Contingency Planning Guide for Emergency Communications Funding

Publication: March 2022
Cybersecurity and Infrastructure Security Agency

Table of Contents

INTRODUCTION

When disaster strikes, the need to communicate is immediate. States, territories, tribes, and localities rely on operable and interoperable communications to respond effectively to incidents, both large and small. While recognized as a priority across the nation, funding for emergency communications remains a challenge, especially in a period of stressed budgets and competing priorities. To ensure public safety stakeholders have the information they need to make effective decisions before, during, and after budget cuts, this guide provides a series of contingency considerations to justify investment in mission-critical components.

Recent national events, such as the COVID-19 pandemic, ongoing geopolitical tensions, and severe weather events have caused public safety agencies to reprioritize funding, often to the emergency communications community's detriment. In an already strained funding environment, budget reductions directly impact everything from project timelines to employment status. While the nation continues to face unprecedented events, it is important to note that the causes of funding cuts may come from multiple sources for various reasons. As a result, this guide provides considerations that help agencies navigate budget decisions, regardless of the event or decision impacting emergency communications funding.

The Cybersecurity and Infrastructure Security Agency (CISA), in partnership with SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC), developed the *Contingency Planning Guide for Emergency Communications Funding* to help decision-makers plan for the continuity of public safety communications budgets. Building off the Contingency Considerations When Facing Reductions in Emergency Communications Budgets fact sheet published in April 2021, this expanded guide provides a more comprehensive look at the considerations public safety officials must weigh when planning for or facing budget reductions. Specifically, this guide focuses on five mission-critical emergency communications components and provides detail on the considerations within each category, including personnel, operational costs, equipment, software, and a catch-all "other." Additionally, the guide features real-world examples showcasing the successful implementation of contingency planning best practices and considerations.

The public safety mission requires agencies to continue the performance of essential functions and deliver critical services across a broad spectrum of emergencies when events disrupt normal operations. Even if agencies' budgets are drastically reduced, emergency services must continue. While this guide focuses on contingency planning for *emergency communications funding*, it includes an overview of continuity planning and the risk analysis process. There are numerous resources to assist public safety agencies in assessing and mitigating risks, which decision-makers can incorporate into contingency plans. Comprehensive continuity planning is a diverse and complex field, with terminology often differing across the disciplines. As such, **Appendix A** provides a glossary with selected definitions of terms used within this guide to ensure consistency with national guidance and standards.[1]

CISA collaborated with the Joint SAFECOM and NCSWIC Funding and Sustainment Committee to gather input from members and other public safety experts to develop this guide. While suggestions in this guide might not apply to every public safety stakeholder or discipline, officials are encouraged to use this document as a resource when preparing for, responding to, or recovering from incidents that necessitate emergency communications budget cuts.

[1] The Federal Emergency Management Agency defines continuity terms at fema.gov/emergency-managers/national-preparedness/continuity/terms.

RISK ANALYSIS

Effective risk analysis relies on a cyclical, multi-step process to help agencies assess and communicate potential hazards and impacts. As seen in **Figure 1**, this process typically consists of four steps: identifying threats and vulnerabilities; conducting a risk assessment; communicating findings; and developing a response approach. In the context of emergency communications, public safety officials can leverage this process to determine mission-critical functions and prioritize areas for funding. For a more comprehensive view and explanation of the risk analysis process, refer to **Appendix B**.

The first step to conducting a successful risk analysis is identifying the specific challenges that a public safety agency is facing or may eventually face. Understanding that these hazards vary across jurisdictions, stakeholders are encouraged to use state, local, and regional resources to determine their most pressing threats and vulnerabilities. For more information, reference the **Available Resources** section of this guide.

Figure 1: Risk Analysis Process

Once public safety officials identify threats and vulnerabilities, they must conduct a risk assessment to determine the probability and impact of potential incidents. While there are multiple approaches to conducting a risk assessment, each evaluation strategy shares the same goal: understanding the likelihood and severity of potential hazards. After officials have completed a risk assessment, it is crucial to communicate findings with leadership and determine an appropriate risk response. These responses should be codified into planning, training, and exercise materials and revisited regularly to ensure viability and continuity.

Available Resources

Table 1 summarizes resources from the Federal Emergency Management Agency (FEMA), CISA, and the National Institute of Standards and Technology (NIST) that provide information on continuity planning and risk assessments, which aid in developing contingency plans.

