Homeland Security

2018 SAFECOM Nationwide Survey Results

National-Level Summary

August 2018

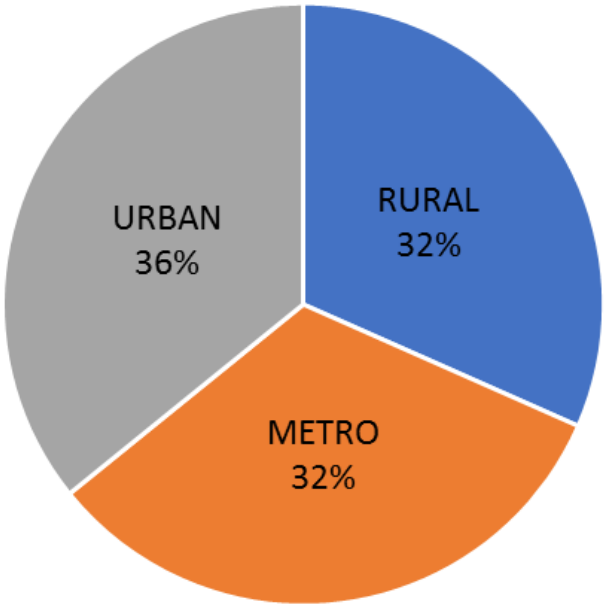
SAFECOM Nationwide Survey

- 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.

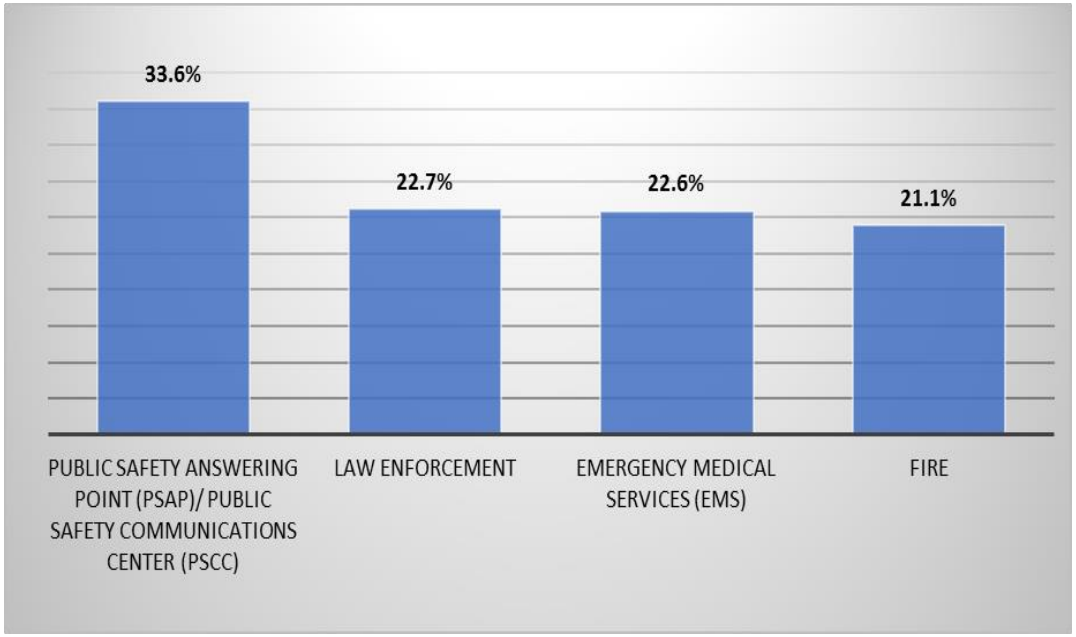
DEMOGRAPHICS

Geographic Environment

Geographic Representation of All Respondents



Discipline Representation of All Respondents



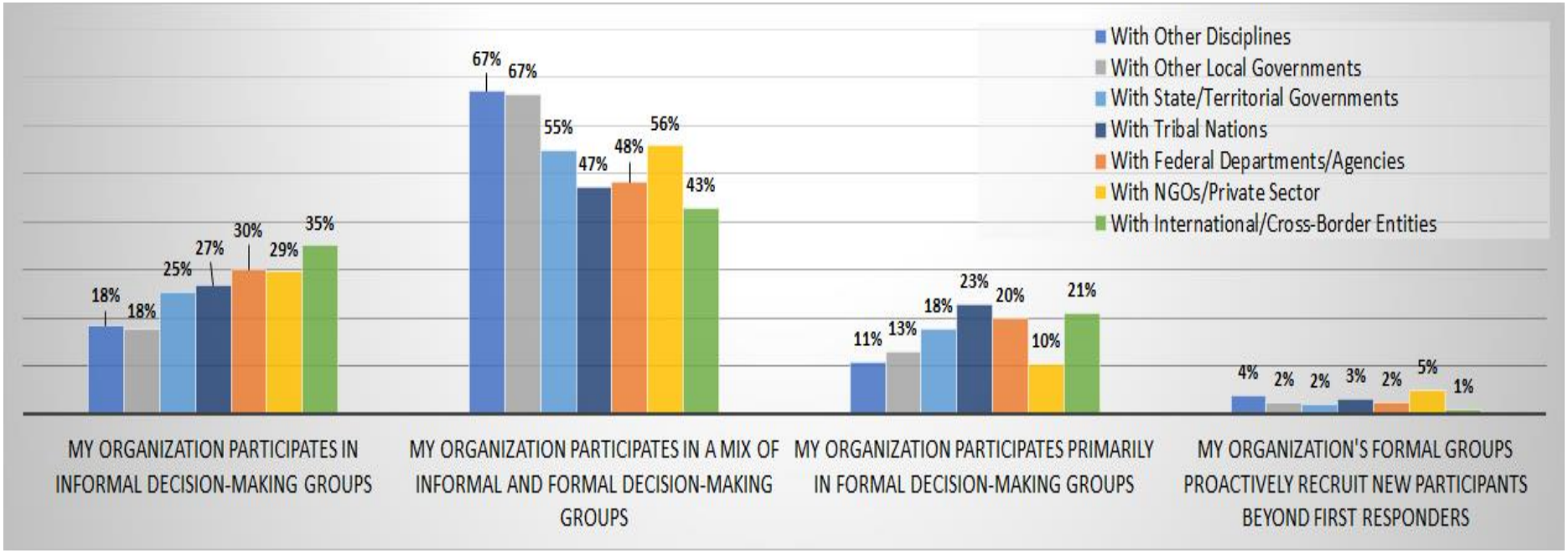
Data Description

- 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

Decision-Making Groups

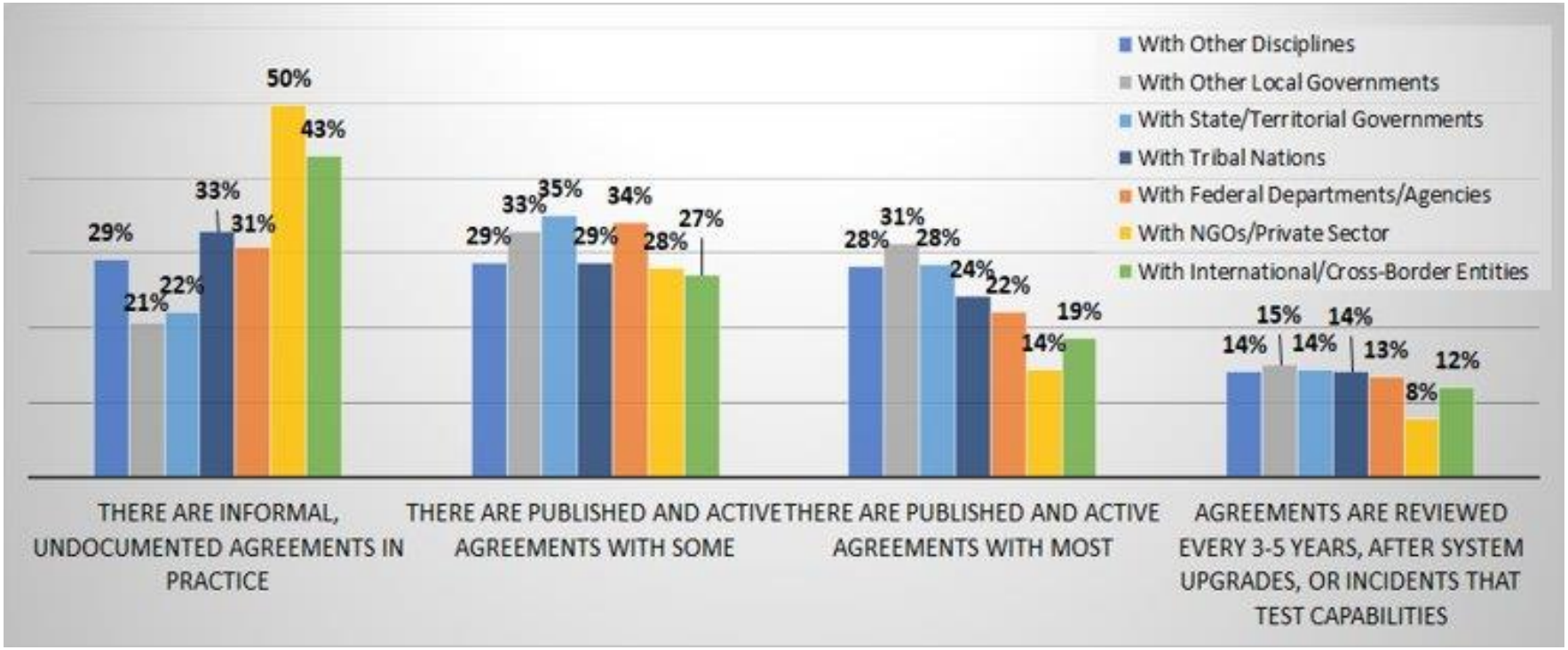
Characterization of an Organization's Involvement in Decision-Making Groups



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



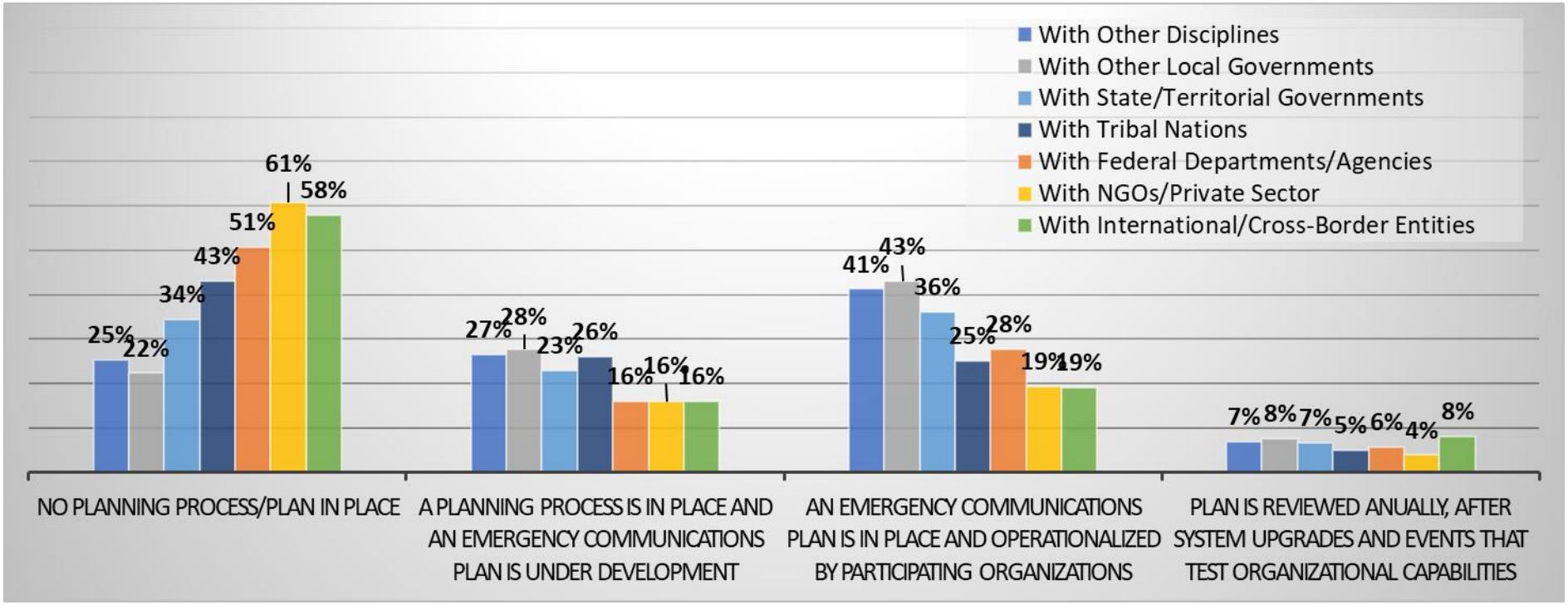
Data Description

- 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.

