

Publication Date: September 25, 2026

Author: Office of the Under Secretary

DCL ID: GEN-26-04

Subject: Guidance to Educational Institutions on Swatting Threats

Summary: This letter provides an overview and refresher for all educational institutions on the criminal nature of anonymized threats, in particular swatting. This includes procedures for responding to these incidents and available resources on this topic.

Dear Colleague:

The U.S. Departments of Education (ED) and Justice (DOJ) are writing this letter to all educational institutions, including institutions of higher education and state and local educational agencies, in response to recent swatting incidents across the country. Anonymized threats are a growing problem for colleges, universities, and K-12 schools, as well as their faculties, staff, and student bodies. These threats often come in clusters, and educational institutions should be prepared to respond when such threats reach their schools.

This letter serves as a reminder to all educational institutions of the importance of preparing for and responding to swatting incidents appropriately. That includes reporting such incidents to necessary authorities and undertaking proper response protocols. At the conclusion, we provide a summary of some available resources with additional information to guide institutions' responses to these serious incidents.

Background

Swatting is a form of harassment designed to deceive an emergency service provider into sending a police or emergency service response team to another person's or organization's address or location based on the false reporting of a serious law enforcement emergency. The individuals ("swatters") who engage in this activity often use technology—such as caller ID spoofing, social engineering, social media, and prank calls and emails—to make it appear that the emergency alert is coming directly from the victim. Traditionally, swatters have directed their actions toward individuals and residences. Increasingly, the FBI has observed swatters targeting not only individuals but also public places and institutions, such as airports, businesses, and especially schools.

Swatting calls are dangerous not only to the targeted victims but also to the first responders involved. The callers include fabricated details that suggest that a severe, ongoing crisis requires an urgent dispatch of resources to a specific location. Threats can include, but are not limited to, an active shooter, bomb threat, or hostage situation. The perpetrator's goal is to provoke an overwhelming law enforcement response, creating chaos and potentially resulting in the use of force against innocent civilians.

Incidents of swatting in educational environments have increased in recent years, causing significant disruption and trauma to students, teachers, and staff, as well as their families.

Swatting also costs taxpayers millions of dollars in personnel and equipment, lost classroom time, and property damage.

Swatting is Criminal Activity

Swatting scenarios can vary and charging options are highly fact dependent. A school swatting incident may violate one or more federal criminal laws in addition to state laws. For example:

- *Interstate Threatening Communication* ([18 U.S.C. § 875](#)): Transmitting any communication containing a threat to injure a person in interstate or foreign commerce violates 18 U.S.C. § 875(c). That federal criminal prohibition can be relevant to the communications at the center of a swatting incident.
- *False Information and Hoaxes* ([18 U.S.C. § 1038](#)): This law criminalizes conveying certain false information, when the conveyor of such information knows it to be inaccurate. Among other things, the law covers communications concerning an attempt or alleged attempt to kill, injure, or intimidate any individual or to damage or destroy any building, vehicle, or other real or personal property.
- *Bomb Threats* ([18 U.S.C. § 844](#)): School swatting incidents that involve bomb threats may also violate 18 U.S.C. § 844(e). That provision makes it a crime to, among other things, threaten to kill or injure any individual “by means of fire or an explosive.” The statute also prohibits maliciously conveying false information about attempts to kill or injure others with fire or explosives if the individual knows the information is false.
- *Fraud and Related Activity in Connection with Computers* ([18 U.S.C. § 1030](#)): If the swatting incident involves hacking into someone else’s phone or computer to make the false report, coupled with circumstances showing an attempt to gain something of value, the offender could be charged under this 18 U.S.C. § 1030, which prohibits unauthorized access to a protected computer to further an intended fraud.

Swatting communications received in the United States can originate abroad, and some [reporting](#) suggests that this may be true of numerous school swatting incidents. Perhaps the largest of these cases involved hundreds of “[violent threats to Jewish Community Centers, schools and other institutions across this nation](#)” in 2017 that came from an overseas actor. Cases where a discrete protected class is targeted for swatting threats may also implicate federal hate crimes laws. See, e.g., [Prosecution of Federal Hate Crimes](#).

For additional resources on when school swatting constitutes a federal crime, and legislative efforts in this regard, please see [School Swatting: Overview of Federal Criminal Law](#) produced by the Congressional Research Service.