Table 1: Continuity Planning and Risk Assessment Resources

Office	Resource	Description
FEMA	National Continuity Programs (NCP)	Serves the public by coordinating the federal programs and activities that preserve the nation's essential functions across a wide range of potential threats and emergencies. On behalf of the White House, the Secretary of Homeland Security, and the FEMA Administrator, NCP guides and assists the planning and implementation of continuity programs that enable federal, as well as state, local, tribal, and territorial (SLTT) governments to perform their essential functions and deliver critical services throughout all phases of a disaster.
	Continuity Guidance Circular	Provides a resource for the whole community to integrate and synchronize continuity efforts and may be used as a reference by organizations developing continuity plans, programs, and processes.

Office	Resource	Description
FEMA	Continuity Assessment Tool	Helps jurisdictions to assess plans and programs and identify shortfalls or gaps to guide requests for technical assistance.
	Continuity Resource Toolkit	Provides examples, tools, and templates for implementing each chapter of the Continuity Guidance Circular.
	Continuity Courses	Delivers training to enhance partners' continuity knowledge and expertise.
	FEMA National Risk and Capability Assessment	Offers a suite of assessment products that measure risk and capability across the nation in a standardized and coordinated process. Products include the Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR). When analyzed together, these products create a measurement of national risks, capabilities, and gaps.
	Comprehensive Preparedness Guide	Provides guidance for conducting the THIRA and SPR process.
	Increasing Resilience Using THIRA/SPR and Mitigation Planning	Assists SLTT governments to recognize opportunities to understand threats and hazards, assess risks, build and sustain capabilities, reduce vulnerability, identify ways to increase resilience, and avoid duplication of effort.
CISA	Cyber and Risk Assessments Suite	Provides services and tools that support an assessment of cybersecurity risks to the agency's operations (i.e., mission, functions, image, or reputation), organizational assets, and individuals.
	Interoperable Communications Technical Assistance Program (ICTAP)	Serves all 56 states and territories and provides direct support to SLTT emergency responders and government officials by developing and delivering training, tools, and onsite assistance to advance public safety interoperable communications capabilities. Technical Assistance service offerings help emergency responders continue to communicate during disasters or large-scale planned events. These ICTAP services, which are provided at no cost, include instruction and assistance with the planning, governance, operational, and technical aspects of developing and implementing interoperable communications initiatives.
NIST	Contingency Planning Guide for Federal Information Systems	Addresses specific contingency planning recommendations for three platform types and provides strategies and techniques common to all systems: 1) Client/server systems; 2) Telecommunications systems; 3) Mainframe systems. In addition, this guide defines a seven-step contingency planning process that an organization may apply to develop and maintain a viable contingency planning program for their information systems.
	Risk Management Framework for Information Systems and Organizations	This publication contains comprehensive updates to the Risk Management Framework. The updates include an alignment with the constructs in the NIST Cybersecurity Framework.

In addition to these national resources, public safety agencies should coordinate with their Statewide Interoperability Coordinator (SWIC) for recommendations specific to their area. SWICs manage the Statewide Interoperability Communication Plans (SCIPs), which are locally-driven, multi-jurisdictional, and multi-disciplinary statewide plans to enhance emergency communications. The SCIP creates a single resource for all stakeholders and a unified approach for improving interoperable communications for public safety and officials at all levels of government. Since SCIPs define the current and future direction for interoperable and emergency communications within a state or territory, agencies should understand the strategic direction of all emergency communications and priorities when planning.

SWIC Roles

In addition to their primary function of planning and implementing the statewide interoperability program and SCIP, SWICs also provide subject matter expertise to decision-makers on emergency communications investments, as summarized in **Figure 2**. These contributions ensure funding is coordinated, aligns to the SCIP, and is compatible with surrounding systems. In addition, during periods of reduced funding, SWICs can help leadership accurately prioritize investments. By understanding the capabilities and gaps in their state's emergency communications posture, SWICs are uniquely positioned to make informed decisions on which mission-critical components require funding.

SWICs additionally act as a liaison to the federal government on issues concerning statewide interoperability, including funding challenges. As they play an integral role in establishing and maintaining statewide governance, it is important for areas with diverse communications systems and geography to include SWICs on all relevant correspondences and governance boards. This coordination will ensure SWICs can identify funding opportunities, leverage shared capabilities, and prevent duplicative purchases. Through coordination, SWICs also share success stories that are instrumental in developing products and strategies to advocate and secure funding for interoperability solutions within their respective states and at the federal level.

How Do SWICs Contribute to Funding Decisions?

