**K-12 Threat Assessment and Management:**

**Process Summary and Selected Resources[[1]](#footnote-1)**

**I. Introduction**

In 2002, the United States Department of Education and the United States Secret Service published *The Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States (“SSI Report”)*.[[2]](#footnote-2) The *Safe School Initiative* study, which examined 37 incidents of targeted school violence that occurred in the United States from December 1974 through May 2000, found that incidents of targeted violence in school were rarely impulsive, that pre-attack behaviors were often observable, and that other people often knew that an attack was pending. Recognizing the prevention implications of these findings, these agencies also published the companion document “*Threat Assessment in Schools: A Guide to Managing Threatening Situations and to Creating Safe School Climates”* (“*Threat Assessment Guide*” or “*Guide*”).[[3]](#footnote-3) The *Threat Assessment Guide* adapts the Secret Service-pioneered threat assessment process to the K-12 school context, and outlines an approach for identifying, assessing and managing students who may pose a threat of targeted violence in schools.[[4]](#footnote-4) The *SSI Report* and the *Threat Assessment Guide* continue to be leading school threat assessment resources, and they were cited with approval by the *Guide for Developing High-Quality School Emergency Operations Plans* (“*Emergency Operations Guide*”), which was published by numerous federal government agencies in June, 2013.[[5]](#footnote-5)

The *Threat Assessment Guide* focuses on threats posed by students, but schools may also wish to have means to identify, assess and manage threats posed by employees, family members, and others, including individuals who do not have any affiliation with the school. Fortunately, because the approach in the *Threat Assessment Guide* was adapted from and has been used by various federal agencies in workplace violence prevention, presidential protection, and other contexts, a school threat assessment and management team (“TAM team”) can use that approach to investigate threats posed by non-students, as well as students. *The* *Handbook for Campus Threat Assessment & Management Teams* cited in the *Emergency Operations Guide*[[6]](#footnote-6)applies that approach to students, employees, and others, and an American National Standard published in Fall, 2011 by ASIS and the Society for Human Resources Management, “*Workplace Violence Prevention and Intervention*” (“*Workplace Violence Standard*”) also advocates the use of a similar, though not identical, threat assessment approach in the workplace.[[7]](#footnote-7)

Schools that follow the threat assessment approach outlined in the *Threat Assessment Guide* will also want to: 1) encourage reporting (and appropriate intervention) by educating students, parents, staff and community members about the existence and function of their TAM team; 2) staff and operate their teams appropriately; 3) adopt appropriate related policies; and 4) create and handle team-related documents well. Schools will also want to educate their staff members about the proper balance between community safety and the rights of persons of concern, so that misunderstandings about, for example, privacy and disability laws, do not unduly restrict their ability to take the steps necessary to promote school safety.

This paper summarizes the threat assessment and management process outlined in the *Threat Assessment Guide*, provides links and citations to pertinent resources, provides some updated information, and addresses some of the privacy law issues that are often implicated by the threat assessment and management process.

**II. Overview of the *Threat Assessment Guide***

The *Threat Assessment Guide* is organized into seven substantive chapters.

Chapter II of the *Guide* contains suggestions for promoting a safe school climate, including discussion of respect, bullying, creating connections between adults and students, and encouraging student reporting of safety concerns. Obviously, much work on these issues has been done since 2002, but Chapter II of the *Guide*, and the related school safety culture action plan outlined in Chapter VII of the *Guide*, provide helpful background information.

Chapter III of the *Guide* describes the key findings of the *SSI Report* and discusses the prevention-related implications of those findings. Chapter IV describes the principles underlying the threat assessment approach, outlines considerations for the development of a threat assessment team and process, and discusses information-sharing issues, including related legal issues. Chapter V outlines the steps for identifying and assessing behavior of concern, and Chapter VI outlines threat management strategies. The contents of these chapters and some related updated information will be summarized in more detail below.

Chapter VII of the *Guide* suggests action plans for school leaders who wish to implement a threat assessment process, and the Conclusion in Chapter VIII summarizes how the threat assessment process can be used as a decision-making tool. The Appendix to the *Guide* consists of an annotated list of resources, as of 2002, regarding bullying and respectful climates, information sharing and legal issues, school violence and crime, risk assessment and general violence, and threat assessment and targeted violence.