Strategic Planning Process

Characterization of an Organization's Strategic Planning Process



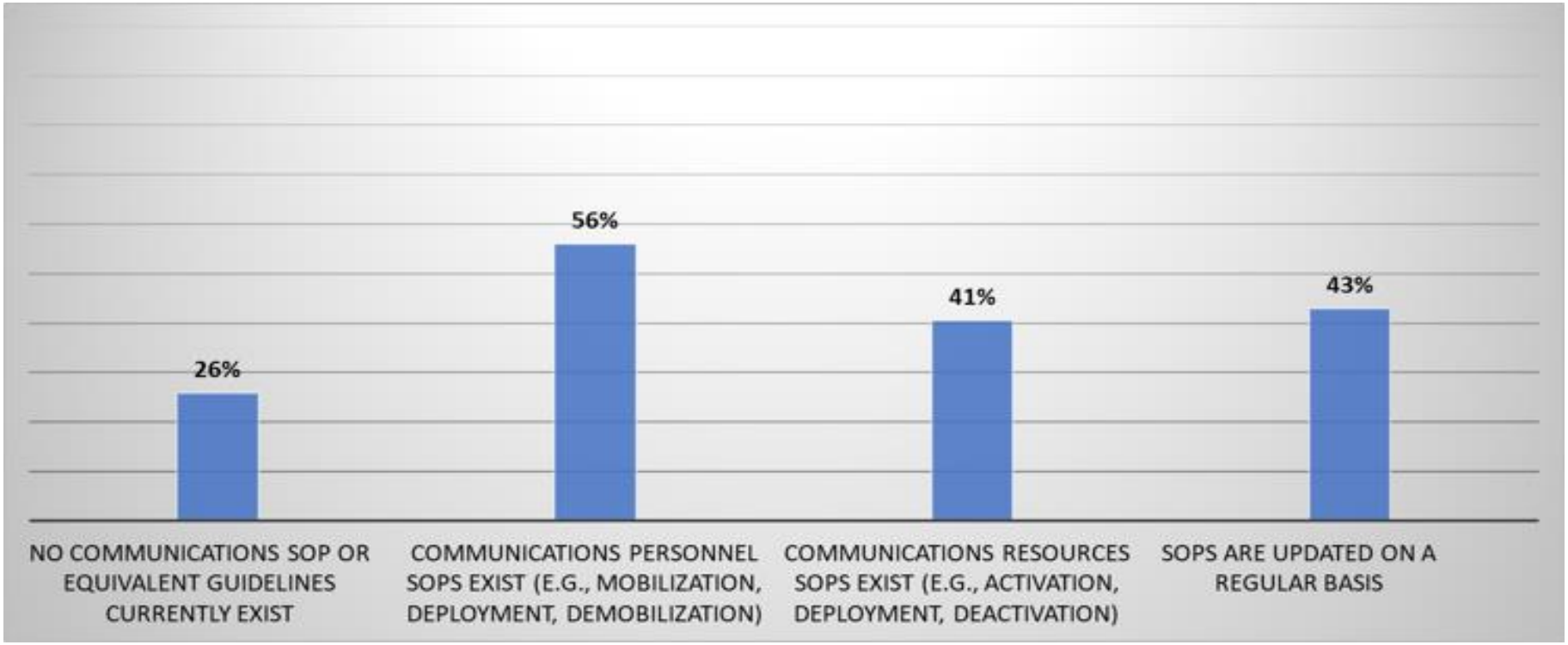
Data Description

- 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

STANDARD OPERATING PROCEDURES

Presence of SOPs

Presence and Type of Standard Operating Procedures

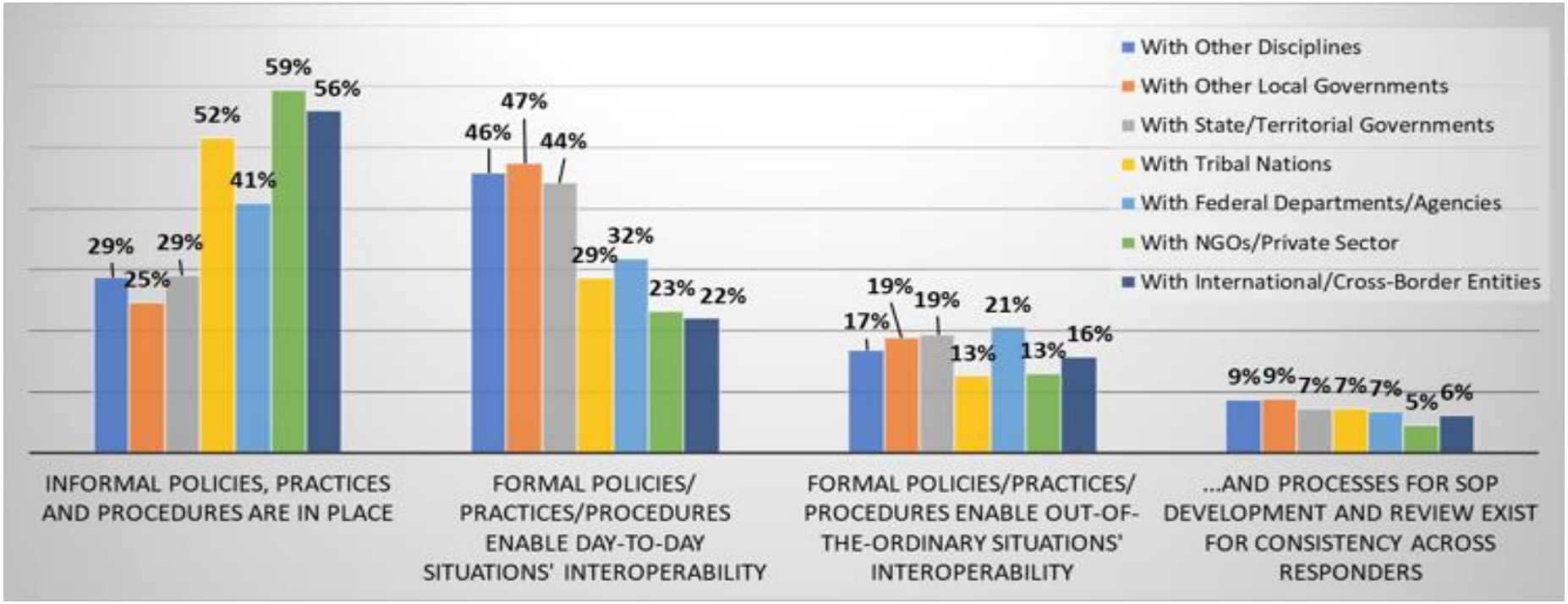


Data Description

- 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



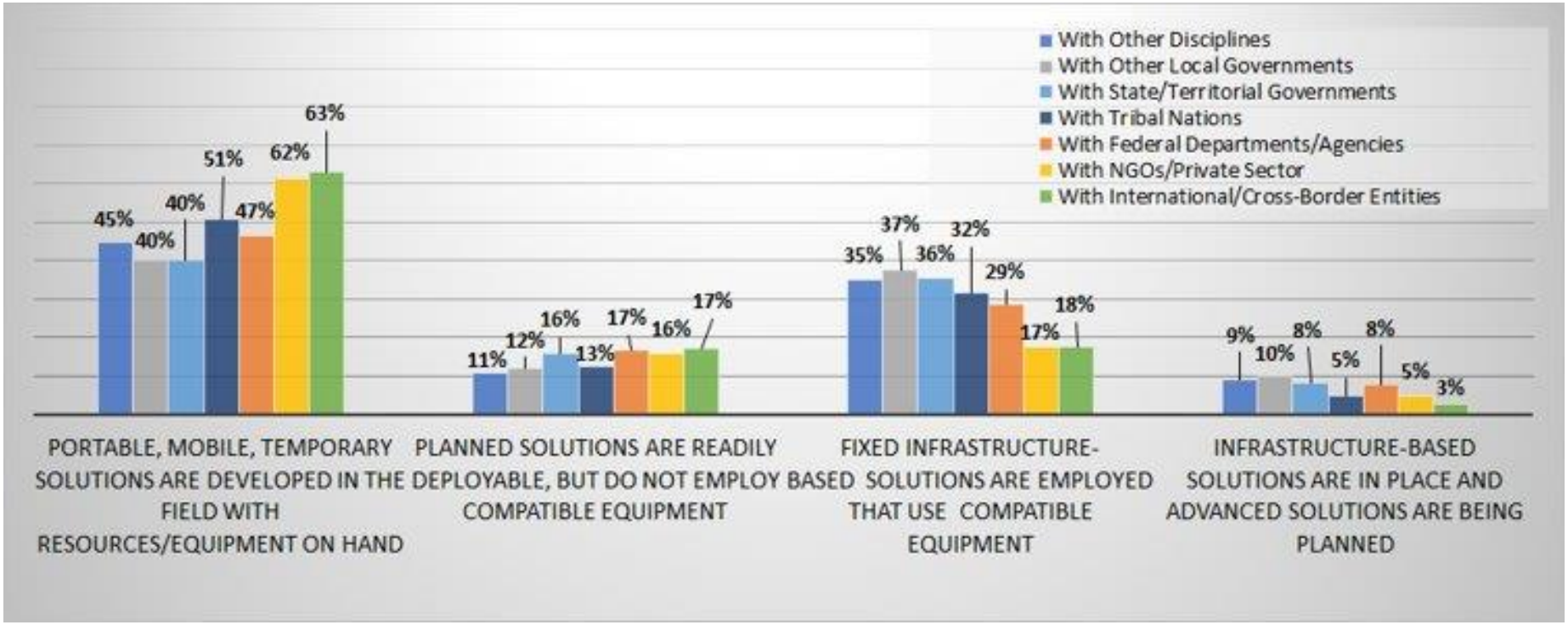
Data Description

- 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

TECHNOLOGY

Solutions for Interoperability with Other Entities

Characterization of the Technology Systems Used by an Organization

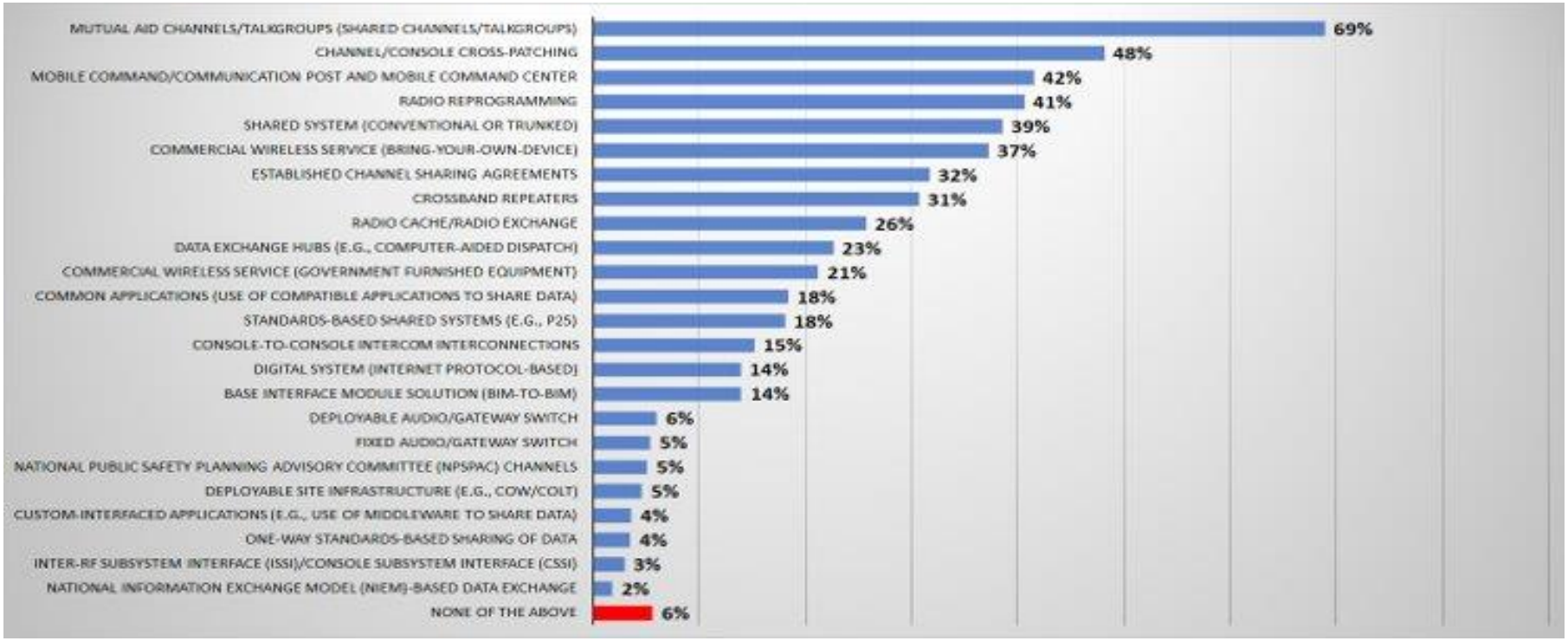


Data Description

- 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