SWICs are experts on their states' emergency communications and can accurately prioritize funding during periods of reduced budgets

SWICs act as a liaison to the federal government on issues concerning statewide interoperability, including funding challenges

Without a designated, full-time SWIC or SWIC Program, states are not eligible for certain federal grants

Figure 2: SWIC Roles in Funding

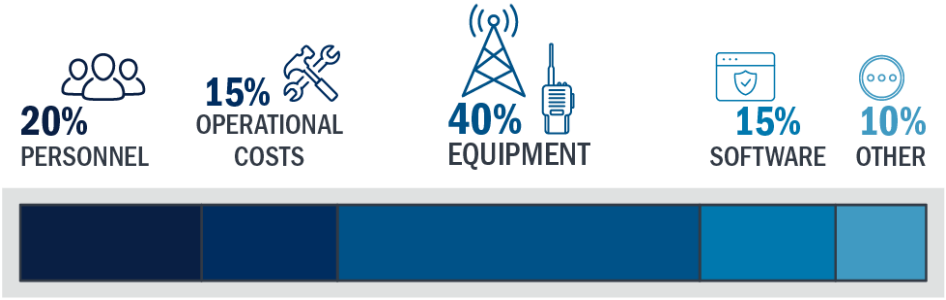
Finally, without a designated, full-time SWIC or SWIC Program, states are not eligible for certain federal financial assistance programs, as noted in **Figure 3**. These programs include the Department of Homeland Security's (DHS) State Homeland Security Grant Program and Urban Area Security Initiative, the two largest federal emergency communications funding sources.[2] Public safety agencies should contact their respective SWIC for more information on roles and responsibilities or to assist with funding decisions.

Figure 3: Grant Eligibility and SWICs

[2] For more information on DHS Preparedness Grants, visit: fema.gov/grants/preparedness.

CONTINGENCY CONSIDERATIONS

This section provides a comprehensive view of the considerations public safety officials must weigh when planning for or facing budget reductions. Specifically, this guide focuses on five mission-critical emergency communications categories, including personnel, operational costs, equipment, software, and a catch-all "other." While **Figure 4** provides an example budget of these categories and potential line items, SAFECOM and NCSWIC recognize each public safety agency's funding posture is different. As a result, the considerations in this guide may not apply to every organization. Any budget decision will come with its particular tradeoffs, and, as such, SAFECOM and NCSWIC do not endorse any one decision or course of action.



Category	Item	Example	Costs
	Full-time positions	Employees who are paid a salary and typically work 40 hours a week	$500,000.00
	Part-time positions	Employees who typically do not work 40-hour weeks	$165,000.00
	Overtime	Surge support from existing staff	$25,000.00
	Backfill	Surge support from new or existing staff	$10,000.00
	Training	Funds for employee development, including courses and workshops	$50,000.00
	Benefits	Health and dental insurance; leave programs; education benefits	$250,000.00
	Facility	The rented or owned location where staff report to work	$565,000.00
	Facility Repairs	Plumbing, electrical, etc.	$30,000.00
	Utilities	Water and electricity	$70,000.00
	Replacement Parts	Capital spares; interchangeable parts	$20,000.00
	Incidentals	Gas, fuel, etc.	$15,000.00
	Services (Contracts)	Vendors used to support facility rental or maintenance	$50,000.00
	Backup Site Rental	Funds for use in case of facility outage	$50,000.00
	Maintenance	Funds to test or repair broken equipment	$75,000.00
	Subscriptions	Cost for total radio rental from a partner organization	$10,000.00
	System Upgrades	Funds for equipment upgrades	$5,000.00
	Capital Investments	Site and tower construction; fixed network equipment	$1,860,000.00
	Licenses	Subscription or one-time purchase costs	$550,000.00
	Maintenance	IT support	$200,000.00
	Other	Expenses that fall outside of normal categorization	$500,000.00

Figure 4: Sample Emergency Communications Budget and Categories

Personnel

CISA, SAFECOM, and NCSWIC continue to recognize the importance of funding and sustaining emergency communications personnel. As demonstrated through Goal 1 of the National Emergency Communications Plan, governance and leadership remain essential to the nation's public safety mission. Without developing and maintaining strong governance, public safety agencies risk losing the capacity to effectively plan, address capability gaps, and contribute to national emergency communications efforts. As noted in the 2018 SAFECOM Nationwide Survey (SNS) findings, 38 percent of respondents reported their SWIC informs state executive leadership on efforts to advance public safety communications and interoperability. Therefore, funding these SWIC positions and other emergency communications personnel is critical to informing state leadership on how to secure both day-to-day and emergency operations. This section explores how to advocate for personnel funding before, during, and after budget cuts to maintain these essential services and positions.

Before

Public safety officials should consider preparing justifications for current staff and their roles in advance of budget cuts. Detailed accounts of each position's contribution to the agency may help maintain essential staffing during times of financial constraint. Officials should also consider connecting roles to mission-critical functions. For example, officials can better convey each position's value to leadership by outlining personnel duties during steady-state and response operations.

