The primary purpose of a threat assessment is to prevent targeted violence. The threat assessment process is centered upon analysis of the facts and evidence of behavior in a given situation. The appraisal of risk in a threat assessment focuses on actions, communications, and specific circumstances that might suggest that an individual intends to mount an attack and is engaged in planning or preparing for that event.

In a situation that becomes the focus of a threat assessment inquiry or investigation, appropriate authorities gather information, evaluate facts, and make a determination as to whether a given student poses a threat of violence to a target. If an inquiry indicates that there is a risk of violence in a specific situation, authorities conducting the threat assessment collaborate with others to develop and implement a plan to manage or reduce the threat posed by the student in that situation.

Six principles form the foundation of the threat assessment process. These principles are:

- Targeted violence is the end result of an understandable, and oftentimes discernible, process of thinking and behavior.
- Targeted violence stems from an interaction among the individual, the situation, the setting, and the target.
- An investigative, skeptical, inquisitive mindset is critical to successful threat assessment.
- Effective threat assessment is based upon facts, rather than on characteristics or "traits."
- An "integrated systems approach" should guide threat assessment inquiries and investigations.
- The central question in a threat assessment inquiry or investigation is whether a student poses a threat, not whether the student has made a threat.

In addition, three elements guide the development and operation of an effective school threat assessment program. These elements are:

- authority to conduct an assessment;
- capacity to conduct inquiries and investigations; and,
- systems relationships.

These principles and elements are discussed below.

**Principles of the Threat Assessment Process**

This Guide is about the systematic use of threat assessment as a central component in preventing targeted school violence. The threat assessment process involves identifying, assessing, and managing individuals who might pose a risk of violence to an identified or identifiable target. Implementation of a threat assessment process is informed by six underlying principles.
**Principle 1:** Targeted violence is the end result of an understandable, and oftentimes discernible, process of thinking and behavior.

Findings of the Safe School Initiative indicate that students and former students who committed targeted attacks at schools almost always thought about their attacks in advance, and did not “just snap” suddenly. These findings suggest that students who carry out school attacks may consider possible targets; talk with others about their ideas and intentions; and record their thinking in diaries and journals or on a web site. They may seek out weapons to use in the attack, and they may practice with these weapons in preparation for the attack. The actions of these attackers may be deliberate and occur over days and weeks, months or years.

**Principle 2:** Targeted violence stems from an interaction among the person, the situation, the setting, and the target.

Understanding and preventing acts of targeted violence require a focus on these four component parts and their interaction:

- The individual, the situation, the setting, and the target.
- The potential attacker: To determine the risk of targeted violence, a threat assessor must gather information about the potential attacker. In a threat assessment inquiry or investigation, a major question is: How has this student dealt with situations that have led him or her to see life as unbearably stressful? Individuals who in times of great stress have considered or acted upon ideas of suicide or violence toward others, or both, should be considered persons of increased concern.
- The situation: Investigators should examine circumstances and significant events in the life of the individual, especially recent events that have been overwhelmingly stressful. For students who engaged in school-based attacks, those events included having been bullied and humiliated, especially in public; loss of significant relationships; and perceived failures or loss of status. Almost all school shooters experienced some major situational stress at some point before their attack.11
- The setting: The third factor to consider is the specific setting at the time that the student came to authorities’ attention as possibly posing a threat of targeted school violence. Do fellow students, friends, or others say—directly or indirectly—that violence is not a solution to problems? Do these people suggest ways to get help and assistance? In a school, are there respectful connections among students and adults, networks of trusting relationships, that facilitate non-violent problem-solving? Or is the idea of violence proposed, supported, accepted, or ignored by those who know the potential attacker? In many school shootings, other young persons knew about the shooter’s interest in mounting an attack. In some cases, clear warnings were dismissed or ignored. In others, friends and fellow students of the shooter encouraged or helped the attacker in his pursuit of violence. Messages about the acceptability of violence that are communicated directly or subtly to a potential attacker by students and/or adults in his or her environment may facilitate, or alternatively help to prevent, an attack.
- The target: When assessing the risk of an attack at school, investigators and others with protective responsibilities also must pay attention to the individual’s choice of a potential target. The attacker may target a particular individual or group of individuals over some perceived injury or loss. In some cases, attackers chose a specific target, such as a particular student or teacher. In other instances, the target was more general: the school, "jocks," or "kids in the cafeteria."

11 It should be emphasized again that many young people experience losses, failures, humiliations, and other kinds of situational stressors, and that few become school shooters.
Principle 3: An investigative, skeptical, inquisitive mindset is critical to successful threat assessment.

An investigative mindset is central to successful application of the threat assessment process. Threat assessment requires thoughtful probing; viewing information with healthy skepticism; and paying attention to key points about pre-attack behaviors. Authorities who carry out threat assessments must strive to be both accurate and fair.