Interoperability Solutions

Interoperability Solutions in Use by Organizations

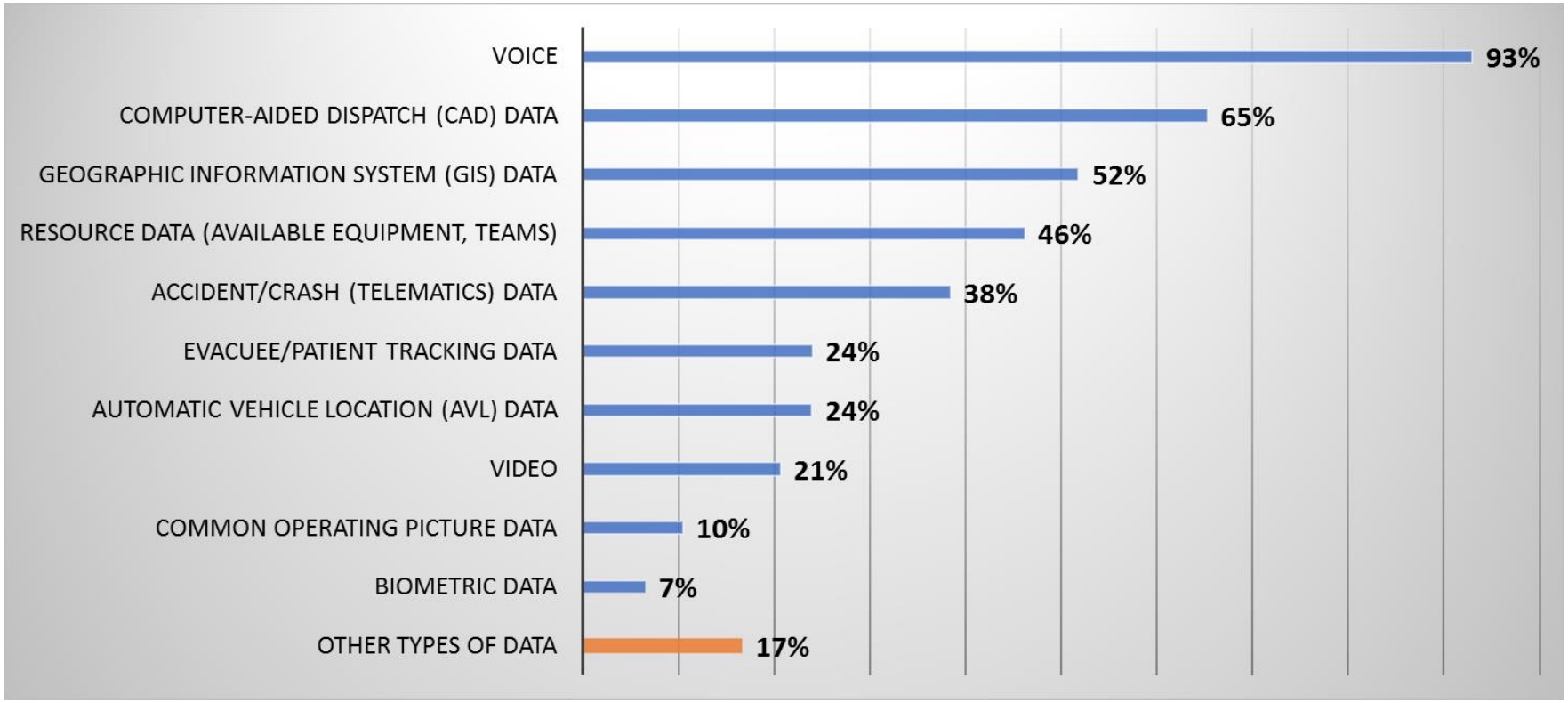


Data Description

- 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%)

Types of Information Exchanged

Types of Information Exchanged between Organizations

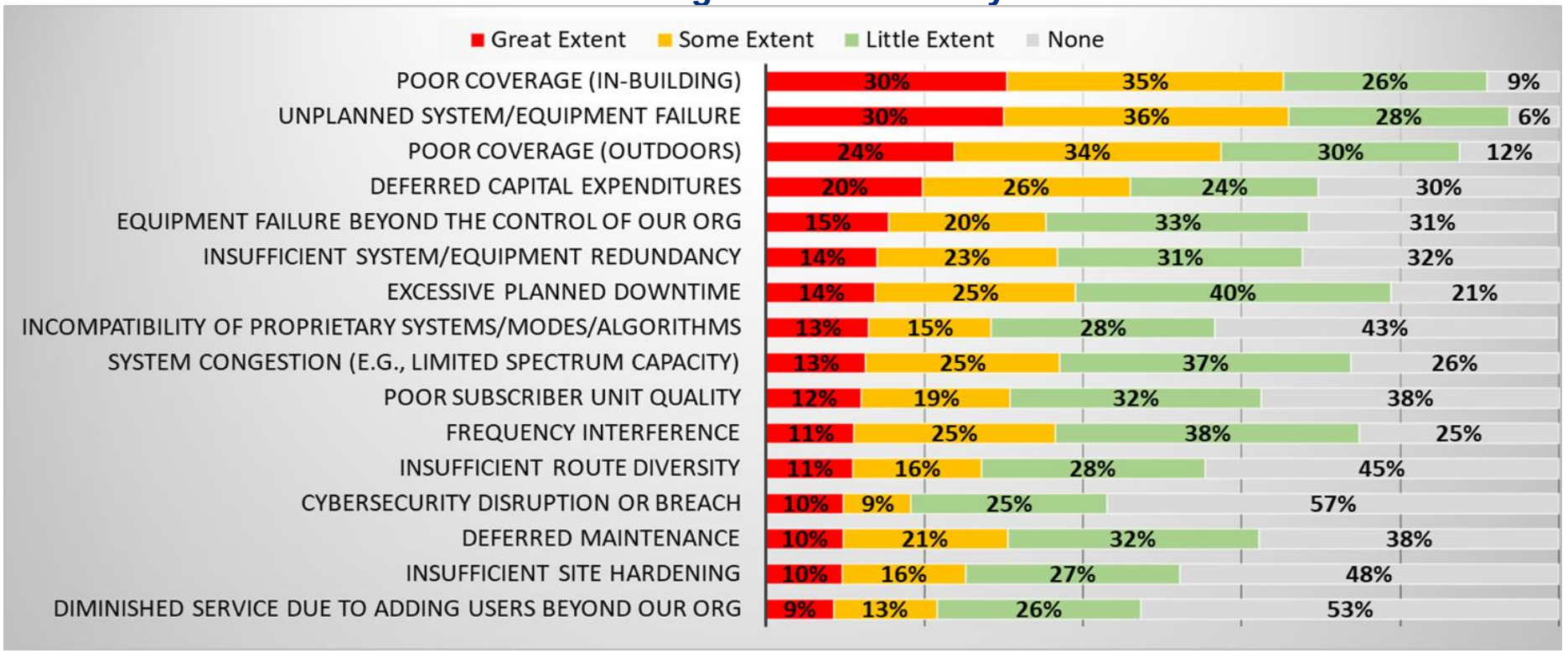


Data Description

- 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



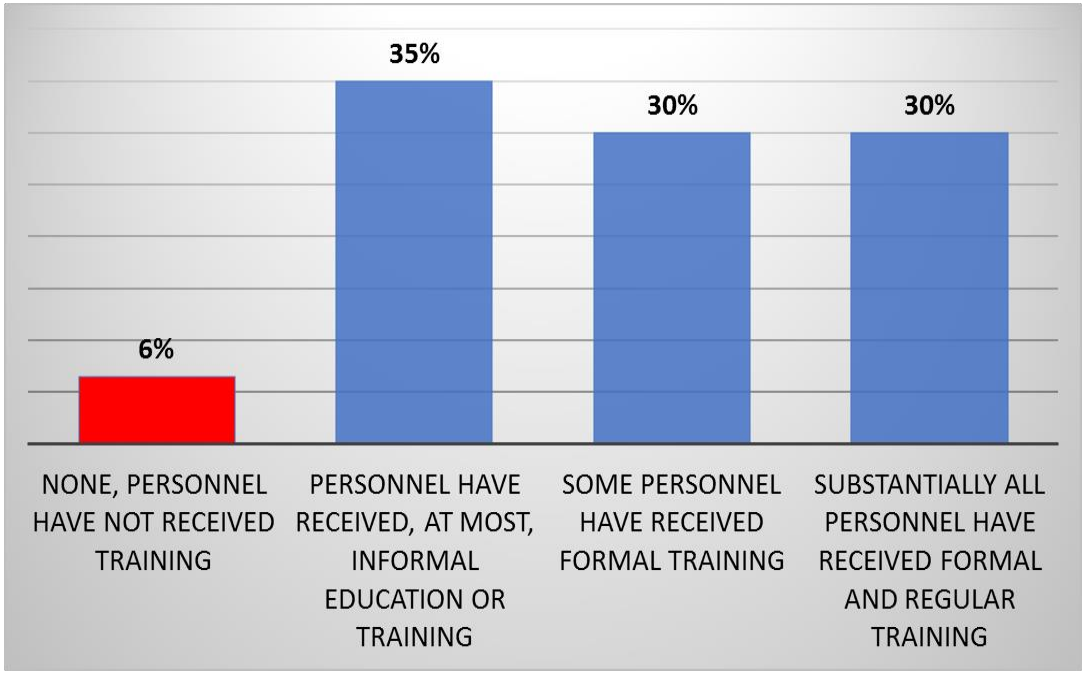
Data Description

- 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
- 30% of organizations reported unplanned system failures greatly affect their organization's ability to communicate
- 44% of organizations identify a cybersecurity disruption/breach as impacting their ability to communicate