Within these justifications, agencies may also consider plans for mitigating financial hardship, including modifications to staff roles. For example, revisions to position hours, duties, and pay schedules can be completed in advance of budget cuts, assisting officials in determining how to best maintain essential staffing and customer service levels through periods of fiscal instability. In addition, public safety officials should consider incorporating a restoration schedule into existing plans. A comprehensive restoration plan that outlines the steps necessary for an eventual "return to normal" can help ease the transition back to routine functions, alleviate uncertainty among staff, and provide budgetary projections for personnel.

In addition to planning activities, officials should consider allocating or reallocating unspent balances from current year budgets to mitigate the effect of potential budget cuts in the future. By collaborating with decision-makers to find ways to roll over unused funding, officials can create a safety net for future funding gaps. For example, Goodhue County, Minn., reallocated part of their unspent personnel budget towards their Radio Infrastructure Fund, allowing the county to retain funding for future capital investments.

Goodhue County, Minn. Creates Emergency Fund

Goodhue County, Minn., utilizes a unique solution to ongoing public safety funding challenges: an enterprise fund. This emergency communications-specific fund, titled the Radio Infrastructure Fund, has been used to offset unforeseen costs due to equipment failures, required or unexpected upgrades, or reduced budgets, as well as fund more routine purchases. Each year, Goodhue County contributes funding which can be either used or saved, at the discretion of the officer in charge. Since 2019, this fund has provided flexible solutions for retaining emergency communications funding, especially following vendor contract and renegotiations. Rather than having unspent personnel funding reallocated to another department or office, Goodhue County continues to retain ownership of the Radio Infrastructure Fund, allowing the county to control how it's used and save for larger investments in the future.

During

During budget cuts, agency leadership often considers staff reductions as the most straightforward path to fiscal balancing. However, the consequences of furloughs and hour reductions often outweigh the benefits. Public safety agencies should recognize the challenges posed by overtime, staff reductions, and eventual rehiring. To start, reducing staff capacity often forces remaining staff to work overtime. While efforts to ensure mission-critical operations are essential, public safety agencies should recognize that overtime is usually more expensive than regular pay and may diminish any savings initially accrued from reduced staffing. Hour reductions and staff furloughs also open public safety agencies to risks with rehiring. By temporarily reducing staff, agencies may permanently lose positions during budget realignment.

Furthermore, furloughing staff often incentivizes personnel to find a new position within competing markets. This challenge, coupled with the potential of hiring freezes, may leave public safety agencies short-staffed even after a budget is restored. Additionally, if a public safety agency can replace staff, officials should recognize that costs associated with training are often more expensive than retaining staff during financial hardships.

Public safety officials should also be aware of existing contractual requirements for personnel. For example, when an agency has backfill contracts or clauses, the organization remains legally obligated to follow through on agreements, even if staff have been furloughed for financial reasons. Without planning for contractual obligations, any difficulties funding personnel may be exasperated.

After

Following budget cuts, there are still steps public safety agencies can take to reduce impacts on personnel. For example, agencies should consider encouraging members to attend conferences, training courses, and other events virtually. Virtual attendance can substantially reduce travel costs while still fulfilling position, governance, education, and networking goals. In addition, while officials may be tempted to cut training budgets outright, planning for employees to attend trainings is often necessary for staff to maintain job-essential certifications. Agencies should also consider that money saved by travel alternatives may be reallocated towards other budget needs or saved to mitigate future financial insecurity.

