

September 25, 2026

AFTER-ACTION REPORT FOR UTAH VALLEY UNIVERSITY

An Independent Review of the Events Surrounding September 10, 2025 and Recommendations for Future Event Safety and Security

TABLE OF CONTENTS

Introduction 4

Objectives of this Assessment 4

Context Regarding the Nature of the Incident 5

The Project Team 5

Cooperation and Access to Information 6

Actions Taken During the Assessment 7

Documents and Evidence Reviewed 8

Professional Standards and Guidance Sources 8

Executive Summary: Key Findings 10

Timeline 17

Pre-Event Planning and Preparation (July 10-September 9) 17

Incident Day Timeline (September 10) 19

Post-Incident Response and Recovery 22

After-Action Report 25

1. Governance, Policies, and Preparedness Framework 25

1.1 Overview of Policies, Protocols, Plans, and Evidence Reviewed 25

1.2 Policy 425 and Major Event Review Framework 25

1.3 UVUPD Policy Manual and Departmental Procedures 26

1.4 Emergency Operations Plan, EOC Framework, and Active Assailant Protocols 27

1.5 ICS, NIMS, and Event Action Planning 28

1.6 Training, Exercises, and After-Action Learning 29

1.7 Mutual Aid and External Support Framework 31

1.8 Crisis Communications and Media Response Planning 32

1.9 Organizational Alignment, Staffing, and Professional Standards 34

2. September 10 TPUSA Event Planning, Response, and Interagency Coordination 37

2.1 Prevention and Preparedness Practices for High-Profile Events 37

2.2 Major Event Classification and MEAC Review 38

2.3 Venue, Ticketing, and MEAC Planning Decisions 39

2.4 Pre-Event Security Coordination and Intelligence 41

2.5 Day-of Security Posture and Operational Adjustments 44

2.6 Initial Interagency Response and Campus Searches 48

2.7 Transition to State and Federal Investigative Command 49
2.8 Fire, EMS, and Emergency Management Interagency Support 51
2.9 Key Interagency Lessons 52
2.10 Assessment and Preparedness Gaps 52
3. Event Security Planning and Operations 54
3.1 Event Security Planning and Security Assessment 54
3.2 Event Security Operations 57
3.3 Access Control, Screening, and Credentialing 58
3.4 Protective Operations and Line-of-Sight Planning for Outdoor Events 62
3.5 Traffic, Parking, and Perimeter Management 64
3.6 Fixed and Temporary Site Security Measures 66
4. Incident Command, Emergency Management, and Emergency Response Implementation 68
4.1 Application of ICS and Event Action Planning 68
4.2 Implementation of the Emergency Operations Plan and Active Assailant Protocols 70
4.3 EOC Activation, Situational Awareness, and Decision Support 72
4.4 Interagency Coordination and Mutual Aid Implementation 74
5. Communications, Security Technology, and Protective Intelligence 77
5.1 Communications and Mass Notification 77
5.2 Physical Security Technology 82
5.3 OSINT, Web, and Social Media Monitoring 86
5.4 Information Sharing and Protective Intelligence 89
6. Behavioral Threat Assessment and Threat Management 92
6.1 Team Structure, Governance, and Case Management 92
6.2 Information Sharing, OSINT, and Protective Intelligence 95
6.3 Integration with Security Planning and Protective Measures 97
6.4 Training, Professional Development, and Continuous Improvement 97
6.5 Intervention Resources and Related Policies 98
7. Post-Incident Recovery, Corrective Actions, and Preparedness Enhancements 101
7.1 Post-Incident Recovery and Community Support 101
7.2 Support for UVUPD Personnel and First Responders 102
7.3 Awareness, Training, and Preparedness Improvements 102
7.4 Crisis Communications Planning and Public Trust 103
7.5 Interagency Security and Preparedness Enhancements 104
7.6 Post-Incident Actions Taken or Initiated 107
7.7 Overall Assessment 111

8. Legal Considerations 112
8.1 Legal and Regulatory Framework 112
8.2 Event Classification, External Use, and Fronting 112
8.3 First Amendment Considerations 113
8.4 Firearms and Security Screening Considerations 114
8.5 Clery Act and Emergency Notification Considerations 115
8.6 Legal Review of Findings and Recommendations 116
9. Recommendations 117

Appendices 129

Appendix A: Project Team Bios 129
Core Law Enforcement and Security Risk Management Team 129
Core Brownstein Team 130
Advisory Board 131
Communications Lead 132
Appendix B: Incident Command System (ICS) Roles and Responsibilities 133
Appendix C: OSINT and Protective Intelligence Technical Considerations 135
Appendix D: Event Security Planning and Protective Measures Reference Guide 140
D.1: Event Security Planning Framework for High-Profile Events 140
D.2: Event Screening Operations Planning Considerations 141
D.3: Access Control, Ticketing, and Credentialing Considerations 142
D.4: Common Event Security Posts and Functions 144
D.5 Protective Operations Considerations for Outdoor Events 146
D.6: Traffic, Parking, and Perimeter Security Considerations 147
D.7: Fixed and Temporary Site Security Measures 150
D.8: Announcements and Scripted Response Protocol Messages 151
D.9: Physical Security Technology Technical Considerations 153
D.10: Post-Event Review Considerations 156

Introduction

Objectives of this Assessment

This external and independent assessment was done at the request of Utah Valley University (UVU). The purpose of the assessment is to establish a clear, factual, and evidence-based understanding of the events leading up to, during, and immediately following the fatal shooting of Charlie Kirk at UVU on September 10, 2025. The assessment was designed to evaluate the University's[1] planning, preparedness, decision-making, operational response, interagency coordination, and post-incident actions related to the event. By its very nature, an after-action report has the benefit of hindsight. This is important to acknowledge when assessing actions or omissions that took place prior to an unexpected tragedy. The objective of this review is not to examine political viewpoints or speculate regarding motivations. Rather, it is to provide an independent assessment of the incident, identify lessons learned, and offer practical recommendations to strengthen security, preparedness, response capabilities, and organizational resilience for future events.

This independent assessment was conducted following the tragic death of Charlie Kirk during a September 10, 2025 event at Utah Valley University. We recognize the profound impact this incident has had on Mr. Kirk's family, friends, colleagues, supporters, event attendees, first responders, and the broader community.

Consistent with the objectives outlined in the UVU Request For Proposal 2026-1172 and the Project Team's proposed methodology, the assessment sought to:

- Establish a validated timeline of events and key decision points.
- Analyze circumstances and operational considerations associated with the incident.
- Evaluate security, emergency management, and response protocols, including coordination among University personnel and external public safety partners.
- Assess communications, command structure, staffing, deployment, and resource allocation associated with the event and response efforts.
- Identify strengths, effective practices, and actions that contributed positively to the incident response.
- Identify vulnerabilities, gaps, and areas for improvement to enhance future preparedness and operational readiness.
- Develop practical, prioritized, and actionable recommendations aligned with recognized practices in higher education safety, emergency management, event security, executive protection, and behavioral threat assessment.
- Support UVU's ongoing commitment to exceptional care, exceptional accountability, and exceptional results through a transparent and independent review process.

[1] We use both University and UVU to refer to Utah Valley University.

- Review and analyze legal issues related to both the event and the incident: these include University policies (ranging from event planning, safety and security, and emergency response), risk, reporting, Clery Act compliance, campus police protocols and resources, and First and Second Amendment challenges unique to a public university.

Context Regarding the Nature of the Incident

The Project Team that performed this assessment views it as unique in one significant respect. Most of the high-profile shooting incidents that have occurred on college campuses over the last several decades have been perpetrated by "insiders" – students, former students, staff or former staff, often motivated by perceived grievances. Research shows there are aspects of such incidents that seem to recur and can be informative in examining how educational institutions can best assess possible threats on their campuses. As a consequence, over the last two decades, primarily in the aftermath of the Virginia Tech shootings in 2007, American colleges and universities, including UVU, have developed comprehensive policies and protocols to assist in identifying on-campus behavioral threats. A Behavioral Threat Assessment and Management (BTAM) Team exists at virtually every public college and university in the country, including UVU.

However, this current assessment and after-action report involves violence alleged to have been perpetrated by someone unaffiliated with UVU and presents issues outside the internal threat assessment framework of the University. Campus firearm violence perpetrated by "outsiders" is much less frequent than by insiders and a political assassination on a college campus is exceptionally rare. This distinction is important because threats originating outside the campus community are inherently more difficult for universities to identify and assess through internal reporting, behavioral threat assessment, and intervention processes. External threats may not involve prior contact with the institution, may not appear in campus records, and may not generate observable warning behaviors known to University personnel before an incident occurs.

The Project Team

The Lake Forest Group (LFG) assembled a highly qualified core team to support Utah Valley University (UVU) in this important review of the September 10, 2025 TPUSA event held at UVU. This core team brought expertise in law enforcement operations, physical and site security assessment, emergency preparedness, and behavioral threat assessment and management. In addition, six subject matter experts conducted a focused review and provided insight in specialized areas relevant to the assessment, including campus safety, security technology, open-source intelligence, counter-sniper tactics, behavioral threat assessment, and crisis communications.

Brownstein Hyatt Farber Schreck, LLP (Brownstein) led the review and analysis of legal issues related to the event, the incident, and the broader legal and policy framework applicable to public institutions of higher education. The attorneys from Brownstein have extensive experience and expertise in conducting external investigations of the nature requested by UVU. That experience includes assessments of several campus-related shooting incidents.

Together, these professionals formed the Project Team responsible for preparing this After-Action Report for UVU. The Project Team's work was further supported by a communications and report-development team that helped organize, synthesize, edit, and present the assessment findings in a clear, integrated, and professionally documented report. Biographies for the Project Team can be found in **Appendix A.**

Cooperation and Access to Information

The Project Team appreciates the cooperation and assistance UVU provided throughout this independent review. University personnel facilitated timely access to relevant documents, video recordings, policies, procedures, and other materials necessary to conduct the assessment. UVU representatives responded to requests for information, answered questions posed by the Project Team, and coordinated interviews with employees and other individuals possessing relevant knowledge of the events under review.

The Project Team also interviewed numerous local, county, state, and federal government officials. We appreciate their cooperation, insights, and detailed information regarding the days surrounding the September 10 TPUSA event.

This cooperation enabled the Project Team to conduct a thorough, fact-based evaluation of the incident and the University's planning, preparedness, response, and recovery efforts. Although UVU fully cooperated with the assessment process, the findings, observations, and recommendations contained in this report are solely independent and those of the Project Team.

The Project Team also sought information from non-UVU individuals and organizations with relevant knowledge of the September 10 TPUSA event, separate from the local, county, state, and federal government officials interviewed as part of this review. The purpose of this outreach was to better understand the actions taken before, during, and after the TPUSA event at UVU, and to obtain any additional information, insights, or perspectives that may have differed from, or supplemented, information provided through UVU and government sources.

Despite repeated outreach attempts, the Project Team did not receive responses from the following individuals or other representatives of their organizations. This information is included solely to document outreach efforts and to provide transparency regarding the scope of information available to the Project Team.

- The Project Team reached out to Brian Harpole, who was identified as the leader of the Integrity Solutions security team working with TPUSA to provide executive protection for TPUSA CEO Charlie Kirk. The Project Team attempted to reach Harpole by telephone and certified letter. The certified letter explained the purpose of the outreach and provided the Project Team's contact information. The Project Team did not receive a response.
- The Project Team also reached out to Dan Flood, TPUSA Security Supervisor, and Maycee Crofts, a TPUSA Senior Field Representative. Flood was identified as the person who coordinated security for the organization with Brian Harpole of Integrity Solutions. Flood was present at UVU on September 10 and had phone and text communications with UVU Police Chief Jeff Long a few days before and the morning of the event. Crofts was identified as a Senior Field Representative of TPUSA and

participated online in the Major Events Assessment Committee (MEAC) planning meeting held on August 25 regarding the September 10 TPUSA event. Neither Flood nor Crofts responded to phone calls or voicemail messages. In Flood's case, the Project Team also sent a certified letter. The Project Team did not have a current address for Crofts.

- The Project Team further contacted senior-level staff members at TPUSA in Phoenix seeking assistance in connecting with Dan Flood and Maycee Crofts. The Project Team did not receive a response to those email and telephone outreach efforts.
- The Project Team also reached out to the then-head of the UVU TPUSA Club, who invited Charlie Kirk to speak at UVU. The Project Team sought his insights and perspectives regarding planning for the September 10 TPUSA event. He did not respond to the Project Team's various outreach efforts, which included a certified letter seeking his cooperation.
- A Utah risk management official had communications with an executive of TPUSA and urged that the above-named individuals who were associated with TPUSA on September 10, 2025 cooperate with this assessment by being interviewed by the Project Team. There was no response.

Actions Taken During the Assessment

To complete this assessment, the Project Team conducted a comprehensive review process that included the following activities:

- Conducted a formal project kickoff meeting and coordinated ongoing communication with University leadership and designated stakeholders.
- Developed a structured assessment methodology, interview strategy, and document request process.
- Conducted over 70 interviews with University leadership, faculty, staff, students, UVU Police Department personnel, and external public safety partners with knowledge of the event and related operations.
- Reviewed thousands of pages of policies, procedures, plans, training and training records, operational records, and other relevant documentation associated with the incident and related preparedness efforts.
- Examined digital and technical evidence, including video footage, Dispatch and communications records, electronic communications, and related investigative materials.
- Evaluated event planning, security operations, emergency response actions, interagency coordination, and decision-making processes associated with the September 10, 2025 event.
- Assessed relevant UVU practices against applicable policies, operational expectations, and recognized emergency management and higher education safety frameworks, including National Incident Management System (NIMS) and Incident Command System (ICS) principles.
- Developed and validated a detailed timeline of significant events, operational actions, and critical decisions.
- Analyzed legal issues related to UVU policies, risk, reporting, Clery Act compliance, campus police protocols and resources, campus speakers, possession of weapons on campus, and First and Second Amendment challenges unique to a public university.

- Identified operational strengths, contributing factors, gaps, and opportunities for improvement.
- Developed findings and recommendations intended to enhance future preparedness, coordination, safety, and emergency response capabilities.
- Provided regular verbal project progress updates to University representatives throughout the assessment process.
- Prepared a comprehensive After-Action Report and supporting materials for University leadership and public release.

Documents and Evidence Reviewed

The Project Team reviewed a broad range of documents, records, communications, and digital evidence relevant to the planning, response, investigation, and follow-up associated with the September 10, 2025 event. These materials included University and Utah Valley University Police Department (UVUPD) written policies and procedures, emergency management and crisis communications plans, event planning and scheduling records, security planning materials, behavioral threat assessment and management protocols, training materials and records, mutual aid and dispatch-related records, incident reports, interview summaries, communications logs, emails, social media monitoring materials, and available video, audio, and digital evidence. Document review occurred throughout the assessment as additional materials were identified, requested, and provided. The information was considered alongside interviews, timelines, and other evidence reviewed by the Project Team.

Professional Standards and Guidance Sources

The observations, findings, and recommendations contained in this report were informed by research, standards, and guidance developed by leading public- and private-sector organizations specializing in law enforcement operations, campus safety, behavioral threat assessment, targeted violence prevention, protective intelligence, emergency management, workplace violence prevention, executive protection, and security operations. Key sources consulted include:

Law Enforcement Operations

- International Association of Chiefs of Police (IACP)[2]
- International Association of Chiefs of Police, University/College Police Section[3]
- Major Cities Chiefs of Police Association (MCCA)[4]
- Police Executive Research Forum (PERF)[5]
- United States Department of Justice, Civil Rights Division, Office of Community Oriented Policing Services (COPS Office)[6]

[2] https://www.theiacp.org/about-iacp

[3] https://www.theiacp.org/working-group/section/universitycollege-police-section

[4] https://majorcitieschiefs.com/

[5] https://www.policeforum.org

[6] https://cops.usdoj.gov/

Higher Education and Campus Safety

- International Association of Campus Law Enforcement Administrators (IACLEA)
- National Association of Behavioral Intervention and Threat Assessment (NABITA)

Threat Assessment and Behavioral Analysis

- U.S. Secret Service National Threat Assessment Center (NTAC)
- Federal Bureau of Investigation (FBI)
- FBI Behavioral Analysis Unit (BAU)
- Association of Threat Assessment Professionals (ATAP)

Security, Protective Intelligence, and Risk Management

- American Society for Industrial Security (ASIS) International
- Department of Homeland Security (DHS)
- Department of Defense (DoD)
- National Insider Threat Task Force (NITTF)

Workplace Violence and Organizational Risk

- Occupational Safety and Health Administration (OSHA)
- Society for Human Resource Management (SHRM)

Laws and Legal Considerations

- Jeanne Clery Campus Safety Act, 20 U.S.C. § 1092(f) ("Clery Act")
- Federal Higher Education Act of 1965
- Federal Gun-Free School Zone Act of 1996
- Utah Code Ann. §§ 53-5a-102; 53H-7-202; 53H-7-602
- HB 128, Utah Code § 76-11-205.5 (2025) and HB 84, Utah Code § 76-11-205.5 (2026)
- U.S. Constitution
- Utah Constitution
- UVU Policies
- Relevant caselaw

Report Structure and Flow

A detailed Timeline follows the Executive Summary: Key Findings and provides a chronological summary of relevant pre-incident planning, incident-day events, and post-incident response and recovery activities. The timeline is followed by a comprehensive After-Action Report that addresses the Project Team's observations and analysis in greater detail. A complete list of recommendations organized by section is provided in Section 9. Appendices provide more granular detail on certain topics and are cross-referenced within the report.



Executive Summary: Key Findings

The Project Team again acknowledges that an after-action review is necessarily conducted with the benefit of hindsight and without the uncertainty, urgency, and confusion that often exist when responding to a crisis. Nevertheless, such a review can be of considerable benefit to an organization committed to learning from past events and preparing to meet the challenges of the future.

The Team also believes it is important, in considering the findings and recommendations in this report, to recognize that on September 10, 2025, UVU was operating within a state legal framework, as detailed in Section 8, that limited some of the security options available to the University.

The Team also recognizes that the September 10 incident was unusual in that the alleged perpetrator was unaffiliated with UVU, placing the event largely outside the University's traditional behavioral threat assessment framework. Threats originating outside the campus community are inherently more difficult for universities to identify and assess because they may involve no prior institutional contact, campus records, or observable warning behaviors known to University personnel.

*This **Executive Summary: Key Findings** section is intended to provide a high-level overview of the principal conclusions that emerged from the Project Team's review. These findings reflect themes and issues that are examined in greater detail throughout the report and form the basis for many of the recommendations that follow. Accordingly, this section may be read as an executive summary of the report, while the subsequent sections provide the underlying facts, analysis, context, and supporting detail.*

It is the opinion of the Project Team, based on our review of all available information, that at no time during the events leading up to the assassination of Charlie Kirk, or in its aftermath, did any employee or agent of UVU act in bad faith or in willful and wanton disregard for the safety of others.

With the benefit of hindsight, however, the Project Team identified several actions, omissions, circumstances, and institutional practices that warrant attention as UVU considers how to strengthen the safety and security of campus events in the future.

The high-level findings that follow capture those principal areas for improvement. They recur throughout the report's more detailed analysis and, together with the recommendations in the final section, are intended to assist UVU in strengthening its planning, preparedness, coordination, communication, and security practices for future campus events.

KEY FINDING 1: UVU Has a Strong Foundation of Policies and Procedures, but Implementation Was Significantly Inconsistent Before and During the September 10 TPUSA Event

UVU has established a substantial foundation of policies, plans, committees, reporting pathways, emergency procedures, and public safety resources relevant to major event planning, emergency response, threat assessment, and campus safety. These include Policy 425, the Major Events Assessment Committee (MEAC) process, the Emergency Operations Plan (EOP), emergency communications protocols, the Behavior Assessment Team (BAT), UVUPD Dispatch, UVUPD procedures, and multiple physical security and notification technologies.

However, the September 10 TPUSA event demonstrated that established frameworks were not always implemented in a consistent, documented, or operationally integrated manner. UVU was not operating without relevant policies, capable personnel, physical security technologies, or an established order of authority. Rather, the primary gap involved the translation of existing policies, structures, and capabilities into disciplined, repeatable, and documented practice for a controversial speaker and high-profile event involving elevated security considerations. This distinction is important.

