Appendix B - What Public Safety Telecommunicators (PSTs) Need to Know About Swatting One-Pager

Swatting is the act of placing a hoax call to emergency services, typically reporting a violent crime or imminent threat, with the intent to provoke a rapid and overwhelming law enforcement response at a targeted location. These incidents are designed to create chaos, intimidate victims and potentially cause harm to innocent people, responders and bystanders. Swatting has evolved from isolated pranks to a recurring, technology-enabled threat that exploits vulnerabilities in telecommunications and emergency response systems.

Swatting directly impacts the daily operations of ECCs and the safety of communities. PSTs are often the first line of defense, responsible for assessing the credibility of incoming calls and making critical decisions under intense time pressure. Swatting incidents can place responders and victims at risk, disrupt normal operations and erode public trust in emergency communications. Recognizing the signs of swatting and following established protocols is essential to minimize harm and ensure an appropriate response.

Cyber threat actors frequently use caller ID spoofing and anonymization tools to disguise their identity and location, making it appear as though calls originate from local numbers or even the victim's own phone line. Increasingly, swatters employ AI-generated or pre-recorded audio to mimic distress and inject realism into their calls, bypassing PST skepticism. They also gather personal information from social media, data brokers and online forums to craft detailed, believable scenarios. Many swatting campaigns are organized through encrypted messaging apps and criminal "swatting-as-a-service" groups, enabling attacks across jurisdictions.

PSTs should follow standardized SOPs for handling suspected swatting calls, including enhanced questioning, verification steps and supervisor notification. Additionally, accurate documentation and reporting of suspected swatting events support trend analysis and intelligence sharing.

Strategic Takeaways for PSTs

- Swatting is a complex, evolving threat that requires vigilance and analytical skills.
- Following established SOPs and protocols is essential for effective response.
- Coordination with law enforcement and external partners strengthens verification and response.
- Accurate documentation and reporting help identify trends and support prevention efforts.
- Ongoing training and awareness are critical to maintaining readiness and resilience.