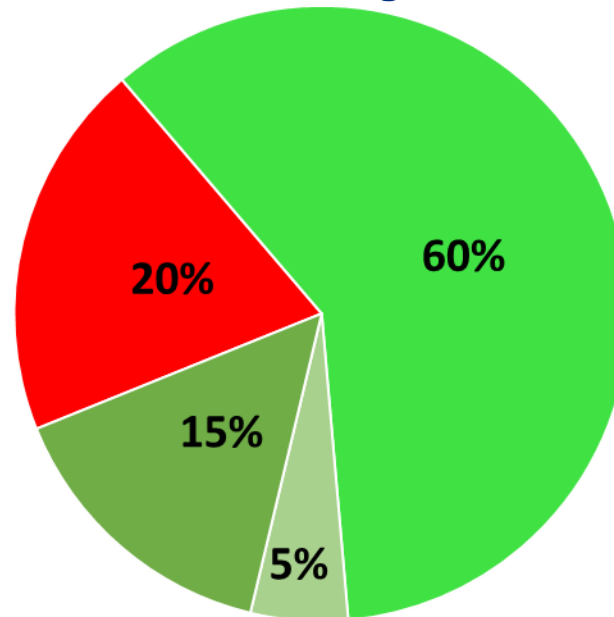
■ Does not participate in or conduct   ■ Participates in   ■ Conducts   ■ Participates in and conducts

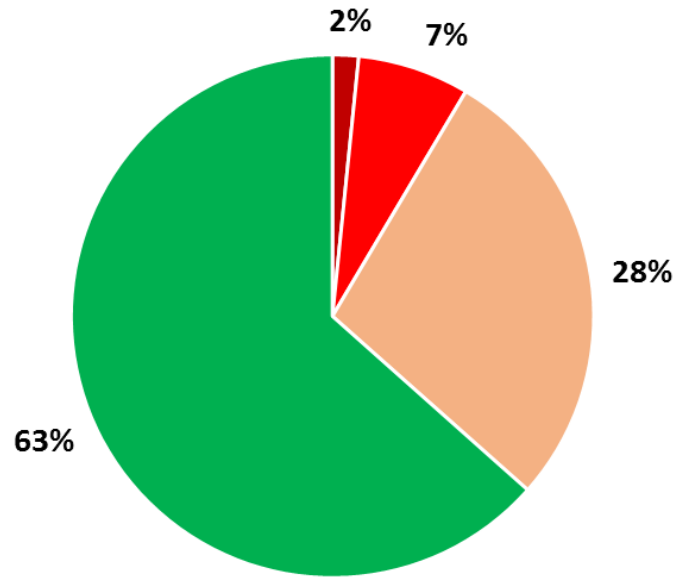| Data Description |
| --- |
| ▪ The majority of organizations (80%) conduct or participate in emergency communications-focused exercises |

CYBERSECURITY

Cybersecurity Impact

Impact of Cybersecurity Incidents on Organizations over the Past 5 Years

Legend: Severe Impact, Some Impact, Minimal Impact, No Impact

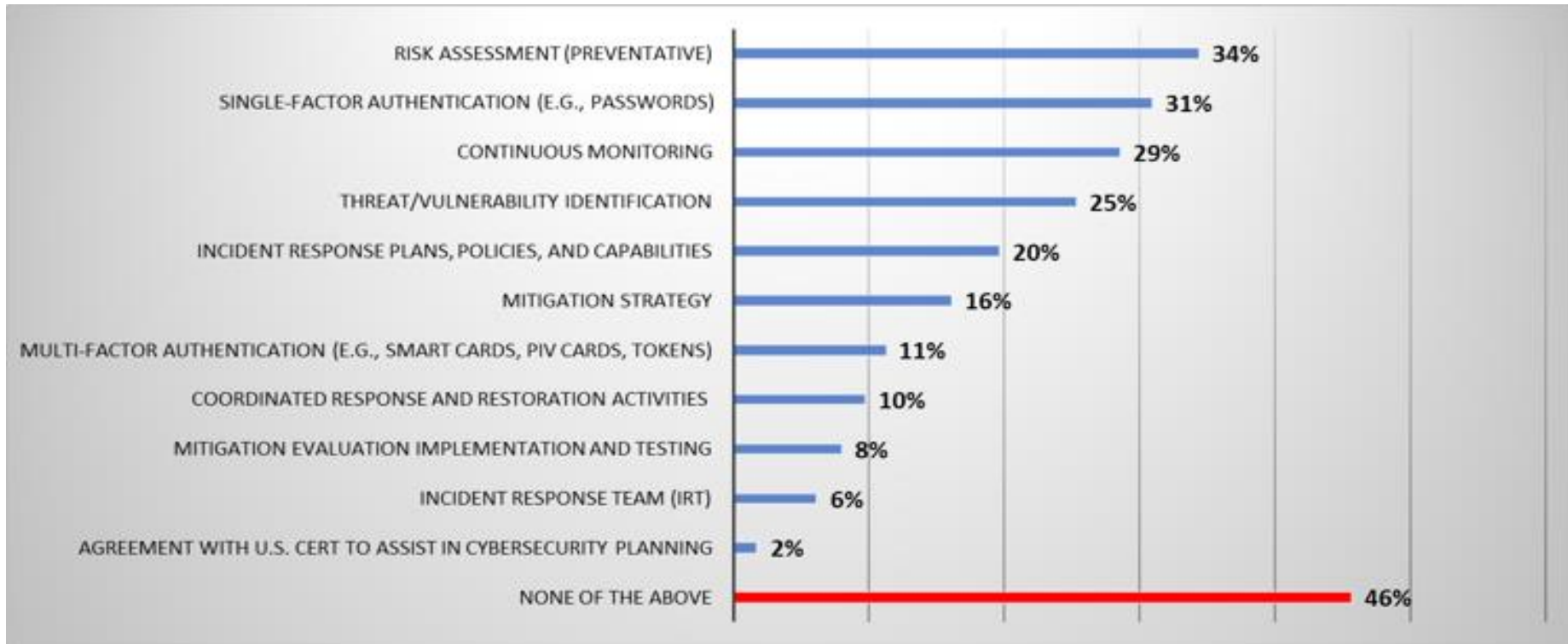Pie chart values: 2%, 7%, 28%, 63%

Data Description

- Over a third of organizations indicated that cybersecurity incidents have had an impact on the ability of their emergency response providers and government officials' ability to communicate over the past five years
- Only 2% of organizations reported a cybersecurity incident having a severe impact on their ability to communicate