For example, the MEAC process was initiated on August 21 to determine whether the event should proceed and to identify security concerns. However, several key event-security decisions were deferred to the TPUSA field representative even though UVU staff members raised concerns, including concerns related to holding the event in the outdoor Fountain Courtyard area and using TPUSA's ticketing process. TPUSA preferred to hold the event in the Fountain Courtyard and use its own ticketing system rather than the University's system. Those decisions placed the event in an area that was more difficult to control and limited UVU's ability to obtain reliable, real-time information regarding anticipated attendance and crowd size. Because the event was held on UVU's campus, UVU should have retained decision-making authority over key security-related issues, including venue selection, ticketing, access control, and other conditions necessary to support campus safety.

After the shooting occurred and the Emergency Operations Center (EOC) was opened, UVU also experienced challenges implementing written plans and procedures for EOC operations and emergency communications. The review identified confusion regarding who was responsible for managing the EOC at various points, who had authority to issue prompt emergency alerts through UVU's notification systems, and what terminology should be used to communicate protective actions to the campus community. This created confusion for some personnel working within the EOC and for individuals on campus awaiting direction from authorities.

These issues do not reflect the absence of planning or commitment by UVU personnel. Rather, they demonstrate the need to strengthen implementation, documentation, role clarity, and operational integration so established policies and plans function effectively during major events and critical incidents. These and related implementation gaps are addressed in greater detail throughout the report.

KEY FINDING 2: High-Profile Event Planning Requires a More Formal and Integrated Event Security Framework

The September 10 TPUSA event presented several characteristics that warranted a more formal event security planning process, including a high-profile speaker, anticipated protest activity, an open outdoor venue, uncertainty regarding attendance, external entity involvement, a private security team, elevated vantage points, and significant public attention.

Although some coordination occurred among University stakeholders, UVUPD, UVU Event Services, and TPUSA representatives, the club event was not supported by a comprehensive written Security Assessment or Event Action Plan which would have identified staffing assignments, command relationships, post responsibilities, Incident Command System (ICS) roles, communications procedures, access-control decisions, protective operations coordination, emergency response procedures, contingency plans, or mutual aid resources specific to the event.

Policy 425 and the MEAC process provide an important foundation for evaluating major events, but future high-profile events would benefit from a more structured framework that connects event classification, site selection, ticketing, attendance forecasting, access control, screening considerations, protective operations, communications, emergency response, and interagency coordination. A more comprehensive event security framework would help ensure that safety and operational considerations are documented and elevated before key event decisions are finalized.

KEY FINDING 3: Protective Operations and Line-of-Sight Planning Were Not Sufficiently Formalized for the Outdoor Venue

The outdoor location insisted upon by TPUSA for their event created significant protective operations considerations. The speaking area was located in an open-access campus environment surrounded by buildings, elevated areas, pedestrian routes, and multiple vantage points. These conditions made line-of-sight assessment, elevated-position review, building access control, arrival and departure planning, crowd control, protest management, and fixed-post assignments especially important.

UVU personnel recognized and responded to some of these concerns, including the Hall of Flags outdoor pedestrian walkway above the speaking location. However, the planning process did not include a documented line-of-sight assessment, protective operations considerations, pre-event briefing, structured walk-through with all key security stakeholders, or clear coordination process with the speaker's private security team and external law enforcement partners.

A site-specific coordination meeting involving UVUPD and the TPUSA protection detail should have occurred several days before the event to assess vulnerabilities, clarify responsibilities, and determine whether available personnel and resources were sufficient to support the security plan. If UVUPD or the TPUSA protection detail lacked sufficient staffing or specialized equipment to address identified vulnerabilities, additional law enforcement support, equipment, or technical resources, such as drone or aerial observation capability, should have been considered or requested when legally permissible and operationally appropriate.

A face-to-face pre-event briefing and walk-through with UVUPD Chief Long and the TPUSA protection detail leadership and TPUSA Security Supervisor Flood should also have occurred on campus in the hours before the event began. Such a meeting would have provided another opportunity to review roles, confirm post assignments, address concerns, identify changes in conditions, and ensure that both groups had a shared understanding of the security posture. Chief Long texted Dan Flood to meet on the Hall of Flags outdoor pedestrian walkway at 11, however this face-to-face meeting did not occur.

This finding does not suggest that every outdoor event must be moved indoors or treated as a high-risk security operation. It does mean that when an outdoor event involves a high-profile speaker, anticipated protest activity, private security, elevated vantage points, or significant public attention, UVU should have a documented process for evaluating whether the venue can be adequately controlled and what mitigation measures are required, including whether the event should be moved to a more secure or controllable location.

KEY FINDING 4: Incident Command, Emergency Operations Center (EOC) Operations, and Emergency Communications Need Greater Standardization and Exercise-Based Validation

The September 10 response placed immediate pressure on UVU's Incident Command Post, EOC, UVUPD Dispatch, emergency communications, decision-making, and notification systems. UVU personnel responded quickly and made substantial efforts under extremely difficult conditions. However, the response also exposed challenges involving role clarity, EOC leadership, succession and delegation of authority, law enforcement representation in the EOC, message approval, emergency terminology, and situational awareness.

Several of these issues were not entirely new. A prior active assailant tabletop exercise had identified communication and situational awareness challenges involving the EOC and Policy Group and recommended additional exercises. Similar issues resurfaced during the September 10 response, suggesting that prior lessons had not been fully implemented, validated, or institutionalized.

Emergency communications were among the most visible challenges. No immediate campus alert was activated by the UVU Police Chief as Incident Commander. Subsequent campus alerts were inconsistent and contradictory. Delays, changing guidance, suspect-status information, and confusion with the term "secure-in-place" affected campus understanding during a fast-moving incident. UVU's emergency notification systems are important assets, but their effectiveness depends on clear authority, plain-language terminology, accurate contact data, tested templates, scripted response protocols, and regular exercises under realistic conditions.

KEY FINDING 5: Security Technology and Situational Awareness Capabilities Should Be More Effectively Integrated Into Real-Time Operations

UVU has several valuable physical security and communications technologies, including video surveillance, access control, Rave, Alertus, public address capabilities, remote lockdown capabilities, radio communications, license plate readers, and related systems monitored or supported through UVUPD Dispatch. These tools provide an important foundation for campus safety and incident response.

The September 10 TPUSA event demonstrated, however, that existing technology was used more effectively as a post-incident investigative resource than as a real-time situational awareness tool. Security camera footage was valuable after the shooting, but no individual had been specifically assigned to monitor relevant camera feeds in real time for event security purposes. Similarly, the broader physical security technology environment would benefit from more integrated workflows that connect alarms, video, access control, mapping, notification, and Dispatch response.

For major events and critical incidents, technology should support a common operating picture for Dispatch, command staff, field personnel, the EOC, and public safety partners. UVU's future planning should include video analytics configured to detect human activity on rooftops or in restricted areas, clarify who monitors relevant systems, which camera views and alerts are prioritized, how information is shared, and how physical security technology is incorporated into Event Action Plans, security plans, and emergency response procedures.

KEY FINDING 6: Protective Intelligence, Open Source Intelligence (OSINT), and Subject-Focused Investigative Capabilities Are Not Yet Fully Developed

UVU has several useful intelligence and monitoring resources, including Campus Sonar, Sprout Social, Meltwater, law enforcement databases, and access to the Utah Statewide Information and Analysis Center (SIAC). These resources provide valuable visibility into media coverage, public sentiment, social media activity, criminal justice information, and threat-related intelligence.

However, these resources are primarily designed for social listening, media monitoring, communications awareness, and law enforcement information sharing. They are not a substitute for a dedicated subject-focused protective intelligence capability. When a specific individual, group, communication, or behavior of concern requires deeper review, UVU needs a formalized process, dedicated capability, or specialized platform for conducting comprehensive open-source investigations or access to an external partner.

This capability gap affects both event security planning and behavioral threat assessment. Subject-focused OSINT and protective intelligence can help identify warning behaviors, grievances, fixation, leakage, stalking, escalation, target focus, prior violence, affiliations, and other information relevant to prevention and intervention. UVU would benefit from documented procedures, trained personnel, authorized investigative accounts, legal and privacy guardrails, and defined workflows for collecting, documenting, analyzing, retaining, and disseminating relevant intelligence.

KEY FINDING 7: Interagency Coordination Was a Response Strength, but Mutual Aid and Statewide Campus Safety Coordination Should Be Formalized

External public safety partners responded quickly and professionally after the September 10 shooting. Orem Police Department, Orem Fire Department, Utah Department of Public Safety (DPS), Utah Highway Patrol, Utah County Sheriff's Office, the FBI, and other local agencies provided essential support during a complex and fast-moving incident. Interviews reflected strong working relationships between UVUPD and Orem Police Department, and those relationships were important during the response.

However, the event also demonstrated the need to formalize mutual aid, resource-request thresholds, specialized capability planning, and interagency integration before major events and critical incidents occur. UVU had access to potential outside resources, including additional sworn personnel, fire and EMS support, emergency management assistance, investigative resources, tactical assets, traffic-control support, and drone capability, but those resources were not fully integrated into pre-event planning.

Post-incident efforts to strengthen interagency coordination are promising. These include steps toward a written mutual aid agreement with Orem Police Department, proposed joint active assailant exercises, Orem Emergency Management's willingness to support UVU planning and preparedness, and emerging statewide efforts to improve coordination among Utah public institutions of higher education. These efforts should be formalized, exercised, and sustained.

KEY FINDING 8: Organizational Alignment, Staffing, and Training Should Be Evaluated Against UVU's Size and Risk Environment

UVU is a large and growing public university with a complex risk environment that includes major events, public speakers, protests, open campus spaces, commuter populations, student activities, athletics, and broad community access. These conditions require public safety functions that are appropriately positioned, staffed, trained, and integrated into University leadership and planning.

The review identified concerns regarding UVUPD staffing levels, training structure, organizational placement, and visibility within the University's leadership framework. The Police Chief is not positioned within the organization in a manner typical for a public safety leader at a large institution of higher education, and UVUPD staffing appears limited when compared to the scale and complexity of the University's operations and event environment. UVU should consider a senior campus safety leadership role, such as a Vice President or Associate Vice President for Campus Safety and Security, with responsibility for all public safety operations, including emergency management. This individual would report either directly to the President or a senior executive leader who reports directly to the President.

UVUPD personnel complete required training hours, but the department would benefit from a formal training needs assessment and written annual training plan aligned to the University's actual risk profile. Particular training attention should be given to the Incident Command System (ICS), event security, active assailant response, protective operations, emergency management coordination, mutual aid, crowd management, and campus-specific public safety practices. UVU should also evaluate professional standards opportunities, including IACLEA accreditation, as part of a broader commitment to public safety maturity and continuous improvement. UVU would also benefit from a formal staffing and pay analysis to help determine the proper staffing levels for its police department, as well as to identify the proper pay scales that would allow it to be competitive in its law enforcement recruitment and retention efforts.

KEY FINDING 9: UVU Made Meaningful Post-Incident Efforts, but First Responder Support and Continuous Improvements Need Additional Attention

Following September 10, UVU and its partners took meaningful steps to support students, improve campus safety awareness, strengthen crisis communications planning, update emergency preparedness materials, improve training, and advance interagency coordination. These efforts reflect a serious commitment to organizational learning and campus recovery.

Student and community support efforts were particularly important. UVU Mental Health Services, community providers, and the FBI Victim Assistance Program provided or supported post-incident services. UVU also advanced awareness and preparedness efforts, including classroom posters, updated flipcharts, website and app improvements, employee training, campus safety outreach, and crisis communications planning. At the same time, post-incident support for responding police personnel and other first responders appeared less structured and less visible than support provided to students and the broader campus community. UVU is benefiting from an ongoing review of processes, assignment of responsible owners for improvements, establishment of timelines, and are now tracking implementation, and validating improvements through drills, exercises, and future event planning.

KEY FINDING 10: Utah Is Expanding Public Safety Intelligence and Collaboration Efforts, and UVU Should Proactively Engage in Those Efforts

Utah public safety and higher education leaders have initiated several efforts to strengthen intelligence gathering, information sharing, and multi-agency collaboration related to campus safety. These include the Utah Department of Public Safety (DPS) assigning a SIAC analyst to focus on public safety concerns affecting Utah's public schools and institutions of higher education; the Utah Board of Higher Education creating a Campus Safety Task Force to identify ways to enhance public safety operations across the statewide higher education system; and the University of Utah Department of Public Safety assigning personnel to support the Real-Time Crime Center being established by the Salt Lake City Police Department.

These efforts are significant because they provide UVU with opportunities to better leverage external intelligence, public safety resources, training, and collaborative planning. UVU took basic steps to plan for the September 10 TPUSA event, but the event was not supported by a written Event Action Plan that fully incorporated available external resources, intelligence, mutual aid, or specialized capabilities. More active participation in statewide information-sharing and campus-safety initiatives would help UVU keep university-centered public safety concerns at the forefront when planning for high-profile events, evaluating threats, conducting Security Assessments, and developing Event Action Plans.

Utah DPS Commissioner Beau Mason's SIAC initiative, Utah Commissioner of Higher Education Geoffrey Landward's Campus Safety Task Force, and University of Utah Chief Safety Officer Keith Squires' work co-leading the Task Force with statewide campus police leaders reflect a broader effort to improve consistency, collaboration, and readiness across Utah's public institutions of higher education. UVU should proactively participate in these efforts, identify appropriate representatives to engage with SIAC and statewide working groups, and incorporate lessons, tools, resources, and intelligence-sharing practices into its own event planning, emergency management, threat assessment, and public safety operations.

Timeline

Pre-Event Planning and Preparation (July 10-September 9)

Date/Time	Event Summary
July 10, 2025	At the request of the TPUSA field representative, UVU TPUSA Club President contacted the Clubs Office requesting the specific use of the Fountain Courtyard for a September 10 TPUSA event.
July 18	Formal event request submitted by UVU TPUSA Club. Event described as an appearance by Charlie Kirk to discuss current events. External ticketing by TPUSA anticipated.
July 28	Clubs Office advised TPUSA Club that annual club registration had to be completed before the event could be considered.
July 29	TPUSA club registration submitted.
August 21	Clubs Office tentatively approved the event and forwarded it to Event Services as a major event. At that time, in response to a UVU questionnaire, TPUSA projected approximately 600 attendees, offered to connect UVUPD with TPUSA security, and stated that they had no risk factor/safety/security concerns.
August 21	Event Services emailed those required to attend the August 25 MEAC meeting. This is when UVUPD Chief Long first became aware of the September 10 TPUSA event.
August 21	UVU Free Speech Committee flagged the event because of anticipated protests and reviewed insights from prior TPUSA appearances, including an appearance of Charlie Kirk at UVU in 2019.
August 24	Brian Harpole stated during a November 17, 2025 public podcast interview that his first meeting to discuss the September 10 TPUSA event occurred on this date, one day before the MEAC meeting.[7]
August 25	Major Events Assessment Committee (MEAC) met with a TPUSA field representative and UVU TPUSA Club President via Microsoft Teams. UVU participants raised concerns about the outdoor courtyard location, anticipated attendance, protest activity, crowd management, and the ability to control access. TPUSA requested the event remain in the Fountain Courtyard despite concerns and suggestions to consider alternate venues. TPUSA preferred the Fountain Courtyard and outside-managed ticketing; the committee ultimately allowed the event to proceed in the requested location and allowed TPUSA to manage ticketing. TPUSA advised UVU it would have approximately eight security personnel. Chief Long requested contact with TPUSA security leadership.

[7] Because Brian Harpole never spoke with the Project Team, we assume this was an internal meeting within TPUSA. There is no record of a meeting with UVU on this day.

August 25	**Key Decision Point:** Venue selection remained Fountain Courtyard, as requested by TPUSA, despite concerns by UVU about controllability, anticipated attendance, protest activity, crowd management, and access control.
August 25	Free Speech Committee discussed possible EOC activation, social media monitoring, communications planning, and coordination measures.
August 27	MEAC formally approved the event. TPUSA requested event support items including barriers, tables, chairs, power, and green room access.
August 27	**Key Decision Point:** Event approved before a documented Security Assessment or written Event Action Plan was developed.
August 29	Free Speech Committee began monitoring complaints and concerns regarding the event. An anonymous caller demanded cancellation.
August 31	UVU President Tuminez requested updates regarding event planning. Free Speech Committee continued monitoring and prepared draft communications.
September 2	Chief Long advised no security request had been received from TPUSA and sought a point of contact.
September 3	**Key Decision Point:** First direct security coordination between UVUPD and TPUSA occurred.
September 3 – 1:08 p.m.	Chief Long held the first security coordination call (5 minutes, 28 seconds) with Dan Flood, TPUSA Security Supervisor. Chief Long asked Flood what TPUSA needed from UVUPD. Discussion focused on arrival, departure, and parking logistics. Flood indicated TPUSA typically used 8-10 security personnel.
September 3 – 2:10 p.m.	Follow-up call (48 seconds) between Chief Long and Flood regarding ticketing and event schedule. Flood confirmed TPUSA's national office handled ticketing. Ticket totals were not available, and thus Chief Long was unable to obtain crowd estimates from the TPUSA ticketing process at that time.
September 3	Free Speech Committee noted increasing anti-Kirk online activity and petitions to cancel the event.
September 4–5	Utah SIAC and UVUPD communicated regarding potential counter-protests.
September 5	Free Speech Committee determined it would observe the event from the Fugal Gateway Building.
September 8	**Key Decision Point:** TPUSA security raised a rooftop/outdoor pedestrian walkway access concern regarding the area above where Charlie Kirk's canopy was to be placed.
September 8 – 4:11 p.m.	Dan Flood initiated a text exchange with Chief Long regarding an accessible rooftop/outdoor pedestrian walkway above the canopy area where Charlie Kirk would be speaking and requested access controls. Long responded, "We got you covered" in reference to the Hall of Flags outdoor pedestrian walkway.
September 9	Free Speech Committee noted increasing protest coordination, attendee conflict discussions, and external media attention.

Incident Day Timeline (September 10)

Time	Event Summary
7:23 a.m.	UVU Police Chief Long contacted the Utah SIAC regarding an anonymous threat. SIAC later determined the threat was unsubstantiated.
~9:00 a.m.	TPUSA security team arrived on campus with Dan Flood. Chief Long later reported that he was not formally introduced to the members of the TPUSA security team upon their arrival.
9:04 a.m.	Dan Flood, TPUSA Security Supervisor, texted Chief Long advising that TPUSA security personnel had arrived on campus. Chief Long engaged in a series of text communications with Flood, to include several regarding individuals located on the Hall of Flags outdoor pedestrian walkway and the Fountain Courtyard area where a canopy would be set up where Kirk would be speaking. These text exchanges revealed the primary security focus for TPUSA was the Hall of Flags outdoor pedestrian walkway above the canopy.
9:28 a.m.	Additional Charlie Kirk staff arrived on campus.
10:28 a.m.	Additional Charlie Kirk staff arrived on campus.
September 10	**Key Decision Point:** The Hall of Flags outdoor pedestrian walkway above the speaking area was restricted to prevent access, but there was no face-to-face meeting between TPUSA security team members and UVUPD before the start of the event to discuss any other security operations concerns.
10:49 a.m.	Dan Flood called Chief Long reporting protesters were on the Hall of Flags outdoor pedestrian walkway above the speaking area and requested the area be cleared. Chief Long texted Dan Flood to meet on the Hall of Flags outdoor pedestrian walkway at 11, however this face-to-face meeting did not occur.
~11:00 a.m.	Initial UVUPD staffing included Chief Long, one patrol officer, and one reserve officer. After observing the crowd size, Chief Long requested that a uniformed UVUPD detective assist, along with a sergeant and an additional officer, representing all officers on duty that day. TPUSA security reported 10-12 security personnel on site. The Free Speech Committee convened in the Fugal Gateway building to monitor the event.
10:58 a.m.	Additional Charlie Kirk staff arrived on campus.
11:20–11:30 a.m.	Sergeant Beveridge, Officer Bagley and Chief Long went to the Hall of Flags outdoor pedestrian walkway and estimated there were 80 to 100 protestors in the area located directly above the canopy where Kirk would be speaking. At the direction of the UVUPD personnel, the protestors cooperated in moving away from that area, which the officers then blocked off with police tape for security concerns.
~11:30 a.m.	Chief Long went to Room 204 on the second floor of the Fugal Gateway Building, where a command post had been established. The room provided visibility over the event area and surrounding buildings.