**III. Key Findings of the *SSI Report* and Prevention-Related Implications**

Based on the collection of information and interviews with attackers and others performed during the *Safe School Initiative*, the SSI Report made the following 10 key findings:

* Incidents of targeted violence at school are rarely sudden, impulsive acts.
* Prior to most incidents, other people knew about the attacker’s idea and/or plan to attack.
* Most attackers did not threaten their targets directly prior to advancing the attack.
* There is no accurate or useful "profile" of students who engage in targeted school violence.
* Most attackers engaged in some behavior, prior to the incident, that caused concern or indicated a need for help.
* Most attackers were known to have difficulty coping with significant losses or personal failures. Many had considered or attempted suicide.
* Many attackers felt bullied, persecuted, or injured by others prior to the attack.
* Most attackers had access to and had used weapons prior to the attack.
* In many cases, other students were involved in some capacity.
* Despite prompt law enforcement responses, most shooting incidents were stopped by means other than law enforcement intervention.

*Threat Assessment Guide* at 17. The *SSI Report* outlined an often-observable “pathway to violence,” in which subjects can move from having an idea about committing violence, to developing a plan, to acquiring the means to carry out an attack, to implementing the attack. *Id*. at 18.

The premise of the threat assessment process outlined in the *Threat Assessment Guide* is that if thoughts and activities commonly found along the pathway to violence can be identified and assessed, then subjects can be moved off that pathway through individually-tailored threat management strategies. The key threat assessment inquiry questions described below were developed in light of these key findings. Chapter III of the *Guide* includes a discussion of the prevention-related implications of each of the key *SSI Report* findings. School officials and TAM team members may wish to review Chapter III to gain a more complete understanding of the relationship between the *SSI Report* findings and the threat assessment and management process outlined in the *Guide*. *See Threat Assessment Guide* at 18-25.

**IV. Implementing a School Threat Assessment Process**

**A. General Implementation-Related Principles**

Chapter IV of the *Guide* begins with the identification of six principles that form the foundation of the threat assessment process. They 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.

*Threat Assessment Guide* at 29. Chapter IV of the *Guide* then explains how these principles should inform the development and operations of a school TAM team. *See id*. at 30-33. Chapter IV then describes how the threat assessment information-gathering process is facilitated by: 1) the team’s being granted the authority to conduct an assessment; 2) the team’s having the capacity to conduct inquiries and investigations; and 3) the team’s need to develop integrated systems relationships that will allow the team to acquire and use information about a person (or situation) of concern. The discussion in Chapter IV is succinct enough that this paper will incorporate it by reference and suggest that school officials and TAM team members may wish to review it, rather than summarizing it further here. *See Threat Assessment Guide* at 33-39.

**B. Information-Sharing Issues**

The success of a TAM team depends heavily upon how readily students, staff and community members will share information about persons of concern. Chapter IV does contain some discussion of legal and other issues related to information sharing, so it is worth addressing separately here changes in the law and other issues that have arisen since the *Guide* was first published in 2002.

Of particular interest is the fact that the “health and safety emergency” exception to the Family Educational Rights and Privacy Act (“FERPA”), which is discussed in the *Guide*, was broadened significantly in 2008, in light of the April 16, 2007 shootings at Virginia Tech. The Virginia Tech Review Panel and other entities found that misunderstandings about the scope of FERPA and the applicability of exceptions to it may have unnecessarily curtailed pre-attack information sharing at Virginia Tech.[[8]](#footnote-8) In response, the U.S. Department of Education amended its FERPA regulations to provide more explicitly that the health and safety exception permits disclosure of education records to any appropriate parties (on or off campus) where necessary to protect the health or safety of a student or others, and that the Department will not second-guess reasonable related judgments made by school administrators.[[9]](#footnote-9)