Cybersecurity Planning

Elements that Organizations Incorporate into Cybersecurity Planning

| Element	Percentage
RISK ASSESSMENT (PREVENTATIVE)	34%
SINGLE-FACTOR AUTHENTICATION (E.G., PASSWORDS)	31%
CONTINUOUS MONITORING	29%
THREAT/VULNERABILITY IDENTIFICATION	25%
INCIDENT RESPONSE PLANS, POLICIES, AND CAPABILITIES	20%
MITIGATION STRATEGY	16%
MULTI-FACTOR AUTHENTICATION (E.G., SMART CARDS, PIV CARDS, TOKENS)	11%
COORDINATED RESPONSE AND RESTORATION ACTIVITIES	10%
MITIGATION EVALUATION IMPLEMENTATION AND TESTING	8%
INCIDENT RESPONSE TEAM (IRT)	6%
AGREEMENT WITH U.S. CERT TO ASSIST IN CYBERSECURITY PLANNING	2%
NONE OF THE ABOVE	46%

Data Description

- Almost half of organizations (46%) do not incorporate the listed cybersecurity measures into their cybersecurity planning
- Only 20% of organizations indicated having incident response plans, policies and capabilities
- Only 16% of organizations have a mitigation strategy in place
- Only 2% of organizations indicated having an agreement with US-CERT for cybersecurity planning

Homeland Security

Office of Emergency Communications

Cybersecurity Planning (cont.)

✓ **Fire departments and organizations located in rural areas tend to be least prepared for cybersecurity attacks**

- 62% of fire departments indicated that they do not conduct any cybersecurity planning
- Almost 60% of public safety disciplines located in rural areas do not participate in cybersecurity planning

Disciplines
Cybersecurity Planning
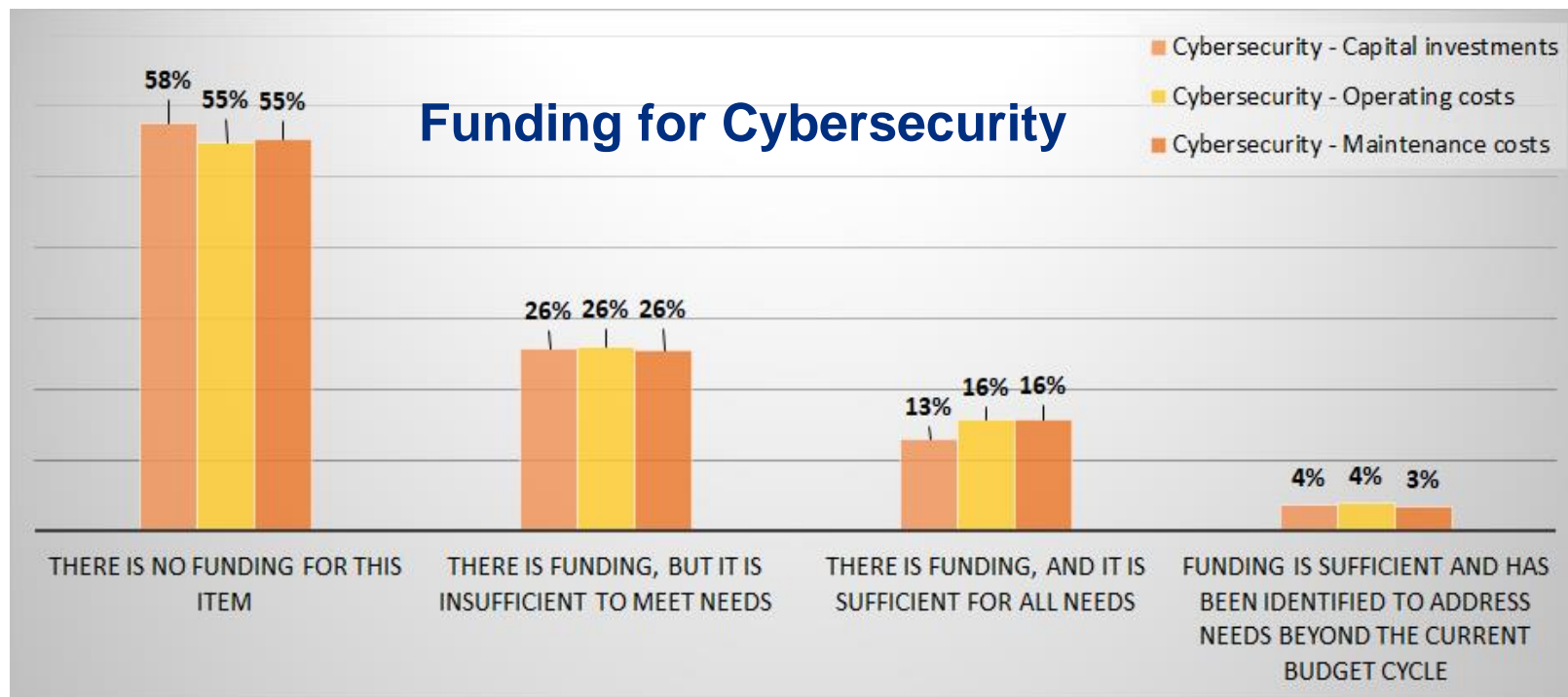### None of the Above