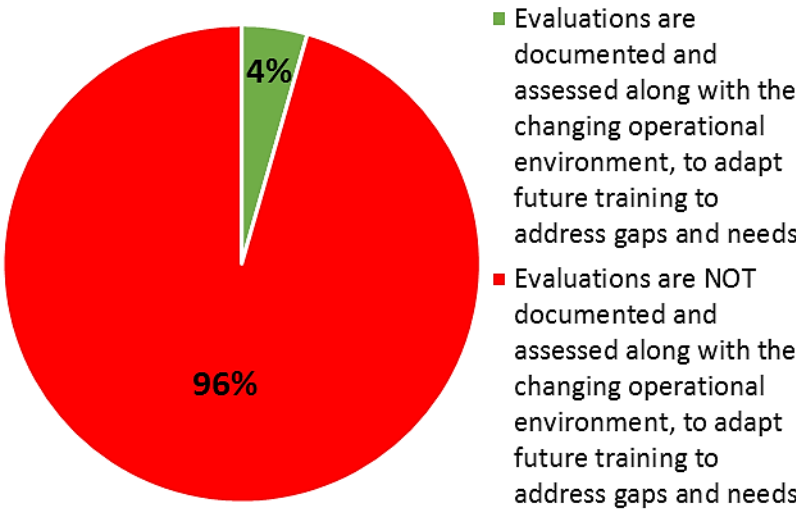
TRAINING & EXERCISES

Training

Characterization of an Organization's Emergency Communications Training



Training Evaluations

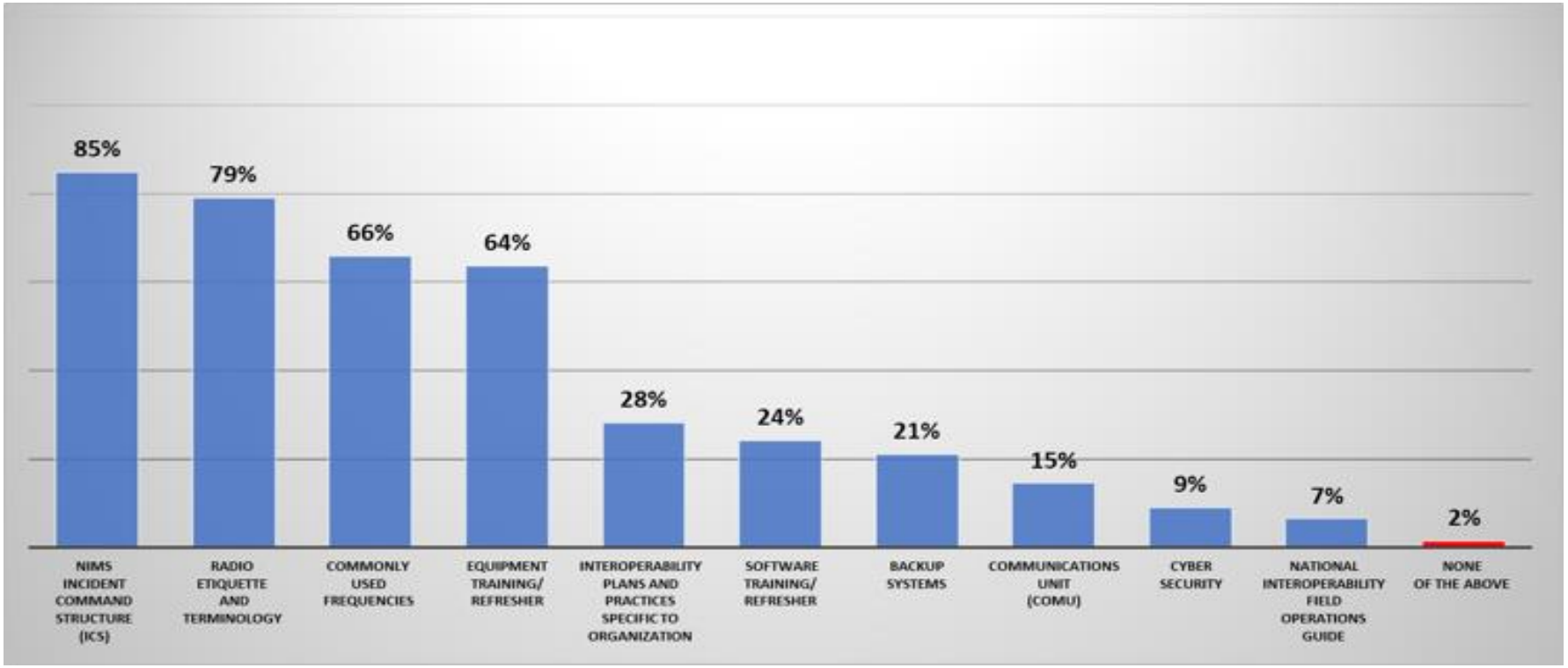


Data Description

- 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

Training Topics

Topics Included in an Organizations Emergency Communications Training

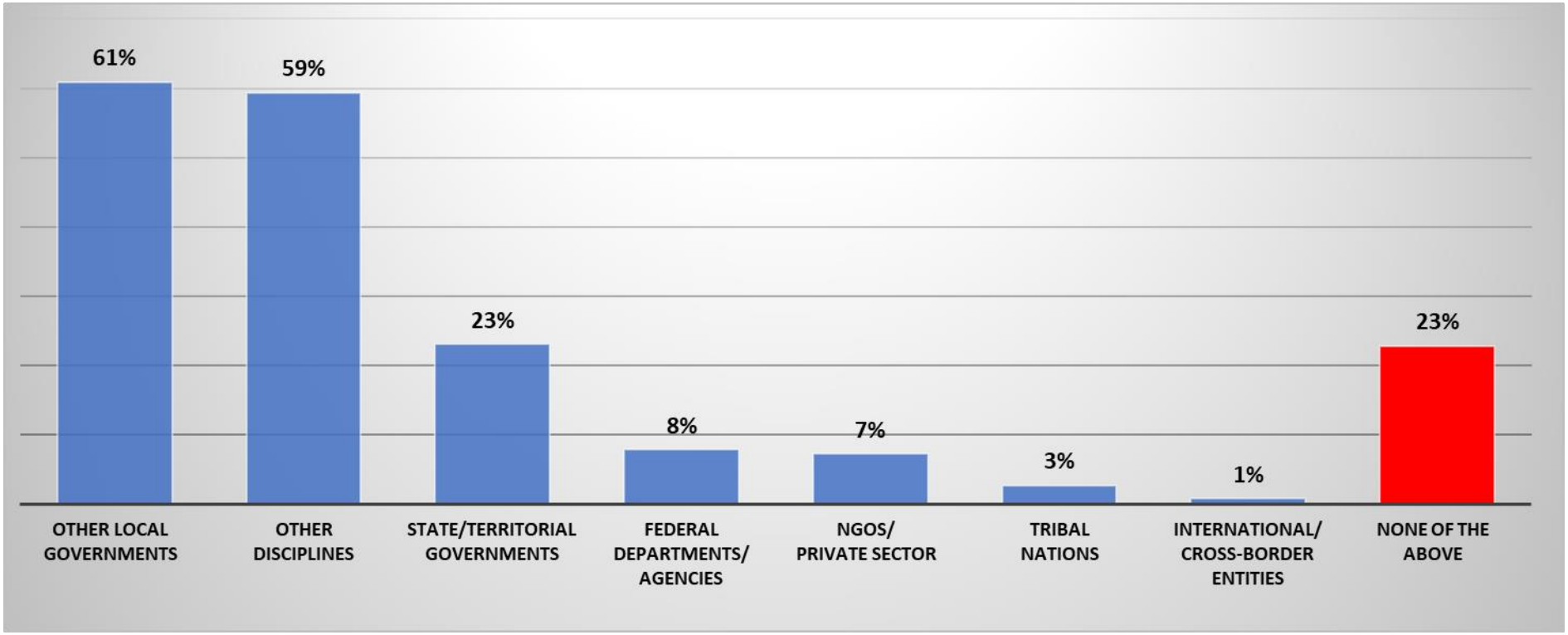


Data Description

- *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%)