~12:00 p.m.	Chief Long addressed an access-control issue inside the Fugal Gateway Building after students and other attendees attempted to reach a third-floor balcony outside the President's Office to observe the event. A staff member from Emergency Management was posted on the second level to help prevent access to that balcony area.
~12:00 p.m.	Charlie Kirk arrived on campus, greeted TPUSA students, posed for photos, and distributed hats from a TPUSA canopy in the Fountain Courtyard. Chief Long reported hearing protesters positioned behind police tape on the second-level Hall of Flags outdoor pedestrian walkway shouting profanities toward Charlie Kirk.
12:17 p.m.	Post-incident surveillance footage review captured the assailant accessing the Losee Center rooftop by climbing over a barrier from an adjacent Losee Center walkway.
12:22 p.m.	Post-incident surveillance footage review captured the assailant running across the Losee Center roof and taking a prone position.
12:23 p.m.	A single gunshot was fired, striking Charlie Kirk. UVUPD radio traffic broadcast "shots fired." Surveillance footage captured the assailant fleeing across the roof and jumping off. Chief Long was in the command post when he heard the gunshot.
12:24 p.m.	Surveillance footage captured the assailant walking northbound across Campus Drive.
12:24 p.m.	The first official dispatch of an Orem Fire Department Medical/EMS unit. Orem Fire personnel from Stations One and Three were initially dispatched. Personnel from Stations Two and Four also responded because the extent of medical need was not yet known.
12:25 p.m.	UVUPD began directing attendees away from the Fountain Courtyard. The Associate Vice President of Facilities notified Vice President of Administration and Strategic Relations Val Peterson of the shooting.
12:25—12:35 p.m.	Utah DPS Commissioner Beau Mason began mustering personnel from the State Bureau of Investigation, SIAC, and the State Crime Lab, directed DPS personnel to assist, and responded to UVU.
12:26 p.m.	UVUPD reported a suspect, George Zinn, an event attendee, was in custody after allegedly admitting involvement in the shooting. It was later determined he was not a suspect.
12:26 p.m.	The first official dispatch of an Orem Police Department Officer to the shooting at UVU.
12:31–12:40 p.m.	Cabinet[8] communications confirmed the shooting and activated the Emergency Operations Center (EOC). Incident Command Post was established in Fugal Gateway Room 205.
12:32 p.m.	The first noted arrival of an OPD Officer and an Orem Fire Department Unit at UVU.

[8] **UVU Cabinet**: The UVU Cabinet includes executive-level administrators and senior staff responsible for overseeing major University divisions and functions. The Cabinet meets regularly and serves as the President's senior advisory and decision-making group for University administration.

~12:35 p.m.	Station Three fire personnel passed the SUV being used by the TPUSA security team to transport the victim to Timpanogos Hospital and relayed that information by radio. Station Two then rerouted to Timpanogos Hospital, where a fire captain assisted with CPR.
12:41 p.m. — 12:53 p.m.	UVU Officer Bagley inspected the Losee Center rooftop after recognizing that the shot sounded consistent with a high-powered rifle rather than a pistol. He advised Chief Long that the shot appeared to have come from a rifle and that the likely line of sight was from the Losee Center area toward the event location. During the inspection of the Losee Center roof area, Officer Bagley located a red-and-black screwdriver on the rooftop and identified a disturbed area of gravel near the roof edge that appeared consistent with a prone firing position, including impressions consistent with feet, knees, and elbows. Based on these observations, Officer Bagley requested review of nearby surveillance footage and requested the Losee Center be cleared.
12:42 p.m.	First Rave Alert issued: "A single shot was fired on campus toward a visiting speaker. Police are investigating now, suspect in custody."
~12:43 p.m.	Orem Emergency Management Director called UVU Emergency Management Director Robin Ebmeyer approximately 20 minutes after the shooting and offered assistance. He later remained at the Orem EOC when assistance was not requested.
12:45 p.m.	The then UVU Dean of Students advised the EOC that the Policy Group had decided to close campus and reopen the following day.
12:47 p.m.	UVU Policy Group[9] begins working with the EOC Staff.[10]
12:48 p.m.	UVU website posted the same message as the first Rave Alert stating, "suspect in custody." Officer Bagley secured the rooftop crime scene.
12:50 p.m.	Chief Long entered the EOC and advised that Charlie Kirk had been shot in the neck, no weapon had been recovered, and the shot may have originated from the Losee Center rooftop. Witnesses reported seeing a person flee from the roof after the shot. Long expressed doubt George Zinn was involved.
12:55–1:10 p.m.	UVU EOC Staff and Policy Group debated whether the situation constituted an active shooter event and discussed messaging regarding evacuation versus sheltering or securing in place.
1:04 p.m.	UVU VP Val Peterson advised by speakerphone that no suspect was actually in custody and the situation could involve an active shooter.

[9] **UVU Policy Group:** When the EOC is activated, Cabinet members who are not assigned to formal EOC roles may convene separately as the Policy Group to provide senior-level guidance, institutional perspective, and operational support. The Policy Group supports the EOC by advising on major institutional decisions, resource needs, continuity issues, public messaging considerations, and other matters requiring executive-level input. Requests for guidance may be routed from the EOC to the Policy Group, with direction or input communicated back to the EOC as needed.

[10] **UVU EOC Staff:** When an emergency situation is declared and the Emergency Operations Center is activated, designated University administrators and key staff members report to the EOC to support incident coordination, situational awareness, resource management, emergency communications, and implementation of applicable emergency policies and procedures. Under UVU's current framework, the Vice President of Administration and Strategic Relations, or designee, serves as the EOC Manager, and the Police Chief typically serves as Incident Commander.

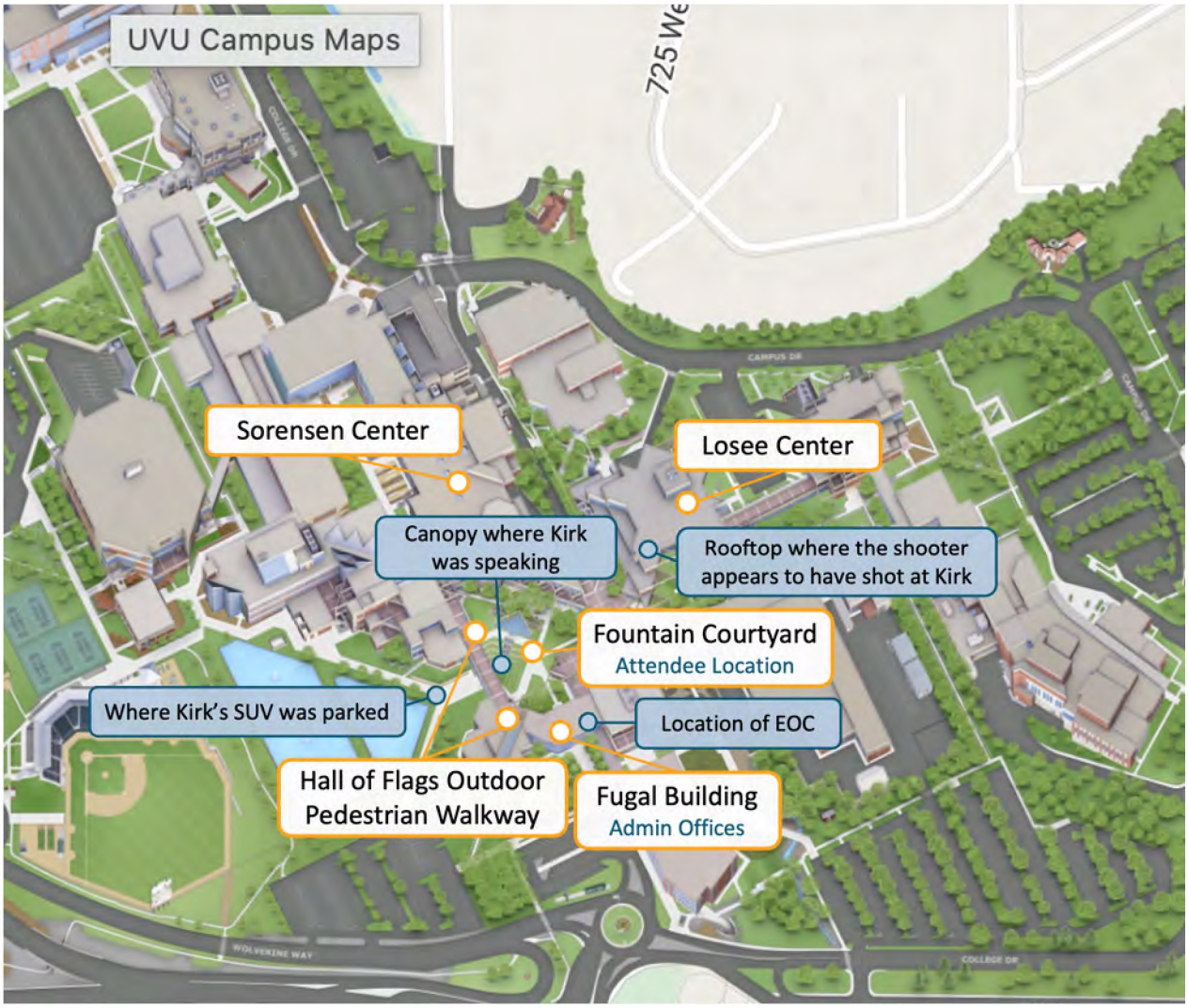
1:11 p.m.	Second Rave Alert issued: "Campus closed until further notice. Ongoing police investigation. If you are still on campus, follow police direction."
1:12 p.m.	Same message posted on UVU website.
1:14 p.m.	UVU distributed a campus-wide email regarding the shooting and campus closure.
1:19 p.m.	Third Rave Alert issued directing people to leave campus immediately.
1:19–1:28 p.m.	Chief Long and an Orem police representative briefed the EOC Staff that the suspect had fled northbound and remained at large. They advised people should remain in place until cleared by police.
1:20 p.m.	UVU website posted the same "leave campus immediately" message.
1:36 p.m.	Fourth Rave Alert issued directing those on campus to "secure in place until police officers can escort you safely off campus."
1:41 p.m.	Chief Long informed the EOC Staff that Charlie Kirk had died.
1:51 p.m.	An erroneous fifth Rave Alert was unintentionally issued: "Shooter in [insert location] … Run-Hide-Fight."
1:53 p.m.	Sixth Rave Alert issued instructing recipients to disregard the prior erroneous message.
1:55 p.m.	President Tuminez advised that she was returning from Atlanta and directed VP Val Peterson to manage University communications.
1:58–5:07 p.m.	Six additional Rave Alerts and website updates provided clearance and escort instructions as law enforcement moved building to building conducting security checks. Campus closure through September 15 was announced.
4:00 p.m.	Governor Spencer Cox and UVU officials conducted a joint press conference regarding the shooting and investigation.
5:45 p.m.	Final Rave Alert issued declaring the campus "ALL CLEAR" and advising there was no ongoing threat.
6:32 p.m.	UVU website posted final "ALL CLEAR" update confirming no ongoing threat and continued campus closure through September 15.

Post-Incident Response and Recovery

Date/Time	Event Summary
September 10	Alumni Building opened as a temporary support location for individuals who could not immediately leave campus or otherwise needed a place to go. The American Red Cross was contacted to support sheltering if needed, although a shelter was not activated.

September 10	UVU Mental Health Services made trained licensed therapists available to speak with students, additional community-provider support was sought, and the FBI Victim Assistance Program became involved quickly after the incident.
September 11–14	Campus remained closed while law enforcement continued investigative activities and UVU coordinated recovery and support operations.
September 12	The alleged assailant surrendered to law enforcement authorities.
September 15	Campus scheduled to reopen following the temporary closure period announced through emergency communications.
September 16	Utah County District Attorney formally charged the alleged assailant with aggravated murder and related offenses.
~September 24	Mental health support remained active for approximately two weeks before demand declined.
After September 10	UVU recognized the need for a more robust crisis communications plan and engaged consultants to support development of a more comprehensive crisis communications framework.
After September 10	Orem Police Department and UVU began formalizing their informal mutual aid relationship through a written mutual aid agreement.
After September 10	Utah DPS Commissioner Beau Mason assigned a DPS member on the SIAC team to focus on safety concerns for Utah public institutions of higher education and requested that each institution designate a representative for regular coordination and information sharing.
After September 10	Orem Fire Chief Marc Sanderson and Orem Police Chief B.J. Robinson discussed approaching UVU to conduct a joint active-shooter training exercise involving UVUPD, OPD, Orem Fire, Orem Emergency Management, and other partners.
Fall 2025	UVU implemented counseling, mental health support, community outreach, and campus healing initiatives, including a university vigil. Interviewees generally viewed these efforts positively.
Fall 2025	UVU launched efforts to improve emergency notification participation and mobile phone registration within the Rave Alert system.
Fall 2025	UVU advanced campus safety awareness and preparedness efforts, including classroom posters, emergency flipchart updates, website and app updates, employee training, campus safety outreach, and Building Marshal/Floor Captain program work.
November 10, 2025	Follow-up testing of the emergency notification system showed significantly improved alert participation rates among students and employees.
November 17, 2025	Brian Harpole discussed the September 10 TPUSA event in a public podcast interview, including event planning, venue concerns, elevated positions, drone use, and coordination with UVU officials.

Illustration: Utah Valley University Campus – Key Locations Referenced in this Review



After-Action Report

1. Governance, Policies, and Preparedness Framework

1.1 Overview of Policies, Protocols, Plans, and Evidence Reviewed

A key component of this assessment involved evaluating the policies, procedures, plans, and governance structures that guided Utah Valley University's preparation for, response to, and recovery from the September 10, 2025 incident. Effective preparedness depends not only on having documented plans and protocols in place, but also on ensuring those plans are aligned with recognized practices, understood by personnel, practiced regularly, and implemented consistently during real-world events.

To assess the quality of these policies and procedures, the Project Team reviewed University and Utah Valley University Police Department (UVUPD) policies, emergency plans, communications protocols, training records, after-action reports, event planning documents, and threat assessment and management procedures. Particular attention was given to those documents governing event planning, emergency management, emergency communications, First Amendment activities, behavioral threat assessment, and law enforcement response.

The Project Team also evaluated the extent to which these policies and procedures aligned with recognized practices in higher education safety, emergency management, behavioral threat assessment and management, and law enforcement operations, as well as how effectively they were implemented before, during, and after the September 10 incident.

This section of the After-Action Report first summarizes the policy, protocol, training, and preparedness framework in place before September 10. It then provides a narrative review of the planning, response, and interagency coordination associated with the September 10 TPUSA event. Later sections of this report provide deeper analyses of specific operational components, including event security planning, access control, protective operations, communications, open-source intelligence (OSINT), emergency management, and mutual aid.



1.2 Policy 425 and Major Event Review Framework

UVU Policy 425 provides the formal framework for evaluating whether the September 10 TPUSA event should be classified and managed as a major event. The narrative that follows then uses that policy framework as the starting point for assessing how the event was reviewed, planned, and supported.

Relevant UVU Policy Framework

UVU Policy 425 establishes the University's framework for event scheduling, facility use, and major-event review. Several provisions are particularly relevant to the September 10 TPUSA event:

- **Policy 425 § 3.5** defines a "major event" to include events that exceed attendance thresholds, events that may pose a significant threat of harm to people or property, events that may substantially interfere with University functions, and gatherings for political activity.
- **Policy 425 § 3.6** establishes the Major Events Assessment Committee (MEAC) as the committee responsible for evaluating potential impacts on the surrounding community, University functions or activities, and safety or security concerns.
- **Policy 425 § 3.7.1** defines University entities authorized to request use of University facilities for University or co-sponsored events.
- **Policy 425 § 4.1.3** states that the policy should not be construed to impede constitutional rights to petition and assemble and cross-references UVU Policy 161 Freedom of Speech.
- **Policy 425 § 4.1.5** requires individuals planning, hosting, or attending events, including guests, vendors, and contractors, to follow University policies, Events Services guidelines and protocols, and applicable law.
- **Policy 425 § 4.8.2** requires events that qualify as major events to undergo a Security Assessment facilitated by the MEAC.
- **Policy 425 § 5.2.1** requires the MEAC to review major event requests for health and safety concerns and for compliance with University policy and state and federal law.

1.3 UVUPD Policy Manual and Departmental Procedures

UVUPD utilizes a policy management system provided by Lexipol, a nationally recognized provider of law enforcement policy manuals used by thousands of public safety agencies throughout the United States. The Lexipol platform provides regularly updated policy guidance reflecting changes in federal, state, and local laws, court decisions, accreditation standards, and emerging best practices within the law enforcement profession. The system also allows agencies to customize policies to reflect local operational needs, management decisions, and jurisdiction-specific requirements.

The use of a professionally managed policy system offers several advantages. It helps ensure policies remain current and legally defensible, reduces the administrative burden associated with manual policy updates, promotes consistency in operational practices, and provides a structured mechanism for communicating policy changes to personnel. For an agency the size of UVUPD, the use of a Lexipol-based policy management system represents a significant strength and demonstrates a commitment to maintaining current, professional, and well-documented operational guidance.

1.4 Emergency Operations Plan, EOC Framework, and Active Assailant Protocols

The University's Emergency Operations Plan (EOP) is comprehensive and generally aligned with recognized emergency management practices. The plan incorporates National Incident Management System (NIMS)[11] principles and establishes a framework for emergency response, resource coordination, emergency communications, executive decision-making, and recovery activities. The EOP is also appropriately tailored to the unique operating environment and challenges commonly faced by institutions of higher education.

NIMS and ICS

NIMS is the national framework used to guide prevention, protection, mitigation, response, and recovery activities for incidents involving multiple agencies, disciplines, and jurisdictions. NIMS provides a common approach to command, coordination, resource management, communications, and information sharing.

ICS is a core component of NIMS and provides a scalable structure for managing both planned events and emergency incidents. It helps define incident objectives, command roles, operational assignments, communications processes, resource needs, and coordination responsibilities.

An Event Action Plan (EAP) applies ICS principles to a planned event. The purpose is not to create unnecessary bureaucracy, but to ensure that key assumptions, decisions, roles, and resource needs are considered and documented before the event occurs. See **Appendix B** for a full list of ICS roles and responsibilities.

The EOP identifies key leadership positions, outlines Emergency Operations Center (EOC) functions, and provides guidance regarding incident management, communications, resource coordination, and executive decision-making. With limited exceptions, such as the absence of certain specialized Incident Command System (ICS) positions, the EOP contains the breadth and depth of guidance one would expect to find within a mature emergency management program.

The University's primary guidance for managing active shooter and active-assailant incidents is included in the EOP. The active shooter/active assailant response plan provides instructions and guidance to effectively address the response of Utah Valley University to an active shooter or violent intruder incident. The plan was prepared in coordination and cooperation of the UVUPD and other local law enforcement agencies and establishes roles, responsibilities, response procedures, communications protocols, and coordination mechanisms for managing such incidents.

Review of these protocols indicates they are generally aligned with recognized practices and contemporary active-assailant response principles. The procedures were updated in October 2024 and incorporate many of the concepts reflected in guidance issued by the U.S. Department of Homeland Security and other leading public safety organizations.[12] The plan appropriately emphasizes rapid law

[11] *Utah Valley University Emergency Operations Plan*, October 2024.

[12] Department of Homeland Security Active Shooter Booklets: https://www.dhs.gov/sites/default/files/2026-04/26_0415_st_aairrecommendedequipmentlist.pdf - April 2026 and https://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf - October 2008.

enforcement response, emergency communications, incident command, resource coordination, and protection of life during a rapidly evolving crisis.

As with any emergency plan, however, the effectiveness of the EOP depends not only on the quality of the written document, but also on regular training, practicing, reviewing, updating, and consistent implementation during actual events. The existence of well-developed policies and procedures provides an important foundation for preparedness, but successful implementation depends on personnel understanding their roles, exercising those roles under realistic conditions, and applying the plan consistently during stressful and dynamic incidents.

> **The primary opportunity for improvement lies not in any major changes to the plan itself, but in ensuring that the plan is operationalized through training, active practicing, role clarification, EOC practice, communications testing, and integration with event-specific planning for major or elevated-risk events.**

For UVU, the EOP provides an appropriate planning foundation. The primary opportunity for improvement lies not in any major changes to the plan itself, but in ensuring that the plan is operationalized through training, active practicing, role clarification, EOC practice, communications testing, and integration with event-specific planning for major or elevated-risk events.