PSAP	LE	EMS	FIRE
11%	30%	38%	62%
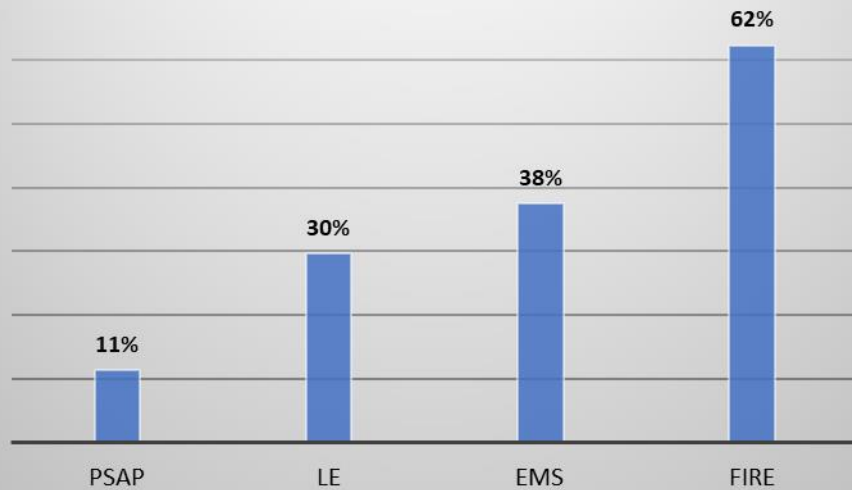
Geographies
Cybersecurity Planning
None of the Above

METRO	URBAN	RURAL
33%	42%	59%
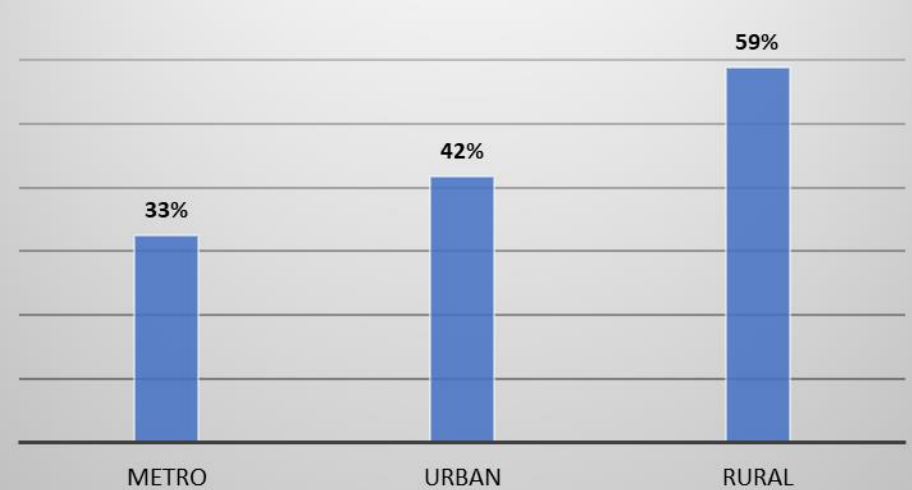
Cybersecurity Funding

✓ *Funding remains a critical gap for organizations when addressing cybersecurity issues*

- Over 55% of organizations indicated that they don't have funding for cybersecurity capital investments or operating and maintenance costs
- Additionally, 26% of organizations indicated that their cybersecurity funding is insufficient to meet their needs
- Organizations reporting they have sufficient cybersecurity funding also reported they are impacted more, than the national average, by cybersecurity disruptions

Funding for Cybersecurity

Legend:
- Cybersecurity - Capital investments
- Cybersecurity - Operating costs
- Cybersecurity - Maintenance costs

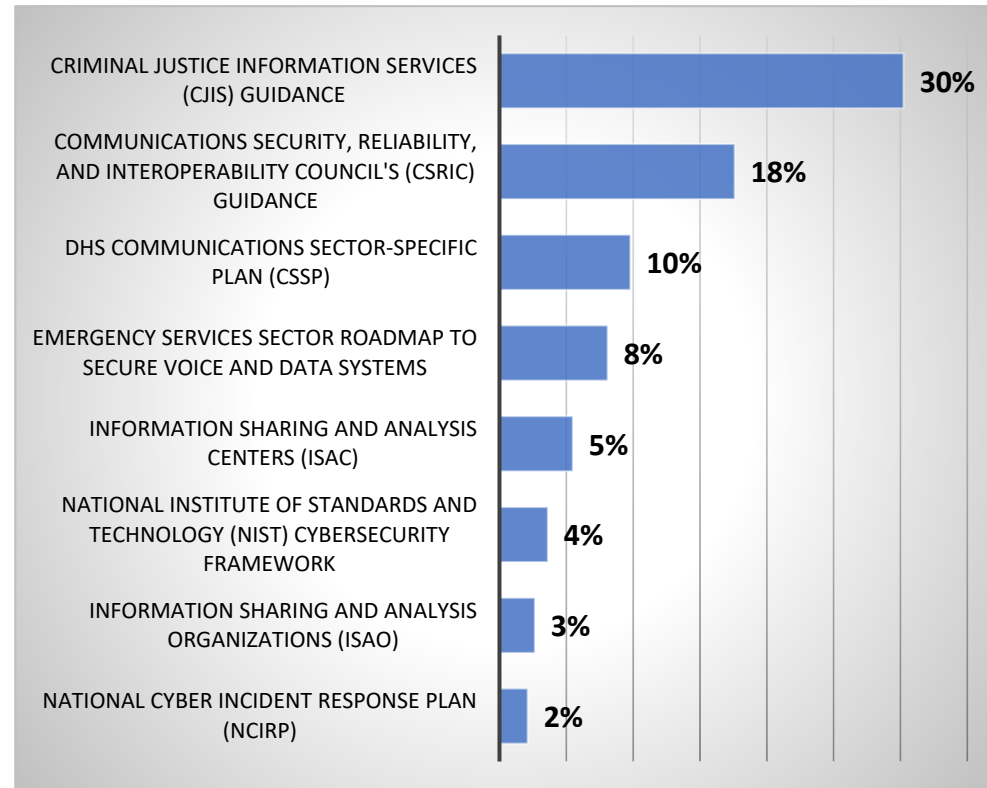|	THERE IS NO FUNDING FOR THIS ITEM	THERE IS FUNDING, BUT IT IS INSUFFICIENT TO MEET NEEDS	THERE IS FUNDING, AND IT IS SUFFICIENT FOR ALL NEEDS	FUNDING IS SUFFICIENT AND HAS BEEN IDENTIFIED TO ADDRESS NEEDS BEYOND THE CURRENT BUDGET CYCLE
Capital investments	58%	26%	13%	4%
Operating costs	55%	26%	16%	4%
Maintenance costs	55%	26%	16%	3%

Additional Cybersecurity Insights

✓ *There is not widespread adoption of existing Cybersecurity guidance documents*

- 30% of organizations reference the Criminal Justice Information Services (CJIS) Guidance when developing their communication SOPs.

