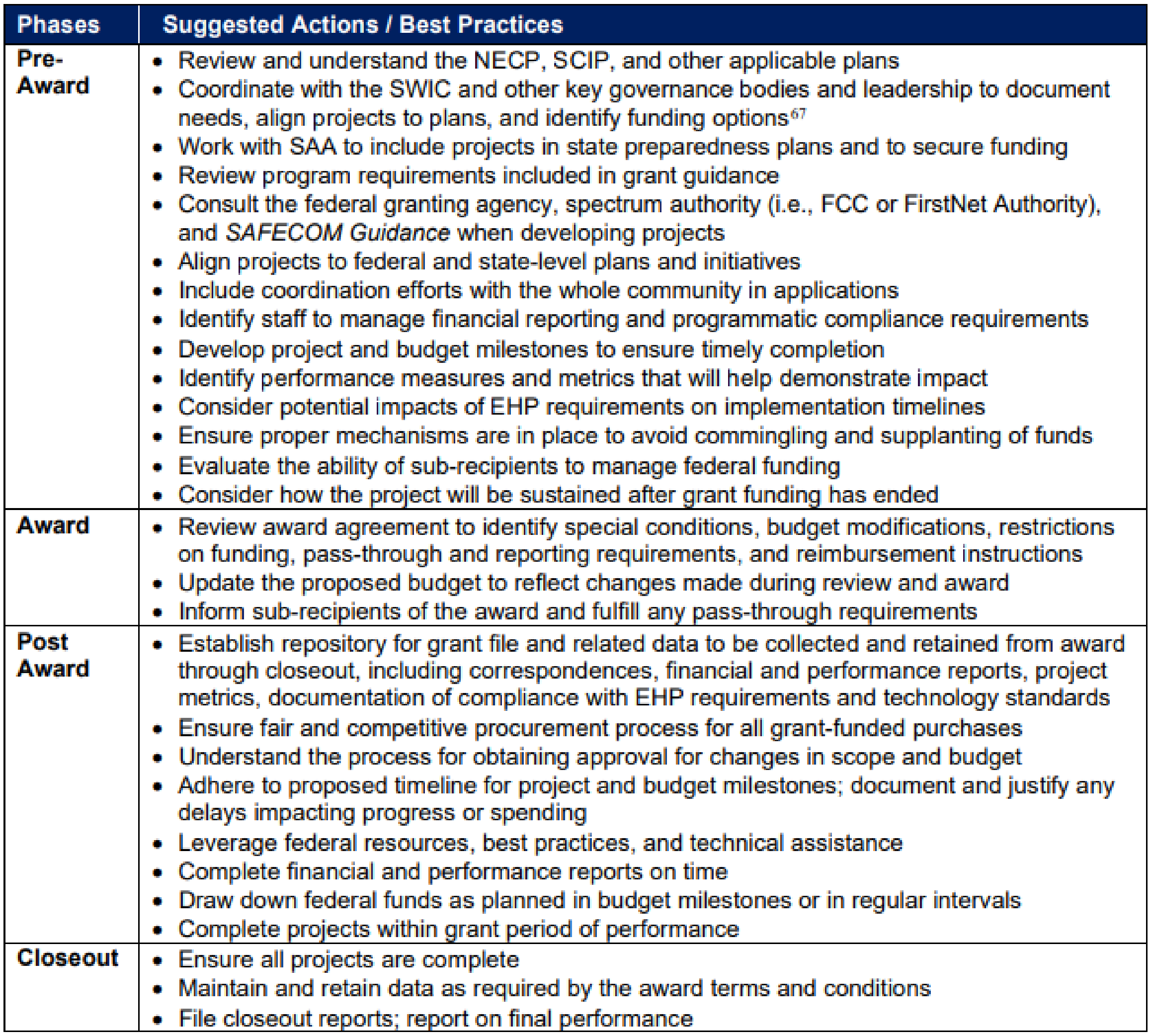
APPENDIX B: GRANT GUIDANCE AND INVESTMENT PRIORITIES

In accordance with ORS 403.455 (Duties of council), the SIEC is responsible for recommending to the Governor investments by the State of Oregon in public safety communications systems. Additionally, the SIEC is tasked to coordinate state, local and as appropriate, tribal and federal activities related to obtaining federal grants for support of interoperability. To fulfill this duty, and to move the state towards the SIEC's vision of "Seamless, interoperable, and resilient emergency communications," the SIEC has established priorities for investment in emergency communications systems and provides the following recommended guidance for use by federal, state, and local grant administrators when determining awards related to communications.

Agencies are strongly encouraged to use the ***SAFECOM Guidance on Emergency Communications Grants*** Suggested Actions and Best Practices for Use during Grant Cycle Phases to assist with planning for communications grant applications.