1.5 ICS, NIMS, and Event Action Planning

Incident Command System (ICS) and National Incident Management System (NIMS) principles provide the command-and-coordination framework for managing complex incidents, planned events, and multi-agency response operations. For institutions of higher education, ICS is particularly important because major events and emergencies often involve campus police, emergency management personnel, fire and EMS services, University leadership, communications personnel, and those from student affairs, facilities departments, legal counsel, outside law enforcement agencies, and external event organizers.

UVUPD Policy 429, First Amendment Assemblies, is particularly relevant to the September 10 TPUSA event because it addresses the use of ICS principles for both planned and unplanned events. The policy states ICS should be established when resources are deployed for unplanned events and that ICS should be considered for planned events, including the development of incident-specific operational plans when appropriate. This guidance is important because events involving political activity, anticipated demonstrations, large crowds, or elevated security concerns often require a more structured operational planning process than routine campus events.

Basic planning and coordination activities occurred before the September 10 TPUSA event, including discussions through the MEAC, coordination among University stakeholders, and engagement with Turning Point USA representatives. Unlike EAPs for other major events, such as for commencement activities and concerts, no formal written Event Action Plan with an incident-specific ICS plan was developed for the September 10 TPUSA event.

A written Event Action Plan with an incident-specific ICS planning document would have provided a structured mechanism for documenting objectives, assignments, resource requirements, staffing plans, command roles, communications procedures, contingency plans, mutual aid needs, and event-specific security measures. The process of developing an Event Action Plan often provides as much value as the final plan itself because it requires stakeholders to identify operational assumptions, vulnerabilities, resource limitations, and response options before an event occurs.

The process of developing an Event Action Plan often provides as much value as the final plan itself because it requires stakeholders to identify operational assumptions, vulnerabilities, resource limitations, and response options before an event occurs.

For high-profile events, prominent speakers, large gatherings, or events involving elevated security concerns, ICS principles should be incorporated into event planning before the event date. This does not mean every event requires a complex command structure. Rather, UVU should use a scalable approach that matches the event's risk profile, attendance, venue, security concerns, and operational complexity. At a minimum, elevated-risk events should have documented objectives, assigned roles, communications protocols, contingency procedures, and a process for requesting additional resources if conditions change.

The September 10 TPUSA event demonstrates the importance of integrating event planning, emergency management, law enforcement operations, event security, executive protection, communications, and executive decision-making into a common planning framework. Stronger use of ICS and Event Action Planning would help UVU document decisions, clarify responsibilities, coordinate with external partners, identify resource needs, and improve situational awareness prior to and during major events and critical incidents.

1.6 Training, Exercises, and After-Action Learning

Training records for 2024 and 2025 indicate that UVUPD personnel regularly participated in training activities designed to satisfy Utah's annual training requirements. Coursework completed during the review period included topics such as First Amendment activities, public demonstrations, active assailant response, and other law enforcement-related subjects.

The Project Team identified an opportunity, however, to move from primarily self-selected training toward a more structured departmental training program. The review did not identify a formal training needs assessment or annual training plan establishing priorities based on UVUPD's responsibilities, operating environment, and emerging risks. A written training plan would help ensure that required training is supplemented by specialized instruction aligned with the Department's operational needs. Priority areas may include Incident Command System (ICS), Event Action Plan development, active assailant response, emergency management coordination, major-event security, crowd management, protective operations, mutual aid, communications, behavioral threat assessment and management, and higher education-specific policing practices.

Formal ICS training warrants particular attention. Training records indicated that only one of UVUPD's 13 sworn personnel was logged as having participated in an ICS-specific training course during 2024 or 2025. Because ICS principles provide the foundation for planning, managing, and coordinating complex incidents and special events, broader participation in ICS training would strengthen operational planning, improve coordination during critical incidents, and reinforce a common command framework shared by public safety agencies nationwide.

Training should also be reinforced through exercises that allow personnel to practice decision-making, communications, coordination, and command responsibilities under realistic conditions. UVU has conducted exercises to evaluate its emergency management capabilities. In January 2023, the University conducted an active assailant tabletop exercise involving Emergency Operations Center and Policy Group personnel. Following the exercise, UVU prepared a detailed After-Action Report and Improvement Plan identifying strengths, lessons learned, and opportunities for improvement.

Of particular significance, the After-Action Report identified challenges related to communication and situational awareness between the Emergency Operations Center and Policy Group. Specifically, the report noted: "**The policy group felt there was a lack of communication and general awareness of the activities occurring within the EOC. There was an electronic spreadsheet documenting all activities available for both groups to view; however, the feelings of not knowing what was going on in the EOC persisted.**"[13]

The report also recommended that the University strengthen its training exercise program and **"consider two exercises a year, open the EOC/Policy Group, work through a scenario, practice, practice, practice."**[14]

> **These observations are particularly noteworthy because several of the same issues identified during the 2023 exercise resurfaced during the September 10, 2025 incident.**

These observations are particularly noteworthy because several of the same issues identified during the 2023 exercise resurfaced during the September 10, 2025 incident. Interviews and document review reflected recurring challenges involving situational awareness, information sharing, communications coordination, and uncertainty regarding decision-making authority within the EOC. While a real-world incident presents unique challenges not often encountered during a tabletop exercise, the recurrence of similar observations suggests that opportunities identified during the 2023 exercise were not fully implemented, validated, or institutionalized before September 2025.

Furthermore, despite the recommendation to conduct additional active assailant exercises, no comparable active assailant exercise was conducted between the January 2023 tabletop exercise and

---

13 *UVU Active Shooter After-Action Report/Improvement Plan*, January 10, 2023, p 5.

14 Ibid, p.6.

the September 2025 incident. It is important to note that upon completion of these exercises and other significant emergency drills,[15] after-action reports and corrective-action tracking are valuable.

UVU should establish a consistent process for documenting lessons learned from significant exercises and drills, assigning corrective actions, identifying responsible parties and completion dates, and tracking improvements through implementation. Training, exercises, after-action review, and corrective-action tracking should function as a continuous cycle in which lessons identified through exercises and actual incidents are incorporated into future training and validated through subsequent exercises.

1.7 Mutual Aid and External Support Framework

Mutual aid agreements are formal arrangements between law enforcement and public safety agencies that establish procedures for providing personnel, equipment, specialized resources, and operational support during emergencies, planned events, or periods of increased demand. Such agreements typically address resource sharing, command authority, liability, reimbursement, and procedures for requesting and providing assistance across jurisdictional boundaries.

Mutual aid agreements are a common and valuable component of modern public safety operations, particularly for smaller agencies that may periodically require additional personnel or specialized capabilities maintained by larger neighboring jurisdictions. For institutions such as the UVUPD, these agreements can provide access to resources such as additional sworn personnel, specialized investigative support, tactical assets, and technologies that may not be practical for the University to maintain independently.

Why Mutual Aid Matters

Mutual aid agreements provide access to specialized resources that UVUPD may not maintain internally, including drones, tactical assets, investigative support, and additional personnel. Establishing these agreements before an incident occurs helps ensure resources can be deployed quickly, responsibilities are clearly defined, and operational options are expanded during both planned events and emergencies.

Interviews with the UVUPD Police Chief and the Orem Police Department (OPD) Police Chief confirmed that strong working relationships and longstanding informal cooperation exist between the agencies. For example, because much of the student housing population resides within Orem's jurisdiction, officers from both agencies routinely collaborate on incidents involving UVU students. Likewise, UVUPD may request assistance from OPD when specialized resources or additional personnel are needed. Interviewees consistently described the relationship between the agencies as positive, collaborative, and effective.

Despite these strong relationships, formal written mutual aid agreements were not in place between UVUPD and certain neighboring jurisdictions at the time of this review. While informal arrangements can function effectively, formal agreements provide several important benefits:

- Clearly identify available personnel, equipment, and specialized resources.
- Establish procedures for requesting and deploying assistance.

[15] The Project Team notes EOC exercises for earthquake (April 2024) and bomb threat (July 2025) were conducted.

- Address liability, authority, and operational responsibilities before an incident occurs.
- Clarify reimbursement and cost-sharing considerations.
- Improve planning and coordination for both emergency incidents and high-profile events.

The importance of mutual aid is also reflected in Utah legislation. Utah Code §53H-3-304 provides additional authority to institutions of higher education when addressing safety concerns and responding to campus disturbances or emergencies. The statute states: **"If a law enforcement agency or security department of an institution of higher education lacks sufficient manpower to deal effectively with a condition of unrest existing or developing on a campus or related facility of the institution of higher education ... the chief administrative officer may call for assistance from the county sheriff of the county, a city law enforcement agency, or the Department of Public Safety."**[16]

The statute further provides that upon such a request, responding agencies: **"must render all necessary assistance without expense to the institution of higher education."**[17] This legislation underscores the State's recognition that institutions of higher education may require external support during significant incidents and that coordinated response capabilities are essential to campus safety.

While these statutory authorities provide an important framework for emergency response, formal mutual aid agreements remain a best practice. Such agreements facilitate planning, establish expectations before an incident occurs, and provide a mechanism for accessing specialized resources during both planned events and unforeseen emergencies.

UVUPD and the Orem Police Department have already begun efforts to formalize written mutual aid agreements, which is commendable. UVUPD has formalized a mutual aid agreement with the Utah County Sheriff's Office. Expanding these agreements to include additional neighboring law enforcement and public safety agencies will strengthen preparedness, improve resource coordination, and provide greater access to specialized capabilities that can enhance both event security and emergency response operations.

1.8 Crisis Communications and Media Response Planning

Crisis communications planning is a fundamental component of emergency management in higher education. Effective plans enable institutions to provide timely, accurate, and coordinated information that protects life safety, supports emergency response operations, reduces misinformation, maintains stakeholder trust, and supports compliance with federal emergency notification and timely warning requirements.

Higher education institutions must communicate with diverse internal and external audiences during rapidly evolving incidents, including students, employees, families, visitors, public safety partners, public officials, media, and the broader community. A well-developed crisis communications plan establishes clear roles, responsibilities, communication channels, approval processes, spokesperson designations,

---

[16] Utah 53H-3-304 (4)(a) Powers of chief administrative officer to order individuals off an institution of higher education's property, Renumbered and Amended by Chapter 8, 2025 Special Session 1.

[17] Utah 53H-3-304 (4)(b) Powers of chief administrative officer to order individuals off an institution of higher education's property, Renumbered and Amended by Chapter 8, 2025 Special Session 1

and message templates before an emergency occurs. These elements are particularly important during active threats, natural disasters, fires, public health emergencies, cyberattacks, hazardous material incidents, protests, and other events that may affect life safety, campus operations, or institutional reputation.

Crisis communications planning also extends beyond the initial emergency notification. Institutions must be prepared to provide operational updates, address misinformation, coordinate with public safety partners, communicate campus closures or operational changes, communicate available mental health and support resources, and explain recovery efforts. Transparent and consistent communication during and after a crisis strengthens stakeholder confidence and supports institutional resilience.[18]

The Project Team reviewed *UVU's Crisis Communications Playbook – Controversial Speaker Invited to Campus*, updated in February 2024. The existence of this playbook reflects a proactive effort to prepare for high-profile speakers, protests, media scrutiny, reputational risks, and related operational concerns. The document identifies key stakeholders, outlines communications workflows, provides audience mapping, and includes pre-developed messaging regarding free speech, academic freedom, and protest activity. These elements are consistent with recognized crisis communications practices and demonstrate that the University devoted meaningful attention to communications planning prior to September 10, 2025.

The playbook is particularly noteworthy because it outlines several protocols that, if fully operationalized, would support planning and preparation for major on-campus events such as the September 10 TPUSA event. These include designation of a communications lead, intelligence gathering, development of a coordinated communications strategy, and continuous monitoring of media and social media activity.

Despite the existence of this guidance, the Project Team identified limited evidence that these practices were consistently implemented before or during the incident. Communications responsibilities were not always clearly defined, particularly when key leaders were off campus or operating remotely, adding to uncertainty regarding message development, approval, and dissemination on September 10.

The Project Team also identified limited evidence of a formal intelligence-gathering process being used to support communications planning and decision-making prior to the September 10 TPUSA event. UVUPD did communicate with the Utah Statewide Information and Analysis Center (SIAC) regarding potential threat information to help guide planning and preparation. However, there was limited evidence of a broader multidisciplinary effort that incorporated social media monitoring, analysis of security concerns arising from previous TPUSA events across the country, or a structured assessment of operational risks associated with similar events held elsewhere.

Available information suggests that monitoring efforts prior to September 10 were focused primarily on protest activity and reputational concerns rather than being integrated into a broader process to identify security implications, emerging threats, or operational vulnerabilities. Such information could

[18] Federal Emergency Management Agency. (2021). Comprehensive preparedness guide (CPG) 101: Developing and maintaining emergency operations plans (Version 3.0). U.S. Department of Homeland Security; Centers for Disease Control and Prevention. (2018). Crisis and emergency risk communication (CERC) manual. U.S. Department of Health and Human Services; International Association of Campus Law Enforcement Administrators. (2023). Standards and accreditation program. IACLEA.

have helped inform communications planning, venue and security discussions, staffing decisions, crowd management strategies, and consideration of additional security resources or technology support.

The playbook provides a strong foundation for future crisis communications planning. The primary opportunity for improvement is ensuring that crisis communications guidance is operationalized through training, exercises, clear role designation, defined message approval authority, and closer integration with emergency management, law enforcement, intelligence, and event security planning functions.

UVU has also developed an in-progress draft of a *Crisis Readiness Plan and Guidebook 2026*. Because that document was not in place before the September 10 TPUSA event, it is addressed more fully in Section 7.4 as a post-incident preparedness enhancement. The draft Guidebook appears to be a significant and comprehensive improvement that, once finalized and aligned with the Emergency Operations Plan and related templates, should strengthen UVU's crisis communications, life-safety alerting, media response, and post-crisis review processes.

1.9 Organizational Alignment, Staffing, and Professional Standards

Campus public safety functions are most effective when they are appropriately positioned within the University's organizational structure, sufficiently staffed for the institution's size and risk environment, supported by clear professional standards, and integrated into senior-level planning and decision-making. At large public universities, the Police Chief or senior public safety leader typically has sufficient access to executive leadership to ensure that public safety considerations are incorporated into event planning, emergency management, resource allocation, facilities planning, student affairs, communications, and institutional risk decisions.

Organizational alignment is not merely an administrative issue. It affects how quickly public safety concerns are elevated, how consistently public safety participates in strategic planning, how resources are prioritized, how emergency preparedness is coordinated, and how senior leaders understand the operational realities facing campus police, emergency management, and security personnel.

Staffing is also a core element of public safety readiness. Universities should periodically evaluate whether sworn staffing, Dispatch capacity, emergency management resources, and physical security staffing are aligned with the institution's size, geography, event profile, call volume, risk environment, and community expectations.

Professional standards frameworks, including those identified through higher education-specific resources such as the International Association of Campus Law Enforcement Administrators (IACLEA), can support policy development, accountability, risk reduction, operational consistency, and continuous improvement.

UVU is a large and growing public university with a complex public safety environment. The University hosts major events, public speakers, athletic events, student activities, and public gatherings while operating in an open campus environment with significant commuter activity and broad community access. These conditions require public safety functions that are visible, integrated, appropriately staffed, and positioned to participate in institutional planning and decision-making.

The Project Team identified concerns regarding the organizational placement and visibility of UVUPD within the University's leadership structure. The Police Chief does not appear to be positioned in a manner typical for the senior law enforcement official at a large public university. The Police Chief's current reporting structure appears to place several organizational layers between UVUPD and the University's senior executive leadership. This structure may limit routine visibility into senior decision-making and reduce opportunities for public safety considerations to be integrated early into planning for major events, emergency preparedness, facilities use, and institutional risk management. At a minimum, to align itself with what are considered best practices for a university with the size and operational scope of UVU, the Police Chief should be reporting to someone who answers directly to the President of the University.[19]

This concern is not a reflection on the professionalism or commitment of UVUPD personnel. Rather, it is an organizational alignment issue. For a university of UVU's size and complexity, public safety leadership should have a sufficiently direct connection to senior administration to ensure that campus safety, emergency preparedness, law enforcement operations, event security, and risk-management issues are regularly considered and understood at the appropriate level.

The Project Team also identified concerns regarding UVUPD staffing. UVUPD has a limited number of sworn personnel relative to the size of the University, the scale of campus operations, and the number and complexity of events that may occur on campus. While staffing needs cannot be determined through a simple formula, the University would benefit from a formal staffing analysis that considers student population, campus geography, call volume, event activity, patrol coverage, supervisory needs, investigative responsibilities, Dispatch demands, mutual aid assumptions, emergency management needs, and major-event security requirements. While a formal study is recommended to identify the appropriate staffing level, it was nevertheless clear to the Project Team that a total sworn staff of 13 is not sufficient for a university of UVU's size and the types of events and activities occurring across its campus.

The Project Team's review also identified an opportunity for UVU to evaluate IACLEA accreditation[20] as part of UVUPD's broader professional standards and continuous improvement efforts. IACLEA provides training, research, policy guidance, conferences, accreditation standards, and professional resources specifically focused on higher-education public safety. IACLEA accreditation provides an externally validated framework for assessing campus police policies, operations, training, administration, accountability, and continuous improvement. For UVU, IACLEA accreditation could provide a structured roadmap for evaluating UVUPD against nationally recognized campus public safety standards.

[19] The Project Team notes that after discussions with UVU leadership concerning this issue during our assessment work, they acted promptly, and the UVU Police Chief now reports directly to Val Peterson, VP of Administration and Strategic Relations, who reports directly to the UVU President.

[20] https://iaclea.org/accreditation/accreditation-process/ - Outlines the IACLEA Accreditation Process.

UVU should also consider leveraging no-cost resources available through the Cybersecurity and Infrastructure Security Agency (CISA). Colleges and universities are part of the Education Facilities Subsector within the nation's critical infrastructure framework, and CISA provides tools, assessments, and technical assistance intended to help institutions strengthen physical security, cybersecurity, emergency preparedness, and infrastructure resilience.

Relevant CISA resources may include Protective Security Advisor engagements, physical security assessments, infrastructure resilience tools, cybersecurity vulnerability assessments, tabletop exercises, and targeted violence prevention resources. These services can help UVU identify vulnerabilities, prioritize mitigation strategies, evaluate preparedness, and align campus safety and security planning with recognized critical infrastructure protection practices.[21]

Recommendations related to the issues addressed in this section are included in Section 9.



[21] Cybersecurity and Infrastructure Security Agency. (2024). Critical infrastructure security and resilience. U.S. Department of Homeland Security. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience

2. September 10 TPUSA Event Planning, Response, and Interagency Coordination

The review and assessment of the formal UVU policies, plans, training records, training exercises, and communications protocols summarized above provides the framework for evaluating how well UVU prepared for and responded to the September 10 TPUSA event. The following narrative reviews in greater detail the planning process, day-of security posture, initial response, and interagency coordination that occurred before and after the September 10 TPUSA event. This detail includes reviewing how well specific policies were followed and implemented.

2.1 Prevention and Preparedness Practices for High-Profile Events

Effective event-security preparation for a high-profile speaker requires early risk identification, structured event classification, venue assessment, protective intelligence, coordination with event organizers, public safety partner engagement, access-control planning, staffing analysis, communications planning, and documented decision-making. When a proposed event involves political activity, large attendance, public visibility, potential protests, or an elevated threat environment, planning should begin early enough to allow security concerns to influence venue selection, ticketing, credentialing, staffing, mutual aid, intelligence collection, and emergency response planning.

Recognized practices include:

- Classifying high-profile, political, controversial, or large-attendance events through a formal review process.
- Conducting a documented security assessment before finalizing venue, ticketing, access-control, and staffing decisions.
- Reviewing a speaker's profile, as well as the outcomes of a speaker's prior events, associated protest activities, online social media discourse, and known threats.
- Coordinating directly with the event organizer and any private or executive protection team.
- Establishing attendance projections and access to ticketing or registration data.
- Evaluating venue suitability, line-of-sight exposure, crowd flow, emergency access, and controlled-entry options.
- Developing access-control, credentialing, screening, and staffing plans based on the event's risk profile.
- Engaging local law enforcement, fire, EMS, emergency management, and other public safety partners when additional resources or expertise may be needed.
- Assigning personnel to monitor relevant security systems, video feeds, communications channels, and emerging conditions during the event.
- Documenting key decisions, assumptions, resource needs, and unresolved security concerns.
- Notifying local, state and federal authorities including Utah SIAC, FBI, Secret Service, and the DHS Protective Security Advisor, when warranted.