- Only 2% of organizations indicated using the National Cyber Incident Response Plan (NCIRP) for developing their communication SOPs

✓ *Cybersecurity is a lower-level priority topic for organizations when developing SOPs and trainings*

- Only 16% of organizations include cybersecurity in their organization's SOPs.

- Only 9% of organizations include cybersecurity in their organization's emergency communication training.

Guidance	Percentage
CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) GUIDANCE	30%
COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL'S (CSRIC) GUIDANCE	18%
DHS COMMUNICATIONS SECTOR-SPECIFIC PLAN (CSSP)	10%
EMERGENCY SERVICES SECTOR ROADMAP TO SECURE VOICE AND DATA SYSTEMS	8%
INFORMATION SHARING AND ANALYSIS CENTERS (ISAC)	5%
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) CYBERSECURITY FRAMEWORK	4%
INFORMATION SHARING AND ANALYSIS ORGANIZATIONS (ISAO)	3%
NATIONAL CYBER INCIDENT RESPONSE PLAN (NCIRP)	2%

Cybersecurity Guidelines and Standards Influencing SOPs

USAGE

Office of Emergency Communications

Homeland
Security

Capabilities Used (or Tested)

Emergency Communications Capabilities Used or Tested

Legend:
- Primary voice
- Primary data
- Interoperable voice
- Interoperable data
- Backup voice
- Backup data

FOR "DAY-TO-DAY" SITUATIONS: 91%, 47%, 52%, 27%, 32%, 22%

FOR "OUT-OF-THE-ORDINARY" SITUATIONS: 59%, 25%, 37%, 15%, 20%, 11%

WITH PERSONNEL BEYOND OUR ORGANIZATION: 51%, 17%, 31%, 11%, 15%, 7%

IN ACCORDANCE WITH STANDARD OPERATING PROCEDURES: 48%, 22%, 28%, 15%, 19%, 14%
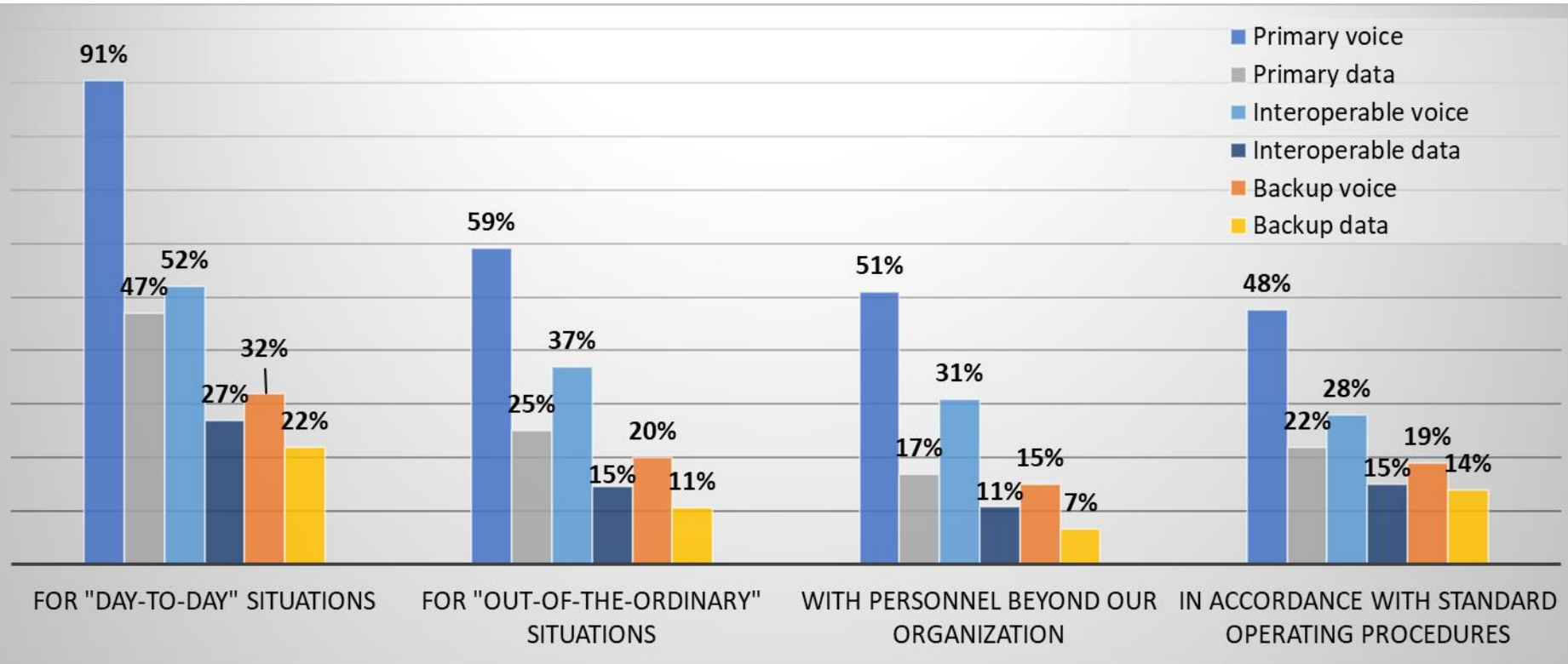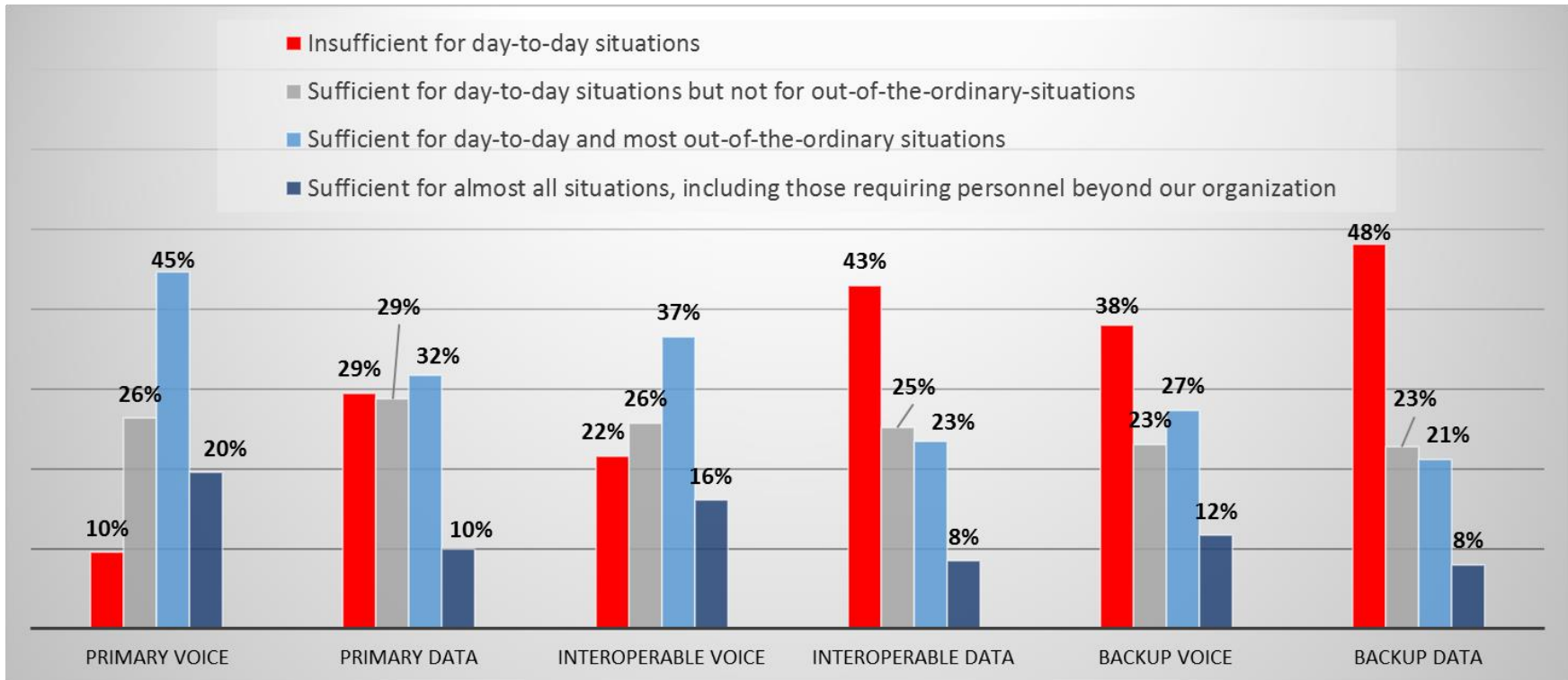
Data Description