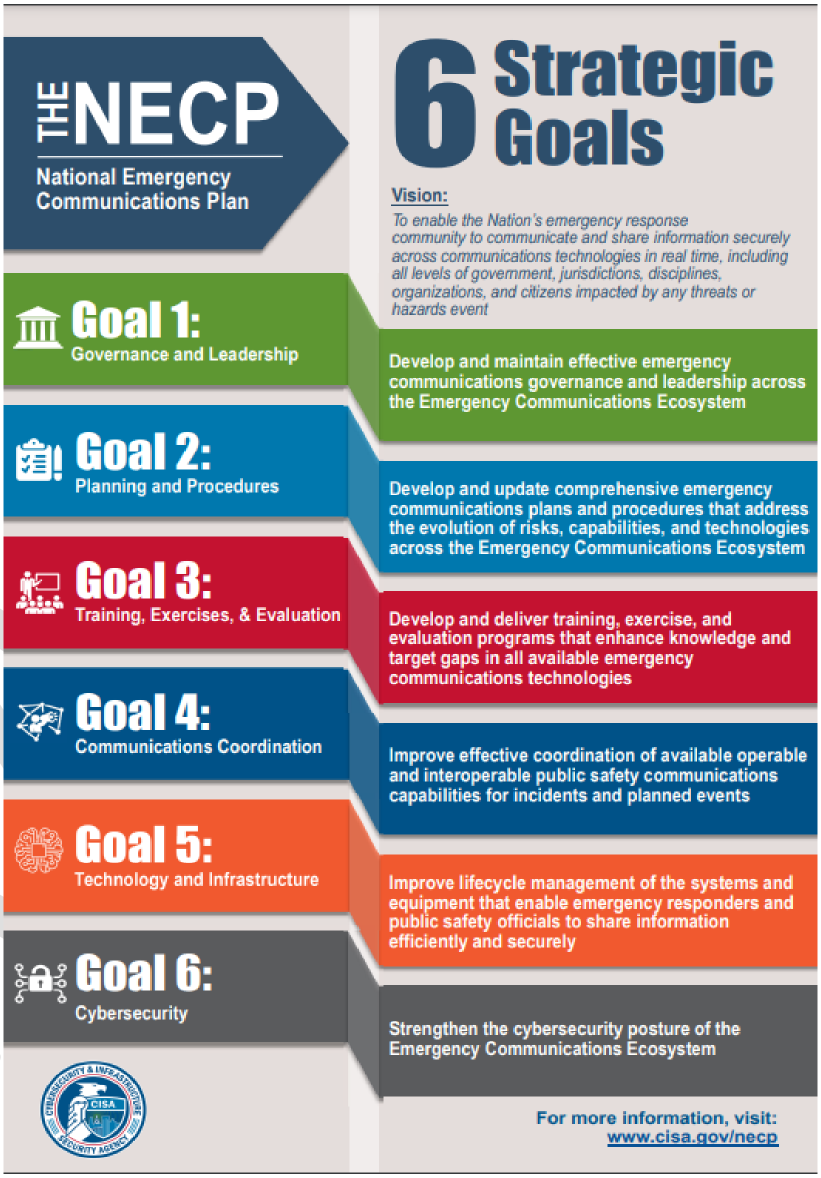


Phases	Suggested Actions / Best Practices
Pre-Award	• Review and understand the NECP, SCIP, and other applicable plans • Coordinate with the SWIC and other key governance bodies and leadership to document needs, align projects to plans, and identify funding options[67] • Work with SAA to include projects in state preparedness plans and to secure funding • Review program requirements included in grant guidance • Consult the federal granting agency, spectrum authority (i.e., FCC or FirstNet Authority), and *SAFECOM Guidance* when developing projects • Align projects to federal and state-level plans and initiatives • Include coordination efforts with the whole community in applications • Identify staff to manage financial reporting and programmatic compliance requirements • Develop project and budget milestones to ensure timely completion • Identify performance measures and metrics that will help demonstrate impact • Consider potential impacts of EHP requirements on implementation timelines • Ensure proper mechanisms are in place to avoid commingling and supplanting of funds • Evaluate the ability of sub-recipients to manage federal funding • Consider how the project will be sustained after grant funding has ended
Award	• Review award agreement to identify special conditions, budget modifications, restrictions on funding, pass-through and reporting requirements, and reimbursement instructions • Update the proposed budget to reflect changes made during review and award • Inform sub-recipients of the award and fulfill any pass-through requirements
Post Award	• Establish repository for grant file and related data to be collected and retained from award through closeout, including correspondences, financial and performance reports, project metrics, documentation of compliance with EHP requirements and technology standards • Ensure fair and competitive procurement process for all grant-funded purchases • Understand the process for obtaining approval for changes in scope and budget • Adhere to proposed timeline for project and budget milestones; document and justify any delays impacting progress or spending • Leverage federal resources, best practices, and technical assistance • Complete financial and performance reports on time • Draw down federal funds as planned in budget milestones or in regular intervals • Complete projects within grant period of performance