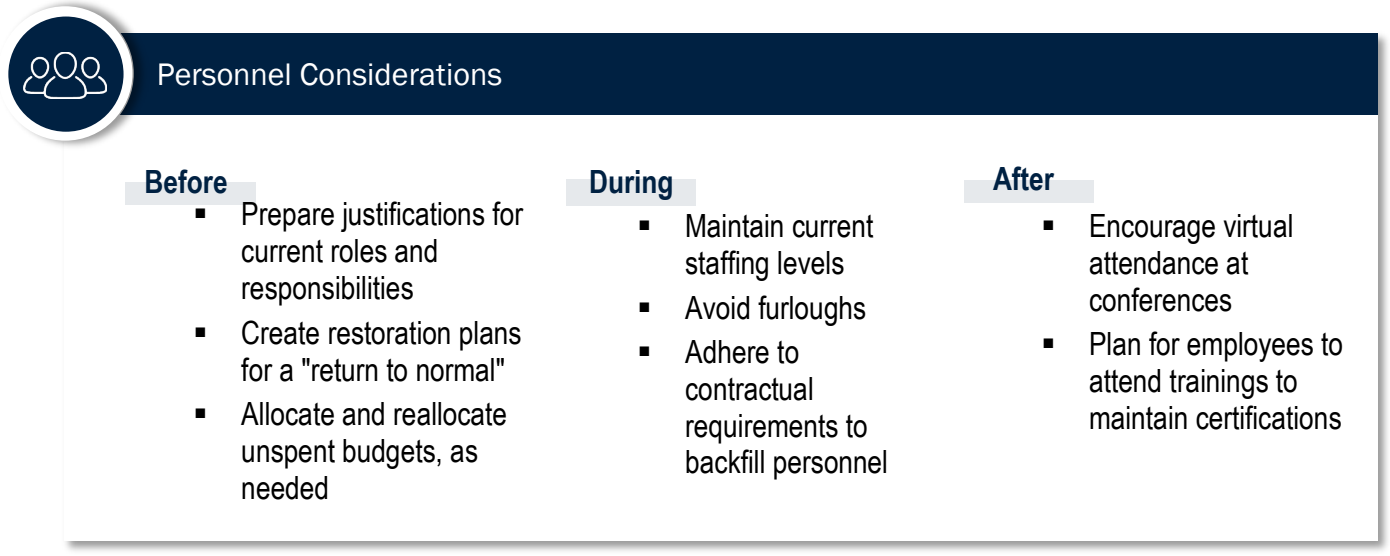


Figure 5: Personnel Considerations

Operational Costs

Operational costs, which typically include ongoing expenses incurred through daily operations, are vital to maintaining mission-critical emergency communications capabilities. Without the ability to fund recurring costs, public safety agencies risk losing essential services and contracts. Therefore, stakeholders should refer to the following section for considerations on how to ensure funding before, during, and after budget cuts.

Before

Before budget cuts occur, there are several steps public safety agencies can take to ensure continued support for operational costs. First, officials should evaluate current incidental consumption and consider setting aside a "rainy day" fund for consumables, such as fuel. In the event of a budget disruption, earmarked funds may help reduce interdepartmental competition and ensure continuity of operations. Additionally, having these funds set aside before fiscal challenges occur may ensure a smoother transition when unexpected events strain budgets. Finally, officials should consider planning for site consolidation in anticipation of future budget cuts. As seen through the 2020 disaster season, many public safety agencies have implemented site consolidation as a cost-savings method for mortgages or leases. Having an emergency site consolidation plan in place, well in advance of budget cuts, will help ensure agencies meet operational costs during unexpected challenges.

During

Amid budget cuts, public safety officials should consider both the immediate and long-term impacts of reduced funding for operational costs. In the near term, reducing existing services or contracts (e.g., subscriptions, rent, leases, licenses) may affect an organization's ability to perform critical response functions. However, agencies should also communicate the lasting impacts of defaulting on contracts to leadership and decision-makers. Officials should understand how terminating or reneging on contracts may result in late or legal fees, increasing the cost of services long-term. Defaulting may also negatively impact credit scores, making it more difficult to secure certain funding mechanisms (e.g., bonds) in the future.

After

Following periods of budget disruption, public safety agencies should consider revisiting existing contract terms to reduce or modify payment schedules. For example, organizations may choose to refinance mortgages or adjust existing interest rates after times of fiscal stress. These renegotiations may reduce operational costs in the short term and lower premiums going forward.

Operational Costs Considerations

Before

- Set aside funding for incidentals or consumables
- Consider funding backup fuel reserves and/or secondary sites
- Plan for site consolidation

During

- Recognize that terminating or defaulting on contracts may result in late/legal fees or reduced credit scores

After

- Consider renegotiating contract terms to modify payment schedules
- Refinance for lower interest rates

Figure 6: Operational Costs Considerations

Equipment

Emergency communications equipment is often one of the most significant investments public safety agencies must account for during annual budget planning. To meet mission-critical needs, agencies must balance financial challenges to maintain and sustain existing equipment, keep pace with rapid technological advancements, and integrate and align technologies to support system reliability, security, and interoperability. The following section offers several considerations to help stakeholders fund equipment before, during, and after budget cuts.

Before

Emergency communications equipment operations and planning can be complex. In preparing annual budgets, agencies should consider reviewing existing equipment and cataloging anticipated maintenance activities. Necessary or preventative maintenance repairs should be identified, prioritized, and aligned to mission-critical needs to help quickly justify costs to leadership.

Public safety officials should also recognize some emergency communications systems have recurring costs associated with their equipment and infrastructure. As such, stakeholders should view contractual obligations for leased or rented resources (e.g., backhaul connection services, subscriber units) as necessary expenses. Compiling a comprehensive view of existing maintenance and contractual costs will help decision-makers understand the necessity of an inclusive equipment budget, even during times of financial stress.

