Resilient Communications: Grant Guidance FY18

Resilient Communications:

Nothing better demonstrates a modern nation than its ability to effectively communicate. The risk imposed by the reliance on communication systems by government and the private sector can be reduced by understanding dependencies, analyzing effects, and taking action. Grantees are encouraged to work with State Emergency Management Agencies. Statewide Interoperability Coordinators, Statewide interoperability governing bodies, and appropriate stakeholders at the regional, state, local, and tribal levels to:

- Establish robust, resilient, reliable and interoperable communications capabilities. Account for the mission impact of communication system disruptions in your planning.

- Ensure mission-related communications (voice, video, data and network security requirements) are adequately planned for and understood. It is important to maintain current documentation of your communication systems architecture and perform regular audits. Your ability to continue operations is dependent on the availability of and access to communications systems with sufficient resiliency, redundancy, and accessibility to perform essential functions and provide critical services during a disruption.

- Ensure critical communication systems connectivity among key government leadership, internal elements, other supporting organizations, and the public under all conditions. As such, organizations should ensure current copies of vital records, including electronic files and software, are backed-up and maintained off-site.

- Ensure all communications systems/networks are traced from end to end to identify all Single Points of Failure (SPF). In doing so, grantees should work with communication service providers to add redundancy at key critical infrastructure facilities as needed. Ensure key communication systems resiliency through:
    - Ensuring availability of backup systems;
    - Ensuring diversity of network element components and routing;
    - Ensuring geographic separation of primary and alternate transmission media;
    - Ensuring availability of back-up power sources;
    - Ensuring availability and access to systems that are not dependent on commercial infrastructure;
    - Maintain spares for designated critical communication systems; and
    - Work with commercial suppliers to remediate communication Single Points of Failure.

- Grantees are encouraged to address the following issues:
    - Integrate communications needs into continuity planning efforts by incorporating mitigation options to ensure uninterrupted communications support;
    - Maintain communications capabilities 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 a communications component such as Radio Frequency (RF)-based communications that do not rely on public infrastructure.
- Consider Electromagnetic Pulse (EMP) protective measures for communications systems where practical.

Summary of Minimum Requirements for Resilient Communications Capabilities:

This establishes a State inter-agency baseline of minimum communications requirements to enable State Department and Agency heads, senior leadership, and emergency operations staffs to collaborate, develop policy recommendations, and direct execution of essential functions from headquarters or alternate locations under all conditions.

All departments and agencies are encouraged, to the maximum extent practicable, to co-locate and share resources to avoid unnecessary duplication of expense and effort. However, each department and agency must have sufficient communications capabilities to accomplish essential functions independently when an alternate location is shared.

Continuity operations are designed to ensure sustained performance of essential functions, and are critically dependent on resilient communications to provide inter-agency connectivity. During an emergency, the ability of a department or agency to execute its essential functions at its primary or alternate location is dependent upon communications connectivity among government leaders at all levels, and must provide contact with internal elements, other agencies, critical stakeholders, and the public under all conditions. Communications capabilities must be interoperable, robust, and secure to enable the exchange of sensitive and classified information, and must support each department and agency's emergency response functions.

All departments and agencies shall ensure that resilient communications capabilities are maintained and readily available for a minimum of 30 days following continuity program activation, and that designated personnel are properly trained in the use of these communications capabilities.

NCP Recommends:

In General:

NCP recommends conducting, at minimum, an annual exercise with internal and external partners to coordinate operational and continuity plans and programs, to include the regular testing of emergency workforce staff activation and accountability procedures.

NCP recommends that an organization conduct regular testing of capabilities to include interoperable and available communications that support identified essential functions, facilities, equipment and systems, and related infrastructure to meet associated critical metrics for operational objectives.