Moreover, threat assessors should question the information in front of them continuously. Ideally, there should be credible verification of all essential "facts." Information about a potential attacker's interests, statements, and actions should be corroborated, wherever possible. The investigative mindset and perspective also rely on common sense. Threat assessors working to understand a given situation should step back periodically from the individual details of an inquiry or investigation and ask whether information gathered makes sense and supports any hypothesis developed concerning the risk posed by the subject of the threat assessment inquiry.

Principle 4: Effective threat assessment is based on facts, rather than characteristics or "traits."

A major principle of threat assessment is that each investigation stands on its own. Inferences and conclusions about risk should be guided by an analysis of facts and behaviors specific to the person of concern and the given situation. Any student with the motive, intent, and ability potentially is capable of mounting a targeted attack at school. Judgments about a student’s risk of violence should be based upon analysis of behaviorally relevant facts, not on "traits" or "characteristics" of a given individual or of a class of individuals.

In the climate of fear that followed recent attacks, students in high schools across the country who appeared angry and wore trench coats were marked as possible school attackers. They were so labeled because of appearance and demeanor. Blanket characterizations, or student "profiles," do not provide a reliable basis for making judgments of the threat posed by a particular student. Even worse, the use of profiles can shift attention away from more reliable facts and evidence about a student’s behavior and communications.

Principle 5: An "integrated systems approach" should guide threat assessment investigations.

In a threat assessment, bits of information might be viewed as pieces of a puzzle. Each bit may appear inconsequential or only slightly worrisome by itself. But, when the pieces are put together—as oftentimes has occurred in "after the fact" analyses of school attacks—the behaviors and communications of a student may coalesce into a discernible pattern that indicates a threat of violence. In many school attacks, information existed within the school and community that might have alerted authorities to the risk of attack posed by a particular student. Relationships with agencies and service systems within the school and the surrounding community are critical to identifying, assessing, and managing students who are on a path toward carrying out a school attack. An integrated systems approach recognizes the necessity of cooperation and partnerships between schools and systems outside of the school. These may include law enforcement, social services and mental health providers, the courts, community agencies, families, worksites, religious organizations, and others.

12 Please refer to Reddy, et. al. (2001), "Evaluating Risk for Targeted Violence in Schools: Comparing Risk Assessment, Threat Assessment, and Other Approaches," for a discussion of the use and limitations of profiling as a tool for assessing the risk of targeted school violence. The full citation for the article is provided in the Appendix, Annotated Resources, of this Guide.
Principle 6: The central question of a threat assessment is whether a student a threat, not whether the student a threat.

Although some individuals who threaten harm may pose a real threat of targeted violence, many do not. The Safe School Initiative found that fewer than 20 percent of school shooters communicated a direct or conditional threat to their target before the attack. By contrast, individuals who are found to pose threats of violence frequently do not make threats to their targets. The study found that in more than 80 percent of the cases, school shooters did not threaten their targets directly, but they did communicate their intent and/or plans to others before the attack.

These findings underscore the importance of making judgments in threat assessment investigations based upon a student’s behaviors and communications, rather than upon whether or not that student threatened his or her target. Authorities conducting threat assessment investigations must distinguish between making a threat, e.g., telling a potential target that he or she may or will be harmed, and posing a threat, e.g., engaging in behavior that indicates furthering a plan or building capacity for a violent act. Nevertheless, threats of violence should not be dismissed out of hand. Students may make threats with a variety of intents and for a wide range of reasons, e.g., to get attention; to express anger or frustration; to frighten or coerce their peers; as a part of joking or "playing around; "or, in some cases, to communicate intent to attack. Consequently, every threat should receive prompt attention. Although voicing a threat should not be used as the principle determinant in making judgments about the likelihood of a school attack, it likewise would be a mistake to assume that individuals who make threats in every instance are unlikely to follow through on those communications.

Elements of a School Threat Assessment Process

Authorities involved in carrying out a threat assessment inquiry or investigation should gather and analyze information about the behavior and communications of the student of concern. This information, in turn, will permit these authorities to make reasonable judgments about whether the student of concern is moving along a path toward an attack on an identifiable target. Three elements are essential to the development and operation of an effective school safety threat assessment program.13

1. Authority to Conduct an Investigation

A teacher comes to the principal’s office to report "the kids are saying that Johnny told his friends not to go to the cafeteria at noon on Tuesday because something big and bad is going to happen." What did Johnny mean by that statement? Is Johnny planning to attack the school? Perhaps Johnny is engaging in idle talk. Perhaps the report of Johnny’s statement is inaccurate. Perhaps Johnny is planning an attack on the school or has knowledge about other students’ plans. Clearly, this information cannot be ignored. How, then, should the principal respond to this report? Should the principal call Johnny to the office and ask him about the report? Should other students be queried about the report? What if Johnny denies making the statement that has been reported, while other students assert otherwise? Schools should have in place clear policies on collecting and reacting to information on potentially threatening situations and determining whether this information merits further attention through a threat assessment inquiry and investigation. Threat assessment inquiry and investigation should be initiated if there is credible information that passes a critical threshold of concern. In creating these policies, school administrators should be aware of and consult with
the school’s legal counsel about legal issues related to the conduct of a threat assessment inquiry or investigation. These legal issues include the effects of laws pertaining to: (1) access to and sharing of information, and (2) searches of a student’s person or property. Each of these issues should be discussed with the school’s legal counsel.