- The majority of organizations (91%) indicated that they use/tested their primary voice capabilities for day-to-day situations
- In each scenario, respondents used/tested their interoperable capabilities about half as much as their primary capabilities
- Few respondents indicated using/testing their data and backup capabilities in accordance with their SOPs

Homeland Security

Office of Emergency Communications

Resource Capacity

Characterization of an Organizations Emergency Communication Resource Capacity

Legend:
- ■ (red) Insufficient for day-to-day situations
- ■ (gray) Sufficient for day-to-day situations but not for out-of-the-ordinary-situations
- ■ (light blue) Sufficient for day-to-day and most out-of-the-ordinary situations
- ■ (dark blue) Sufficient for almost all situations, including those requiring personnel beyond our organization

	Insufficient	Sufficient day-to-day not ordinary	Sufficient most ordinary	Sufficient almost all
PRIMARY VOICE	10%	26%	45%	20%
PRIMARY DATA	29%	29%	32%	10%
INTEROPERABLE VOICE	22%	26%	37%	16%
INTEROPERABLE DATA	43%	25%	23%	8%
BACKUP VOICE	38%	23%	27%	12%
BACKUP DATA	48%	23%	21%	8%

Data Description

- 45% of respondents indicated that their primary voice was sufficient for day-to-day and most of out-of-the-ordinary situations
- Over 40% of respondents indicated that their interoperable data and backup data capacity is insufficient for day-to-day situations
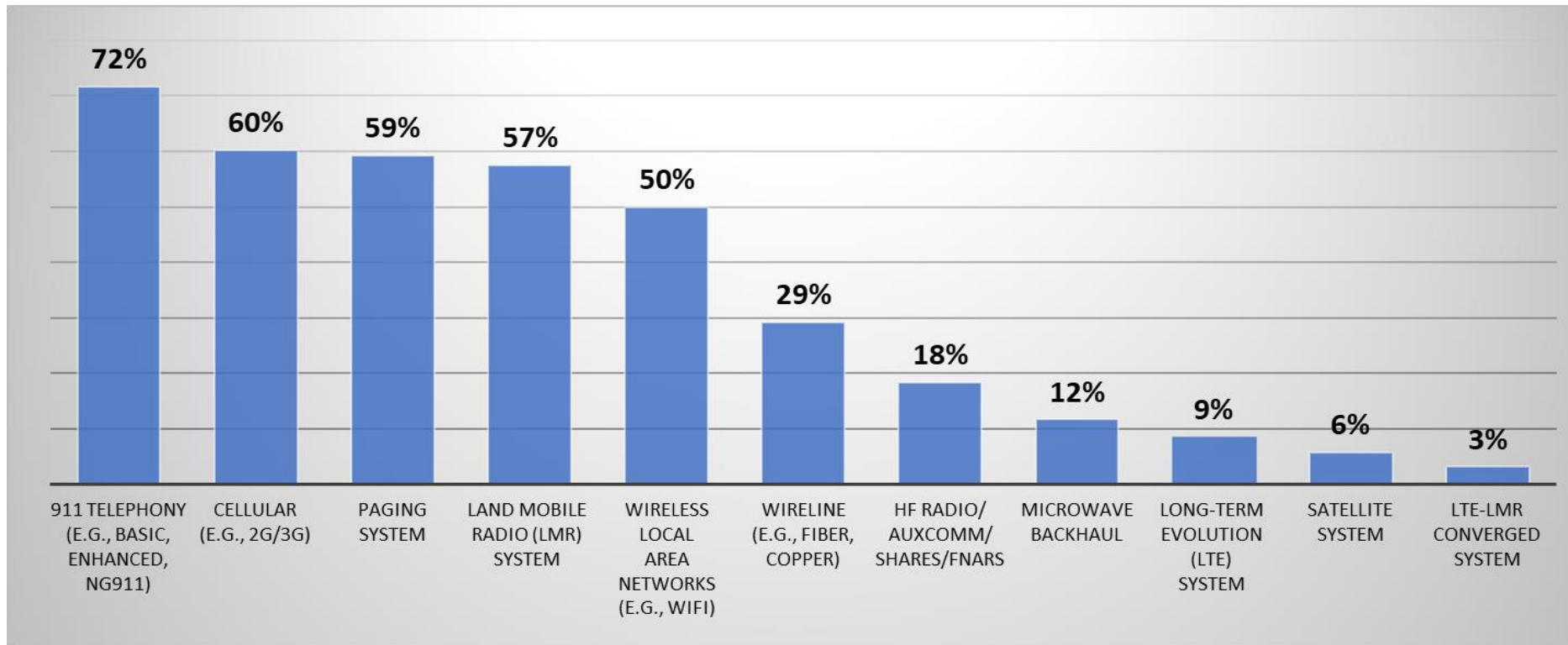
Homeland Security