Schools may also wish to consider other methods to promote appropriate information sharing, notwithstanding FERPA. These could include training programs, publications and/or web pages designed to educate the school community about FERPA, the exceptions under which information can be shared, and the limited remedies for inappropriate disclosure of FERPA-protected information (as school personnel are often surprised to discover, for example, neither individuals nor schools can be sued for violating FERPA). Schools may also wish to promote information sharing by ensuring that their FERPA notice definition of “school officials” (that is, employees, contractors and others with whom education records and information therefrom may be shared freely),[[10]](#footnote-10) is broad enough to encompass TAM team members. To support their education efforts, schools may wish to consult resources published relatively recently by the U.S. Department of Education regarding the application of FERPA in the school safety context.[[11]](#footnote-11)

In light of increasing public awareness of the privacy protections of the Health Insurance Portability and Accountability Act (“HIPAA”), which are not addressed in the information-sharing section of the *Threat Assessment Guide*, schools may also wish to ensure that any misperceptions about the scope or applicability of HIPAA do not unduly hamper the sharing of health-related information that may be possessed by school nurses, psychologists, and other licensed health care providers employed by schools. The HIPAA Privacy Rule prohibits the disclosure of personal health information by covered health plans, health care clearinghouses and those health care providers that conduct certain health care transactions electronically. According to the U.S. Department of Health and Human Services, “it is expected” that most elementary and secondary schools will not be covered by HIPAA, because they do not conduct covered billing or other covered transactions electronically.[[12]](#footnote-12) Further, even in the rare case where school health care operations are covered by HIPAA, it is not likely that their records will contain HIPAA-covered “protected health information” because student health records are generally covered by FERPA (and its exceptions), not HIPAA.[[13]](#footnote-13)

Finally, even if HIPAA did somehow apply to certain records maintained by schools, HIPAA regulations provide that HIPAA permits disclosure of protected health information if a covered entity believes in good faith that disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and such disclosure is made to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.[[14]](#footnote-14) Given these parameters, the information-gathering activities of TAM teams should not be hampered unduly by HIPAA-related concerns, and schools may wish to undertake educational efforts if there is any concern that misunderstandings about HIPAA might interfere with those activities.

Post-2002 developments in the utilization of social media may also be considered by TAM teams that are seeking to optimize the receipt of information from students, parents, employees and community members. For example, as teams develop their protocols, they may wish to determine: 1) whether and how they might use social media for outreach about the team’s existence, function and mission in order to promote information sharing; and 2) how they might use social media (including anonymous reporting mechanisms, if deemed appropriate) to promote reporting of information about persons of concern.

**C. Additional Implementation-Related Resource**

In addition to considering the implementation-related information provided in Chapter IV of the *Threat Assessment Guide*, schools may also wish to consider a more recently-published resource, *Implementing Behavioral Threat Assessment on Campus, A Virginia Tech Demonstration Project*.[[15]](#footnote-15) This document summarizes the decisions faced and policies adopted by Virginia Tech in its implementation of a robust threat assessment process following the April 16, 2007 shootings. While not all of the information in the document will be applicable to the K-12 context, school administrators and TAM team members may wish to review the document given its relative currency, its discussion of steps taken by Virginia Tech to build community confidence in the TAM team and to encourage reporting and information sharing, and its discussion of potential TAM-related pitfalls and ongoing challenges that could affect a TAM team in either the higher education or K-12 context.

**V. Conducting a School Threat Assessment**

Chapter V of the Threat Assessment Guide begins by making a distinction between “threat assessment inquiries,” which are carried out by a school TAM team, and “threat assessment investigations,” which are carried out by a law enforcement agency if the TAM team’s initial inquiry determines that there is a valid risk of targeted school violence. *See* *Threat Assessment Guide* at 43. In making this distinction, the Guide emphasizes that different communities may make different choices, all valid, about how to handle what should properly be understood as “two complementary parts of a threat assessment continuum.” *Id*. Schools may decide to give primary responsibility for all threat assessment inquiries to law enforcement officials, they may give primary responsibility for initial inquiries to school officials, or they may adopt a “blended” system where, presumably, law enforcement officials essentially work on initial inquiries as part of a TAM team, then work to transition the inquiry to a law enforcement-focused threat assessment investigation if that appears necessary. *Id*. The Guide indicates that the process is “presented in this manner as a means of underscoring the proposition that not all situations that become the focus of school threat assessment inquiries will require referral to and follow-up threat assessment investigations by law enforcement officials.” *Id*. This does not mean, of course, that law enforcement officials cannot be at the table as TAM teams perform initial inquiries, and schools may wish to consult early and often with law enforcement officials regarding whether a particular case should transition to a law enforcement investigation.[[16]](#footnote-16) These issues are covered in more detail in Chapter V of the *Guide*. *See Threat Assessment Guide* at 43-44.