Establishing Authority to Conduct an Inquiry or Investigation

A formal policy authorizing school officials to conduct a threat assessment should cover the following topics:

- the purpose and scope of the policy;
- the role of educators and the threat assessment team vis a vis the role of law enforcement;
- the identity of, and delegation of authority to, school officials concerning determination that a threat assessment inquiry or investigation should be pursued;
- the definition of the threshold of concern for initiating a threat assessment inquiry or investigation, i.e., a description of the nature and extent of behavior or communication that would trigger a threat assessment inquiry or investigation;
- the description of the types of information that may be gathered during the assessment;
- the designation of the individuals or group of individuals who would be responsible for gathering and analyzing information; and
- the steps and procedures to be followed from initiation to conclusion of the threat assessment inquiry or investigation.

Information-Sharing in Support of the School Threat Assessment Process

Much emphasis in this Guide is placed upon the importance of sharing information about a student who may pose a risk of violence. In most previous school shootings, there was information available prior to the incident that suggested that the student was planning an attack at school. However, when conducting an inquiry or investigation regarding a potential threat, the inquirer or investigator will find that different people in the student’s life may have different– and possibly small–pieces of the puzzle. It is the responsibility of the threat assessment team to gather this information from what may be multiple sources—teachers, parents, friends, guidance counselors, after-school program staff, part-time employers, and others. Once information is gathered from the various sources contacted during a threat assessment inquiry, the threat assessment team may wish to explore options for storing this information in an accessible format. The team likewise may wish to consider keeping the information in a central location.

Legal Considerations in Developing Information-Sharing Policies and Procedures

Although the need to gather information about a student who may pose a threat of violence is clear, the ability to share this information requires some advance consideration. Laws, rules, regulations, and policies, for example, may place limitations on access to student records and restrict the use of accessible information in conjunction with investigations. In formulating information-sharing policies and procedures, threat assessment teams should consult with their respective school’s—or school district’s—legal counsel to ensure that team members are well-briefed on existing laws and regulations and their implications for the development of policies and procedures for accessing and disclosing student information. In particular, threat assessment teams should examine provisions of these laws and regulations to identify opportunities for including threatening situations in schools as exceptions to constraints on the disclosure of information contained in education records. Two principal areas of law—federal
statutes and state statutes may affect access to and sharing of information about a particular student. An overview of the implications of these areas of law for conducting threat assessment investigations is provided in the following.

Federal Statutes

Under existing federal law, a school’s authority to release information about a student is governed by the Family Educational Rights and Privacy Act (FERPA). The intent of FERPA is to protect the privacy of “education records,” a term that is defined as any records that contain information directly related to a student and that are maintained by the educational agency or institution or by a person acting for the agency or institution. Under provisions of FERPA, a school may not disclose personally identifiable information about a student from any education records without the prior written consent of the student’s parent or, in the case of students who are 18 or older, the consent of the student.

FERPA does allow for various exceptions to privacy protections covering access to student records, specifying situations and conditions under which a school may disclose information from a student’s education records without consent. A detailed analysis of these exceptions is beyond the scope of this Guide. However, there are two exceptions that are worth noting because of their specific relevance to accessing and sharing information for threat assessment inquiries:

- Health and Safety Emergencies: FERPA provides that schools may disclose information from a student’s education records in situations where there is an immediate need to share that information in order to protect the health or safety of the student or others. Under this exception, schools must define the term "health or safety emergency" narrowly and are permitted to disclose information from education records only to those individuals who need the information in order to protect the student and others.

- Law Enforcement Unit Records: FERPA regulations draw a distinction between records created by a school law enforcement unit for law enforcement purposes, such as the enforcement of a local, state, or federal law, and records created by a school law enforcement unit for non-law enforcement purposes, such as the enforcement of school policies concerning behavior or disciplinary actions. FERPA also distinguishes between student information that school law enforcement unit officials gathered from education records, and student information that unit officials obtained from other sources. With respect to disclosure of student information contained in school law enforcement unit records, FERPA provides that:

  - Personally identifiable information about a student may be disclosed by school officials if that information is held in a school law enforcement unit record that was created to enforce a federal, state, or local law.
  - Information in school law enforcement unit records that was not obtained from a student’s education records may also be disclosed without the consent of the student’s parents or the student.