Training with Other Organizations

Groups Included in an Organizations Emergency Communications Training



Data Description

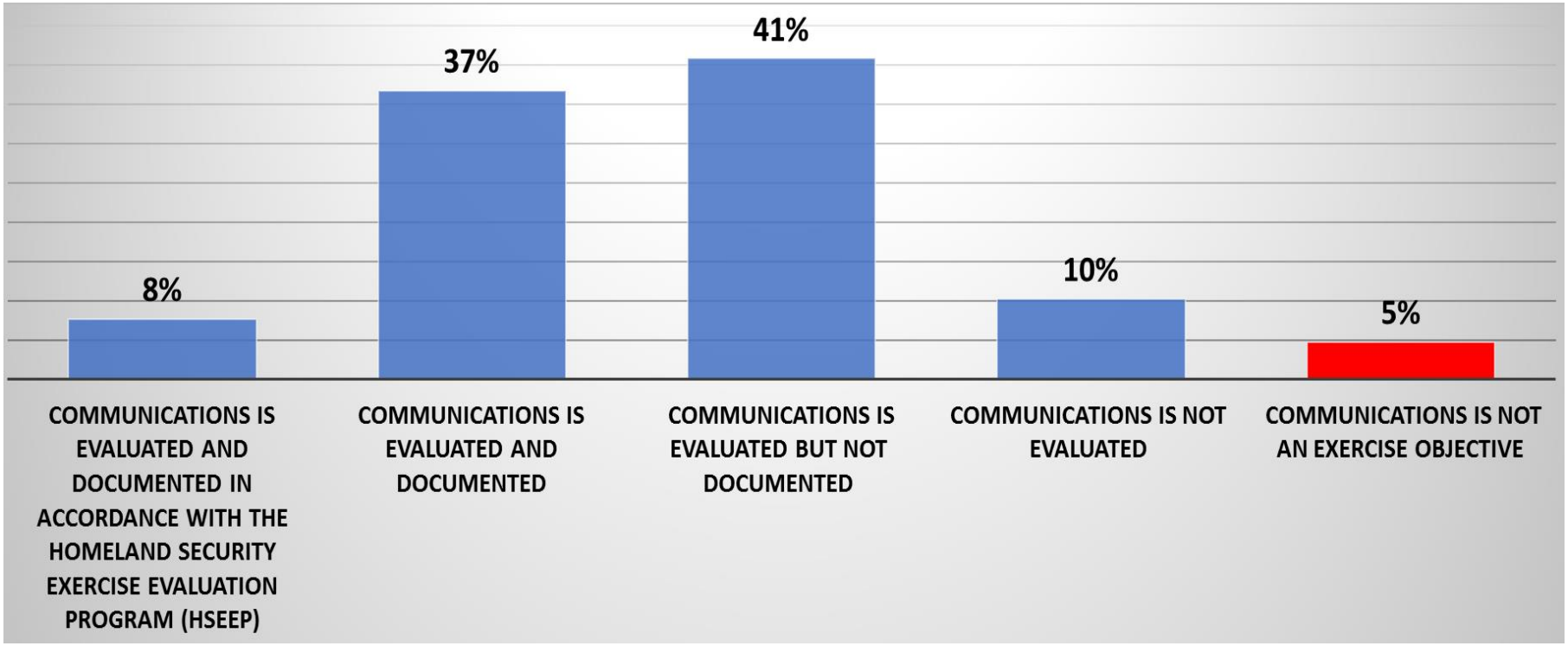
- *Of the 95% of organizations that train,* most organizations (roughly 60%) train with other disciplines or other local governments; and
- Nearly a quarter (23%) train with state/territorial governments; and
- Nearly a quarter (23%) do not train with other organizations

Exercises

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

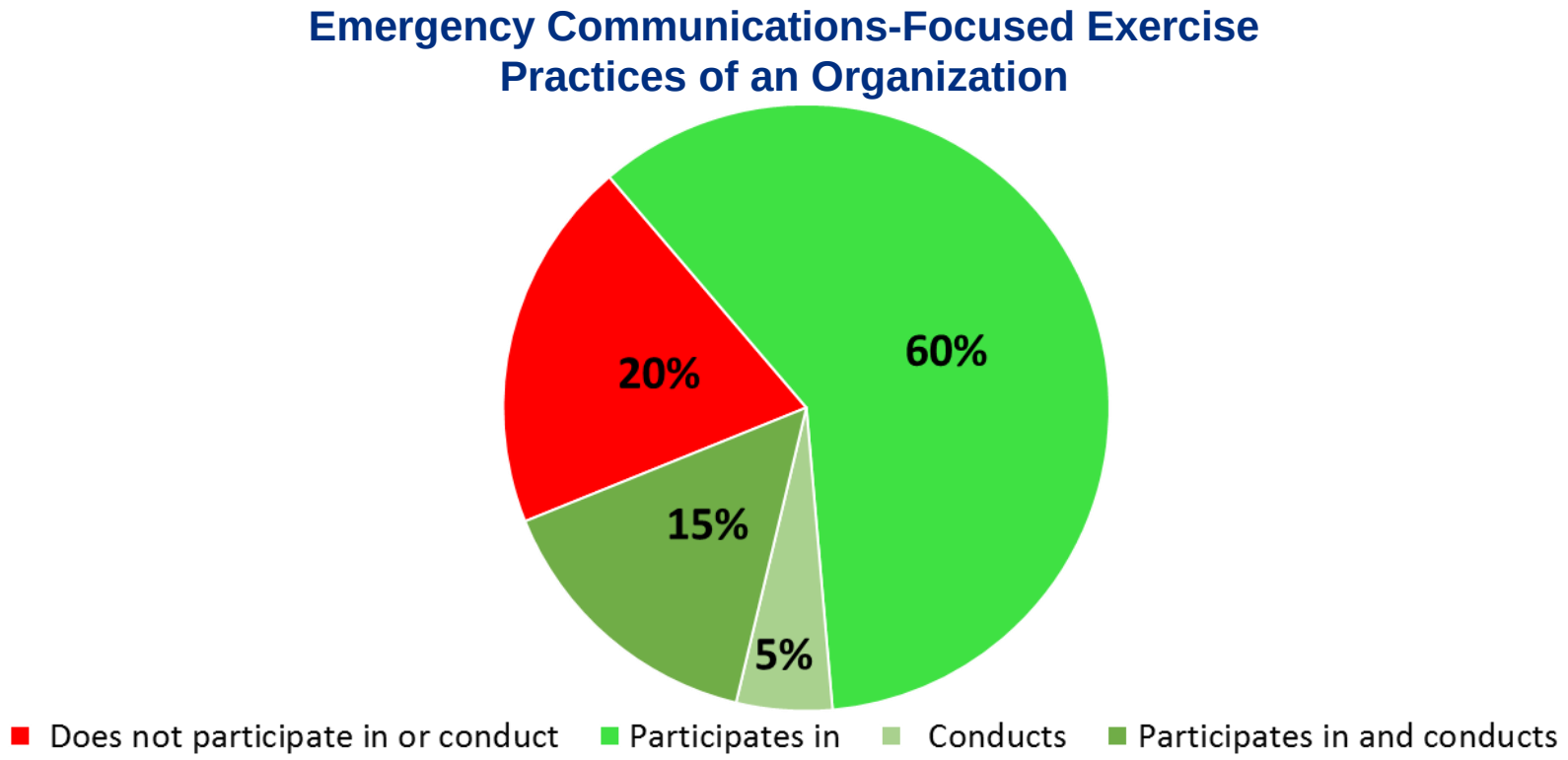
Communications as an Exercise Objective

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

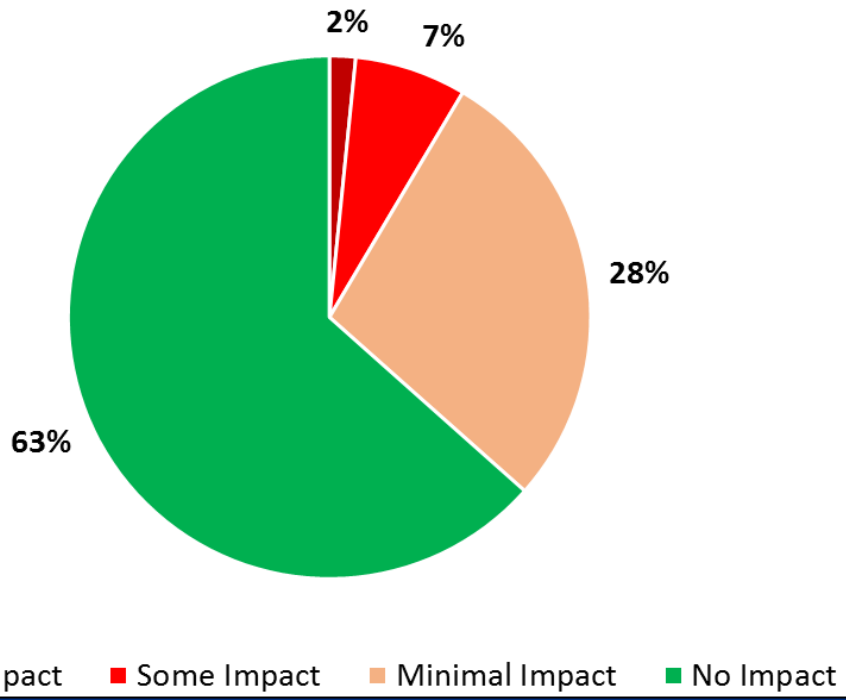


Data Description
▪ The majority of organizations (80%) conduct or participate in emergency communications-focused exercises

