Informational Primer for Grant Recipients
Investing in Emergency Communications

December 2018

Communications Continuity and Resiliency

The Department of Homeland Security (DHS) Emergency Communications Division (ECD) and the Federal Emergency Management Agency (FEMA) prepared this guidance for grant recipients to ensure consistent investments for public safety communications technologies, equipment purchase, and compliance enforcement. This primer includes background on communications continuity and resiliency, best practices, and resources for additional information. It serves as a reference guide to assist when developing projects.

Background

Lessons learned from major disasters, unplanned events, and full-scale exercises have identified a need for greater coordination of emergency communications among senior elected officials, emergency management agencies, and first responders at all levels of government. Responders arriving on the scene of a domestic incident are not always able to communicate with other response agencies, particularly when the incident requires a multi-agency, regional response effort, or when primary communications capabilities fail. This lack of operability and interoperability between agencies is further complicated by problems with communications continuity, survivability, and resilience, which hinders the ability to share critical information, and can compromise the unity-of-effort required for an effective incident response. The DHS Cybersecurity and Infrastructure Security Agency's (CISA) ECD, formally known as the Office of Emergency Communications, will lead the Nation's operable and interoperable public safety and national security and emergency preparedness communications efforts. CISA will enhance public safety communications at all levels of government and will provide training, coordination, tools and guidance to assist partners in developing their emergency communications capabilities.

Best Practices

Grant recipients should target funding toward activities that address communications continuity, survivability, and resiliency. Activities can include system assessments, analysis of threats and vulnerabilities, and strategic plan and procedural updates to mitigate identified risks. Recipients investing in emergency communications are encouraged to work with Statewide Interoperability Coordinators, Statewide Interoperability Governance Bodies, and appropriate stakeholders at the regional, federal, state, local, territorial, and tribal levels to:

- Establish robust, resilient, reliable, secure, and interoperable communication capabilities;
- Plan for mission-related communications and connectivity among government leadership, internal elements, other supporting organizations, and the public under all conditions;
- Trace all communications systems/networks from end-to-end to identify Single Points of Failure;
- Recipients should also address the following issues:
  - Integrate communications needs into continuity planning efforts and emergency operations plans by incorporating mitigation options to ensure uninterrupted communications support;
  - Maintain and protect communications capabilities against emerging threats, both man-made and natural, to ensure their readiness when needed;
  - Frequently train and exercise personnel required to operate communications capabilities;
  - Test and exercise communications capabilities; and
  - Establish a cybersecurity plan that includes continuity of an "out of band" communications capability such as High Frequency (HF) Radio Frequency (RF), fiber-based communications pathways that do not rely on public infrastructure.
- Ensure key communications systems resiliency through:
  - Availability of backup systems;
  - Diversity of network element components and routing;
  - Geographic separation of primary and alternate transmission media;

- Availability of backup power sources;
- Access to systems that are not dependent on commercial infrastructure;
- Maintained spare parts for designated critical communication systems; and
- Agreements with commercial suppliers to remediate communications Single Point of Failures.

Resources

FEMA National Continuity Programs (NCP): These programs highlight the national policy and guidance for continuity of operations initiatives. They provide guidance and assistance to support continuity preparedness for federal departments and agencies; state, local, tribal, and territorial government jurisdictions; and private sector organizations.

DHS Regional Resiliency Assessment Program (RRAP): This program is a cooperative assessment of specific critical infrastructure within a designated geographic area. DHS works with selected areas each year to conduct a regional analysis of surrounding infrastructure and address a range of resilience issues that could have significant regional or national consequences if disrupted.

DHS Ten Keys to Obtaining a Resilient Local Access Network: This document introduces resiliency concepts and provides ten keys to obtaining and maintaining resiliency in a local access network, such as knowing the exact network infrastructure in the local loop, interfacing with commercial service providers, and properly maintaining alternative path solutions. DHS developed these ten fundamental steps, supported by descriptive text and visually-appealing graphics, as recommendations to help organizations maintain critical communications in emergency situations.

DHS Priority Services Programs: The Telecommunications Service Priority (TSP), Government Emergency Telecommunications Service (GETS), and Wireless Priority Service (WPS) Programs support national leadership; federal, state, local, tribal, and territorial governments; first responders; and other authorized national security and emergency preparedness users. They are intended to be used in an emergency or crisis situation when data, landline, or wireless networks are congested and the probability of completing a normal transmission or call is reduced.

Federal Interoperability Assistance Support – Funding Strategy Best Practice Report – Public Safety Wireless Network: This report presents best practices and lessons learned applicable to any state or region seeking funding for an interoperable wireless communications system. This report also serves to educate public safety officials and decisions makers on the need for, and process of, developing a successful funding strategy.

Interoperability Business Case: An Introduction to Ongoing Local Funding: This document helps emergency response officials develop a compelling business case by presenting steps and considerations to follow in order to tap into critical local funding sources for interoperability efforts.

SAFECOM Guidance on Emergency Communications Grants: This guidance provides information for grantees developing emergency communications projects for federal funding—including the latest government directives, best practices, and standards on alert and warning systems. Decision makers and grantees should read this guidance, coordinate proposals with the Statewide Interoperability Coordinator, and encourage compliance with the recommendations contained therein. For DHS / FEMA preparedness grants, recipients must comply with requirements listed in SAFECOM Guidance Appendix D as a condition of funding.

For Additional Information:

Contact **OECGrants@hq.dhs.gov**