The threat assessment inquiry section of the *Guide* explains that the inquiry should begin with the TAM team’s first determining whether the information that brought the individual of concern to the team’s attention indicates that there may be an imminent risk of violence. If that is the case, law enforcement should of course be contacted without delay. *See Threat Assessment Guide* at 48. If there does not appear to be an imminent risk, the TAM team can work to gather information about the person of concern and the circumstances that will help it determine whether to request that law enforcement conduct a threat assessment investigation. The threat assessment inquiry process involves TAM team members’ gathering of information about, for example:

* the facts that drew attention to the person of concern, the situation, and possibly potential targets;
* identifying, background, and current life information about the student;
* “attack-related” behaviors;
* motives; and
* target selection.

*See Threat Assessment Guide* at 48-51. The *Guide* then provides examples of sources of information for the threat assessment inquiry, which can include: 1) school information (such as school records, teacher interviews, and other easily-accessed information); 2) collateral school interviews (with bystanders and others who may have information about the person of concern’s behaviors, ideas or intentions in relation to the behavior that brought the person to the team’s attention, or otherwise); 3) a parent/guardian interview, where applicable; 4) an interview with the person of concern; and 5) an interview of potential targets, where appropriate. The *Guide* provides detailed information about the pros and cons of various types of interviews, strategies for seeking information, and suggested questions. *See id*. at 51-55.

Of course, TAM teams operating in 2016 and beyond will also want to view social media and other internet-based media as potentially rich sources from which to collect information about persons of concern, and to learn about threats and/or threatening behavior. Further, TAM teams will generally want to be cognizant of the rising incidence of cyber-bullying and other electronically-based harassment, and if they determine that use of the threat assessment process by the TAM team might be helpful in investigating and addressing such issues, to ensure that they have the authority to do so.

The *Guide* then outlines 11 key inquiry questions that should be considered when evaluating the information gathered in the threat assessment inquiry. As noted above, these key inquiry questions are informed by the key findings of the *SSI Report*. The questions outlined in the *Guide* are:

* What are the person of concern’s motive(s) and goals?
* Have there been any communications suggesting ideas or intent to attack?
* Has the subject shown inappropriate interest in school attacks or attackers, weapons (including recent acquisition of a relevant weapon), incidents of mass violence (terrorism, workplace violence, mass murderers)?
* Has the person of concern engaged in attack-related behaviors (such as, e.g., developing an attack idea or plan, making efforts to acquire or practice with weapons, casing or checking out possible sites for an attack, or rehearsing attacks)?
* Does the person of concern have the capacity to carry out an act of targeted violence (i.e., is the person’s thinking organized enough to carry out an attack [organizational capacity can wax and wane], and does the person have access to weapons)?
* Is the person of concern experiencing hopelessness or desperation [given the *SSI Report*’s findings that many of the attackers studied were suicidal]?
* Does the person of concern have a trusting relationship with at least one responsible adult [such a person can represent a powerful protective factor and be an extremely valuable resource in implementing case management strategies], and is the person emotionally connected to or disconnected from others?
* Does the person of concern see violence as an acceptable, desirable, or the only way to solve problems?
* Is the person of concern’s conversation and “story” consistent with his or her actions (i.e., does the information from collateral interviews and sources confirm or dispute what the person says is going on)?
* Are other people concerned about the person of concern’s potential for violence?
* What circumstances might affect the likelihood of an attack (i.e., what factors in the person of concern’s life might increase or decrease the likelihood of an attack, and will the reaction of others, such as peers, encourage or discourage an attack)?

