Emergency Communications Security and Operational Recommendations

January 2021

The Department of Public Safety, division of Emergency Communication Networks (DPS-ECN) has prepared these recommendations to help our stakeholders anticipate, plan, and implement strategies and actions to mitigate potential threats to local, regional, or statewide emergency communication systems.

Cybersecurity: Public safety agencies, large and small, should develop a robust cyber security strategy that includes the following best practices:

- Collaborate with information technology (IT) staff to discuss potential cyber threats and vulnerabilities.
- Ensure that hardware and software have the most current security updates and patches installed.
- Ensure that staff are trained to identify and respond to cyber-related incidents, including knowing who to contact (especially after hours) if an incident occurs.

911 Denial of Service Attack: A Telephony Denial of Service (TDoS) is an external attack intended to overwhelm networks (including 911 systems) so that they cannot process legitimate calls. The following links contain more information:

- DHS CISA Telephony Denial of Service Fact Sheet
- NENA Best Practices Checklist for Denial of Service Attacks Against 911 Centers

911 Network Disruption or Degradation: Occasionally, 911 networks may represent a target that, when disrupted, may significantly impact the ability to provide emergency services to those in need. In some situations, it may be difficult for a Public Safety Answering Point (PSAP) to determine the source, size, scope and severity of the problem. If there is a concern that 911 calls are not being routed as expected, agencies may take these recommended steps and escalate the issue:

- Maintain an up-to-date contact list of local solution providers.
- Create a log of date, time and telephone number (if available).
- Run local tests to see if the issue can be replicated on both a landline and/or mobile devices from multiple cellular service providers.
- Contact solution providers (CPE, CAD, etc.) and/or Lumen (800-357-0911) to report the issue.
- Engage DPS-ECN to promote regional/statewide situational awareness, communicate with the public, and provide assistance as needed.

Physical Security: Physical security is fundamental component of protecting our emergency communication systems.

- Ensure that the dispatch center is properly secured (inside and out). Gates and doors should not be propped open and access should be limited.
- Security procedures, including badging/identification/credentialing for staff and outside vendors, should be reviewed and enforced.
- Fixed communication infrastructure sites should be secured with proper signage to prevent trespassing.
- Law enforcement should be engaged to monitor suspicious activity at fixed communication infrastructure locations (ARMER sites, cellular towers, telephone switching facilities, etc.).

ARMER System Administration: System administrators play a vital role in keeping the land mobile radio system, known as the Allied Radio Matrix for Emergency Response (ARMER) system, operational.

- Identify local/regional system administrators and know how to contact them (especially after hours).

- Ensure that local/regional system administrators have the proper tools, credentials and permissions to monitor system performance and conduct necessary actions as needed.
- Develop contingency plans for situations when the local/regional system administrator is unavailable.

Missing ARMER Radios: An ARMER radio in the wrong hands can be a significant threat to responder safety. Efforts to inventory and disable missing radios will mitigate the threat.

- Maintain a current and accurate radio inventory.
- Engage the ARMER system administrator to identify and disable missing, lost or stolen radios.

ARMER Talkgroup Coordination: ARMER is a statewide system with finite talkgroup resources. When reserving talkgroups in StatusBoard, be aware that other response efforts may be occurring across the region/state that require the use of STAC, LTAC, and regional interoperability talkgroups.

- Understand the operational benefits and limitations of using encrypted ARMER talkgroup resources.
- Acknowledge the need for clear, concise communication using plain language during multi-agency/multi-discipline operations.

Dragging ARMER Resources: "Dragging talkgroups" occurs when an uninvolved responder selects (parks on) a talkgroup to monitor radio traffic. This can have an adverse effect on ARMER system performance and is strongly discouraged. If a responder is not actively involved in the response, they should not select a talkgroup just to monitor radio traffic.

Wireless Broadband: Emergency responders are becoming increasingly reliant on voice and data communication services provided by cellular service providers.

- Understand the impact that large crowds and increased demand may have on the ability of emergency responders to access their cellular service provider's network.
- Collaborate with cellular service providers to identify and request operational support and/or deployable resources (FirstNet Dedicated Care: 800-574-7000/Verizon Response Team: 800-981-9558).

Public Alert & Warning: The Integrated Public Alert & Warning System (IPAWS) provides local alerting authorities with the capability to issue Wireless Emergency Alert (WEA) messages to the public via cellular devices (smartphones & tablets) and Emergency Alert System (EAS) messages via commercial broadcast partners (television, cable, radio, etc.).

- Understand the public alert and warning capabilities that are available locally/regionally to support response operations.

Communications Unit (COMU) and Strategic Technology Reserve (STR) Resources: COMU and STR resources are available on a local, regional and statewide level to support response operations.

- Engage Communications Unit Leader (COM-L) and Communications Unit Technician (COM-T) personnel to develop an ICS-205 (Incident Radio Communications Plan) and maintain communications equipment.
- Available STR resources include 300 ARMER system portable radios and seven radio repeater tower trailers.
- Requests for COMU/STR resources should be directed to the regional Emergency Communications/Services Board and/or the DPS-ECN Deputy Director/Statewide Interoperability Coordinator (SWIC), Cathy Clark (cathy.clark@state.mn.us).

Event Reporting: Any malicious acts and/or adverse impacts on emergency communication system performance should be reported to the DPS-ECN Deputy Director/Statewide Interoperability Coordinator (SWIC), Cathy Clark (cathy.clark@state.mn.us). The information will be vetted and shared, as appropriate, with the DPS-ECN program managers and the State Emergency Operations Center (SEOC) for situational awareness, support and follow-up.