

Managing **Swatting** in Your Center



PLACE STATE
AGENCY/DEPT/DIV/
CAMPAIGN
LOGO OR SEAL

[INSERT NAME OF STATE AGENCY/DEPT/DIVISION]

SWATTING: WHAT IS IT?

Swatting is the criminal act of deceiving emergency services into sending heavily armed response teams to an unsuspecting victim's address by falsely reporting a serious emergency situation, such as a hostage situation, bomb threat, or active shooter.

Swatting originated as a prank within the gaming community. In recent years, it has expanded to target individuals across other aspects of society with goals of fear, intimidation, harassment, or diversion of law enforcement resources in preparation for a larger event in the community. Swatting calls may also be a lead-in to cyberattacks – such as Telephony Denial of Service (TDoS) – targeting the 9-1-1 center.

Characteristics of a potential Swatting call may include, but not limited to:

- The call is received on a non-emergency/administrative phone line
- The call may arrive with no Caller ID information, or appear as all zeros, ones, or nines
- The call being processed is the only call received about the potential incident
- The caller's demeanor is inconsistent with the reported incident

IMPORTANT CONTACTS

(INSERT OFFICE/DEPT/DIV NAME)

- [State] 911 Office
[Insert Contact #]
- [State] Fusion Center
[Insert Contact #]
- FBI [City] Field Office
[Insert Contact #]



KEY POINTS TO CONSIDER

- Any incoming call should be treated as legitimate until proven otherwise
- Always follow locally defined policy and procedures for information gathering, dispatch of responders, incident escalation, and information sharing
- Initially, it may be difficult to determine if a call is a hoax
- Reported situations may vary, but are often reported to be serious incidents (e.g., hostage situations, murder, active violence/active shooter) to prompt a larger response to the victim
- The caller's story or provided information may change or escalate during the call. Note inconsistencies in provided information, following up with additional questions

PARTNERS

- Local Law Enforcement Agencies
- Local Emergency Management Agency
- Internet Crime Complaint Center (IC3) www.ic3.gov
- Cybersecurity and Infrastructure Security Agency (CISA)
(888) 282-0870 or www.cisa.gov
- Multi-State Information Sharing and Analysis Center® (MS-ISAC®) (866) 787-4722

CALLER MANAGEMENT AND INFORMATION GATHERING

- ✓ Information gathering plays a key role in the identification of a potential Swatting Incident
- ✓ Additional questions may be added to the call taking process to aid in identification of these incidents. Some of these may include:
 - What is your full name?
 - Where are you calling from?
 - Why didn't you call 911 directly?
(for calls received on non-911 lines)
 - Why is there no noise in the background?
(or other questions about noises that may be inconsistent with the information being provided)
- ✓ Repetition of questions may identify inconsistencies in the caller's story, leading to higher confidence of a hoax call
 - Caller may initially provide a large amount of information as if reading from a script

PLANNING AND COORDINATION

- ✓ Coordinate with Law Enforcement partners to identify potential Swatting targets and review and update as needed
- ✓ Develop a process to verify the legitimacy of requests for service placed for targeted locations
 - Collect contact information for potential targets *(This should be used to contact a targeted individual in the event a request for service is not received from a pre-identified telephone number)*
 - With a targeted individual, develop a code word or phrase for call verification
 - Document contact information and verification word/phrase in the 911 Center's CAD system
 - Develop a process for routine change of verification words/phrases
- ✓ Information sharing with neighboring jurisdictions and State Agencies may identify common elements across identified Swatting incidents