*See Threat Assessment Guide* at 55-57.[[17]](#footnote-17) The *Guide* provides substantial sub-questions and suggestions for inquiry, and explains in detail what the 11 key inquiry questions are seeking to determine. *See id*. The *Guide* suggests that a TAM team’s consideration of the answers to these questions will, if sufficient information has been gathered, “produce a sound foundation for the threat assessment team’s response to the overarching question in a threat assessment inquiry: Does the [person] of concern pose a threat of targeted violence at school?” To be clear, the *Guide* is suggesting that the TAM team should answer these questions for itself based on the information gathered, not that it should necessarily pose each of these questions directly or literally to each witness, particularly where considerations such as the age of interviewees, their relationship to the person of concern, or other factors suggest that a less literal interviewing approach is required.

The *Guide* indicates that if sufficient information has been gathered to answer the key inquiry questions, and “the weight of the information is convincing that the [person of concern] does not pose a threat of targeted school violence,” then the TAM team can close the threat assessment inquiry (subject to re-opening if new information comes to light), and/or refer the person of concern to supportive resources as necessary. *Id*. at 57. If, on the other hand, the team concludes that there is insufficient information for the team to be “reasonably certain” that the person of concern does not pose a threat, or the person appears to be on a path to cause harm, then the team should, according to the *Guide*, recommend that the matter be referred to, and partner with, law enforcement for a law enforcement investigation and appropriate intervention. *Id*. at 58.

The *Guide* also includes advice about appropriate documentation of a threat assessment investigation. *Id*. Documentation should be done carefully whether or not the threat assessment inquiry results in a referral to law enforcement.

Chapter V of the *Guide* concludes with a succinct description of a law enforcement threat assessment investigation that law enforcement officials may wish to review. *See id*. at 58-59.

**VI. Managing a Threatening Situation**

Chapter VI of the *Guide* summarizes some key components and considerations that may come into play in a TAM team’s and school’s management of a potentially threatening situation. The *Guide* emphasizes that threat management inherently requires a case-by-case determination of what strategies will best divert persons of concern from the pathway to violence. For example, it may be helpful for schools and TAM teams to recognize that targeted violence is a dynamic process. Therefore, if information gathered in response to the 11 key inquiry questions suggests that particular stressors may make the person of concern more likely to engage in targeted violence, then TAM teams may, if practicable, want to identify and implement strategies designed to mitigate such stressors.

Chapter VI of the *Guide* includes discussion of strategies for the short-term and long-term management of potentially threatening situations, and emphasizes that an integrated systems approach, which utilizes the support and expertise of school officials, law enforcement officials, mental health professionals, youth service workers, court, probation and correctional staff, and others, can be crucial to convincing a person of concern that there is reason for hope, thereby reducing the likelihood of threatening behavior in the future. *Id*. at 65. The threat management suggestions in Chapter VI of the Guide are concise enough that they can be incorporated by reference rather than summarized further here. *See id*. at 63-66. Though the scale of devoted case management resources needed at an institution the size of Virginia Tech will not likely be necessary in most K-12 school environments, further helpful information about threat management strategies is provided in the Case Management chapter of the *Implementing Behavioral Threat Assessment* resource.[[18]](#footnote-18)

**VII. Conclusion**

The *Threat Assessment Guide* outlines a process for the identification, assessment and management of potentially threatening behavior that could, if not addressed, culminate in targeted violence at a school. When supplemented by the updated information provided above, and implemented thoughtfully by school officials in collaboration with law enforcement officials as necessary, the threat assessment process outlined in the *Guide* can divert persons of concern from the pathway to violence, and enhance safety in our schools.

1. This summary and resource paper was prepared primarily by Jeffrey J. Nolan, Esq., in collaboration with Eugene R. Deisinger, Ph.D., William Modzeleski, Marisa R. Randazzo, Ph.D. (f/k/a Marisa Reddy), and Jeffrey W. Pollard, Ph.D., ABPP.

