Appendix A - Cybersecurity and Cyber Physical Implications of Swatting One-Pager

Swatting is no longer a sporadic prank but a sophisticated, technology-driven threat that exploits the intersection of digital deception and real-world emergency response. At its core, swatting involves the use of cyber tools to generate false reports of critical incidents, such as active shooters or bomb threats, with the intent to provoke an immediate and overwhelming law enforcement response at a targeted location. This convergence of cyber tactics and physical outcomes creates unique risks for emergency communications centers (ECCs) and the communities they serve.

Swatting begins with digital deception. Perpetrators use caller ID spoofing, Voice over Internet Protocol (VoIP) services and anonymization tools to mask their identities and locations. Increasingly, attackers employ AI-generated or pre-recorded audio to mimic distress, inject realism and bypass PST skepticism. Open-source intelligence (OSINT) and doxxed personal data are harvested from social media, data brokers and illicit forums to craft convincing narratives that exploit the trust and urgency inherent in emergency communications. Many swatting campaigns are coordinated through encrypted messaging platforms and criminal "swatting-as-a-service" communities, allowing threat actors to orchestrate attacks across jurisdictions with minimal risk of detection. The physical consequences are immediate and severe. Swatting calls routinely trigger armed law enforcement deployments, school and facility lockdowns, evacuations and widespread service disruptions.

Strategic Takeaways for ECC Leadership

- Treat swatting as a cyber-physical risk: Recognize that swatting exploits both digital vulnerabilities and emergency response protocols, demanding a holistic approach to risk management.
- Integrate into cybersecurity and continuity planning: Ensure that swatting scenarios are included in cybersecurity strategies, business continuity plans and regular training exercises.
- Strengthen partnerships: Build and maintain robust relationships with cybersecurity teams, telecommunications providers, law enforcement and intelligence partners to improve information sharing, verification and coordinated response.
- Invest in tools and training: Prioritize investments in advanced call verification tools, scenario-based training for telecommunicators and supervisors, and standardized policies and SOPs tailored to swatting.
- Enhance tracking and reporting: Support the development of centralized reporting mechanisms and consistent definitions to improve situational awareness and inform strategic decision-making.