Closeout	• Ensure all projects are complete • Maintain and retain data as required by the award terms and conditions • File closeout reports; report on final performance

Investment Priorities

National Emergency Communications Plan (NECP) Priorities

The SIEC fully supports the ~~6~~ national priorities identified in the ~~2019~~ most recent version of the National Emergency Communication Plan (NECP) and has included a general overview and examples of projects as Appendix E. Agencies should review the NECP and SAFECOM Grant Guidance and ensure projects align with national goals and priorities.



THE NECP
National Emergency Communications Plan

6 Strategic Goals

Vision:
To enable the Nation's emergency response community to communicate and share information securely across communications technologies in real time, including all levels of government, jurisdictions, disciplines, organizations, and citizens impacted by any threats or hazards event

Goal 1: Governance and Leadership — Develop and maintain effective emergency communications governance and leadership across the Emergency Communications Ecosystem

Goal 2: Planning and Procedures — Develop and update comprehensive emergency communications plans and procedures that address the evolution of risks, capabilities, and technologies across the Emergency Communications Ecosystem

Goal 3: Training, Exercises, & Evaluation — Develop and deliver training, exercise, and evaluation programs that enhance knowledge and target gaps in all available emergency communications technologies

Goal 4: Communications Coordination — Improve effective coordination of available operable and interoperable public safety communications capabilities for incidents and planned events

Goal 5: Technology and Infrastructure — Improve lifecycle management of the systems and equipment that enable emergency responders and public safety officials to share information efficiently and securely

Goal 6: Cybersecurity — Strengthen the cybersecurity posture of the Emergency Communications Ecosystem

CISA CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

For more information, visit:
www.cisa.gov/necp

SIEC Investment Priorities

In addition to priorities outlined in the ~~2019~~ NECP, the SIEC specifically recommends the state make investments in projects that address the following areas:

- Projects that increase cyber resilience of public safety communications networks and systems including implementation of cybersecurity measures identified in a formal system assessment or cybersecurity plan.
- Projects that assess the cyber vulnerabilities and/or result in the creation/update of a cybersecurity plan for public safety and emergency communications[1] networks.
- Projects that support goals and objectives outlined in the State Homeland Security Strategy.
- Hardening, increasing resiliency of, and/or reducing all-hazards risks to public safety communications systems, emergency communications systems[2], and dependent Infrastructure. ~~This may~~ Examples include but are not limited to:
  - Installation of security infrastructure such as fences, cameras, and alarm systems
  - Insulation of generators, batteries, solar systems, and fuel tanks allowing for a minimum of five days of utility disruption

[1] ORS 403.105 defines "Emergency communications system" as the network, database, servers, other equipment and services that provide the means to communicate with a primary public safety answering point to request and provide assistance to preserve human life or property. For the purposes of this section, public safety communications networks include emergency communications networks, land mobile radio, public safety broadband, and emergency alerts and warning systems. This term is an all-encompassing term meant to describe the entire public safety communications ecosystem.

  - Making sites seismically resilient in accordance with the current Oregon Structural Specialty code for essential facilities.
  - Installation of redundant backhaul connectivity at strategic sites
  - Natural-hazards mitigations actions (Examples include fuels reduction, seismic retrofitting, lightning protection installation, etc.)
- Replacement of non-standard conforming mobile or portable radios with dual or tri-band equipment that meets or exceeds the technical requirements of the most recent version of the ***SAFECOM Grant Guidance*** for use by frontline responders and dispatch centers
- Equipment and training needed to establish SHARES stations for medical facilities that provide emergency, burn, and disaster related services.
- Equipment and training needed to establish SHARES stations for county and tribal emergency operations centers.
- Caches of dual/tri band radios [3] for use during a disaster, terrorist attack, or large-scale emergency
- Deployable communications equipment including tactical repeaters, gateways, antennas, power systems, satellite connectivity (low earth orbit), devices designed to make us of the 3GPP MCPTT standard, and associated accessories.
- Staff dedicated to increasing interoperability and regional interagency cooperation within the emergency communications ecosystem as well as communications between PSAPs/Public Safety Dispatch Centers, EOCs, and other critical facilities. Investments should especially be targeted towards projects that support underserved, rural areas and/or where tribal involvement may be better facilitated.
- Funding subsequent phases of multi-phased projects previously funded and successfully carried out.
- Funding for Next-Generation 911 planning, implementation, and deployment.
- Continued funding of OR-Alert.
- Continued funding of the SIEC and the Statewide Interoperability Program
- Funding of the Oregon Emergency Response System (OERS) Call Center
- Refurbishment, update, and maintenance of the State's Strategic Technology Reserve, as well as funding for training and exercise related to use of the Reserve.
- Continued funding of the State Preparedness and Incident Response Equipment (SPIRE) grant program with expanded eligibility for communications equipment.
- Projects that support multi-agency, regional, and/or statewide strategic planning efforts related to emergency and public safety communications.
- Projects that enhance public safety's ability to detect, respond to, and mitigate sources of intentional and unintentional interference (jamming).

Funding Priority Recommendations

- When limited funding is available or funding is available through a competitive process, funding priority should be given to projects that have a statewide/interstate impact, followed by projects

[3] Radio equipment must meet or exceed the technical requirements in the most current version of the ***SAFECOM Grant Guidance***

that have a regional/multi-agency impact. Lowest priority should be given to projects that only affect a single agency. Priority should also be given to projects that leverage or expand existing infrastructure, either through the state or regionally, whenever possible.

- Priority should be given to projects that address identified gaps in capabilities through a formal assessment or promulgated plan.
- Priority should be given to projects that support goals and objectives identified within the Statewide Communications Interoperability Plan.