Office of Emergency Communications

EQUIPMENT

Systems In Use

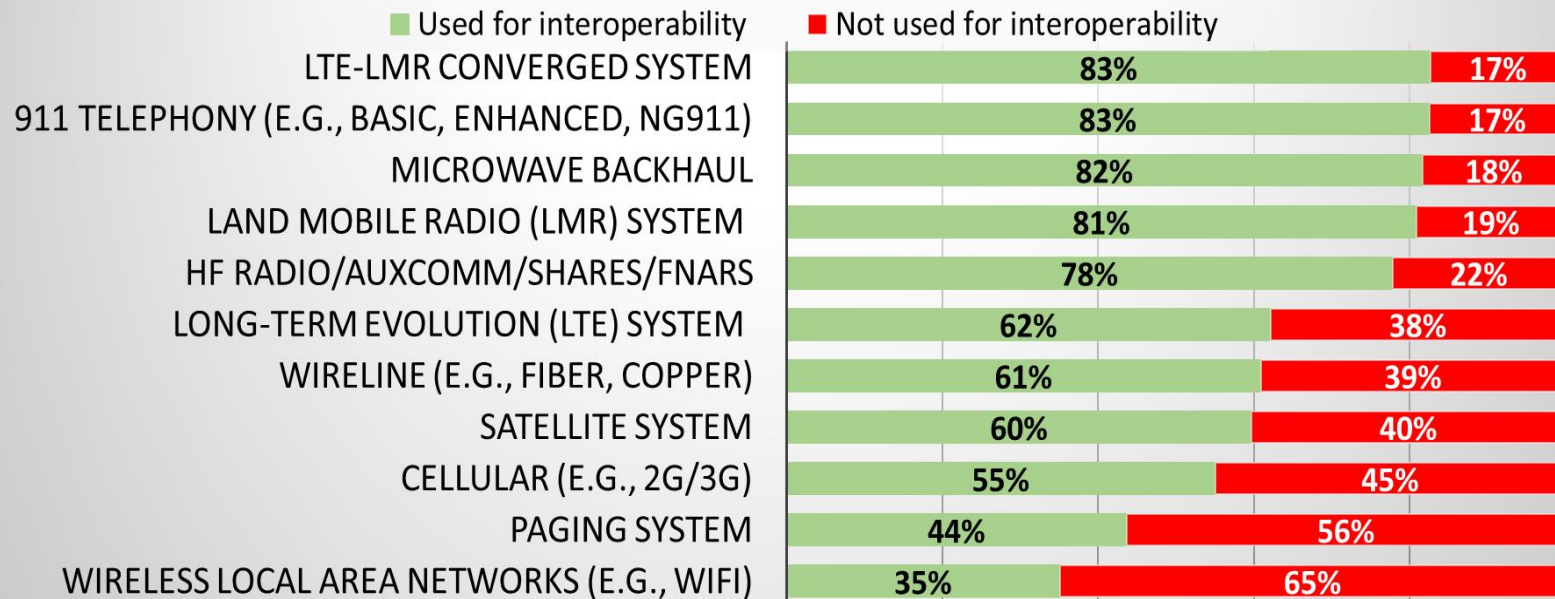## Characterization of an Organizations Technology Systems in Use

Data Description

- Majority of respondents (72%) indicated that they use a 911 system
- Nearly the same percentage of organizations use cellular systems as those who use LMR systems
- Only 3% of organizations use LMR-LTE systems

System Usage – Interoperability

Characterization of an Organizations Technology Systems in Use for Interoperability