   Mr. Nolan is a director at Dinse, Knapp & McAndrew, P.C. in Burlington, Vermont, [www.dinse.com](http://www.dinse.com), is admitted to practice as an attorney in Massachusetts, New York, Texas and Vermont, and regularly serves in a training and consulting role with Sigma Threat Management Associates, www.SigmaTMA.com (“Sigma”). Mr. Nolan worked with a team that developed Margolis, Healy & Associates’ U.S. Department of Justice-funded national curriculum, *Campus Threat Assessment Training—A Multidisciplinary Approach for Institutions of Higher Education*, and served as one of the faculty members for that curriculum, which was presented at 10 locations throughout the United States in 2009, 2010 and 2011. Dr. Deisinger is a Managing Partner of Sigma, and served before that as the Deputy Chief of Police and Director of Threat Management Services for Virginia Tech. Mr. Modzeleski is a Senior Consultant to Sigma and a former Associate Assistant Deputy Secretary for the U.S. Department of Education’s Office of Safe and Drug Free Schools. Dr. Randazzo is a Managing Partner of Sigma and formerly served as Chief Research Psychologist for the U.S. Secret Service. Dr. Pollard is the Senior Consulting Psychologist with Sigma and a founding member of George Mason University's Threat Assessment Team, where he is an Affiliate Professor in the Department of Psychology. [↑](#footnote-ref-1)
2. Bryan Vossekuil, Robert Fein, Marisa Reddy, Randy Borum, and William Modzeleski, *Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States.* Washington, DC: U.S. Department of Education and U.S. Secret Service, 2004. Available at: http://www2.ed.gov/admins/lead/safety/preventingattacksreport.pdf. [↑](#footnote-ref-2)
3. Robert Fein, Bryan Vossekuil, William Pollack, Randy Borum, William Modzeleski, and Marisa Reddy, *Threat Assessment in Schools: A Guide to Managing Threatening Situations and to Creating Safe School Climates.* Washington, DC: U.S. Department of Education and U.S. Secret Service, 2004. Available at: http://www2.ed.gov/admins/lead/safety/threatassessmentguide.pdf. [↑](#footnote-ref-3)
4. It is noteworthy that the threat assessment approach outlined in the *Threat Assessment Guide*, while developed for early identification and intervention regarding targeted and mass violence, has been effectively utilized to facilitate early identification and intervention with a range of school safety concerns including but not limited to bullying, harassment, and suicidality. [↑](#footnote-ref-4)
5. The *Emergency Operations Guide* is available at: http://rems.ed.gov/docs/REMS\_K-12\_Guide\_508.pdf. Agencies involved in producing the *Emergency Operations Guide* included the U.S. Department of Education, the U.S. Department of Health and Human Services, the U.S. Department of Homeland Security, the U.S. Department of Justice, the Federal Bureau of Investigation, and the Federal Emergency Management Agency. In addition to the *SSI Guide* and the *Threat Assessment Guide*, the *Emergency Operations Guide* cited the following threat assessment resources: Frederick Calhoun and Stephen Weston, *Contemporary Threat Management: A Practical Guide for Identifying, Assessing, and Managing Individuals of Violent Intent* (San Diego, CA: Specialized Training Services, 2003); Gene Deisinger, Marisa Randazzo, Daniel O’Neill, and Jenna Savage, *The Handbook for Campus Threat Assessment and Management Teams* (Stoneham, MA: Applied Risk Management, 2008); Robert Fein, Bryan Vossekuil, and Gwen Holden, *Threat Assessment: An Approach to Prevent Targeted Violence* (Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, 1995); John Monahan, Henry Steadman, Eric Silver, Paul Appelbaum, Pamela Robbins, Edward Mulvey, Loren Roth, Thomas Grisso, and Steven Banks, *Rethinking Risk Assessment: The MacArthur Study of Mental Disorder and Violence* (New York, NY: Oxford University Press, 2001). [↑](#footnote-ref-5)
6. *See* footnote 5. [↑](#footnote-ref-6)
7. The ASIS/SHRM Workplace Violence Standard is available for a modest charge at: http://www.asisonline.org/guidelines/published.htm. For a comparison of the threat assessment approach outlined in *The* *Handbook for Campus Threat Assessment & Management Teams* and that outlined in the ASIS/SHRM Workplace Violence Standard, *see* Jeffrey Nolan, *Implementing Threat Assessment and Management Best Practices in the Higher Education Workplace*, available at: http://www.sigmatma.com/resources.html. [↑](#footnote-ref-7)