Funding Requirement Recommendations

It is the SIEC's recommendation that grant funding administered by any state or federal agency operating within Oregon related to any emergency communication project should include the following requirements:

- Coordination with the Office of the Statewide Interoperability Coordinator and the SIEC's Technical Committee early in the project development process. It is possible, depending on the nature of the project, that coordination with other entities may be necessary.
- Identification of the project in a jurisdiction or region's Strategic Communications Plan, Hazard Mitigation Plan, Community Wildfire Protection Plan, Dam Safety Plan, or other strategic all-hazards preparedness plans.
- Demonstrate that a lifecycle funding plan has been identified for any equipment/infrastructure investments.
- That a full project plan with timelines, budget, and milestones identified be developed
- For radio equipment purchased with grant funding, the programming of national interoperability channels and public safety mutual aid channels shall be programmed as listed in the National Interoperable Field Operations Guide for all bands the radio can operate on.
- For standards based (P25) radio equipment purchased with grant funding, equipment must meet be on the Dept. of Homeland Security's P25 Compliance Assessment Program Authorized Equipment List and meet the encryption standards as tested.

Exclusions

The SIEC recommends that projects in the following categories be excluded from grant funding or other investment eligibility:

- Alerting Software that duplicates the capabilities provided to counties, tribes, and state agencies through the OR-Alert program.
    - This exclusion does not apply to capabilities that are outside the scope or OR-Alert or that expand the capabilities of OR-Alert. Ex: EAS hardware, devices capable of receiving alerts, siren systems, visible messaging systems, etc.
    - This exclusion does not apply if OR-Alert does not meet a county's needs as determined by the grant administrating agency or the funding body.
    - To the extent possible, investments in alerting infrastructure should be compatible with OR-Alert and be capable of receiving and/or transmitting in Common Alerting Protocol (CAP).
- Equipment, software, or services offered by an entity identified by the State Chief Information Officer which may pose a national security threat in accordance with OAR 128-020-0010.

    - Certain law enforcement purchases for specific purposes may be exempt.

- Equipment or services offered by certain telecommunications providers identified in Section 2 of the Secure Networks Act.
- Equipment or services offered by certain telecommunications providers identified in the John S. McCain National Defense Authorization Act of 2019, current SAFECOM Guidance on Emergency Communications Grants or any applicable notice of funding opportunities.
- GMRS and FRS equipment under an emergency communications justification. [4]
- Amateur radio equipment not utilized for HF SHARES, or not installed in public safety communications command posts or emergency operations centers where standards-based equipment is also installed.

Resources

- SAFECOM guidance on Emergency Communications Grants
- National Emergency Communications Plan
- Roadmap to the Envisioned State of Emergency Communications
- SAFECOM FAQ: Understanding Project 25 Standards and Compliance
- List of Federal Financial Assistance Programs Funding Emergency Communications – October 21, 2021
- NECP Frequently Asked Questions
- Oregon State Preparedness and Incident Response Equipment (SPIRE) Grant Program
- Oregon Emergency Management Performance Grant (EMPG) Program
- Oregon Homeland Security Grant Program
- Assistance to Firefighters Grant Program
- Tribal Homeland Security Grant
- Port Security Grant

[4] This type of equipment may qualify under community resilience justifications.

APPENDIX E: PRIORITIES IDENTIFIED IN THE NATIONAL EMERGENCY COMMUNICATIONS PLAN (NECP)

Governance & Leadership (NECP) Activities including:

- Funding of SIEC or Regional Interoperability Groups' activities
- Formation of Regional Interoperability Groups
- Other investments in emergency communications governance and leadership structures for coordinating statewide and regional initiatives that reflect the evolving emergency communications environment
- Outreach and education efforts
- Review and updating of key documents related to emergency communications, including charters, policies, procedures, and agreements to address new technologies