CYBERSECURITY

Cybersecurity Impact

Impact of Cybersecurity Incidents on Organizations over the Past 5 Years

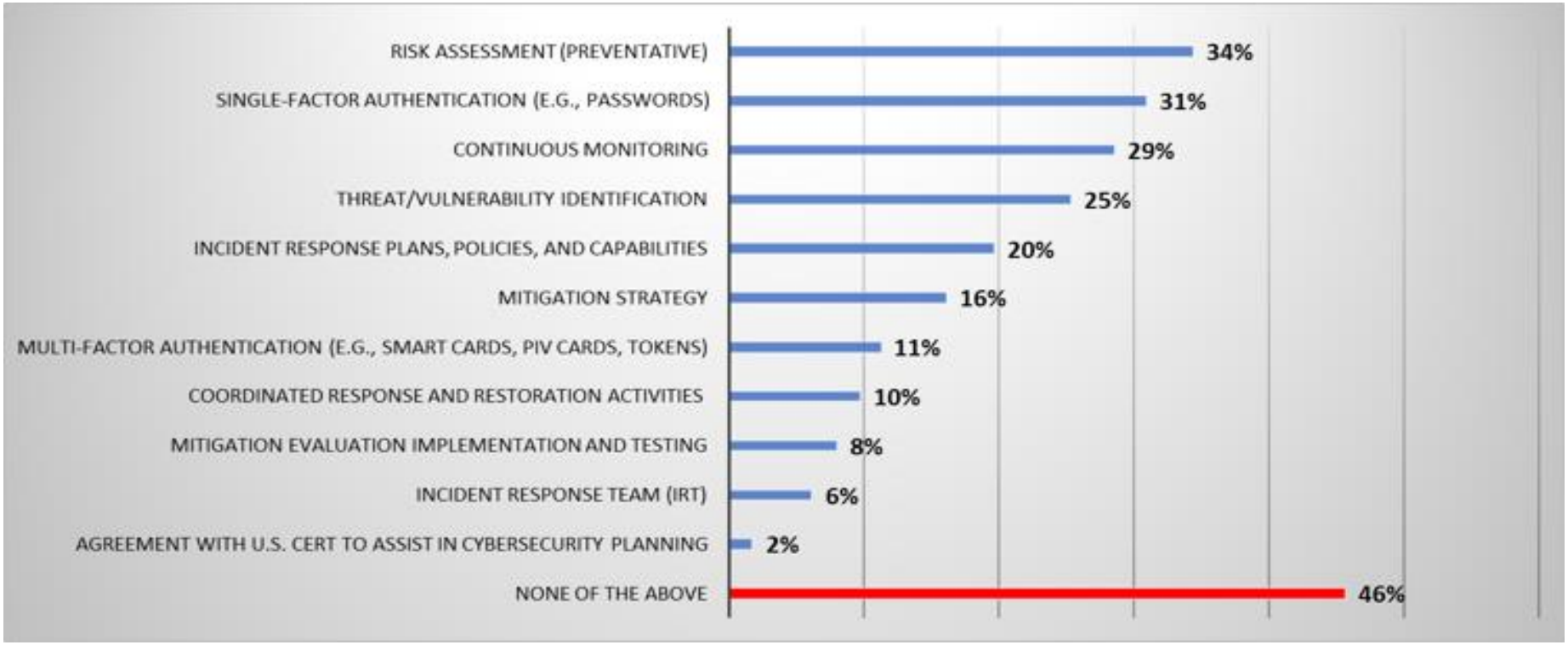


Data Description

- 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

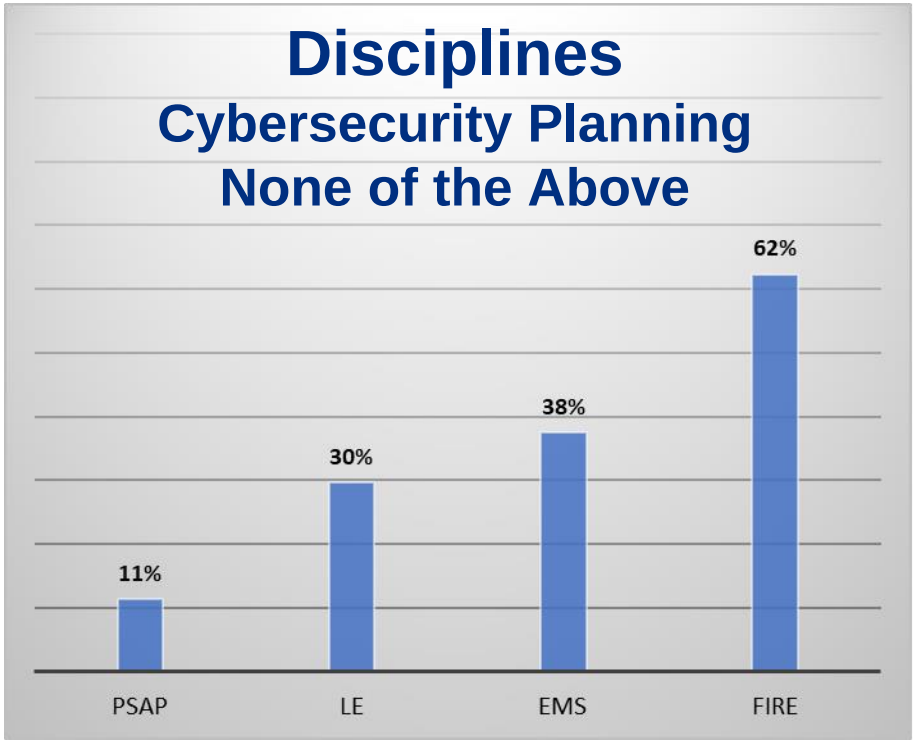


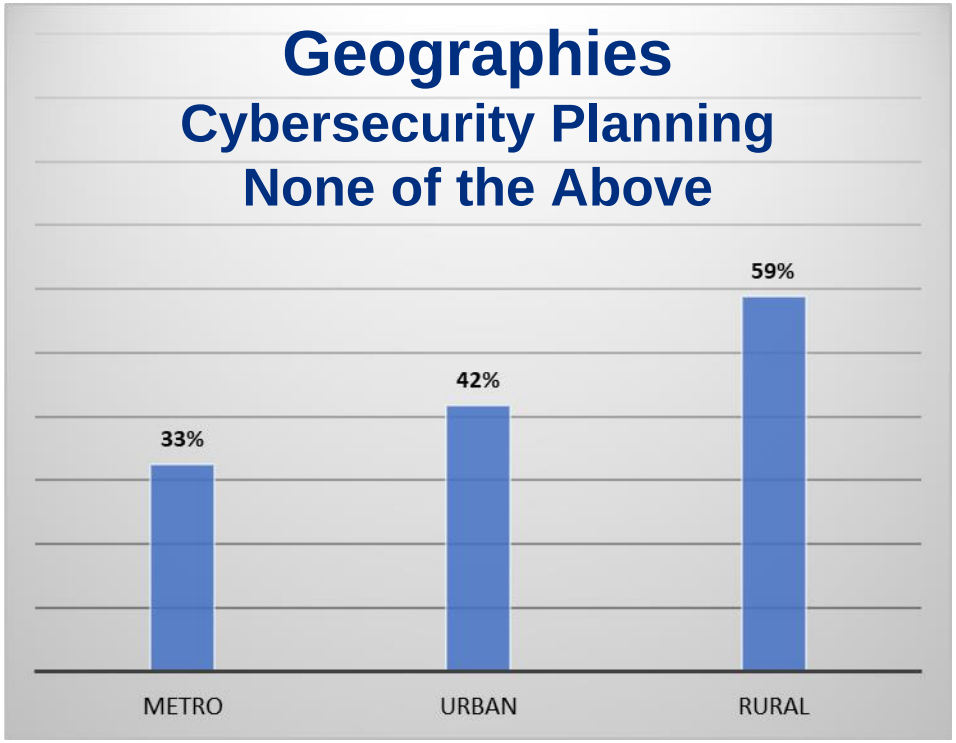
Data Description

- 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

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

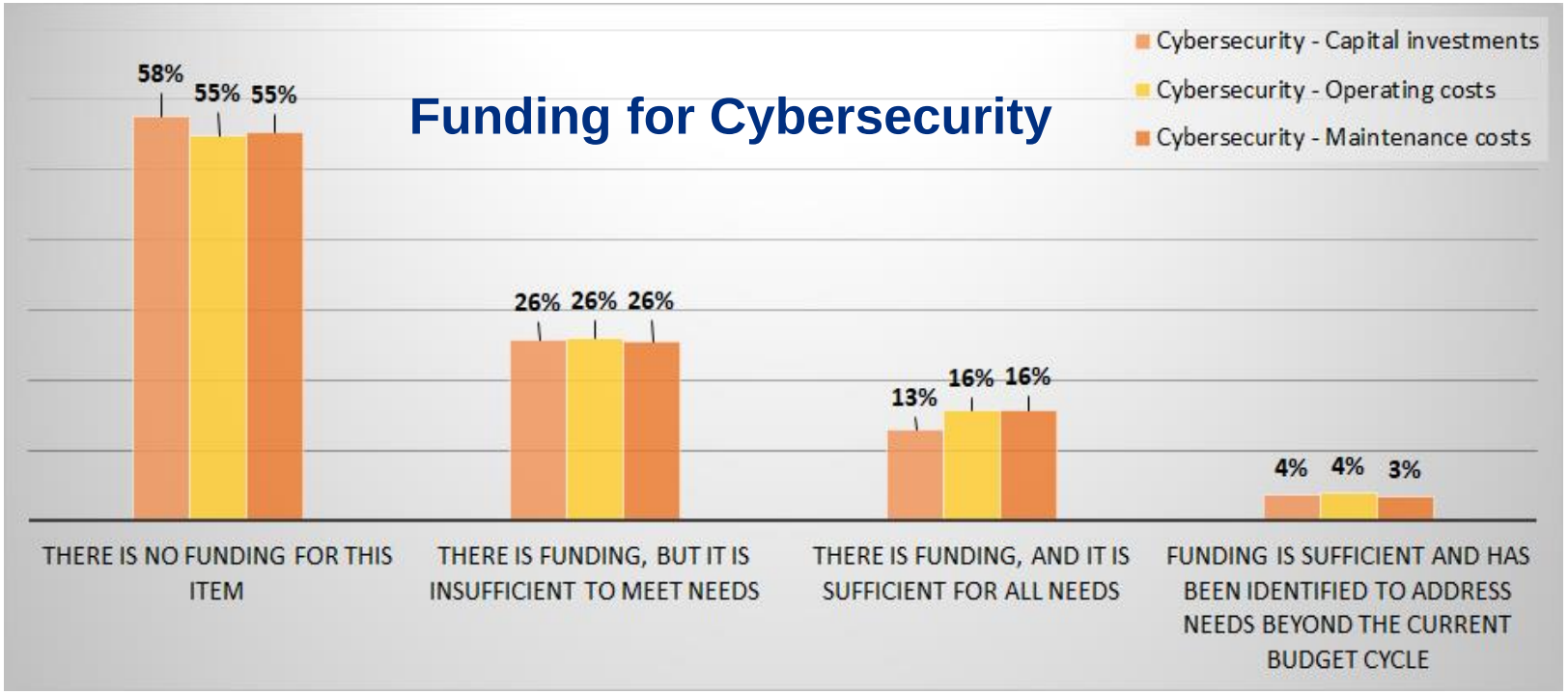




Cybersecurity Funding

✓***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



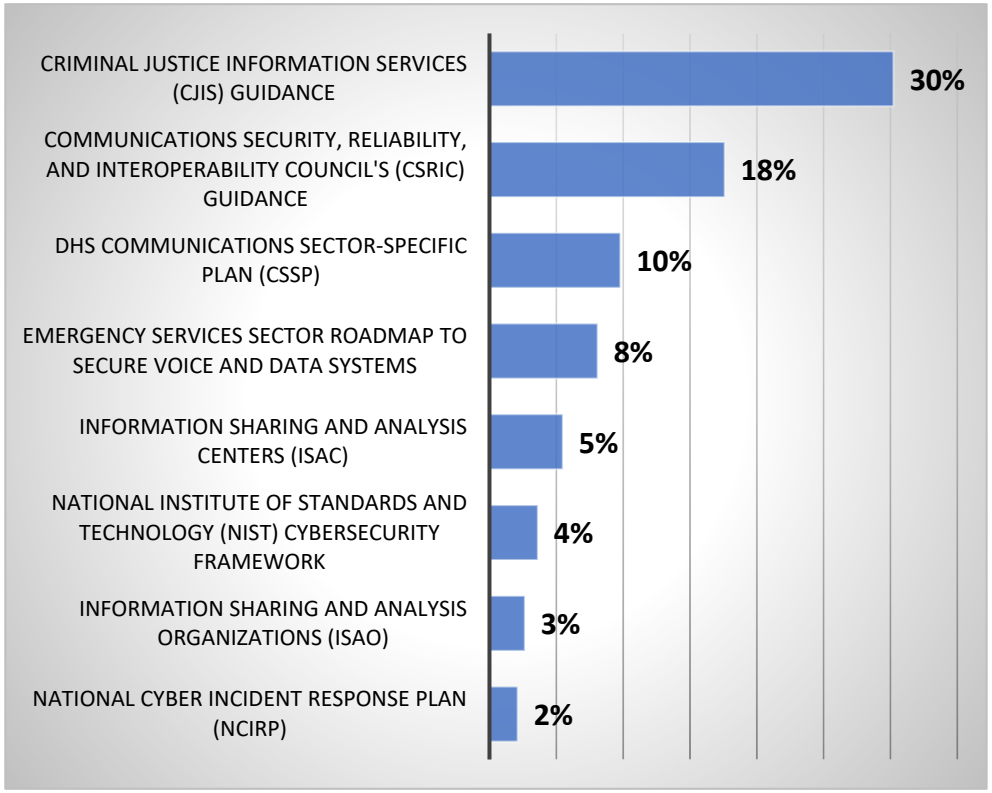
Additional Cybersecurity Insights

✓ ***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.