It is important to note that FERPA regulations govern the disclosure of student information from education records and any information about the student that is based upon information contained in education records. FERPA regulations do not restrict the authority of school

14 20 U.S. C. 1232g. See “Information Sharing” in the Appendix, Annotated Resources, of the Guide for referral to additional sources of information on FERPA.
15 34 CFR 99.31(a)(10).
officials to share other information about a student that is not contained in education records. For example, information such as a school official’s personal observations about or interactions with a student that is not contained in education records may be disclosed.

State Law and Access to Student Records

State laws governing access to and sharing of information about students vary from state to state. Moreover, in the wake of highly publicized school shootings in the 1990s, several states enacted laws that revise restrictions on disclosure of information contained in student records. In some states, these amendments, in effect, make it easier to share this information among schools, law enforcement agencies, and others in furtherance of protecting the safety of students at school.\(^{16}\)

2. Capacity to Conduct School Threat Assessments

Proactive planning is a critical element in the implementation of a school threat assessment program. School administrators should consider creating a multidisciplinary threat assessment team that is based in the school or the school district. Schools should not wait until a crisis occurs to establish a threat assessment team. Many schools across the country already have established teams to respond to a wide range of situations, from suicides to meeting special education needs. The expertise and knowledge of any existing teams may be useful in developing a threat assessment team.

The roles and responsibilities of the team as a whole, and of members of that team individually, should be clearly defined. The information gathering and assessment procedures to be used by the team should be formalized. Team members should be trained together in the threat assessment process. Multidisciplinary training sessions provide opportunities for professionals in different systems to build relationships and to consider how to address issues before a crisis arises. Training that uses practical exercises—"what should we do if…"—can enhance threat assessment and management programs and processes.

The multidisciplinary threat assessment team’s principal responsibility is to guide the assessment and management of situations of concern. A senior school administrator should chair the team. Regular members of the team ideally should include: 1) a respected member of the school faculty or administration; 2) an investigator, such as a school resource officer or other police officer assigned to the school; 3) a mental health professional, such as a forensic psychologist, a clinical psychologist, or a school psychologist; and 4) other professionals, such as guidance counselors, teachers, coaches, and others, who may be able to contribute to the threat assessment process.

In addition, the chair of the threat assessment team may wish to consider including as an ad hoc member of the team someone who knows the student of concern in the threat assessment inquiry. This ad hoc position might be held by an individual from the school community, such as a teacher, counselor, coach, nurse, other school employee, or someone from the community who may know or have knowledge of the student, such as a probation officer, member of the clergy, or a social service worker.

\(^{16}\) See “Information Sharing” in the Appendix, Annotated Resources, of the Guide for references that review some of the more recent changes to state laws that affect access to and disclosure of student information contained in education records.
If the student of concern is being provided services under the Individuals with Disabilities in Education Act (IDEA), a representative from the team that developed or manages that student’s Individualized Education Plan (IEP) also should be brought onto the threat assessment team as an ad hoc member for the inquiry regarding this particular student.

**Skills and Training**

Developing the capacity to conduct school threat assessments involves recruiting, training, and supporting professionals with special skills. The qualifications, skills, knowledge and experience of the members of the threat assessment team should include:

- a questioning, analytical, and skeptical mindset;
- an ability to relate well to parents, colleagues, other professionals, and students;
- familiarity with childhood and adolescent growth and development, the school environment, the need for safe schools, and the community;
- a reputation within the school and the community for fairness and trustworthiness;
- training in the collection and evaluation of information from multiple sources;
- discretion, and an appreciation for the importance of keeping information confidential, and of the possible harm that may result in the inappropriate release of information; and
- cognizance of the difference between harming and helping in an intervention.

**3. Integrated Systems Relationships**

In order to identify, assess, and manage students who might pose threats of targeted violence, a threat assessment program must build relationships among individuals and organizations both within the school and external to the school. These relationships can help the team acquire and use information about a given situation, and aid those with protective responsibilities in developing strategies to prevent targeted school violence.

Ideally, community systems concerned with education, safety, and child welfare would have well-established policies and procedures for cooperation and collaboration. In practice, these systems oftentimes are large and overburdened and tend to carry out their functions independently. In a well-functioning threat assessment program, effective systems relationships are most likely to occur between individuals, not institutions. Individuals who build and maintain these relationships across disciplines and agencies are called "boundary spanners." They serve as a formal link or liaison between various systems and meet regularly with them. Boundary spanners have credibility, respect, and strong interpersonal skills. In addition, they should understand the needs and operation of other systems. This understanding helps in integrating ongoing interagency relationships, in developing written protocols, and in facilitating the resolution of conflicts.