2.2 Major Event Classification and MEAC Review

UVU had a formal policy framework in place for event scheduling, facility use, and major-event review. Policy 425 was directly relevant to the September 10 TPUSA event because it defines major events, establishes the role of the Major Events Assessment Committee (MEAC), requires major events to undergo a MEAC-facilitated Security Assessment, and requires a MEAC review to identify health and safety concerns and compliance with University policy and applicable law.

Key Event Security Planning Terms

Security Assessment. A Security Assessment is the process used to translate identified concerns into practical planning decisions. It evaluates the event, speaker, venue, audience, threat environment, and operational requirements. The assessment should inform venue recommendations, staffing, access-control measures, communications needs, Command Post planning, EOC readiness, mutual aid considerations, credentialing, screening, and the development of an Event Action Plan, appropriate to the size and nature of the event.

A Security Assessment should also examine the physical environment, including the proposed stage or speaking location, backstage or support areas, audience areas, approach and egress routes, secure perimeter, elevated positions, adjacent buildings, rooftops, balconies, windows, elevated walkways, parking structures, tree lines, and other areas that may overlook or provide access to the event site.

Risk Assessment. A Risk Assessment is a component of the broader Security Assessment. It evaluates whether the event presents a significant threat of harm to people or property. This process includes identifying potential threats, assessing vulnerabilities, evaluating potential consequences, and determining appropriate mitigation measures. Common factors include anticipated attendance, protest activity, speaker profile, venue characteristics, historical incidents, and available intelligence information.

Event Action Plan. For major or elevated-risk events, the Security Assessment should inform a written Event Action Plan. The Event Action Plan translates assessment findings into operational decisions and helps ensure that all responsible parties share a common understanding of the event security posture.

Security Plan. The Security Plan is typically part of the Event Action Plan. It identifies staffing assignments, command relationships, post responsibilities, communications procedures, access-control decisions, protective operations coordination, emergency response procedures, contingency plans, and mutual aid resources. For complex events, the Event Action Plan should also include emergency management procedures and Incident Command System role assignments.

The September 10 TPUSA event met multiple criteria requiring major event review under Policy 425 § 3.5. The event involved political activity, was expected to draw significant attendance, had the potential to attract protest activity, and presented safety and security considerations requiring coordinated planning. Event Services appropriately recognized the need for MEAC review and convened the committee to support planning consistent with Policy 425 §§ 3.6, 4.8.2, and 5.2.1.

UVU policy was followed regarding the process to seek approval for an event. The UVU TPUSA Club President received guidance from Event Services while working to submit the event as a co-sponsored event involving the UVU TPUSA club and the national TPUSA organization, consistent with Policy 425 § 3.7.1, which defines how University entities may request use of University facilities for University or co-sponsored events. However, UVU did not invite the speaker for this event. It was coordinated through the UVU TPUSA Club. The University is legally required to allow student clubs to bring speakers on campus.

UVU's adherence to Policy 425 § 4.1.5 is also relevant because it requires individuals planning, hosting, or attending events, including guests, vendors, and contractors, to follow University policies, Event Services guidelines and protocols, and applicable law. For co-sponsored events involving external entities, these provisions underscore the need to clearly define planning responsibilities, compliance obligations, access to event information, and coordination expectations. After the application was processed, University officials recognized that the event should be reviewed as a major event. On August 21, 2025, Event Services sent an email to those required to attend the MEAC meeting scheduled for August 25, 2025. This appears to have been the point at which UVU Police Chief Long first became aware of the event.

The MEAC process outlined several issues relevant to security planning, including the nature of the event, the requested outdoor location, anticipated attendance, protest activity, ticketing, staffing, and site-control concerns. However, the MEAC review did not lead to the creation of a documented Security Assessment that evaluated whether the event posed a significant threat of harm to people or property or that documented the operational implications of the requested venue and event configuration.

This documentation gap is important because the Security Assessment is the mechanism through which identified concerns should be translated into planning decisions, venue recommendations, staffing levels, access-control measures, communications needs, Command Post planning, Emergency Operations Center readiness, mutual aid considerations, and, when appropriate, an Event Action Plan. Without completing a documented Security Assessment, it becomes more difficult to identify security concerns and evaluate them, consider mitigation measures, determine who is responsible for implementation, and identify why certain planning decisions were made.

The September 10 TPUSA event planning process also reflected considerable deference on UVU's part to TPUSA's expressed desires regarding event logistics, including the Fountain Courtyard as the venue and the ticketing process. While the University was required to permit the lawful expressive activity to be conducted at an event on the campus, it had the ability to impose reasonable time, place, and manner restrictions on the event. Future MEAC processes should more clearly balance accommodating expressive activity with the need to retain control over site selection, ticketing processes, security requirements and operational conditions necessary to protect students, staff, and visitors on campus.

2.3 Venue, Ticketing, and MEAC Planning Decisions

During the August 25 MEAC Teams meeting, Maycee Crofts,[22] a Senior Field Representative for TPUSA, participated at the request of TPUSA. UVU participants raised concerns regarding TPUSA's requested

[22] The Project Team made multiple attempts to contact Maycee Crofts to obtain her perspective and recollection regarding the August 25 MEAC meeting, including what was discussed and decided during that meeting. These outreach efforts

location in the large, tiered Fountain Courtyard near the main campus entrance. Concerns included anticipated attendance, potential protest activity, crowd management, and the ability to control access to the event area. UVU officials suggested alternative locations such as the Fulton Library Quad or interior locations where access could be more effectively controlled. UVU also suggested using the University's ticketing system so anticipated attendance could be tracked and incorporated into planning.

According to meeting participants, Crofts insisted on the use of the Fountain Courtyard location because Charlie Kirk had previously spoken on campus and TPUSA was familiar with that location. Crofts also reportedly preferred that TPUSA manage online ticketing through its national office in Phoenix. Some MEAC members continued to express reservations, including Robin Ebmeyer, UVU's Director of Emergency Management and Safety. The committee ultimately allowed the event to proceed in the requested location and allowed TPUSA to manage ticketing.

July 10, 2025

Verbatim Email from TPUSA UVU Club President to UVU Club Services

"My field representative for Turning Point USA has asked me to reach out to the UVU Club Department to ask about availability on hosting an event on the Courtyard on September 10 from 9am-4pm

Shes [sic] being quite vague on what this event is, so unfortunately this is all the information I have in regards to it. Are you able to tell me if this space is currently available for that date and time?

Thanks!"

In our assessment, those decisions were consequential. The selected location presented greater open-access, crowd-management, high-ground vulnerabilities, and line-of-sight challenges than a more controlled venue. In addition, allowing the outside organizer to retain control over ticketing limited UVU's ability to obtain reliable attendance projections, monitor crowd-growth expectations, and align staffing and security resources with anticipated attendance.

Because Policy 425 § 4.8.2 requires major events to undergo a MEAC-facilitated Security Assessment, the planning process should document how venue selection, ticketing, access control, credentialing, screening, staffing, communications, emergency response, and legal considerations were evaluated. For the September 10 TPUSA event, several of these issues were discussed, but the process did not result in documented security requirements tied to the decision to approve the requested location and outside-controlled ticketing process. Had an Event Action Plan (EAP) been prepared, it may have helped to highlight in writing the various concerns UVU officials were identifying before and during the MEAC meeting on August 25, and this may have helped strengthen their resolve to specify what UVU could have required of TPUSA officials prior to authorizing the location, ticketing, and operational details of the event.

included telephone calls with voicemail messages, email requests, and outreach to the TPUSA national office seeking assistance in facilitating contact. A certified letter was not sent because Crofts' current mailing address was unknown. Crofts did not respond to these outreach efforts.

Policy 425 § 4.1.3 and Policy 161 are also relevant because security planning for political or controversial events must balance safety, lawful expression, access to University facilities, and operational control. In this context, security-related decisions regarding venue selection, access control, protest locations, screening, signage, and crowd management should distinguish between lawful expressive activity and conduct that creates safety, security, or operational concerns.

2.4 Pre-Event Security Coordination and Intelligence

On August 21, the UVU TPUSA Club President emailed the Clubs Office a completed MEAC questionnaire, indicating that it provided answers "straight from the TPUSA team." The questionnaire projected approximately 600 attendees, described the event as primarily student-focused with some potential public interest, represented no risk factors/ safety/security concerns or need for emergency medical services, and offered to connect UVUPD with TPUSA's head of security. That same day, the UVU Free Speech Committee flagged the event because of the potential for protests and noted that a small Emergency Operations Center (EOC) had been used for a prior TPUSA event on UVU campus.

After the August 25 MEAC meeting, Chief Long took the lead on security planning, with support from Event Services staff. Over the next 16 days, Chief Long and other UVU personnel took steps to prepare for the event, including attempting to identify TPUSA security points of contact, communicating with TPUSA representatives, addressing TPUSA concerns about the Hall of Flags outdoor pedestrian walkway above the speaking location, contacting the Utah SIAC for threat-related information, and arranging UVUPD staffing.

During the MEAC process, Chief Long provided his contact information to Maycee Crofts and asked that she share it with the appropriate TPUSA representative so that he could coordinate security matters directly with the organization's security team. When he did not hear from Crofts or a member of the TPUSA security team following the MEAC meeting, Chief Long attempted to follow up but did not have Crofts' direct contact information. On September 2, he emailed a staff member in the University's Clubs Office seeking contact information for TPUSA's security representative because no member of the TPUSA security team had contacted him following his request to Crofts.

On September 3, Chief Long received a call from Dan Flood, TPUSA Security Supervisor.[23] Chief Long asked Flood what was needed by TPUSA from the UVU police. Flood stated that approximately 10 to 12 TPUSA security personnel would attend, which was an increase from the eight referenced during the August 25 MEAC meeting. Flood asked Chief Long to arrange for TPUSA staff to park as close as possible to the canopy location in the Fountain Courtyard where Charlie Kirk would speak and facilitate his entry to and exit from the venue.

Later on September 3, Chief Long called Flood again to ask whether the event was ticketed. Flood confirmed that TPUSA's national office in Phoenix was handling ticketing so TPUSA could gauge how many people planned to attend. Chief Long also asked whether Charlie Kirk would speak at any other

[23] The Project Team made multiple attempts to contact Dan Flood to obtain his perspective and recollection regarding his telephone call with the UVU Police Chief, subsequent text message exchanges, and discussions that occurred in the hours before the September 10 TPUSA event. These efforts included telephone calls with voicemail messages, email requests, and outreach to the TPUSA national office in Phoenix seeking assistance in facilitating contact. The Project Team also sent Flood a certified letter requesting an interview. Flood did not respond to these outreach efforts.

time that day. Flood advised that Charlie Kirk would speak only from noon until approximately 2:00 p.m. Chief Long did not ask Flood about updated ticketing numbers, nor did Flood offer any information about crowd estimates from TPUSA's ticketing process at that time.

On September 8, at approximately 3:12 p.m., Dan Flood sent Chief Long a text message regarding the Hall of Flags outdoor pedestrian walkway located above the canopy area where Charlie Kirk would be speaking. Flood advised that the walkway could allow individuals to be positioned directly above Charlie Kirk and expressed concern that the access point presented a security problem. Chief Long advised that the area above the canopy would be covered for security purposes. The following text exchange between Dan Flood and Chief Long reveals the primary security focus for TPUSA was the Hall of Flags outdoor pedestrian walkway above the canopy.

September 8, 2025, starting at 3:12 p.m.

Verbatim Text Exchange between Dan Flood and Chief Long

Dan Flood: Hello Chief Long – We received this message today from the student group . FYSA

"there is student roof access pretty close to where CK will be set up at Utah Valley (The Sorensen Student center has a couple stair cases that go up to the walkways on the roof)"

Chief Long: You want access to the roof?

Dan Flood: I was told students have access above us, if this is true, it would be nice to either have it controlled access or allow one of my guys to be there as well. If possible.

Chief Long: I got you covered

Dan Flood: Thank you, Sir.

Chief Long also contacted SIAC by e-mail at approximately 7:30 a.m. on September 10 to share an anonymous tip UVU received regarding a potential threat involving an electronic-magnetic-pulse device that a suspect might use at the event. Chief Long was seeking to determine whether any threat-related intelligence update was available regarding the tip. Long was advised e-mail was the best method to request information from the Utah SIAC. SIAC responded shortly thereafter to Chief Long that it was not a credible threat, as it appeared the tipster had provided similar information in the past that was determined to be unreliable.

On the morning of September 10, the TPUSA security team arrived at UVU with Dan Flood at approximately 9:00 a.m. Chief Long reported that he was not formally introduced to the members of the TPUSA security team upon their arrival, as he did not reach out to them to meet, nor did TPUSA security staff reach out to him to do so. At approximately 9:04 a.m., Dan Flood texted Chief Long advising he had arrived and they exchanged several texts. At approximately 11:00 a.m., Flood texted Chief Long again regarding individuals on the Hall of Flags outdoor pedestrian walkway above the canopy where Charlie Kirk would be speaking and requested that the area be taped off and secured. Chief Long, Sergeant Beveridge, and Officer Bagley went to the walkway location and had attendees move out of the area, then taped it off with police tape. Sergeant Beveridge and Officer Bagley remained in that area to secure it through the time of the shooting.

Coordination with the TPUSA security team was limited before and during the event on September 10. Other than limited communications on September 3, the review did not identify a sustained or structured planning process between UVUPD and the TPUSA security detail before the event or on the morning of the event before Charlie Kirk arrived on campus. Chief Long texted Dan Flood to meet on the Hall of Flags outdoor pedestrian walkway at 11:00 a.m., however this face-to-face meeting did not occur.

September 10, 2025, starting at 9:04 a.m.

Verbatim Excerpt of Text Exchange between Dan Flood and Chief Long

Dan Flood: Hello sir, we're on site walking around the table location

Chief Long: Copy
What do you need

Dan Flood: Just learning the ingress for meeting before hand and table.

Chief Long: Copy, we'll link up in a bit and chat

Dan Flood: Sounds good
Concerns of agitators above us.
[Photo of canopy area where Kirk would be speaking and two individuals who appear to be hanging an LGBTQ flag from the walkway railing above the canopy area.]

Chief Long: Yeah Student Life is dealing with them
I will have an officer up there
My event officers get here at 11:00

Dan Flood: Can we tape right above us to prevent people from throwing stuff over?
[Photo of student on the walkway above the canopy area where Kirk would be speaking.]
Already have one guy right above our tent

Chief Long: Let's meet there at 11 if that works for you

Dan Flood: Yes.
The guy up here now asked the Dean's office if they can stand above us and they said yes, you can.
If we could, it'd be nice to tape off the upper barrier directly over us to prevent anyone throwing stuff over, etc.

Chief Long: Somebody throws something from there, they go to jail!!!
Ill bring some police tape

The absence of a formal pre-event briefing and coordinated walk-through with Brian Harpole, Dan Flood, and the TPUSA security team was a critical missed opportunity.

The absence of a formal pre-event briefing and coordinated walk-through with Brian Harpole, Dan Flood, and the TPUSA security team was a critical missed opportunity. For events involving a high-profile speaker accompanied by private security, campus police and the protective detail should conduct a documented pre-event briefing addressing roles, communications, arrival and departure, line-of-sight concerns, high-ground vulnerabilities, building access, emergency response, medical contingencies, use-of-force expectations, emergency egress, post assignments, and coordination with University personnel and any external public safety partners. This type of briefing is also consistent with the planning and compliance obligations reflected in Policy 425 § 4.1.5 for individuals and entities planning, hosting, or participating in events on University property.



The Project Team finds it particularly significant that an on-site pre-event briefing was not requested by the TPUSA protection detail. Traditional law enforcement and executive protection serve related but distinct functions. Law enforcement officers are generally trained to engage in crime prevention efforts, respond to criminal behavior, investigate incidents, make arrests, collect evidence, and prepare reports. Executive protection, by contrast, is primarily preventive. Its core purpose is to protect a specific person or group of people by reducing exposure, controlling access, identifying vulnerabilities, and preventing an attack before it occurs.

The Project Team finds it particularly significant that an on-site pre-event briefing was not requested by the TPUSA protection detail. Traditional law enforcement and executive protection serve related but distinct functions. Law enforcement officers are generally trained to engage in crime prevention efforts, respond to criminal behavior, investigate incidents, make arrests, collect evidence, and prepare reports. Executive protection, by contrast, is primarily preventive. Its core purpose is to protect a specific person or group of people by reducing exposure, controlling access, identifying vulnerabilities, and preventing an attack before it occurs.

Although some law enforcement officers receive specialized executive protection training, most do not. For that reason, coordination between a visiting protection detail and campus law enforcement is especially important. A pre-event briefing would have allowed the TPUSA protection detail and UVUPD to clarify roles, identify vulnerabilities, review arrival and departure plans, assess line-of-sight concerns, confirm post assignments, and ensure that both groups shared a common understanding of the protective strategy for the event.

2.5 Day-of Security Posture and Operational Adjustments

At approximately 11:00 a.m. on September 10, Chief Long began coordinating with UVU officers arriving to provide security for the event. UVUPD staffing initially included Chief Long, one patrol officer, and one reserve officer, for an initial total of three UVU law enforcement officers. After observing the size of the crowd, Chief Long requested that a uniformed UVUPD detective assist, as well as an additional officer and a sergeant, bringing the UVU team to six. This group represented all of the UVUPD sworn staffing on duty on that day and at that time.

Two plainclothes officers from Utah State University (USU) were also present. Those officers had previously contacted Chief Long and arranged to observe the event because the same TPUSA tour was scheduled to occur at USU on September 30. The two USU officers were not assigned specific operational duties during the September 10 TPUSA event and were reportedly located outside the second-level area of the Fugal Building when the shooting occurred.

Between approximately 11:20 a.m. and 11:30 a.m., UVUPD Chief Long, UVUPD Sergeant Beveridge, and Officer Bagley went to the Hall of Flags outdoor pedestrian walkway above the canopy where Charlie Kirk would be speaking. They cleared the area of individuals who had gathered there and placed security tape in two locations on either side of the canopy below to prevent the estimated 80 to 100 protesters from entering the area directly above the speaker's location. According to Chief Long, most individuals complied with officers' directions, and some protesters complied with a request to remove a large LGBTQ flag that had been hung from the railings in that area. Chief Long stated Sergeant Beveridge and Officer Bagley remained in the area to maintain compliance.

Chief Long then went to Room 204 on the second floor of the Fugal Gateway Building, where a Command Post had been established. The room had floor-to-ceiling windows and provided visibility over the event area and surrounding buildings. Chief Long and other UVU officials planned to use the location to observe the event and coordinate operations.

At approximately noon, Charlie Kirk arrived and began moving toward the canopy where he would speak. Chief Long reported hearing protesters who were positioned behind the police tape on the second-level Hall of Flags outdoor pedestrian walkway shouting profanities toward Charlie Kirk. Charlie Kirk looked up toward the protesters but did not respond verbally. He then began engaging with the crowd, including throwing TPUSA baseball caps to attendees.

Before entering the Command Post, Chief Long spent time addressing an access-control issue inside the Fugal Gateway Building. Students and other attendees had entered the administration building and proceeded up a stairwell from the second floor to the third floor to access a balcony area outside the University President's Office, where they hoped to observe the event. After removing those students, Chief Long secured the area and stationed a staff member from the Director of Emergency Management and Safety's staff on the second level to prevent people from entering the stairwell and accessing the third-floor balcony area. Chief Long then entered the second-floor Command Post and joined other UVU officials as Charlie Kirk began speaking. Chief Long was present in the Command Post when, at approximately 12:23 p.m., he heard the gunshot and saw Charlie Kirk get shot.

The section on the following pages summarizes statements made by Brian Harpole regarding the September 10 TPUSA event.

November 17, 2025

Brian Harpole's Podcast Interview on November 17, 2025

Although the Project Team did not receive a response to its requests to interview Brian Harpole, head of the Integrity Solutions security team working for TPUSA on September 10, the Team was able to gain additional insight into his involvement in the event through his November 17, 2025 appearance on the *Shawn Ryan Podcast*, titled *"Brian Harpole – Groundbreaking Evidence From Charlie Kirk's Head of Security / SRS #254.*

During the interview, Harpole discussed several issues relevant to this assessment, including event planning, the venue location, elevated positions near the speaking area, drone use, and coordination with UVU officials. The summary below is included solely to document information Harpole shared publicly and to help provide additional context regarding planning and security activities before and during the September 10 TPUSA event.

