Suspicious Activity Reporting

March 2, 2021

Minnesota's 104 Public Safety Answering Points (PSAPs) are potentially vulnerable to malicious acts intended to disrupt their ability to receive 9-1-1 calls and/or communicate with emergency responders. A proactive approach to Suspicious Activity Reporting (SAR) and information sharing can help mitigate this threat. The Minnesota Department of Public Safety division of Emergency Communication Networks (DPS-ECN) has prepared this document to provide recommendations for reporting suspicious activity that may be a precursor to a criminal/terrorist act executed against a PSAP.

Suspicious activity is described as "observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity." These behaviors include:

- Eliciting Sensitive Information: Questioning individuals or otherwise soliciting information regarding PSAP operations at a level beyond mere curiosity and in a manner that would arouse suspicion of terrorism or criminal activity in a reasonable person (e.g., staffing levels, work hours, physical security, access points, etc.).
- Testing or Probing Security/Breach or Attempted Intrusion: Deliberate acts to identify PSAP security capabilities and protocols; unauthorized personnel attempting to enter or actually entering a restricted area, secured protected site, or nonpublic area; impersonation of authorized personnel/vendors, etc.
- Observation/Surveillance/Photography: Demonstrating unusual, prolonged, or surreptitious interest in the actions of PSAP personnel, facilities, and/or emergency communications infrastructure beyond mere casual or professional interest and in a manner that would arouse suspicion of terrorism or criminal activity in a reasonable person (e.g., observation through binoculars; taking notes/pictures/video of entry points, building access systems, security cameras, utilities, fencing; attempting to mark off or measure distances, etc.).
- Cyber-Attack: Compromising or attempting to compromise or disrupt a PSAPs information technology infrastructure. This includes Telephony Denial of Service (TDoS) attacks designed to disrupt call handling platforms for 9-1-1 and/or administrative telephone lines.
- Sabotage/Tampering/Vandalism: Damaging, manipulating, defacing, or rendering inoperable fencing, security cameras, doors, gates, access control systems, utilities, and/or other equipment and infrastructure.

NOTE: A number of the behaviors noted above are considered lawful, constitutionally protected activities. No single act should be viewed as the basis for investigative/enforcement action. The totality of circumstances should be considered when determining the appropriate course of action.

Reporting:

Suspicious activity and/or malicious acts related to PSAP operations or emergency communications infrastructure should be documented and investigated by the local law enforcement jurisdiction. For situational awareness and information sharing purposes, these types of incidents should be reported to:

- The MN Fusion Center at 651-793-3730 / 800-422-0798 or MN.FC@state.mn.us. The Fusion Center is a section of the Minnesota Bureau of Criminal Apprehension (BCA). The mission of the Fusion Center is to collect, evaluate, analyze, and disseminate information regarding organized criminal, terrorist, and all-hazards activity in Minnesota, while complying with state and federal law to ensure the rights and privacy of all.
- DPS-ECN at ECN_ALERT.dps@state.mn.us.

Questions?

Questions regarding Suspicious Activity Reporting (SAR) protocols for PSAPs should be directed to Cathy Clark, the DPS-ECN Deputy Director, at 651-201-7549 or cathy.clark@state.mn.us.