Policies and Procedures

ED and DOJ encourage educational institutions to prepare in advance by reviewing best practices and other resources designed to help institutions respond to instances of swatting effectively. This guidance is intended to aid institutions in developing comprehensive processes, procedures, and training protocols to determine which threats are false and how to respond appropriately. At the same time, institutions should have adequate controls to avoid falsely identifying a real threat as a swatting attempt. To these ends, institutional leaders should consider the following actions:

- Build awareness about incident reporting. Educate faculty, staff, and administrators on typical characteristics of a swatting event so they can detect false threats sooner. Institutions should establish procedures so that personnel can first seek to evaluate the nature of the threat, and, if they believe that threat to be a hoax, then work to break the anonymity of the perpetrator as quickly as possible.
- Develop a partnership structure that will help address anonymized threats. This should include coordination between on-campus officials and security and external law enforcement. Both internal and external parties should have policies and procedures in place governing potential swatting incidents and should have clear communication lines to coordinate a response.
- Consider convening a multidisciplinary threat assessment team that can use their expertise to help assess and address anonymous threats. The team may be made up of internal or external actors, or both, who have been trained or are familiar with the resources outlined in this letter in order to respond appropriately to a given threat.
- Conduct tabletop exercises to familiarize leadership with emergency decision-making protocols in advance. For example, just as institutions have emergency drills related to inclement weather or a live threat, drills should be established that allow an institution to evaluate, as quickly as possible, whether a given threat is a hoax.
- Develop and socialize a plan for law enforcement notification, and update law enforcement throughout an incident.
- Ensure emergency communications protocols are updated. Federal law requires institutions to maintain emergency communication protocols. Those protocols should cover a wide range of possible emergencies but should also establish specific communication procedures for swatting events. Institutions may also be required to include information on whether a given event is a hoax or a live threat in their Annual Security Report statistics.
- Designate responsible officials to lead efforts to publish campus-wide communications, notify law enforcement, and evaluate the level of threats. Officials should know their roles far in advance of a threat occurring and should build experience by participating in simulated situations to ensure awareness and clarity in the event of a real threat. Educational institutions may adopt standard messaging templates to ensure only need-to-know information is released during a threat or investigation.

- Understand that safety is paramount, while also acknowledging that any such threat may be a hoax. Responsible officials must first take steps to ensure the campus community is safe while determining whether the threat is real or a hoax.
- After ensuring the safety of the community, continue to evaluate the validity of the threat. If the threat is phoned in, this includes staying on the line with the caller to ascertain additional information while coordinating with law enforcement, in real time, to obtain an external evaluation of the threat. Similar procedures should exist for obtaining additional information if the threat comes in via social media or other digital technology.

Staff preparation is key and should be the foremost priority in front-line awareness of and development of appropriate responses to swatting incidents. Institutions should consider training all staff members who could be in a position to receive or answer a swatting report. That training should cover procedures to assist in breaking the anonymity of the reporter, as well as de-escalation strategies. Such strategies may include repeated question scenarios, which are intended to reveal additional details about the perpetrator(s) and determine the severity and viability of the threat.

All threats should be treated as credible when received. Schools may be required to provide communications on the threat to local, state, or federal authorities under school policy and applicable law. Educational institutions should take the following actions when responding to a credible threat:

- Take planned steps to ensure students, faculty, and staff are safe first. These steps should occur rapidly, most likely before it is possible to confirm whether the threat is real or the possibility of the threat being a hoax. These first steps should include utilizing existing, mandated, emergency protocols such as student alerts, community contact lists, and shelter-in-place orders to alert individuals to the situation.
 - Such notifications are already required in emergency situations under the Jeanne Clery Campus Safety Act (Clery Act) (20 U.S.C. § 1092(f)), and institutions may be able to easily adapt these notifications for the purposes of responding to swatting events.
- Take planned steps to notify law enforcement and establish continued communications with emergency services. Be prepared to determine the imminence of the threat by proactively engaging with law enforcement agencies and federal resources. Working with law enforcement helps institutions recognize the characteristics of a hoax. In particular, actively sharing facts with law enforcement during an incident is an important part of assessing the nature of a given threat (see *Resources below*).
- Take proactive steps in broader communication. That includes encouraging the community to follow a “Report, Don’t Repost” approach to active threats spread via social media. Follow any standard messaging templates your institution has developed to control information access and help maintain the integrity of an ongoing threat assessment or investigation.