Harpole stated that he began providing security services to Charlie Kirk and TPUSA in 2018 while working for a separate security firm. He later formed his own company, Integrity Solutions, and continued providing those services through that company approximately three years before the date of the podcast. Harpole stated that, before this work, he served with a law enforcement agency in Texas for approximately 14 years.

Harpole described members of his Integrity Solutions security team as having backgrounds as SWAT team members or commanders, professional athletes, jiu-jitsu experts, Navy SEALs, and Marines. He also described the training his team receives. He did not specifically identify any team members as having prior careers or backgrounds in executive protection details before joining his team.

Harpole stated that his first meeting to discuss the September 10 TPUSA event occurred on August 24. This was one day before the UVU MEAC meeting, during which TPUSA representative Maycee Crofts advised UVU of TPUSA's preferred venue location and ticketing process, which UVU approved.

Harpole also stated that Dan Flood was the "security guy" for TPUSA. He said Flood did not share any specific security concerns or threats with him during pre-event planning. Harpole stated that Flood would "meticulously" share any intelligence he believed was important.

In the podcast, Harpole gave no indication he considered requesting an on-site pre-event meeting with campus police to evaluate vulnerabilities and make security assignments. Harpole explained that his team focused on securing what he called "the bubble," meaning the area in front of and around where Charlie Kirk would be speaking. Harpole stated that when he and his team arrived at UVU a few hours before the event, they surveyed the area and believed the venue location was "horrible." He specifically identified the concern that someone in an elevated position would have a 180-degree view of the area where Charlie Kirk would be speaking. Harpole described this as "ignorance" and "a security fail" but he acknowledged that Charlie Kirk "liked" the venue.

Harpole further stated that the venue location was selected by UVU and that UVU told TPUSA, "Nope, this is where you have to have it." This was one of the primary reasons the Project Team sought to speak directly with Harpole, since this particular statement and a number of others Harpole made conflicted with what the Project Team learned from reviewing evidence and conducting numerous interviews with those who attended the MEAC meeting and were present on the day of the event. Indeed, multiple interviews the Project Team conducted indicated that UVU had expressed concerns about the outdoor location, including during the August 25 MEAC meeting, but ultimately agreed to TPUSA's requested venue location when TPUSA representative Maycee Crofts insisted on it. A direct interview with Harpole would have assisted the Project Team in clarifying this issue, because the initial e-mail request from TPUSA to UVU on July 10, 2025, also specifically requested that the event be held at the Fountain Courtyard.

The Project Team also sought to learn more about any pre-event planning related to the possible use of aerial drones. During the podcast, Harpole discussed the lack of a drone camera in the air during the event. He stated that the TPUSA "video team" used what he described as a "little-bitty" drone to take a quick shot of the venue before the event. Harpole also stated that although his team had drones, they did not use them during the event because of FAA restrictions related to Provo Airport airspace.

The Project Team's basic research indicated that drone operations are restricted within a five-mile radius of Provo Airport in Class D airspace. UVU is located in the City of Orem, which borders the City of Provo, and is located at least six miles from Provo Airport. Harpole also expressed concern that UVUPD did not have a drone available. Without being able to speak directly with Harpole, it remains unclear to the Project Team why, during the hours before Charlie Kirk's arrival, Harpole's team and UVU did not discuss efforts to secure a drone, particularly after Harpole had stated in the podcast that his team had concerns about the venue location. A drone from the neighboring Orem Police Department could have been requested.

Harpole also stated during the podcast that "federal law" would not allow his team to post a counter-sniper on a roof in the area for the event. However, it was unclear why he did not post any members of his team in elevated locations for general security observation purposes. Flood did request UVUPD to clear the Hall of Flags outdoor pedestrian walkway area above the canopy where Charlie Kirk would be speaking. UVUPD cleared that area, taped it off with police tape, and posted two officers there. The podcast did not include any discussion of whether Harpole's team worked with UVUPD to address other elevated roof area concerns near the venue.

These issues and statements contributed to the Project Team's desire to speak directly with Harpole. However, based upon the information available to the Project Team, it appears that the lack of a face-to-face meeting between Harpole, his security team, and UVUPD Chief Long after Harpole's arrival, or even a telephone conversation between them in the days leading up to the event, significantly impacted the effectiveness of security planning and coordination for the September 10 TPUSA event. It is also unclear why Harpole did not make arrangements to meet with Chief Long immediately after he identified his concerns with the Fountain Courtyard being a "horrible" location upon his arrival.

2.6 Initial Interagency Response and Campus Searches

The shooting immediately shifted the event from a planned campus security operation to a complex public safety emergency involving victim protection, suspect identification, campus-wide searches, crime-scene protection, emergency communications, investigative coordination, traffic control, and external agency support.

In addition to reviewing UVU's policies, procedures, and protocols for planning, managing, and responding to major on-campus events, the Project Team also reviewed UVU's interactions with external law enforcement, fire, emergency management, and public safety partners during the immediate response to the September 10 TPUSA event. This review included interviews with representatives from several responding agencies and provided important insight into the emergency response, initial investigative activity, and opportunities to strengthen future interagency coordination.

Personnel from numerous partner agencies responded to assist UVU after the shooting, including the Orem Police Department, the Utah DPS, the Utah Highway Patrol, the Utah County Sheriff's Office, the Salt Lake City Office of the Federal Bureau of Investigation (FBI), the Orem Fire Department, and other nearby police departments. Their response was timely, professional, and essential given the scale, speed, and complexity of the incident.

Responding partner agencies arrived quickly and gathered at the Command Post located in the conference room on the second floor of the Fugal Gateway Building. Command personnel from the Orem Police Department quickly mustered OPD resources and helped organize resources from other responding departments. A critical early task was assisting UVUPD by organizing officers to conduct room-by-room searches of UVU buildings to identify any additional victims and locate any suspect or suspects.

This support was particularly important because Chief Long and the UVUPD personnel who were on campus when the shooting occurred were quickly faced with multiple urgent and competing responsibilities. These included helping to ensure TPUSA security team was able to evacuate Charlie Kirk from the area immediately, locating a suspect or suspects, identifying and securing crime scenes, protecting students and others still on campus, addressing traffic-control needs, coordinating with the UVU Emergency Operations Center, and managing the immediate operational demands of an active and uncertain public safety emergency. Under those circumstances, the assistance from outside agencies was both necessary and appreciated.

During the initial response, Officer Chris Bagley identified the elevated roof area of the Losee Center as a possible source location of the assailant. Officer Bagley went to that area, where he located a screwdriver and an area of disturbed gravel on the roof that appeared consistent with a possible prone shooting position. Officer Bagley's quick recognition of the likely shooting position was significant because it helped focus the investigation on the elevated roof area and prompted a review of security surveillance video focused on that location. That review contributed to the identification of a suspect

leaving the roof area, and follow-up search activity nearby led to the recovery of a rifle believed to have been used in the crime.

Members of the Orem Police Department, together with Orem Fire Department personnel trained in emergency medical services, arrived almost immediately. OPD command personnel stepped in quickly to help lead certain operations within the Command Post. Their assistance helped address the urgent need to search the campus for suspects while also ensuring there were no additional victims in UVU's many buildings across the large and sloped campus terrain.

The Project Team also interviewed Orem Police Chief B.J. Robinson. That interview indicated that a positive and collegial relationship existed between OPD and UVU before, during, and after the events of September 10. Chief Robinson responded to the scene after receiving information suggesting that a suspect was in custody. Once he made his way to the command post, he took steps to provide the resources his command personnel and others needed, including support for sweeping searches of the campus.

Chief Robinson also confirmed that OPD and UVU had operated under an informal mutual aid understanding to assist one another as needed. Since the incident, he has taken steps to formalize that relationship through a written mutual aid agreement between OPD and UVU. At the time of the interview, drafts of that agreement were being developed. *This is an important post-incident enhancement and is addressed in Section 7.*

Based on interviews conducted for this assessment, representatives from the Orem Police Department, the Utah DPS, the Utah County Sheriff's Office, the Utah Highway Patrol, Orem Fire Department, and other local agencies who responded were competent, capable, and professional in their response. Their collective actions reflected the type of coordinated law enforcement, fire, EMS, and public safety support a community would hope to see during a tragic and fast-moving incident.

2.7 Transition to State and Federal Investigative Command

Commissioner Beau Mason of the Utah Department of Public Safety acted quickly upon learning of the shooting while at DPS headquarters approximately 35 miles northwest of UVU. He immediately began mustering key personnel from his department, including personnel from the State Bureau of Investigation (SBI), the Utah SIAC, and the State Crime Lab. He directed DPS personnel to assist in any way possible and left for UVU within approximately 15 minutes of learning about the shooting and after meeting with the staff he had gathered.

While en route, Commissioner Mason attempted to call Chief Long to coordinate but was unable to connect because Chief Long was occupied with urgent command responsibilities at the scene. Commissioner Mason then contacted Utah County Sheriff Mike Smith to discuss tactical resources that may be needed to locate and confront a suspect or suspects, along with other pressing operational needs.

Upon arrival at UVU, Commissioner Mason immediately engaged with other law enforcement officials to help determine what actions needed to be taken. He coordinated with state leadership, local law enforcement leaders, and FBI representatives as the response transitioned from UVUPD's initial campus response to a larger state and federal investigative operation.

Interviews indicated that once Commissioner Mason arrived at UVU, he helped organize the investigative command structure among agencies at the scene. He gathered law enforcement officials and advised them that the Governor had directed him to take the lead on the investigation. At the same time, he emphasized that the investigation would require coordinated participation among all involved agencies. This helped establish a clearer lead-agency framework while reinforcing the need for continued interagency cooperation.

Upon meeting with the Special Agent in Charge (SAC) of the Salt Lake City Office of the FBI at UVU, Mason learned the SAC was told to lead the investigation. After discussing this with the SAC, they determined the Utah DPS and the FBI would co-lead the investigation. This approach was appropriate given that both had major crimes occur requiring distinct follow-up, with the state's homicide investigation focusing upon Utah Criminal Code violations requiring local prosecution and the federal interests involving potential federal hate crimes and domestic terrorism.

When the local FBI Special Agent in Charge concurred with the decision to co-lead the investigation with Commissioner Mason, the investigative command structure continued to evolve in a coordinated manner. This shared leadership arrangement was also reflected during the press conference held on the afternoon of September 10.

Overall, the transition from UVUPD's initial campus response to a multi-agency state and federal investigation occurred quickly and with significant outside agency involvement. The early actions by UVUPD personnel, the rapid engagement of the Orem Police Department, Utah County Sheriff's Office and other local partners, the quick and collaborative response of the local FBI field office, and the leadership shown by the Utah Department of Public Safety helped establish investigative direction quickly during a chaotic and fast-moving incident. *The broader interagency coordination lessons from this transition are addressed in Section 4.4.*

Post-Incident Statewide Higher-Education Information Sharing

Following the September 10 incident, Commissioner Beau Mason of the Utah Department of Public Safety took additional steps to strengthen statewide safety coordination for institutions of higher education. Commissioner Mason on his own initiative assigned a DPS member on the SIAC team to focus on locating and analyzing available information associated with safety concerns for Utah's colleges and universities.

Commissioner Mason also requested that each Utah institution of higher education designate at least one representative to participate in a new group intended to support regular interaction, coordination, and information sharing among institutions. Had these steps not already been initiated, they would have been appropriate recommendations stemming from this After-Action Report.

These actions represent a meaningful enhancement to statewide situational awareness and should be incorporated into UVU's ongoing threat intelligence, event-planning, and emergency management processes. *They are also discussed in Section 7 as post-incident security enhancements.*

2.8 Fire, EMS, and Emergency Management Interagency Support

The Project Team also interviewed Chief Marc Sanderson of the Orem Fire Department. Chief Sanderson was in Wisconsin on September 10 coordinating the building of a new fire truck for the department, but he provided detailed information regarding Orem Fire's response.

Fire personnel from Station One and Station Three were initially dispatched to the scene of the shooting. Personnel from Stations Two and Four also responded because the extent of medical need was not yet known. While en route, the Station Three fire truck passed near the SUV being used by the TPUSA security team to transport Charlie Kirk to Timpanogos Hospital. Station Three personnel provided that information over the radio. Station Two then rerouted to Timpanogos Hospital, where the Fire Captain from Station Two assisted in providing CPR to Charlie Kirk at the hospital.

In addition, one Orem Fire Captain went to the UVU Command Post to provide assistance, and two Orem Fire paramedics joined a police officer on scene to help search for victims who may have needed medical assistance.

Chief Sanderson also advised that he had recently spoken with Chief Robinson about approaching UVU with an offer to conduct a joint active shooter training exercise. The purpose of such an exercise would be to help ensure that UVU, OPD, and Orem Fire are able to operate as efficiently and effectively as possible should another major public safety incident occur on campus.

The Project Team also interviewed Keith Stevenson, Emergency Management Director for the City of Orem. The purpose of this interview was to understand what role Orem Emergency Management played on September 10, what mutual aid assistance may have been available, and how Orem Emergency Management may be able to support UVU in the future. Stevenson demonstrated strong familiarity with the National Incident Management System (NIMS) and the Incident Command System (ICS) framework, both of which are national standards for multi-agency emergency response.

When Stevenson learned of the shooting moments after it occurred, he recalled from a prior Local Emergency Planning Committee (LEPC) meeting that UVU Emergency Management Director Robin Ebmeyer was scheduled to be out of state on vacation that day. The LEPC meets twice a month at the Utah County Sheriff's Office, and Ebmeyer is a member. Stevenson estimated that he called Ebmeyer approximately 20 minutes after the shooting and offered any assistance he could provide. According to Stevenson, Ebmeyer declined assistance.

Because he was not asked to respond to UVU, Stevenson remained at the Orem EOC located within the Orem City Hall complex. From there, Orem City officials coordinated fire operations for personnel dispatched to UVU and remained prepared to assist if requested. Stevenson advised that those present in the Orem EOC included the City Manager, Assistant City Manager, a Deputy City Manager, and personnel from the Police and Fire Departments. He also advised that Orem Emergency Management remains willing to assist UVU with future emergency management policy development, training, and preparedness efforts.

2.9 Key Interagency Lessons

The September 10 response demonstrated the value of UVU's relationships with external law enforcement, as well as fire, emergency management, and other public safety partners. OPD, Orem Fire, Utah DPS, the Utah County Sheriff's Office, the FBI, and other responding agencies provided critical support during a fast-moving and highly complex incident.

At the same time, the incident showed the importance of identifying, requesting, and integrating external resources early and in advance, particularly when an event involves uncertainty, high-profile speakers or government officials, potential mass-casualty concerns, an active or unknown suspect or threat, extensive campus searches, multiple crime scenes, and significant public communication demands. External public safety and emergency management partners had both the willingness and capability to assist UVU. In some cases, those resources were used effectively. In other cases, available support was not fully leveraged in advance.

Available Partner Resources and Future Event Planning

Several external partners described capabilities that were available to UVU or could support future major-event planning. Chief B.J. Robinson advised that the Orem Police Department has aerial drone capability that can provide live video footage. He would have provided that resource to Chief Long had it been requested and had OPD known more in advance about the event details, including the specific location of the event on campus.

Orem Emergency Management Director Keith Stevenson also advised that he was willing to assist UVU on September 10 and remains willing to support future emergency management policy development, training, and preparedness efforts. Orem City officials were present in the Orem EOC and prepared to assist if requested.

These observations reinforce the importance of identifying external resources before major events, including drones, tactical assets, traffic-control support, fire/EMS staging, emergency management personnel, investigative resources, and communications support. These capabilities should be identified in advance, documented in event plans, and incorporated into exercises and major-event planning protocols.

2.10 Assessment and Preparedness Gaps

In the Project Team's assessment, UVU personnel made some meaningful preparation efforts under compressed timelines. Event Services recognized the TPUSA Club event required major event review under Policy 425 § 3.5. The MEAC convened a meeting for the event consistent with Policy 425 §§ 3.6, 4.8.2, and 5.2.1. UVUPD also identified concerns regarding location, ticketing, crowd size, potential protest activity, and elevated access areas. Event Services subsequently provided bicycle rack barriers that TPUSA requested to help secure the area where Charlie Kirk would be speaking. Chief Long was unsuccessful in attempts to coordinate with Maycee Crofts but was able to interact with Dan Flood of TPUSA. Chief Long also contacted SIAC; arranged available UVUPD staffing; responded to concerns raised by TPUSA by clearing the Hall of Flags outdoor pedestrian walkway located above the speaker's canopy; and established a Command Post with visibility over the event area.

At the same time, the preparation process revealed several important gaps. There was limited time between Chief Long first learning of the event and the event date. The Security Assessment process did not result in documented requirements for venue modification, University-controlled ticketing, controlled access, credentialing, screening, or additional staffing. UVU did not have reliable access to ticketing or registration data. Coordination with TPUSA's security team was very limited and did not include a structured pre-event briefing or site walk-through before or on September 10 between Brian Harpole, Dan Flood, and UVUPD. Chief Long did not initiate a mutual aid request to the Orem Police Department or other local public safety partners before the event, and additional external resources were not requested after the crowd size became apparent. There also was not a dedicated assignment for real-time security video monitoring by UVUPD Dispatch personnel or others from another operational location during the event.

The primary security concern among many UVU officials appeared to be potential disruption or safety issues associated with student or non-student protest activity. That concern was reasonable given the First Amendment nature of the event, addressed in Policy 425 § 4.1.3, and UVU Policy 161. However, a broader site Security Assessment was warranted. Protest activity, crowd size, open access, line-of-sight exposure, the speaker's public profile, the external organizer's control over ticketing, and the involvement of private security all should have prompted a more comprehensive Event Action Plan and earlier coordination with public safety partners. TPUSA was the final decision maker for the event site selection, but this authority should be with the University.

In the Project Team's assessment, the preparation for September 10 reflected committed efforts by UVU personnel but also demonstrated the limitations of relying on informal coordination, ad hoc decision-making, and available internal staffing and equipment for a high-profile outdoor event. The event required a more structured planning process, stronger documentation of security decisions under Policy 425, earlier protective intelligence review, more formal coordination with external security and public safety partners for personnel and technology resource assistance, and a clearer process for elevating unresolved concerns to University leadership before final venue and operational decisions were accepted.

Recommendations related to the issues addressed in this section are included in Section 9.

3. Event Security Planning and Operations

The preceding section provides the main narrative of how the September 10 TPUSA event was classified, planned, staffed, and supported. The following section takes a deeper look at the specific event-security planning practices that should guide future high-profile events at UVU. These topics are introduced in the narrative above but are analyzed here in greater operational detail.

3.1 Event Security Planning and Security Assessment

Recognized Practices

For major events, the security planning process should include a documented Security Assessment that evaluates the event, speaker, venue, audience, threat environment, and operational requirements. The purpose is not to predict a specific act of violence, but to identify foreseeable conditions that could affect safety, disrupt operations, or require enhanced planning.

A Security Assessment should inform decisions regarding venue selection, staffing, access control, screening, crowd management, emergency response, communications, traffic control, Command Post operations, Emergency Operations Center readiness, and coordination with external partners. For outdoor events, the assessment should also consider emergency egress routes, protest activity, arrival and departure routes, surrounding buildings, elevated vantage points, line-of-sight vulnerabilities, emergency vehicle access, security camera coverage, and staffing needs.

For major or elevated-risk events, the Security Assessment should typically inform a written Event Action Plan. The Event Action Plan translates assessment findings into operational decisions and helps ensure that responsible parties have a common understanding of staffing assignments, command structure, communications protocols, venue controls, emergency procedures, mutual aid resources, and post-event review expectations.