During

Agencies should take several considerations into account when reviewing equipment costs during periods of budget instability. First, public safety officials must recognize that sustaining operable and interoperable communications requires funding for both system-level support (e.g., managing software, access, outages) and maintenance activities (e.g., repairs, batteries). Second, while each agency may have multiple systems, often at different stages of the equipment lifecycle, it is imperative to account for the total cost of all equipment accurately and immediately communicate findings to leadership. Quick and transparent communication with public safety decision-makers will ensure any immediate challenges are flagged and mitigated.

City of Kilgore, Texas Signs MOU to Share Upgrade Costs

In 2021, the City of Kilgore, Texas approved the Interlocal Agreement for Statewide Emergency Radio Infrastructure to upgrade their existing public safety communications system. By partnering with the East Texas Council of Governments, Kilgore plans to reduce the costs of purchasing system upgrades while improving regional and statewide interoperability. This partnership also benefited from an award to Gregg County for $500,000 in FY 2021 State Emergency Radio Infrastructure grant funds, which will be used to finance site improvements. In return, Kilgore plans to independently finance the town's radio equipment upgrades.

Public safety officials should additionally recognize that equipment may require system upgrades during periods of financial insecurity to ensure the success of mission operations. In addition, agencies should upgrade equipment, as needed, to provide available support as older systems may outlast available technical assistance, reducing vendor options and increasing operational costs. Equipment may also require upgrades in order for stakeholders to avoid negative impacts to compatibility with partner agencies, security, access, and functionality. SAFECOM and NCSWIC encourage officials to reference the Emergency Communications System Lifecycle Planning Guide for more information on technology lifecycle management and planning.

Finally, agencies should consider that servicing outdated equipment becomes increasingly difficult and expensive over time due to shortages in replacement parts or available labor. Therefore, officials should

communicate the benefits of sustaining a regular maintenance schedule to leadership during budget cuts by noting how routine and early maintenance often reduces costs over time.

After

Following budget cuts, public safety agencies should consider incorporating cost-saving strategies into regular operations. For example, officials may choose to integrate the Shared Communication Systems and Infrastructure (SCSI) approach into existing procedures to encourage resource sharing among public safety, emergency management, and national security partners. While this approach requires extensive coordination among agencies and disciplines, equipment sharing may ultimately reduce capital investments and ongoing costs, ensuring the continuation of mission-critical operations.

Figure 7: SCSI Approach Overview

In addition, officials should consider using lessons learned from periods of budget instability to request investments in interoperability solutions. Highlighting ongoing issues caused by a lack of equipment funding, public safety agencies can advocate for one-time purchases that may mitigate continued challenges. For example, one-off identity, credential, and access management advancements, standards-based compliance (e.g., Project 25, Long-Term Evolution), or encryption purchases may be vital to ensuring reliable, secure, and interoperable emergency communications during future periods of financial stress.

Equipment Considerations

Before

- Prepare a prioritized list of maintenance activities necessary for mission-critical support
- Review contractual obligations for leased or rented equipment

During

- Recognize the need to sustain both system-level support and maintenance activities
- Understand the increased difficulty of servicing outdated equipment, including higher repair costs

After

- Consider partnering with other agencies in a SCSI approach
- Use lessons learned to advocate for additional interoperability solutions

Figure 8: Equipment Considerations

Software

Software refers to the programs and systems required by computers and other devices for operation. Unlike hardware, software is typically intangible and does not include physical elements; rather, it encompasses the programs, routines, and procedures that control a computer's internal functioning. Emergency communications systems often rely on several forms of software to ensure the operability and interoperability of networks and equipment. For example, software systems are necessary for the functionality of mass notification systems, computer-aided dispatch systems, and trunked radio systems.

Stakeholders should be aware that CISA, SAFECOM, and NCSWIC continue to advocate for the importance of software, especially as the public safety community faces increased cybersecurity threats. As reported in the 2018 SNS, although 57 percent of state public safety agencies reported a cybersecurity incident impacted their communications capabilities between 2013–2018,[3] only 21 percent reported sufficient funding to meet cybersecurity needs (via capital investments). Understanding the critical role of software in system security, officials should consider the following points before, during, and after budget cuts.

City of Alexandria, Va. Launches Award Winning Remote 911 Call-Taking System

In 2020, the City of Alexandria's Department of Emergency and Customer Communications (DECC) pioneered a telework-based solution for 911 call-taking. Recognizing the need to ensure continuity of operations in the event of a COVID-19 outbreak, DECC developed a remote-based system which allowed employees to answer calls at home through FirstNet rather than a traditional internet connection. This innovative software approach ensured the safety of DECC staff and also earned the city the Computer Technology Industry Association and Public Technology Institute's 2020 Solutions Award.