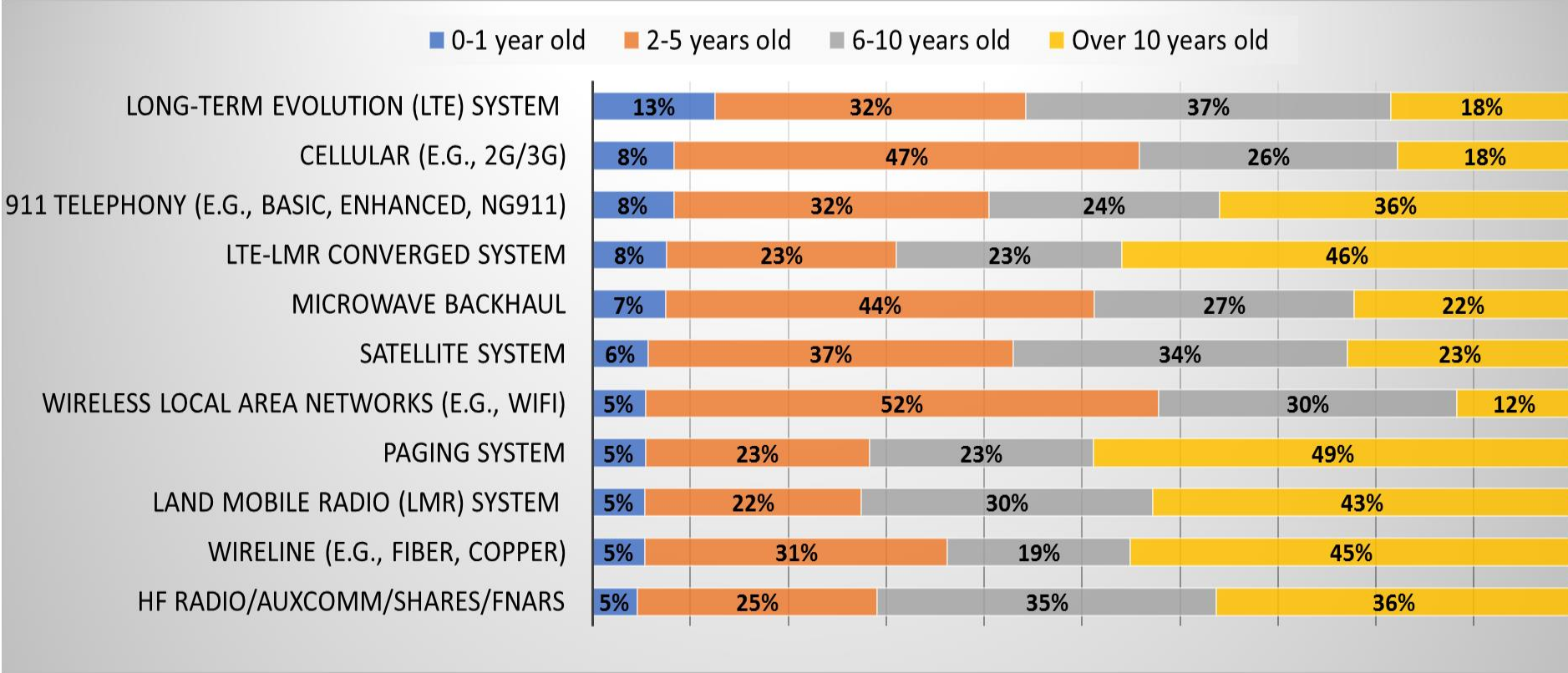|	Used for interoperability	Not used for interoperability
LTE-LMR CONVERGED SYSTEM	83%	17%
911 TELEPHONY (E.G., BASIC, ENHANCED, NG911)	83%	17%
MICROWAVE BACKHAUL	82%	18%
LAND MOBILE RADIO (LMR) SYSTEM	81%	19%
HF RADIO/AUXCOMM/SHARES/FNARS	78%	22%
LONG-TERM EVOLUTION (LTE) SYSTEM	62%	38%
WIRELINE (E.G., FIBER, COPPER)	61%	39%
SATELLITE SYSTEM	60%	40%
CELLULAR (E.G., 2G/3G)	55%	45%
PAGING SYSTEM	44%	56%
WIRELESS LOCAL AREA NETWORKS (E.G., WIFI)	35%	65%

Data Description

- The majority of organizations (over 80%) indicated that the 911, LMR-LTE, microwave backhaul, or LMR systems that they use are used for interoperability
- The majority of organizations (65%) indicated that they do not use wireless local area networks (e.g., WiFi) for interoperability

Homeland Security

Office of Emergency Communications

System Age

Characterization of an Organizations Technology Systems Age

Legend: ■ 0-1 year old ■ 2-5 years old ■ 6-10 years old ■ Over 10 years old

| System	0-1 year old	2-5 years old	6-10 years old	Over 10 years old
LONG-TERM EVOLUTION (LTE) SYSTEM	13%	32%	37%	18%
CELLULAR (E.G., 2G/3G)	8%	47%	26%	18%
911 TELEPHONY (E.G., BASIC, ENHANCED, NG911)	8%	32%	24%	36%
LTE-LMR CONVERGED SYSTEM	8%	23%	23%	46%
MICROWAVE BACKHAUL	7%	44%	27%	22%
SATELLITE SYSTEM	6%	37%	34%	23%
WIRELESS LOCAL AREA NETWORKS (E.G., WIFI)	5%	52%	30%	12%
PAGING SYSTEM	5%	23%	23%	49%
LAND MOBILE RADIO (LMR) SYSTEM	5%	22%	30%	43%
WIRELINE (E.G., FIBER, COPPER)	5%	31%	19%	45%
HF RADIO/AUXCOMM/SHARES/FNARS	5%	25%	35%	36%

Data Description

- Fewer than one in seven organizations is using a system less than a year old
- Almost 50% of organizations that use a paging system indicated that it is over 10 years old
- The majority of organizations (51%) that use microwave backhaul have systems that are less than 5 years old