Planning & Procedures

- Update SCIPs, Regional Interoperability Group Plans documents, Tactical Interoperable Communications Plans (TICPs) and other strategic plans, and procedures to:
    - Support statewide and regional emergency communications and preparedness planning efforts through allocation of funding to the following planning activities:
    - Conduct and attend planning meetings
    - Engage the whole community in emergency communications planning, response, and risk identification
    - Develop and perform risk, resiliency, and vulnerability assessments (e.g., cyber, Threat and Hazard Identification and Risk Assessment [THIRA], communications security [COMSEC]
    - Incorporate risk management strategies for cybersecurity, continuity, and recovery (e.g., National Risk Index [NRI])
    - Integrate emergency communications assets and needs into state-level, regional, and county plans
- Coordinate with SWIC, State Administrative Agency (SAA), and state-level planners (e.g.,911 planners, utilities commissions) to ensure proposed investments align to statewide plans and comply with technical requirements
- Establish a cybersecurity response plan including continuity of vulnerable communications components and implementing resilient network designs (e.g., segmenting essential functions, strong access controls, two-factor authentication for staff logins) to limit the impact of cyber incidents.
- Identify, review, establish, and improve SOPs in coordination with response agencies at all levels of government to:
    - Ensure federal, state, local, tribal, and territorial roles and responsibilities are clearly defined

  - Ensure communications assets and capabilities are integrated, deployed, and utilized to maximize interoperability
  - Address threats, mitigate vulnerabilities, and identify contingencies for the continuity of critical communication

Training, Exercise, and Evaluation

- Conduct National Incident Management System (NIMS)-compliant training (e.g., training in:
    - Incident Command System [ICS] and the ICS Communications Unit such as:
        - Communications Unit Leader [COML],
        - Communications Technician [COMT],
        - Radio Operator [RADO],
        - Incident Tactical Dispatcher [INTD],
        - Auxiliary Communications [AUXCOMM], and
        - Incident Communication Center Manager [INCM])
        - Information Technology Services Unit Leader [ITSL]
        - Incident Tactical Dispatcher [INTD]
- Conduct frequent training and exercises involving personnel from all levels of government who are assigned to operate communications capabilities, to test communications systems and personnel proficiency (e.g., include emerging technologies and system failure), and utilize third party evaluators with communications expertise
- Incorporate human factors in training and exercises to address the demands that voice, video, and data information place on personnel, to ensure that responders effectively use and are not overloaded by available information
- Perform exercises that support and demonstrate the adoption, implementation, and use of the NIMS concepts and principles
- Hold cross-training and state, regional, or national level exercises to validate plans and procedures to include tribes, nongovernmental organizations, and public sector communications stakeholders
- Provide training and exercises on new and existing systems, equipment, and SOPs
- Develop or update training and exercise programs to address new technologies, data interoperability, cybersecurity, use of federal and national interoperability channels, personally identifiable information, and continuity of communications
- Test communications survivability, resilience, and continuity of communications, to include validation of continuity procedures and operational testing of backup systems and equipment
- Develop and support instructor cadres to expand training for communications-support personnel
- Assess and update training curriculums and exercise criteria to reflect changes in the operating environment and plain language protocols
- Identify opportunities to integrate private and public sector communications stakeholders into training and exercises, as well as cost-effective approaches (e.g., distance learning)
- Offer cybersecurity training and education on the proper use and security of devices and applications, phishing, malware, other potential threats, and how to guard against attacks
- Provide regular training and exercises for Alerting Authorities incorporating the use of IPAWS and OR-Alert