Event Security Planning Framework Summary

A detailed Event Security Planning Framework is included in **Appendix D.1.** The framework provides a practical tool for planning high-profile events, high-profile speakers, large gatherings, and events involving elevated security concerns. It is intended to help UVU document planning assumptions, identify resource needs, assign responsibilities, and communicate operational decisions to relevant stakeholders before the event. The framework addresses:

- Event intake and risk classification
- Threat, vulnerability, and venue assessment
- Historical research and intelligence considerations
- Stakeholder coordination and executive protection planning
- Venue selection and site-layout considerations
- Ticketing, registration, and attendance forecasting
- Staffing, post assignments, and access-control decisions
- Screening, credentialing, and restricted-area management
- Traffic, parking, perimeter, and pedestrian-flow planning
- Communications, emergency notification, and public messaging
- EOC, ICS, and Event Action Plan integration
- Mutual aid and external public safety coordination
- Pre-event briefing, day-of monitoring, and post-event review

UVU Application and Assessment

The September 10 TPUSA event presented a complex security environment. The outdoor venue requested by TPUSA was located in an open-access campus setting surrounded by adjacent buildings, elevated walkways, and multiple vantage points overlooking the event area. These physical conditions created line-of-sight concerns, high-ground vulnerabilities, complicated perimeter management, and increased the difficulty of maintaining situational awareness across the surrounding environment.

Interviews and document review indicated that concerns regarding venue selection, anticipated crowd size, and protest activity were raised during planning discussions beginning with the August 25 MEAC meeting. The Project Team's review also identified pre-event coordination activities among University stakeholders, event organizers, and UVUPD. However, the planning process did not produce a formal written Security Assessment documenting identified concerns, mitigation measures, planning assumptions, or resource requirements for the TPUSA event.

Illustration: Major Event Security Planning



The Project Team learned that a written Event Action Plan was not created for the September 10 TPUSA event. The absence of a written Security Assessment and Event Action Plan limited UVU's ability to establish a coordinated security posture among UVUPD, Event Services, TPUSA representatives, TPUSA's security detail, University stakeholders, and potential external public safety partners. It also limited the ability to document planning assumptions, identify resource gaps, assign responsibilities, and adjust the plan as attendance, protest activity, or other conditions changed.

> **The absence of a written Security Assessment and Event Action Plan limited UVU's ability to establish a coordinated security posture among UVUPD, Event Services, TPUSA representatives, TPUSA's security detail, University stakeholders, and potential external public safety partners.**

2018-2025

Historical Security Concerns Associated with TPUSA and Charlie Kirk Events

Event security planning for high-profile speakers should consider not only the specific event being planned, but also reasonably available information about comparable events. Prior events involving the same speaker, organization, venue type, audience profile, protest activity, or security concerns can provide useful context for evaluating foreseeable conditions, even when they do not predict a specific threat or outcome. Several of our interviewees stated that UVU made no inquiries with previous event sites because they were hosting the first TPUSA campus speaking event of the academic year.

For the September 10 TPUSA event, prior Charlie Kirk and TPUSA campus speaking events were relevant because they could have informed UVU's assessment of venue suitability, anticipated attendance, protest activity, access control, crowd management, staffing, communications planning, and the potential need for enhanced security measures. The examples below are not included to suggest that prior incidents predicted the violence at UVU. Rather, they illustrate that similar events at other institutions had generated protest activity, crowd-control concerns, physical confrontations, and enhanced security measures. This type of historical context should be considered as part of the Security Assessment and Event Action Plan process for major or elevated-risk events. For example, the following TPUSA events held over the last several years could have provided some useful operational considerations had they been a part of the MEAC discussion held on August 25:

- **October 23, 2018 – California State University, Long Beach:** Large-scale protests and disruptions required security intervention.
- **February 21, 2019 – UC Berkeley:** A Turning Point USA supporter was physically assaulted during campus activity associated with the organization.
- **March 14, 2023 – UC Davis:** Approximately 100 protesters gathered outside a Charlie Kirk event, blocked entrances and pathways, threw eggs and other objects, damaged venue doors, and assaulted a police officer. In anticipation of these risks, the university implemented extensive security measures including ticketing controls, identification verification, metal detectors, bag restrictions, and a significant law enforcement presence.
- **April 3, 2025 – UC Davis:** Protesters disrupted a Turning Point USA event before it began, resulting in reported assaults, physical altercations, and property damage.

Footnotes for the above incidents:[24]

[24] https://www.presstelegram.com/2018/10/24/cal-state-long-beach-conservative-meeting-prompts-protest/; https://www.foxnews.com/us/conservative-activist-assaulted-at-uc-berkeley-campus-during-recruitment-drive; UC Davis official news release; Sacramento Bee reporting; ABC10 local reporting; UC Davis statement.

Recommendations related to the issues addressed in this section are included in Section 9.

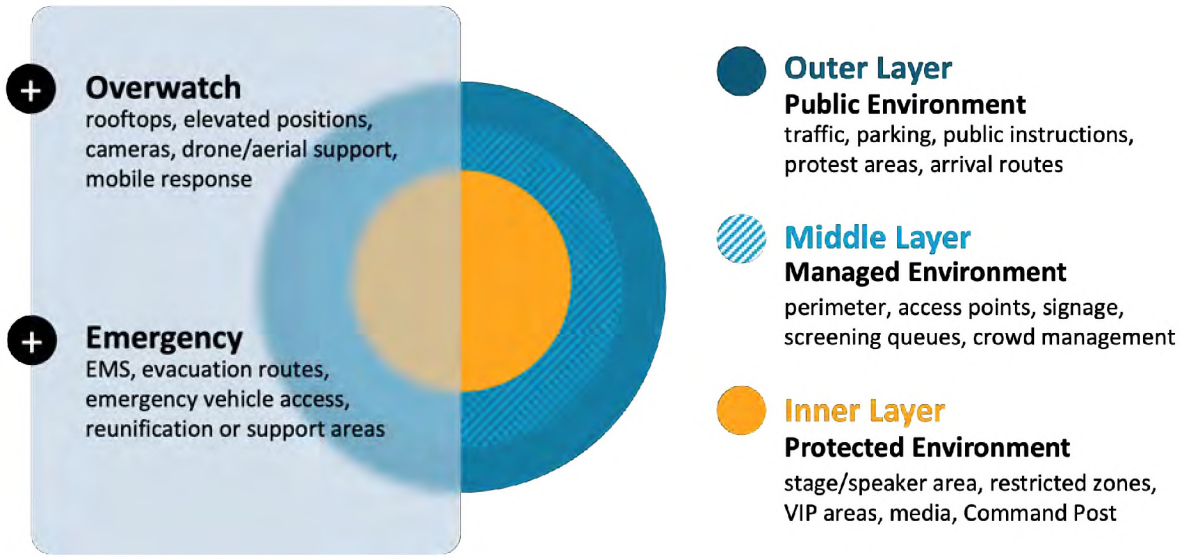
3.2 Event Security Operations

Recognized Practices

Event security operations translate planning assumptions into real-time protective measures designed to maintain safety, facilitate lawful activity, manage crowds, and support effective response if conditions change. For major or elevated-risk events, operational planning should connect Security Assessment, venue conditions, staffing, post assignments, access control, communications, executive protection coordination, emergency response procedures, and contingency planning.

A well-designed event security plan uses layered protection across the outer, middle, and inner perimeters. The outer perimeter generally encompasses public areas, the middle perimeter controls access to the event, and the inner perimeter includes the event space and restricted areas. This layered model supports deterrence, detection, delay, response, and recovery.

Illustration: The Layered Event Security Model



UVU Application and Assessment

Based on interviews, documentation, and available video evidence, UVUPD personnel were deployed throughout the event area and performed a range of security functions before, during, and after the event. Officers monitored crowd activity, supported event operations, managed protest-related concerns, and responded to emerging incidents. However, while UVUPD coordinated some security issues with event organizers just prior to the event, such as the concern of the Hall of Flags outdoor pedestrian walkway located above the speaker's canopy, no actual face-to-face contact or pre-event debriefing activities occurred between the UVUPD Police Chief or TPUSA security representatives. This represents a lost opportunity to identify and mitigate any real-time security concerns prior to the beginning of an event. UVUPD did not establish fixed or mobile security posts, which limited its visible law enforcement presence during the event.

The outdoor venue presented significant operational challenges. The event area included multiple access points, adjacent buildings, elevated walkways, open pedestrian areas, and numerous locations from which attendees, protesters, and bystanders could observe the event. These features increased the complexity of crowd management, situational awareness, perimeter security, and response operations.

Staffing decisions appear to have been made based on information available at the time. However, the absence of a formal Security Assessment, reliable attendance estimate, and written Event Action Plan limited the ability to systematically evaluate staffing needs and resource requirements. Historical incidents involving similar events may also have supported consideration of additional security measures.

The Project Team also identified the importance of clearly defining operational responsibilities and command relationships during major events. Leadership and decision-making roles, such as Incident Commander and EOC Manager need to include both primary and backup personnel. Security operations are most effective when assignments, reporting relationships, emergency procedures, communications protocols, and contingency plans are documented and briefed before the event. This provides a common operating picture and supports effective decision-making if conditions change rapidly.

Officers responded quickly following the shooting and initiated emergency response actions. The incident nevertheless demonstrated the challenges associated with managing a high-profile event in a complex, open-access environment. Future planning efforts would benefit from a more formalized process that links Security Assessments, staffing decisions, command structures, security technologies, and emergency response procedures into a unified operational framework.

For the September 10 TPUSA event, the Director of Emergency Management and Safety assigned two UVU Emergency Medical Services (EMS) personnel. Both were Emergency Medical Technicians (EMTs) trained to provide prehospital emergency medical care before patients reach a hospital. EMTs may deliver non-invasive, lifesaving interventions and help stabilize patients during emergencies. Both EMTs were equipped with trauma packs and rendered aid after the shooting, including assisting individuals who experienced trips and falls, breathing difficulty, and panic attacks during the ensuing chaos following the shooting. It is important to note that the EMTs could not transport patients, including Charlie Kirk, to the hospital. No ambulance was staged on site for the September 10 TPUSA event.

Recommendations related to the issues addressed in this section are included in Section 9.

3.3 Access Control, Screening, and Credentialing

Recognized Practices

Access control, screening, and credentialing are core components of event security planning. Together, they help define who may enter an event space, what items may be brought into the venue, which areas are restricted, how attendance is monitored, and how security personnel identify authorized individuals. Effective access-control planning integrates personnel, technology, physical barriers, written procedures, emergency management, event organizers, and coordination with law enforcement, fire, EMS, and other critical partners.

For elevated-risk events, access-control planning typically addresses whether the venue can support controlled entry, ticket verification, credentialing, screening, designated entry and exit points, restricted-access areas, and emergency egress. These decisions are influenced by the event's risk profile, venue characteristics, anticipated crowd size, speaker profile, threat environment, legal considerations, and operational capacity.

Traditional magnetometers and X-ray systems provide structured screening but require adequate staffing, training, calibration, and queue management. Emerging weapons-detection systems and video analytics may allow less-invasive screening and faster throughput, but they also raise considerations regarding reliability, legal compliance, cost, staffing, false alarm rates, privacy, and integration with law enforcement response. See **Appendix D.2: Event Screening Operations Planning Considerations** for more information.

Typical Screening Measures

Screening measures vary depending on the event and may include:

- Visual screening
- Bag checks
- Handheld metal detectors
- Walk-through magnetometers
- Video analytics for weapons detection
- X-ray screening for personal items
- Clear-bag requirements
- Express lanes for attendees without bags
- Designated lanes for medical devices or ADA-related needs
- Secondary screening procedures

Because Utah law places specific limits on how public institutions may regulate firearms on campus, event access-control and screening practices must be developed with legal constraints in mind. The legal framework governing concealed carry, open carry, campus firearms restrictions, state preemption, and weapons screening is addressed in ***Section 8: Legal Considerations****. This section focuses on the operational planning implications, including how firearms laws affect access control, screening, staffing, signage, communications, and emergency response planning.*

Permitted and prohibited-items policies, when legally permissible and operationally appropriate, are also part of effective event planning. Clear pre-event communication helps attendees understand screening procedures, bag restrictions, prohibited items, and conditions of entry before they arrive. Signage, ticketing language, event websites, social media, and pre-event communications can all be used to reduce confusion and improve compliance at entry points.

Ticketing and credentialing are security tools, not merely administrative functions. Ticketing systems support attendance projections, crowd-density planning, occupancy management, staffing decisions, emergency planning, and access-control operations. For major events, attendance projections and real-time registration data can help determine whether the selected venue remains appropriate, whether additional staffing or mutual aid is needed, whether access-control measures are required, whether

Operational Value of Ticketing Data

- Attendance forecasting
- Venue capacity management
- Crowd-density planning
- Staffing decisions
- Emergency planning
- Access-control operations
- Real-time attendance reporting
- Life-safety compliance

emergency departure routes are sufficient, and whether the Emergency Operations Center or Command Post should be activated or staffed in advance.[25]

Credentialing provides an additional layer of access control by allowing event planners to differentiate public areas, restricted areas, controlled-access zones, VIP areas, media areas, technical areas, Command Posts, vendor areas, and other secure locations. Credentials may include staff badges, contractor passes, media credentials, law enforcement or emergency responder credentials, VIP passes, digital tickets, parking passes, or other event-specific identifiers. See **Appendix D.3: Access Control, Ticketing, and Credentialing Considerations** for more information.

Post coverage and personnel deployment are also fundamental to access-control operations. Event security plans typically identify where security personnel will be assigned, define the purpose of each post, establish supervisory responsibilities, and document how personnel will communicate and respond to incidents. Depending on the size and complexity of the event, post assignments may include entrances, exits, checkpoints, crowd-management positions, stage and VIP areas, perimeter locations, rooftops, roving patrols, command posts, arrival and departure areas, parking operations, and emergency response resources.

Common Event Security Posts and Functions

- Supervisory posts
- Access-control and screening posts
- Crowd-management posts
- Stage and VIP protection posts
- Perimeter security posts
- Roving patrol posts
- Parking and traffic posts
- Command-post staffing
- Emergency response teams

Additional information regarding common event security posts, responsibilities, staffing considerations, and deployment models is provided in **Appendix D.4.**

UVU Application and Assessment

The September 10 TPUSA event was conducted in a largely open-access outdoor campus environment. The selected location near the large, tiered Fountain Courtyard allowed broad public access and was surrounded by adjacent buildings, elevated walkways, and multiple vantage points. These conditions made controlled entry, attendance monitoring, restricted-area management, and line-of-sight mitigation more difficult than they would have been in a more controlled venue.

Registration was managed by TPUSA through its national office rather than through UVU's ticketing system. The Project Team noted that TPUSA never issued tickets to those who registered for the event, nor did they require tickets at the actual event. As a result, UVU had limited visibility into anticipated attendance levels leading up to the event. Several individuals interviewed during this assessment indicated that uncertainty regarding expected crowd size complicated planning efforts and limited the ability to evaluate staffing requirements, venue suitability, access-control measures, emergency egress planning, Command Post and EOC readiness, and other operational considerations. The lack of reliable attendance data reduced UVU's ability to align crowd-management, staffing, emergency communications, access-control, and Event Action Plan decisions with expected turnout.

[25] https://www.academia.edu/109320797/Analysis_of_Event_Marketing_Registration_and_Ticketing_Digitalization; Online Events Ticketing Management System: A Case Study of Namboole Stadium (2023); A Study into the Aspect of Crowd Management (2025); Framework for Efficient Crowd Management with Modern Technologies (2024).

No formal attendee screening operation was established at entry points. Attendees generally accessed the event area without passing through a controlled security perimeter. No formal credentialing process was used to differentiate event participants, TPUSA personnel, University staff, vendors, media representatives, VIPs, emergency responders, or other authorized personnel. While legal and operational constraints may affect the feasibility of screening and weapons-related restrictions on public University property, the absence of controlled access points, credentialing procedures, and attendee screening reduced UVU's ability to manage entry, monitor attendance, identify unauthorized access, and enforce event-specific security protocols.

The event also presented access-control concerns beyond the immediate audience area. Before the shooting, individuals entered the Fugal Gateway Building and attempted to access an upper balcony area outside the University President's Office to observe the event. Chief Long addressed this issue and had a staff member from the Director of Emergency Management and Safety's staff posted on the second level to help prevent people from entering the stairwell and accessing the third-floor balcony area. This incident illustrated the difficulty of managing access to surrounding buildings and elevated viewing areas during an open-air campus event.

The elevated Hall of Flags outdoor pedestrian walkway above the speaker location presented another access-control issue. TPUSA Security Supervisor Dan Flood raised concerns through text messaging with Chief Long before the event about individuals being able to access the area above the canopy where Charlie Kirk would speak. On the morning of September 10 and prior to Charlie Kirk's arrival on campus, Chief Long and UVUPD personnel cleared people from the Hall of Flags outdoor pedestrian walkway, placed security tape in two locations, and assigned two sworn personnel to the area to maintain compliance. This action addressed a visible and immediate access concern, but it also demonstrated the need for more formal pre-event identification of restricted areas, post assignments, and access-control responsibilities.

The absence of a written access-control, screening, credentialing, and post-coverage plan limited the ability to document how public areas, restricted areas, elevated positions, building access points, command-post access, media areas, staff areas, VIP areas, and emergency response routes would be managed. It also limited the ability to define responsibilities for entry management, exception handling, late entry, re-entry, restricted-area enforcement, suspicious activity reporting, and escalation to law enforcement.

The September 10 TPUSA event presented access-control challenges that were foreseeable given the outdoor location, open campus environment, political nature of the event, protest concerns, external organizer involvement, and presence of a private security team. UVU personnel took practical steps to address access concerns as they emerged, including clearing the elevated Hall of Flags outdoor pedestrian walkway and limiting access to the third-floor balcony area. However, those actions occurred without the benefit of a comprehensive written access-control and credentialing plan developed before the event.

Recommendations related to the issues addressed in this section are included in Section 9.

3.4 Protective Operations and Line-of-Sight Planning for Outdoor Events

Recognized Practices

Outdoor events, public speaking engagements, rallies, concerts, and other open-air gatherings present unique security challenges, particularly when the event involves a high-profile speaker. Protective operations for these events require attention not only to the event site itself, but also to the surrounding environment. Relevant considerations include line-of-sight exposure, elevated positions, adjacent buildings, windows, rooftops, balconies, elevated walkways, parking structures, tree lines, arrival and departure routes, crowd placement, protest activity, emergency access, and the ability of law enforcement and security personnel to control or monitor areas that may affect event security.

For high-profile outdoor events, recognized practices include conducting a site-specific Security Assessment before approving or finalizing the event location. This assessment typically evaluates the proposed stage or speaking location, backstage or support areas, audience areas, approach routes, egress routes, secure perimeter, elevated positions, adjacent buildings, rooftops, balconies, windows, elevated walkways, parking structures, tree lines, and other areas that may overlook or provide access to the event site.

Protective operations planning also includes direct coordination among event organizers, campus police, emergency management, local law enforcement, and any private security or executive protection detail assigned to the speaker or VIP. While campus police are not expected to function as the speaker's private protective detail, campus police and event planners need sufficient executive protection awareness to evaluate site conditions, identify vulnerabilities, coordinate movement, clarify roles, and support emergency response. Pre-event briefings and walk-throughs allow stakeholders to evaluate the venue together, identify vulnerabilities, clarify responsibilities, and determine whether mitigation measures are sufficient or whether the event should be relocated to a more controllable environment.

When an outdoor location presents significant exposure, the planning process should include a documented review of mitigation options. These may include controlling access to buildings, rooftops, balconies, windows, elevated walkways, and other observation points; assigning fixed posts; maintaining mobile response capacity; designating protest areas; protecting arrival and departure routes; preserving emergency access and egress; establishing medical contingency plans; identifying emergency movement routes; and coordinating support from external law enforcement partners.

Protective intelligence is also part of this planning process. The speaker's profile, prior event history, associated protest activity, publicly available rhetoric, known threats, concerning communications, and information from law enforcement or fusion center partners can inform decisions regarding venue suitability, staffing numbers, post locations, incident response capacity, building access, protest locations, emergency preparedness, mutual aid support, indoor relocation, or other protective measures.

> **For high-profile events involving a private security or executive protection detail, coordination should occur early enough to influence site selection, staging, crowd configuration, staffing, communications, emergency response procedures, and the Event Action Plan.**

For high-profile events involving a private security or executive protection detail, coordination should occur early enough to influence site selection, staging, crowd configuration, staffing, communications, emergency response procedures, and the Event Action Plan. Protective details can provide important information regarding the speaker's threat environment, movement preferences, arrival and departure needs, known concerns from prior events, and protective expectations. Event security planning should integrate, as appropriate, the resources and information available from the event organizer, the protective detail, UVUPD, emergency management, and external public safety partners.