Before

In advance of budget cuts, public safety officials should be prepared to outline how software directly impacts the operability, interoperability, security, and continuity of emergency communications systems. Each day, personnel rely on voice and data software to fulfill mission requirements. Educating decision-makers on the importance of these systems is crucial to gaining buy-in for sustained funding in times of budget fluctuations.

Emergency communications personnel should also work to understand software dependencies and interdependencies in advance of financial disruption. In many cases, the functionality of one software depends on the functionality of another; removing or defunding certain software may lead to system collapse. Officials should document and communicate these vulnerabilities to decision-makers well in advance of budget challenges.

In the event of additional funding, officials should invest in cybersecurity software. For example, improving emergency communications systems by patching, hardening, and adding firewalls will reduce the likelihood of a successful attack and improve system integrity.

During

During budget cuts, public safety agencies should focus on maintaining software support and system access. Given the complexities of public safety communications software, many agencies rely on outside sources, including commercial vendors and external departments, to provide software services. Officials must recognize that continuing payments to these vendors are often required to retain support and system access. This

[3] The SNS State-level survey solicited responses from a limited set of state and territorial public safety agencies. This data may not be reflective of all state-level agencies.

funding becomes increasingly important when software programs are paid in installments rather than a one-time licensing fee. Forgoing vendor support can hinder emergency communications and increase cybersecurity vulnerabilities as certain protections may be removed.

Similarly, officials should be prepared to advocate for ongoing software maintenance costs. Delaying routine or emergency maintenance not only makes future maintenance more expensive but can additionally impair an agency's ability to communicate effectively as a result of outages or failures.

After

After budget cuts occur, there are still steps emergency communication officials can take to mitigate the impacts of financial disruption. Public safety agencies should consider using lessons learned from previous budget cuts to justify sustained investment in current software necessities. Real-world examples and case studies may encourage leadership and decision-makers to remediate existing vulnerabilities and fund sustainable solutions.

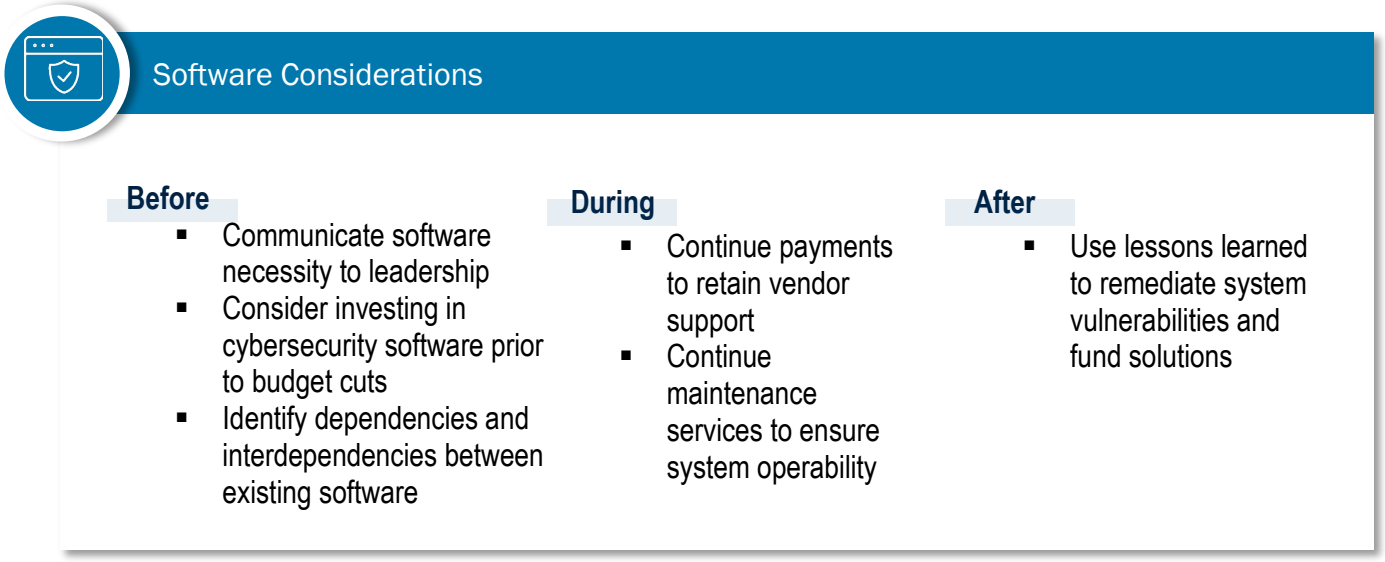


Figure 9: Software Considerations

Other

For all emergency communications expenses, including nontraditional purchases, stakeholders should be aware of the public safety community's push towards data-driven decision-making. Before, during, and after budget cuts, public safety officials should collect, analyze, and communicate data and performance metrics to leadership that highlight the impact and necessity of emergency communications funding. The more evidence a program can produce, the more likely stakeholders are to justify continued funding in the face of budget cuts or uncertainty.