Resources

The federal government provides a wide array of resources designed to help institutional leaders prepare for swatting incidents. These include the following:

- [*First Responder Toolbox*](#) (Department of Homeland Security (DHS)): This resource provides helpful tips and information for those who may receive anonymized threats or swatting calls. Within the First Responder Toolbox, DHS provides additional resources for institutions, including guides regarding violence prevention, resources for schools to use to raise public awareness of instances of violence, terrorism, or swatting, and fact sheets to assist schools in developing and sustaining productive relationships with law enforcement and community stakeholders. The Toolbox also provides substantial resources from agencies across the federal government to help emergency responders address potential swatting incidents.
- [*Resources for Swatting and Hoax Threats*](#) (DHS): The resources in this link assist those facing swatting calls and hoax threats with proactive steps to take to prepare for, respond to, and recover from a related incident. Throughout the country, schools, hospitals, businesses, places of worship, non-governmental organizations, and individuals such as U.S. government officials, journalists, celebrities, online gamers, and many others have increasingly been victims of swatting calls and hoax threats, which cause fear and potentially dangerous interactions with law enforcement. DHS offers this set of resources to prepare a wide range of potential victims to respond to such threats.
- *Responding to and Investigating Bomb Threats and Swatting Hoaxes* (FBI): This is a free 90-minute course that provides information on patterns, statistics, and best practices. This course is best suited for dispatchers, law enforcement, school administrators, call takers, and decision makers. Interested parties can reach out to the FBI at FBIBostonJTTF@fbi.gov to ask about participation in these sessions.
- [*Swatting: Awareness for Law Enforcement*](#) (DHS): This video provides swatting information tailored for all law enforcement personnel, both sworn and non-sworn, and will be especially helpful to school-based law enforcement. This video aims to provide foundational knowledge about swatting incidents and strategies to ensure an appropriate response. It is the first in a series of short videos designed to educate law enforcement and subcommunities about swatting events and how to mitigate harm.
- [*Swatting: Indicators for Public Safety Telecommunicators*](#) (DHS): This video overview on swatting is primarily for public safety telecommunicators and their supervisors. It is also useful for school personnel who regularly receive incoming communications that may include potential swatting efforts. This video aims to provide potential swatting indicators, de-escalation strategies, and helpful practices to public safety telecommunicators who may receive swatting calls directly to 911 or calls routed through non-emergency lines.

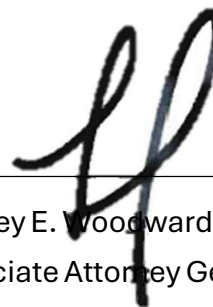
- [*Responding to and Investigating Bomb Threats and Swatting Hoaxes*](#) (DOJ): DOJ also provides periodic training on this topic. This virtual training offers an overview of the realities of bomb threats and swatting hoaxes and includes a detailed review of statistics and current trends seen across the country. The training also covers the characteristics of hoax calls, law enforcement best practices for assessment and response, and the decision-making process for evacuating or sheltering in place.
- [*Swatting: Mitigation Strategies and Reporting Procedures*](#) (ED): Through the Readiness and Emergency Management for Schools Technical Assistance Center, ED also provides access to state-based resources such as these materials, which were produced by the State of Washington using resources developed by New Jersey.

ED and DOJ intend to provide continued guidance on this subject to educational institutions when available and necessary. We are committed to the safety of students, teachers, and staff across the country and take all incidents of swatting and violence seriously. We welcome further conversations with educational institutions to determine how best to solve this crisis, which increasingly affects people and organizations across the country.

Sincerely,



Nicholas Kent
Under Secretary
U.S. Department of Education



Stanley E. Woodward, Jr.
Associate Attorney General
U.S. Department of Justice

Note: This letter is intended to provide guidance and resources to educational institutions who may need them in responding to incidents of swatting. This guidance is not legally binding and is not intended to bind educational institutions to certain resources, policies, or procedures, but rather to provide information and flexibility to tailor their responses to their needs.