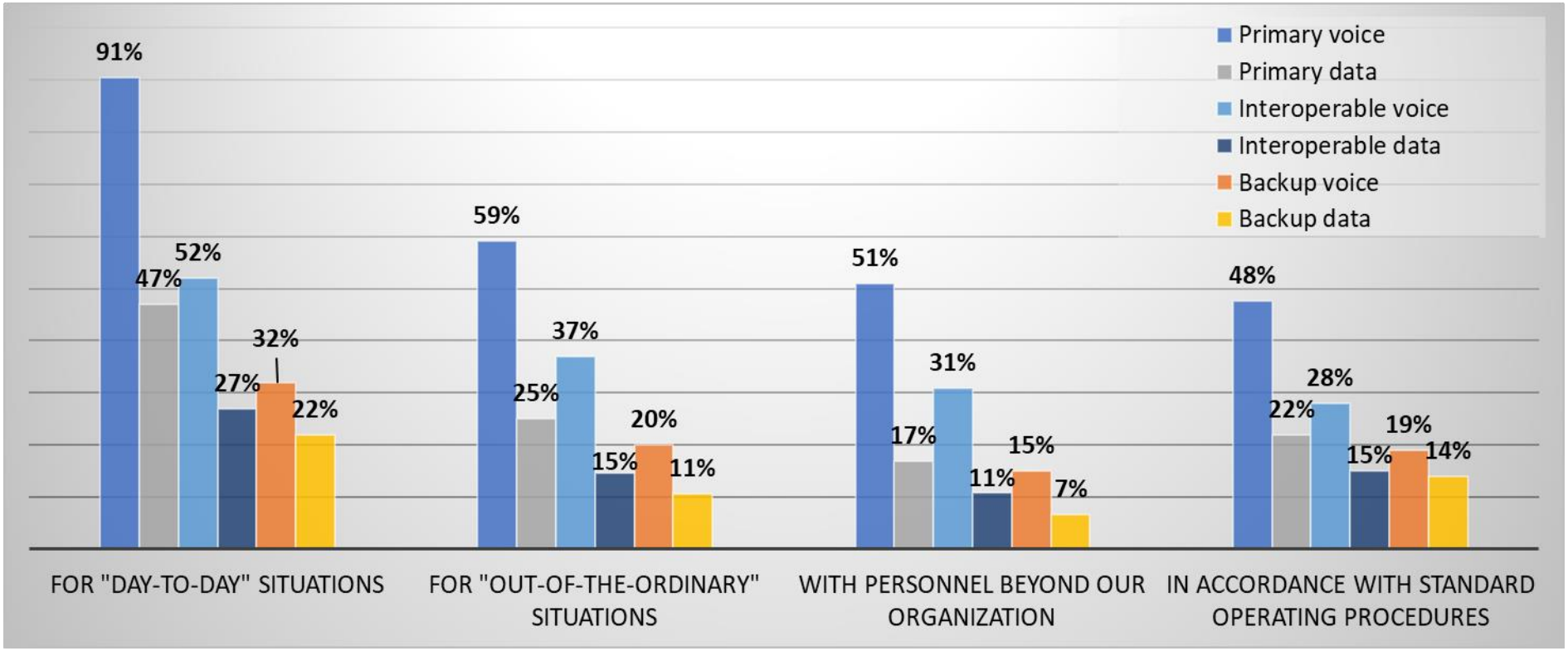


Cybersecurity Guidelines and Standards Influencing SOPs

USAGE

Capabilities Used (or Tested)