Homeland Security

Office of Emergency Communications

36

System Usage – Type of Use
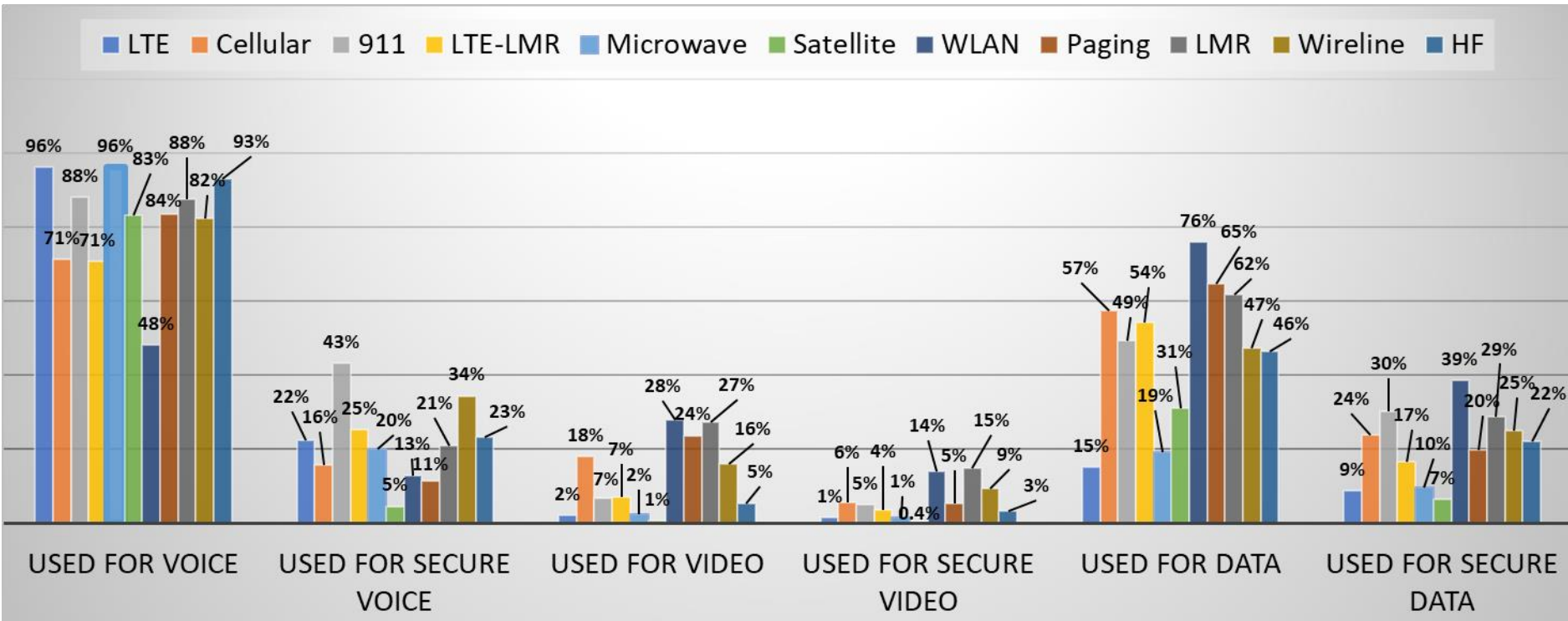
Data Description

- Except for wireless local access networks (e.g., WiFi), the majority of systems are used for voice
- Over a third (39%) of organizations that use a wireless local access network (e.g., WiFi) are using it for secure data
- Organizations indicated that few (2%) of their LMR systems are being used for video

Office of Emergency Communications

System Usage – Reliability

Characterization of an Organizations Technology Systems Reliability
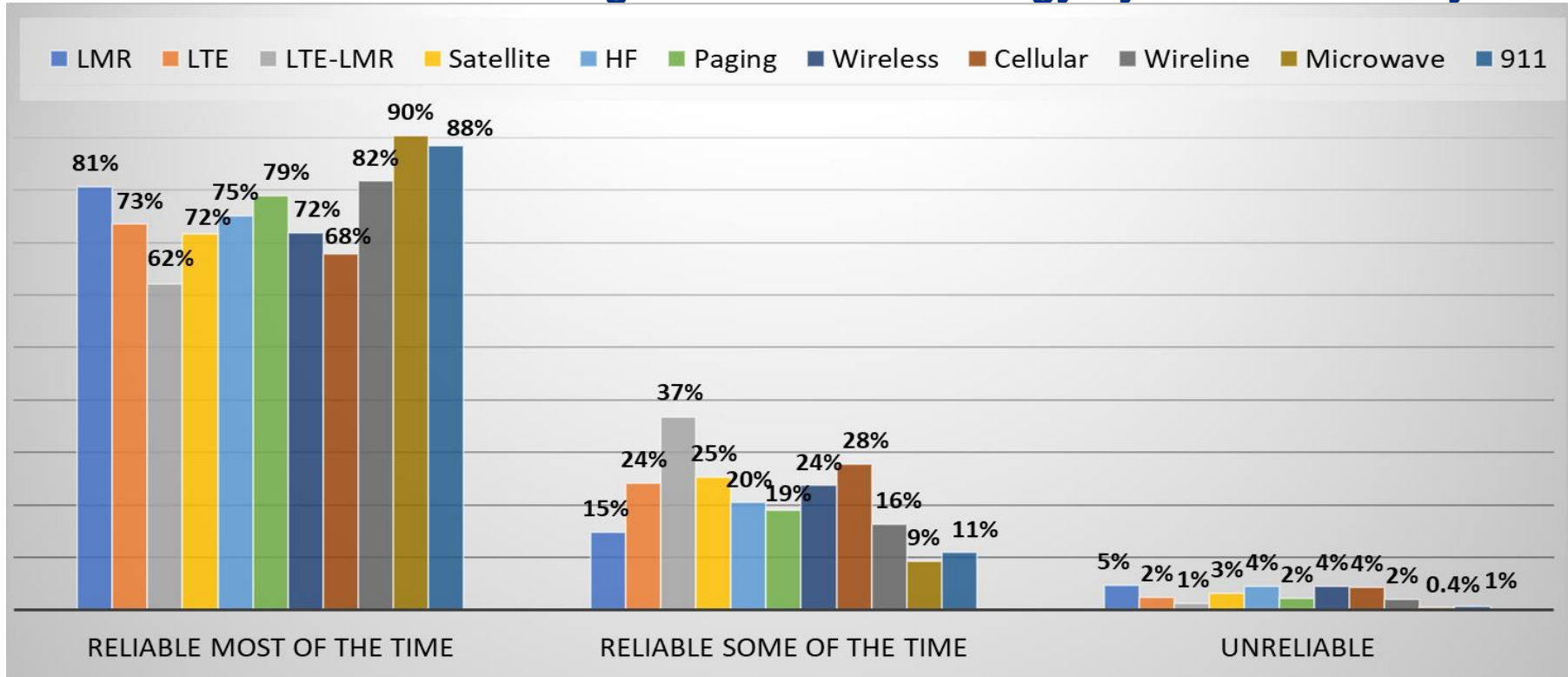
Data Description

- The majority of organizations (60-90%) indicated that the systems they use are reliable most of the time
- Over 5% of organizations indicated that the LMR system that they use is unreliable
- Over a third (37%) of organizations reported that their LTE-LMR system is only reliable some of the time

Homeland Security

Office of Emergency Communications