Communications Coordination

- Promote projects that confirm NIMS implementation, integrate members of the All-Hazards COMU Program, support continued use of ICS, and promote information sharing
- Establish or enhance primary, secondary, and backup communications capabilities and share appropriate ICS forms and information illustrating the status of an agency's capabilities
- Assess and improve the timeliness of notification, activation, and response of communications systems providers to support the Incident Commander, Incident Management Team(s), and EOC's requirements at incidents and planned events
- Enhance the coordination and effective usage of communications resources
- Ensure inventories of emergency communications resources are updated and comprehensive, and readily share information about features, functionality, and capabilities of operable and interoperable communication resources with partners o Promote assessment of communications assets, asset coordination, and resource sharing
- Implement projects that promote regional, intra- and inter-state collaboration
- Support initiatives that engage the whole community, including commercial and nontraditional communications partners (e.g., auxiliary communications, volunteers, utilities)
- Develop or update operational protocols and procedures
- Develop, integrate, or implement NIMS aligned SOPs to facilitate the integration, deployment, and use of communications assets
- Test communications capabilities and personnel proficiency through training, exercises, and real-world events and address needs identified in statewide plans, AARs, or assessments through comprehensive action plans
- Develop recommended guidelines regarding the use of personal communications devices (e.g., bring your own device) for official duties based on applicable laws and regulations
- Review usage of Priority Telecommunications Services (e.g., Government Emergency Telecommunications Service, Wireless Priority Service, and Telecommunications Service Priority), and ensure SOPs govern the programs' use, execution, and testing
- Plan for Alerting Authorities to ensure the highest state of readiness of OR-Alert for resilient and interoperable alerts, warnings, messaging and notifications
- Review uses of the NPSBN, also known as FirstNet, and other public safety broadband capabilities, and ensure SOPs govern the programs' use, execution, and testing
- Strengthen resilience and continuity of communications
- Inventory and typing of resources and other activities that strengthen resilience and provide backup communications solutions (e.g., radio caches, cell on wheels [COWs])
- Establish testing and usage observations of primary, secondary, and backup communications
- Address system and staffing for continuity of operations planning

Technology and Infrastructure

- Sustain and maintain current LMR capabilities based on mission requirements
- Purchase and use P25 compliant LMR equipment (see P25 Compliance Assessment Program [CAP] approved equipment list) for mission critical voice communications
- Support rapid and far-ranging deployment of the NPSBN and use of FirstNet devices and applications dedicated for public safety using multi-layered, proven cybersecurity and network security solutions

- Transition towards NG911 capabilities in compliance with NG911 standards
- Support standards that allow for alerts, warnings, and notifications across different systems
- Secure and protect equipment, information, and capabilities from physical and virtual threats
- Employ standards-based information exchange models and data sharing solutions
- Secure standards-based interconnectivity gateway subsystems
- Sustain and ensure critical communication systems connectivity and resiliency, including backup solutions, among key government leadership, internal elements, other supporting organizations, and the public under all conditions
- Support standards and practices that enhance survivability and resilience to electromagnetic effects
- Ensure all communications systems and networks are traced from end-to-end to identify all Single Points of Failure, including redundancy at critical infrastructure facilities, and:
    - Sustain availability of backup systems (e.g., backup power, portable repeaters, satellite phones, High Frequency [HF] radios)
    - Ensure diversity of network element components and routing
    - Plan for geographic separation of primary and alternate transmission media
    - Maintain spares for designated critical communication systems
    - Work with commercial suppliers to remediate single points of failure
    - Maintain communications capabilities to ensure their readiness when needed

Cybersecurity

- Develop and maintain cybersecurity risk management
- Implement the CISA Cyber Essentials Toolkits
- Implement the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) to complement an existing risk management process or to develop a credible program if one does not exist. The NIST Cybersecurity Framework establishes five functions to integrate cybersecurity into mission functions and operations, including:
    - Identify, evaluate, and prioritize risks
    - Protect against identified risks
    - Detect risks to the network as they arise
    - Deploy response capabilities to mitigate risks
    - Establish recovery protocols to ensure the resiliency and continuity of communications
- Perform a Cyber Resilience Review
- Employ the Cyber Resiliency Resources available for public safety
- Identify and implement standards for cybersecurity that fit system and mission needs while maintaining operability and interoperability
- Develop incident response plans, recovery plans, resiliency plans, and continuity of operations plans in anticipation of physical or cybersecurity incidents
- Mitigate cybersecurity vulnerabilities with consideration of potential impacts of cybersecurity risk management on interoperability with the broader community
- Identify and mitigate equipment and protocol vulnerabilities