8. *See* The Virginia Tech Review Panel Report, August 2007 (http://www.vtreviewpanel.org/report/index.html). Similar observations were also made in several of the Virginia Tech review-related documents cited as resources in Raymond Thrower, Steven Healy, Gary Margolis, Michael Lynch, Dolores Stafford and William Taylor, *The IACLEA Blueprint for Safer Campuses* (IACLEA Special Review Task Force, April 18, 2008), a document published by the International Association of Campus Law Enforcement Administrators, which is available at: http://www.iaclea.org/visitors/PDFs/VT-taskforce-report\_Virginia-Tech.pdf. [↑](#footnote-ref-8)
9. *See* 34 C.F.R. § 99.31(a)(10) and 34 C.F.R. § 99.36. [↑](#footnote-ref-9)
10. *See* 34 C.F.R. § 99.34(a)(1). [↑](#footnote-ref-10)
11. *See* *Balancing Student Privacy and School Safety: A Guide to the Family Educational Rights and Privacy Act for Elementary and Secondary Schools*, available at: http://www2.ed.gov/policy/gen/guid/fpco/brochures/elsec.pdf (discussing transfer of education records from one school to another, health and safety emergency issues, the inapplicability of FERPA to law enforcement unit/security unit records, the fact that video images are not considered to be education records for FERPA purposes, and the fact that personal observations, as opposed to recorded information, are not covered by FERPA); *Family Educational Rights and Privacy Act (FERPA) and the Disclosure of Student Information Related to Emergencies and Disasters* (June 2010), available at: http://www2.ed.gov/policy/gen/guid/fpco/pdf/ferpa-disaster-guidance.pdf. [↑](#footnote-ref-11)
12. *See* HIPAA Frequently Asked Questions, “Does the HIPAA Privacy Rule Apply to an Elementary or Secondary School?,” available at: http://www.hhs.gov/ocr/privacy/hipaa/faq/ferpa\_and\_hipaa/513.html. [↑](#footnote-ref-12)
13. *See* *id*. *See also* HHS-DOE *Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) And the Health Information Portability and Accountability Act of 1996 (HIPAA) To Student Health Records* (http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf). [↑](#footnote-ref-13)
14. *See* 45 C.F.R. § 164.512(j). [↑](#footnote-ref-14)
15. *See* Marisa Randazzo, Ellen Plummer, *Implementing Behavioral Threat Assessment on Campus, A Virginia Tech Demonstration Project* (November 2009) (“*Implementing Behavioral Threat Assessment*”), available at: http://rems.ed.gov/docs/VT\_ThreatAssessment09.pdf. This resource, along with other resources that school officials and TAM team members may wish to consult, is also available on Virginia Tech’s web site at:

    <http://www.threatassessment.vt.edu/Implementing_Behavioral_Threat_Assessment.pdf> [↑](#footnote-ref-15)
16. Given the FERPA issues referenced above, schools and/or TAM teams may wish to consult with legal counsel regarding what information about students can be shared with law enforcement officials, and/or the means by which such information can be shared (for example, in response to a subpoena), in cases where the health or safety exception or some other exception does not apply. In employee cases, schools may also wish to consult with counsel about the implications of any information-sharing restrictions that might be contained in applicable collective bargaining agreements. [↑](#footnote-ref-16)
17. The *Threat Assessment Guide* refers to “students” rather than “persons of concern” in the cited section because the *Guide* is focused on potential threats posed by students. However, as noted above, because the threat assessment process outlined in the *Guide* may also be used to assess threats posed by employees, parents, community members of others, the broader “person of concern” term is used here. [↑](#footnote-ref-17)
18. *See* *Implementing Behavioral Threat Assessment* at 41-46. *The Handbook for Campus Threat Assessment Teams* cited in the *Emergency Operations Guide*, *see* footnote 5 above, also contains a useful discussion of case management strategies that can be adapted in many respects to the K-12 context. [↑](#footnote-ref-18)