Emergency Communications Capabilities Used or Tested

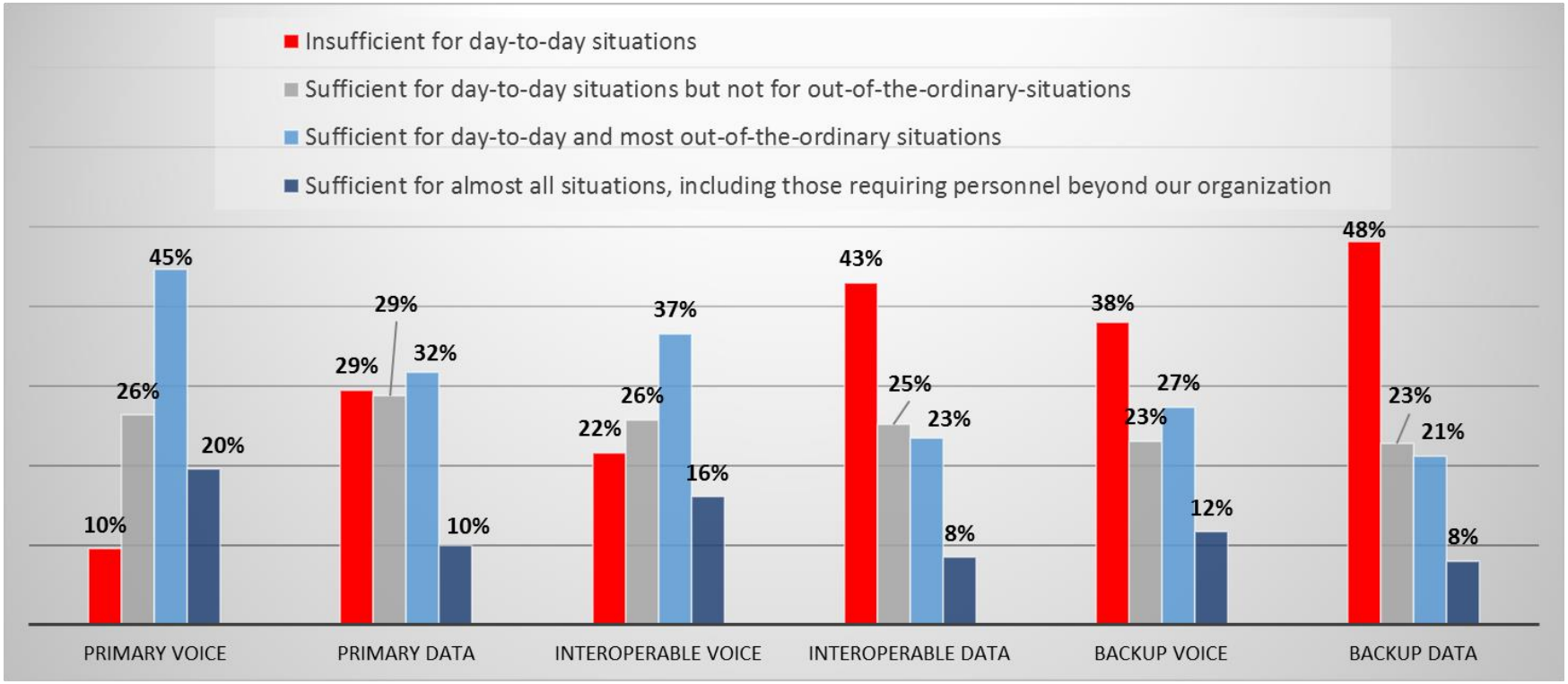


Data Description

- 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

Resource Capacity

Characterization of an Organizations Emergency Communication Resource Capacity



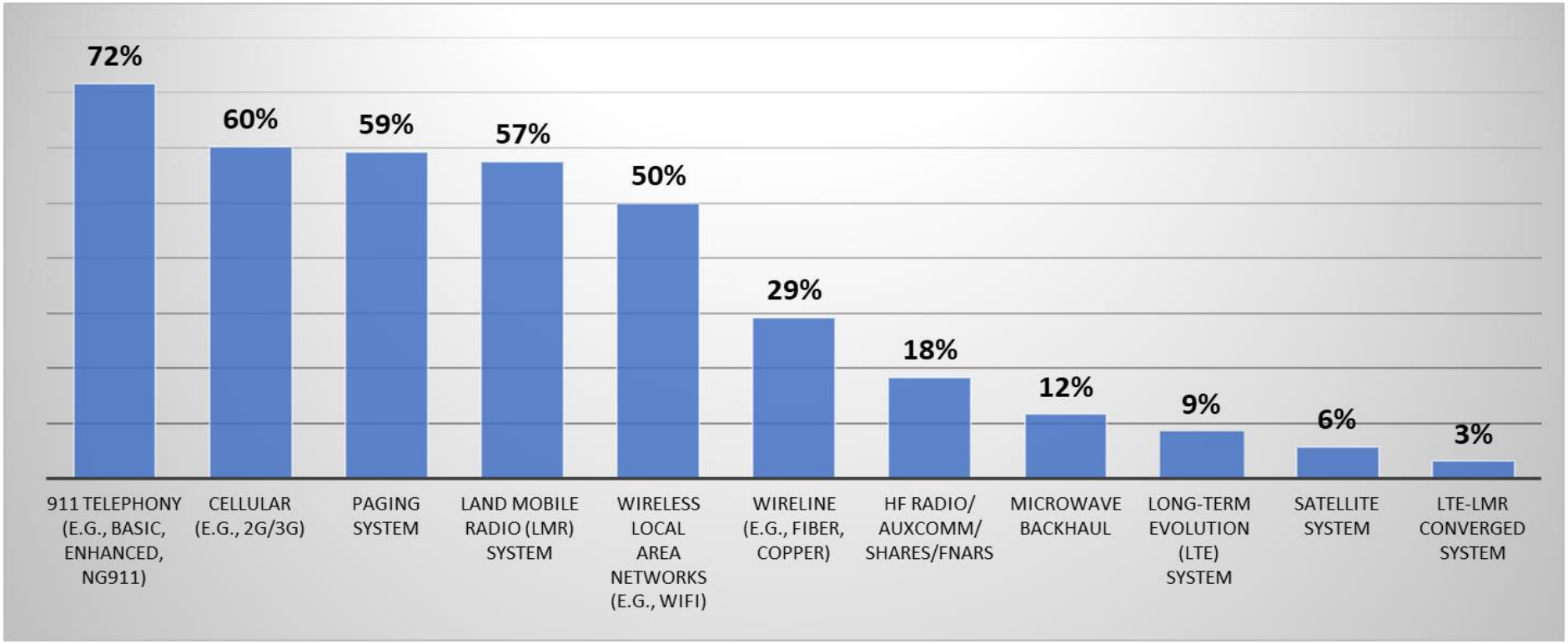
Data Description

- 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

EQUIPMENT

Systems In Use

Characterization of an Organizations Technology Systems in Use

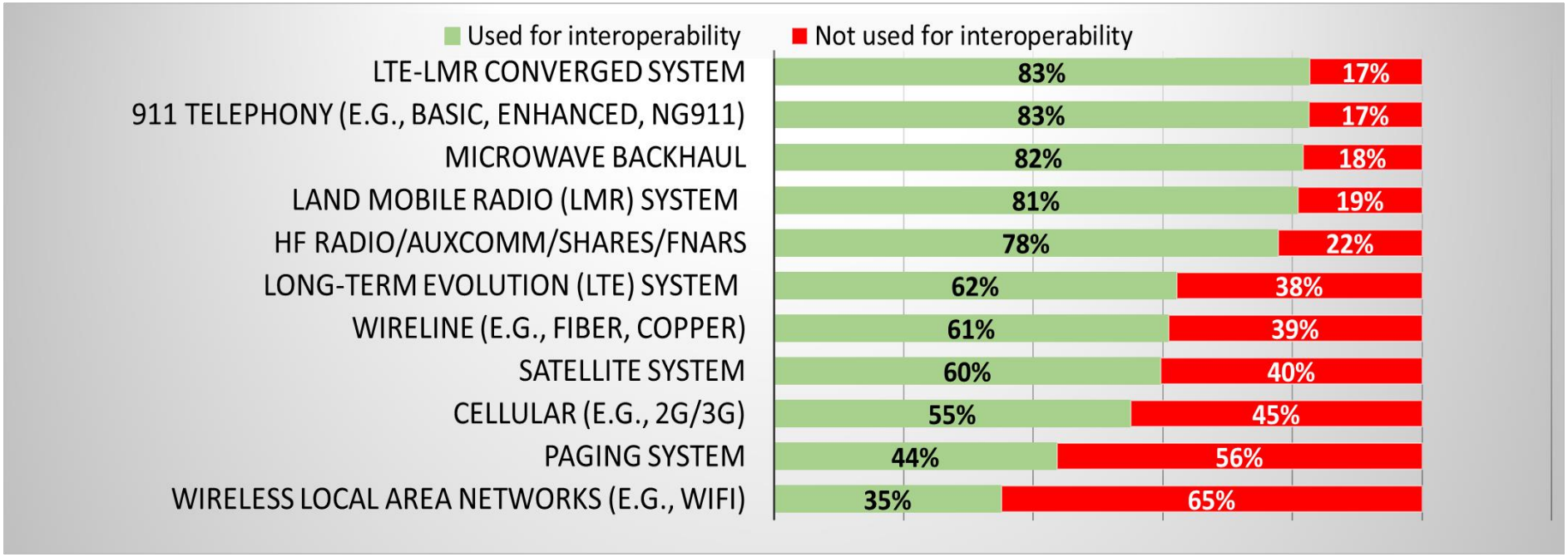


Data Description

- 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

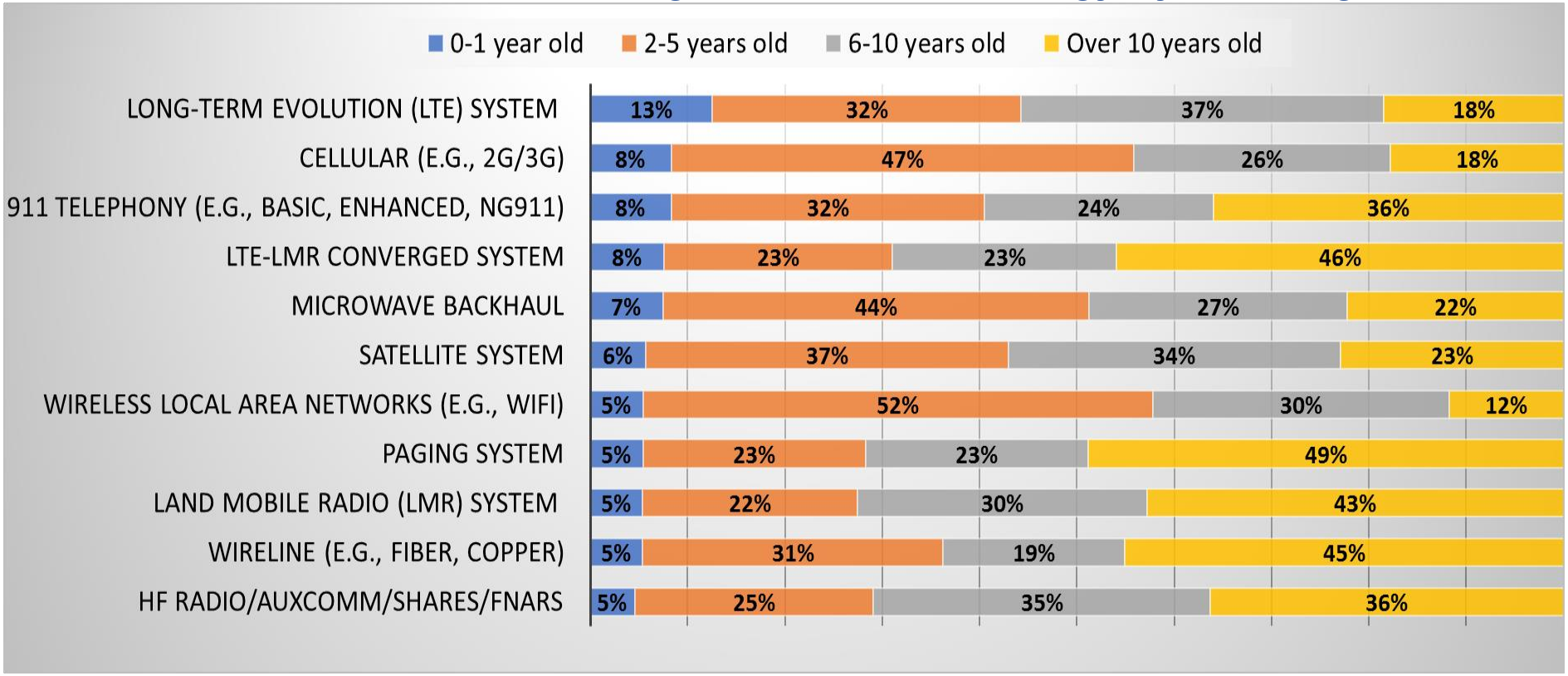


Data Description

- 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

System Age

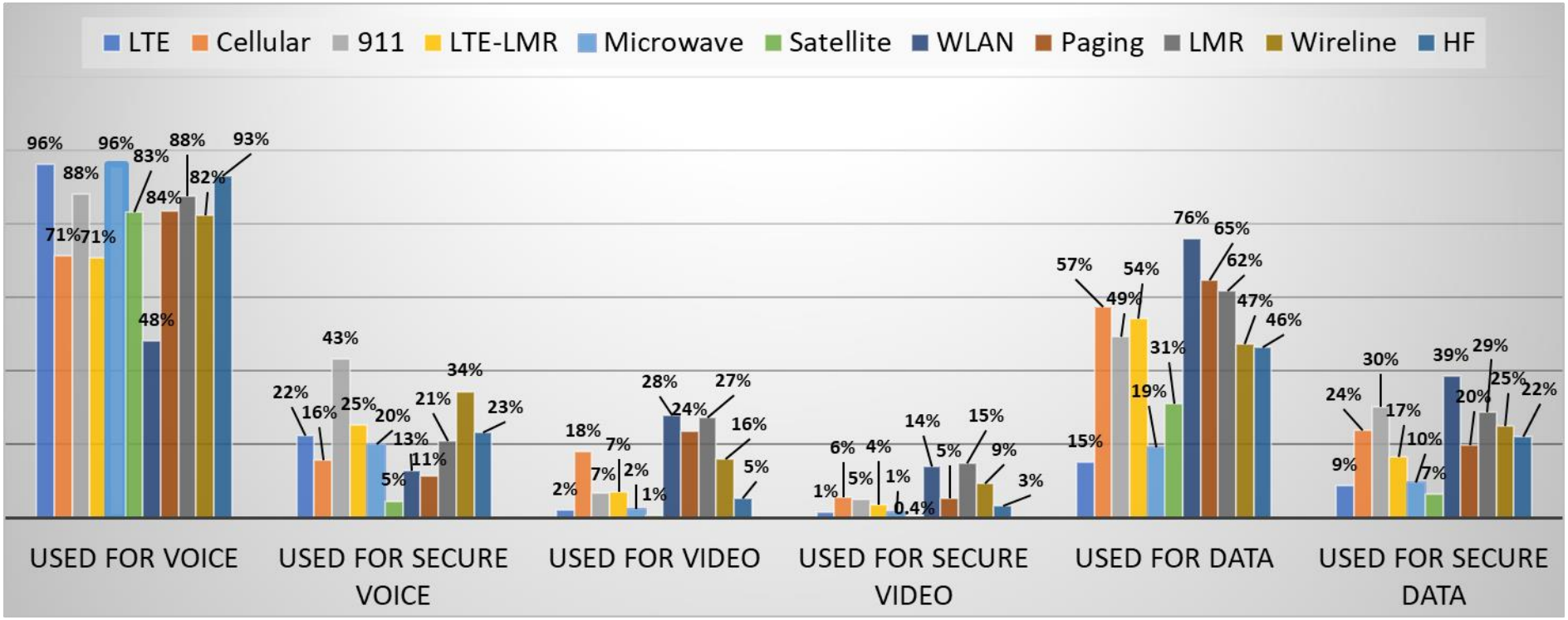
Characterization of an Organizations Technology Systems Age



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

System Usage – Type of Use

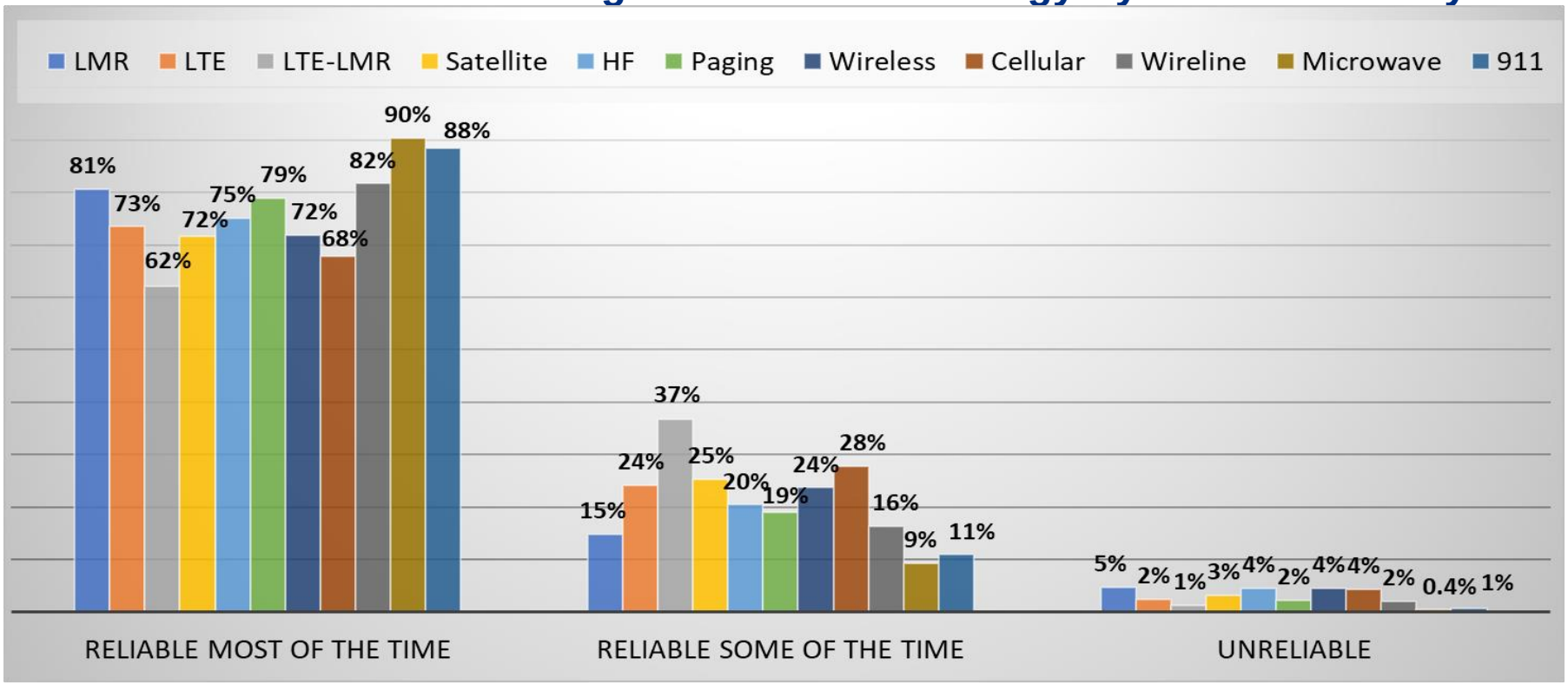


Data Description

- 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

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