CONCLUSION

While funding emergency communications is a recognized priority within public safety, fiscal insecurity remains a significant challenge for many agencies. Recent national events have highlighted these challenges as agencies faced budget cuts and competing priorities due to the COVID-19 crisis, geopolitical tensions, and severe weather events. Regardless of the cause, officials across all disciplines should recognize the steps public safety organizations can take to mitigate budget cuts before, during, and after funding reductions. Although there is no "one size fits all" solution for budgetary challenges, officials should use the considerations within this guide to advocate for both the funding and sustainment of emergency communications capabilities.

About SAFECOM and NCSWIC

SAFECOM includes more than 70 members representing federal, state, local, and tribal emergency responders, and major intergovernmental and national public safety associations, who aim to improve multi-jurisdictional and intergovernmental communications interoperability through collaboration with emergency responders and policymakers across federal, SLTT, and international partners. SAFECOM members bring years of experience with emergency communications during day-to-day operations, and natural and man-made disasters. SAFECOM members offer insight and lessons learned on governance, planning, training, exercises, and technologies, including knowledge of equipment standards, requirements, and use. SAFECOM members also provide input on the challenges, needs, and best practices of emergency communications, and work in coordination with DHS to share best practices and lessons learned with others.

NCSWIC encompasses SWICs and their staff from the 56 states and territories. NCSWIC assists states and territories with promoting the critical importance of interoperable communications and sharing best practices to ensure the highest level of interoperable communications within and across states and with their international partners along the borders.

The Joint SAFECOM and NCSWIC Funding and Sustainment Committee developed the *Contingency Planning Guide for Emergency Communications Funding* with support from CISA. This document reflects the expertise and knowledge of SAFECOM and NCSWIC members, and the coordination efforts of CISA in bringing stakeholders together to share best practices, lessons learned, and real-world examples of funding and sustaining emergency communications during periods of budget instability. Questions on this document can be sent to: SAFECOMGovernance@cisa.dhs.gov and NCSWICGovernance@cisa.dhs.gov.

APPENDIX A: GLOSSARY

Contingency – A provision for an unforeseen event or circumstance.

Contingency Planning – Seeking to avoid a crisis through risk analysis and mitigation, as well as preparing for a crisis through the development of plans, agreements, and policies.

Continuity – The ability to provide and maintain acceptable levels of communications during disruptions in operations.

Continuity Plan – A documented plan that details how an individual organization will ensure it can continue to perform its essential functions during a wide range of incidents that impact normal operations.

Risk – The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. The more likely it is that a threat event will occur, the greater the risk. Every instance of exposure is a risk. When written as a formula, risk can be defined as follows: Risk = Threat × Vulnerability.

Risk Assessment – A formal risk assessment consists of employing software programs or recognized expert analysis to assess risk trends. Examples of informal assessments include a manual study of fire loss, burn injuries, or lives lost over time and the causative factors for each occurrence. A product or process that collects information, assigns values to risks, informs priorities, develops or compares courses of action, and enables decision-making.

Risk Management – The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

Threat – Natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and property.

Vulnerability – A weakness in a system, network, or asset that could enable an undesired outcome.

APPENDIX B: RISK ANALYSIS PROCESS

This appendix provides an expanded Risk Assessment Cycle, as noted in **Figure B-1** and described in the **Risk Analysis** section of this document.

IDENTIFY THREATS & VULNERABILITIES

The first step in a risk assessment is to identify threats and vulnerabilities of concern. As noted in FEMA's National Risk and Capability Assessment process, stakeholders should identify hazards through a combination of experience, forecasting, subject matter expertise, and other available resources. This list of threats should include context, such as how they will impact emergency communications operations.

DEVELOP RESPONSE APPROACH

A response approach should be structured to help an agency address capability gaps, sustain current capabilities, and build new capabilities. Stakeholders are encouraged to view the National Response Framework, and supplemental resources, for additional information.

CONDUCT RISK ASSESSMENT

When conducting a risk assessment, agencies should first assess existing departmental capabilities. Using these capabilities, stakeholders should examine their list of existing threats to determine where capability gaps lie. Finally, agencies should describe the impacts of these capability gaps on daily and emergency operations.

COMMUNICATE FINDINGS

Once an agency has completed their risk assessment, it is imperative to communicate findings directly to leadership or decision-makers. This early communication will ensure the largest chance of mitigation for documented challenges.

Figure B-1: Risk Assessment Cycle and Steps