UVU Application and Assessment

The September 10 TPUSA event was held in an outdoor, open-access campus location near the large, tiered Fountain Courtyard. The venue was surrounded by adjacent buildings, elevated areas, and the Hall of Flags outdoor pedestrian walkway above the canopy where Charlie Kirk was scheduled to speak. These conditions created line-of-sight and elevated-position concerns that were directly relevant to protective operations planning.

As discussed in Section 2, UVU participants raised concerns during the MEAC process regarding the controllability of the requested outdoor location and suggested an alternative location where access could be more effectively managed. The event ultimately proceeded in the Fountain Courtyard, as requested by TPUSA. In our assessment, that decision increased the importance of conducting a documented line-of-sight assessment, identifying elevated positions, assigning fixed posts, documenting mitigation measures, and coordinating protective operations before the event.

The elevated Hall of Flags outdoor pedestrian walkway above the speaking area became a specific security concern before the event. TPUSA Security Supervisor Dan Flood raised this concern with Chief Long on September 8, and UVUPD personnel promptly cleared, taped off, and assigned two UVUPD officers to the walkway shortly before the event began. This action addressed an immediate and visible vulnerability, but it occurred without the benefit of a documented Security Assessment or Event Action Plan developed before the event.

The selected location also presented broader environmental concerns beyond the elevated Hall of Flags outdoor pedestrian walkway. The surrounding buildings, elevated vantage points, open pedestrian areas, and multiple access routes made it difficult to fully control or monitor the event environment. These conditions affected line-of-sight planning, crowd placement, protest management, emergency access, and the ability to identify and control restricted or sensitive areas before the event began.

Coordination with TPUSA's security team was also limited. UVUPD, TPUSA's security team, emergency management, and event organizers did not conduct a formal pre-event briefing and walk-through focused on line-of-sight concerns, elevated positions, arrival and departure routes, building access, communications, emergency response, staffing, emergency egress, medical contingencies, post assignments, and responsibility for specific security functions. If local law enforcement or other external public safety agencies are asked to support future events, those agencies should also participate in pre-event briefings and walk-throughs.

Event-related protective intelligence was another relevant planning consideration. Prior incidents involving similar speakers or organizations did not predict violence at UVU, but they provided relevant information regarding protest activity, crowd-control issues, disruption, and security measures used at other institutions. That information could have supported a more structured discussion of venue

suitability, staffing, access control, protest management, screening, mutual aid, and other protective measures.

In our assessment, UVU personnel recognized and responded to some protective operations concerns, particularly the elevated Hall of Flags outdoor pedestrian walkway. However, the planning process did not produce a Security Assessment documenting line-of-sight concerns, a formal Event Action Plan providing specific protective operations measures, or a structured coordination process among the speaker's security team, UVUPD, emergency management, event organizers, and external law enforcement partners before the event. For future high-profile outdoor events, UVU would benefit from a more formal process for identifying line-of-sight concerns, advising University leadership and event organizers of protective operations issues, documenting mitigation options, and determining whether an outdoor venue remains appropriate. See **Appendix D.5: Protective Operations Considerations for Outdoor Events** for more information.

Recommendations related to the issues addressed in this section are included in Section 9.

3.5 Traffic, Parking, and Perimeter Management

Recognized Practices

Traffic, parking, and perimeter management are important components of event security planning, particularly for outdoor events, large gatherings, and events involving high-profile speakers or elevated security concerns. These functions support attendee safety, emergency response access, crowd movement, and overall site control.

For major events, planning typically addresses how attendees, participants, vendors, emergency responders, and event staff will arrive, move through the area, park, access the venue, and depart. Traffic and parking plans also help identify where pedestrians and vehicles may intersect, how emergency vehicles will reach the event site, and what conditions may require law enforcement, parking, transportation, or mutual aid support.

Parking areas are part of the event security environment. They are often the first and last points of interaction attendees have with an event and may present opportunities for criminal activity, suspicious behavior, unattended property, traffic congestion, or emergency incidents. Parking operations should therefore be considered as part of the event's broader security and Event Action Plan.

Perimeter management helps define the event boundary, direct pedestrian movement, support access-control operations, and protect emergency access routes. Depending on the venue, risk environment, and event layout, perimeter measures may include physical barriers, staffed posts, signage, vehicle-control points, or other controls designed to manage movement and reduce unauthorized access.

Emergency departure planning is also important. During a fast-moving incident, attendees, students, faculty, staff, and visitors may need clear instructions regarding which areas to avoid, which routes are available, and how to leave campus safely. These decisions are most effective when identified before the event and coordinated with Dispatch, the EOC, Communications, UVUPD, parking personnel, and public safety partners.

UVU Application and Assessment

The September 10 TPUSA event was held in an open outdoor area on an active campus, near campus buildings, pedestrian routes, parking areas, and public access points. These conditions made traffic, parking, pedestrian movement, emergency vehicle access, and perimeter management important operational considerations.

Parking and vehicle access were discussed primarily in relation to TPUSA's request for parking close to the canopy location. The available information does not reflect a broader documented traffic, parking, or perimeter plan tied to anticipated attendance, pedestrian flow, protest activity, emergency access, pre-event arrival, post-event departure, or first responder movement.

UVU also had limited visibility into anticipated attendance because TPUSA managed ticketing through its national office and did not share anticipated attendee numbers, which limited UVU's ability to forecast vehicle volume, pedestrian movement, parking demand, crowd-density patterns, and departure needs. It also made it more difficult to determine whether additional traffic-control, parking, perimeter, or mutual aid resources were needed before the event.

Traffic, Parking, and Perimeter Considerations

- Arrival and departure routes
- Emergency vehicle access
- Parking-lot capacity and overflow plans
- Shuttle and rideshare operations
- Pedestrian and vehicle interaction points
- Parking security and patrols
- Road closures and traffic control
- Perimeter barriers and access points
- Signage and wayfinding
- Emergency evacuation routes

Additional information is provided in **Appendix D.6: Traffic, Parking, and Perimeter Security Considerations**.

The open-access location further complicated perimeter management. Attendees generally accessed the event area without passing through a controlled security perimeter, and no formal screening or credentialing perimeter was established. These conditions limited UVU's ability to define the event boundary, manage access routes, monitor attendance, and establish controlled operational zones.

The incident also underscored the importance of emergency departure planning. During a fast-moving incident, emergency messages may need to direct people to avoid certain areas, leave by designated routes, remain away from specific roads or buildings, or wait for law enforcement direction. Pre-identified departure routes and traffic-control assumptions would have supported more informed emergency communications and EOC decision-making.

In our assessment, the event would have benefited from a documented traffic, parking, and perimeter plan. Such a plan would have helped identify vehicle routes, pedestrian routes, emergency access points, restricted areas, staff or VIP parking, protest areas, signage needs, departure routes, and conditions requiring assistance from local public safety partners.

Recommendations related to the issues addressed in this section are included in Section 9.

3.6 Fixed and Temporary Site Security Measures

Recognized Practices

Fixed and temporary site security measures help control movement, define event boundaries, protect pedestrian areas, support screening operations, reduce unauthorized access, and preserve emergency access and egress. These measures are selected based on the event's risk profile, venue characteristics, crowd size, traffic patterns, pedestrian flow, and emergency response needs.

For outdoor events, common measures include temporary fencing, gates, barricades, stanchions, signage, concrete barriers, water-filled barriers, vehicles, planters, bollards, and other physical controls. These measures can help establish event perimeters, guide pedestrian movement, limit vehicle access, protect screening areas, create buffer zones, and distinguish public spaces from restricted or controlled areas.

When roads, vehicle routes, parking lots, or public access points remain open near an event site, physical controls are typically evaluated in connection with staffing, traffic management, emergency vehicle access, and law enforcement support. Temporary barriers are most effective when they are incorporated into a broader security plan that identifies who will staff, monitor, inspect, and adjust them as conditions change.

Site security measures also support screening and access-control operations. When screening is used, planning accounts for queueing areas, screening tables, lighting, signage, secondary screening locations, express lanes, ADA or medical-device lanes, staff or participant lanes, vendor and delivery access, and backup procedures if equipment fails or crowd conditions change. Detailed screening considerations are addressed in Section 3.3. And additional information is provided in **Appendix D.7: Fixed and Temporary Site Security Measures.**

UVU Application and Assessment

The September 10 TPUSA event occurred in a largely open-access outdoor environment. The Project Team learned that UVUPD did not establish a comprehensive physical perimeter around the event area, use temporary fencing or barricades to define controlled entry points, or create a screening area through fixed or temporary site security measures. Bicycle racks placed to help secure the area near the speaker's canopy were the only barriers used on September 10, but they were not intended to be used as entry- and exit-point controls. Immediately after the shooting, the crowd knocked down the racks by running towards the canopy area and away from where the assailant was located.

The most notable temporary control measure used before the event was security tape placed on the elevated Hall of Flags outdoor pedestrian walkway along with two UVUPD officers posted above the canopy where Charlie Kirk would speak. This measure helped restrict access to the area directly above the speaker location after TPUSA raised concerns about that location. While this was a practical response to an immediate access concern, it also reflected a reactive measure rather than a documented site-security plan developed before the event.

The open nature of the event site also affected nearby buildings. Individuals entered the Fugal Gateway Building and attempted to access an upper balcony area overlooking the event. UVU personnel took steps to limit access to that area, but the issue illustrates the importance of incorporating adjacent

buildings, stairwells, balconies, rooftops, and other elevated viewing areas into site-security planning for outdoor events.

No attendee screening operation was conducted at entry points, and non-ticketed attendees generally accessed the event area without passing through a controlled security perimeter. No formal credentialing process was used to distinguish staff, vendors, media, VIPs, private security personnel, emergency responders, or other controlled-access groups. While legal and operational factors may affect what measures are feasible on public University property, the absence of defined site-security controls reduced UVU's ability to manage movement, control restricted areas, support screening, and maintain a clear event boundary.

In the Project Team's assessment, UVUPD personnel addressed specific access concerns as they emerged, including the elevated Hall of Flags outdoor pedestrian walkway and access to an upper balcony area. However, the event was not supported by a documented site-security plan that identified physical controls, staffing responsibilities, perimeter boundaries, screening-support measures, adjacent building controls, emergency routes, or backup measures before the event began.

Recommendations related to the issues addressed in this section are included in Section 9.

4. Incident Command, Emergency Management, and Emergency Response Implementation

Section 1 describes the policies, plans, and preparedness framework that existed before September 10. Section 2 summarizes planning, security, response, and coordination related to the September 10 TPUSA event. Section 3 addresses event security planning and operations. This section focuses on how specific emergency management systems were applied in practice on September 10 and where implementation could be strengthened for future major events and critical incidents.

Emergency management systems are most effective when written plans, command structures, communications procedures, resource coordination, and decision-making processes are understood before an incident and applied consistently during an incident. In a university environment, these systems must account for students, employees, visitors, academic operations, public events, media attention, outside public safety agencies, legal considerations, and senior leadership decision-making.

4.1 Application of ICS and Event Action Planning

Recognized Practices

Incident Command System (ICS) principles provide a scalable structure for managing both planned events and emergency incidents. In a university setting, ICS helps clarify event objectives, command roles, operational assignments, communications procedures, resource needs, contingency plans, and coordination responsibilities among campus police, emergency management, University leadership, fire and EMS, communications personnel, facilities, student affairs, partner law enforcement agencies, and external event organizers.

For major or elevated-risk events, an Event Action Plan or similar operational document is a practical way to apply ICS principles before the event occurs. An Event Action Plan may document event objectives, staffing assignments, command structure, communications procedures, access-control measures, contingency plans, mutual aid resources, and post-event review expectations. The purpose is not to create unnecessary administrative burden, but to ensure that key assumptions, decisions, roles, and resource needs are identified and documented before the event.

Event Action Plans are particularly useful when an event involves one or more of the following conditions:

- A high-profile or controversial speaker
- Anticipated protest or counter-protest activity
- A large or uncertain crowd size
- An outdoor venue with open access or elevated-position concerns
- An external organizer or private security team
- Multiple university departments with operational responsibilities
- A need for law enforcement, fire, EMS, or emergency management coordination
- Potential need for mutual aid or specialized resources
- Significant media, public, or government attention
- An elevated risk environment based on a credible threat(s)

The following is an example of a standard Incident Command System (ICS) organizational chart based on models FEMA provides to agencies across the nation. Additional information regarding commonly used ICS command and general staff positions is provided in **Appendix B: Incident Command System Roles and Responsibilities.**

Illustration: FEMA ICS Organizational Chart[26]



UVU Application and Assessment

UVUPD Policy 429, First Amendment Assemblies, is particularly relevant to the assessment because it addresses the use of ICS principles for both planned and unplanned UVU events. The policy states that ICS should be established when resources are deployed for unplanned events and that ICS should be considered for planned events, including the development of incident-specific operational plans when appropriate.

Basic planning and coordination occurred before the September 10 TPUSA event. The Major Events Assessment Committee (MEAC) convened on August 25 via Microsoft Teams, during which University and UVUPD stakeholders discussed the event and engaged with TPUSA representative Maycee Crofts. On September 3, Chief Long received a call from Dan Flood, TPUSA Security Supervisor. Chief Long asked Flood what was needed by TPUSA from the UVU police. Later on September 3, Chief Long called Flood again to ask whether the event was ticketed. Flood confirmed that TPUSA's national office in Phoenix was handling ticketing so TPUSA could gauge how many people planned to attend. Chief Long did not ask Flood about updated ticketing numbers, nor did Flood offer any information about crowd estimates from TPUSA's ticketing process at that time. On September 8 and 10, Chief Long coordinated directly with TPUSA Security Supervisor Dan Flood by text.

[26] Retrieved from https://emilms.fema.gov/is_0552/groups/51.html.

Unlike other major events, such as previous commencement activities or concerts, no formal written Event Action Plan or incident-specific ICS planning document was developed for the September 10 TPUSA event. This was significant because the event involved political activity, a high-profile speaker, expected protest activity, an outdoor open-access venue, uncertain attendance, a private security team, and multiple operational concerns involving access control, line-of-sight exposure, staffing, communications, and emergency response.

The absence of a written operational plan limited the opportunity to formally document planning assumptions, resource requirements, assignments, communications procedures, contingency plans, mutual aid thresholds, and real-time monitoring responsibilities. It also limited UVU's ability to create a shared written record of decisions regarding the selected outdoor venue, attendance uncertainty, protest activity, line-of-sight concerns, high-ground vulnerability, TPUSA security coordination, security-post assignments, and the role of external public safety partners.

The lack of a written Event Action Plan did not mean that planning was absent. Chief Long and other UVU personnel took practical steps to prepare for the event, including attempting to identify TPUSA security contacts; contacting SIAC; arranging available UVUPD staffing; responding to TPUSA concerns regarding the Hall of Flags outdoor pedestrian walkway; clearing, taping off, and posting two UVUPD officers at the Hall of Flags outdoor pedestrian walkway above the speaker location; and establishing a Command Post in Room 204 of the Fugal Gateway Building. However, these efforts were not captured in a formal Event Action Plan that assigned responsibilities, identified resource gaps, clarified command relationships, or established escalation thresholds before the event began.

In our assessment, the September 10 TPUSA event illustrates the operational value of using ICS and an Event Action Plan for major events before conditions deteriorate. A scalable Event Action Plan could have helped UVU document who was responsible for specific functions, how security personnel would be deployed, how information would move, when additional resources would be requested, how TPUSA's security team would be integrated, and how the University would transition from event monitoring to emergency response if conditions changed. It also might well have highlighted the need to insist that UVU determine the venue location due to security concerns, as well as insist that the UVU ticketing system be used instead of TPUSA's as part of the agreement requirements for using UVU facilities.

Recommendations related to the issues addressed in this section are included in Section 9.

4.2 Implementation of the Emergency Operations Plan and Active Assailant Protocols

Recognized Practices

An Emergency Operations Plan provides the framework for managing significant incidents. In practice, an EOP connects field response, emergency communications, EOC operations, executive decision-making, public information, resource coordination, and recovery efforts. The plan is most useful when personnel understand their roles, know when and how the plan is activated, and have practiced the procedures on a regular basis, either in training, such as a practical exercise, or under realistic conditions.

Active assailant protocols are a critical component of campus emergency preparedness. Effective protocols emphasize protection of life, rapid law enforcement response, emergency notification, lockdown or evacuation decision-making, coordination with fire and EMS, public information, reunification considerations, crime-scene preservation, and transition from immediate response to investigation and recovery.

Emergency preparedness also depends on whether students, employees, visitors, and event participants and attendees understand what actions to take during an active threat. Public education and emergency messaging should reinforce plain-language protective actions, including active assailant response; lockdown; evacuation; and shelter-in-place.

UVU Application and Assessment

UVU's Emergency Operations Plan (EOP) is comprehensive and generally aligned with recognized emergency management practices. The plan incorporates NIMS principles and establishes a framework for emergency response, resource coordination, emergency communications, executive decision-making, and recovery activities. The EOP also identifies key leadership positions, outlines Emergency Operations Center functions, and provides guidance regarding incident management, communications, resource coordination, and executive decision-making.

The University's primary guidance for managing active shooter and active-assailant incidents is contained within the EOP which establishes roles, responsibilities, response procedures, communications protocols, and coordination mechanisms for managing such incidents. The procedures were updated in October 2024 and appropriately emphasize rapid law enforcement response, emergency communications, incident command, resource coordination, and protection of life during a rapidly evolving crisis.

The September 10 incident placed significant pressure on UVU's emergency management framework. The incident involved a high-profile outdoor event, an open campus environment, uncertainty regarding suspect status, multiple responding agencies, emergency notifications, campus searches, crime-scene protection, traffic concerns, media attention, and public anxiety. These conditions required rapid coordination among Chief Long and UVUPD personnel, command post, Dispatch, the Emergency Operations Center, University leadership, communications personnel, and external public safety partners.

The incident demonstrated that even well-developed plans can be difficult to execute when personnel are managing competing operational demands, incomplete information, and rapid escalation. UVU's plan had an appropriate written foundation, but implementation depended on how quickly personnel could activate the relevant structures, understand their roles, obtain accurate information, coordinate with outside agencies, and communicate protective actions to the campus community.

The September 10 response also underscored the importance of aligning active-assailant protocols with emergency messaging. Emergency terms and instructions must be understandable to students, employees, visitors, and event participants and attendees in real time. When emergency messages use similar-sounding terms or do not provide clear protective actions to take using commonly understood language, recipients may be uncertain about whether to leave, hide, lock down, shelter, avoid an area, or wait for further instructions.

In our assessment, UVU's EOP and active-assailant protocols provide an appropriate planning foundation. The greater opportunity lies in translating those plans into practical tools, training, exercises, and plain-language emergency instructions that can be used quickly during rapidly evolving incidents.

Recommendations related to the issues addressed in this section are included in Section 9.

4.3 EOC Activation, Situational Awareness, and Decision Support

Recognized Practices

An Emergency Operations Center supports incident management by bringing together personnel, information, resources, and decision-makers in a coordinated environment. The EOC does not replace a Command Post or field command. Instead, it supports field operations by maintaining situational awareness, coordinating resources, supporting emergency communications, documenting decisions, briefing senior leadership, coordinating with external partners, and helping manage broader institutional consequences.

Effective EOC operations require clear activation criteria, defined roles, trained personnel, reliable information flow, shared situational awareness, and a common understanding of decision-making authority. During a fast-moving incident, EOC personnel need timely and verified information regarding the nature of the threat, suspect status, victim information, campus conditions, law enforcement activity, emergency notifications, building status, traffic conditions, media attention, and public safety partner activity.

For high-profile or elevated-risk events, some institutions use an EOC monitoring posture even when full activation is not required. This approach allows emergency management, communications, the Command Post, Dispatch, public safety personnel, senior administration, and Policy Group representatives to maintain awareness and transition quickly if conditions change. The Policy Group also plays an important role in communicating with governing bodies and other stakeholders as needed and supporting the emergency management and business continuity roles and responsibilities identified in the Emergency Operations Plan.

UVU Application and Assessment

UVU's Emergency Operations Plan establishes an Emergency Operations Center framework and identifies key leadership positions, EOC functions, Incident Command System principles, incident management responsibilities, communications processes, resource coordination mechanisms, and executive decision-making roles. This framework provided an important foundation for the September 10 response.

Following the shooting, UVU activated its EOC in the Fugal Gateway Trustees Conference Room and assembled EOC personnel and the University's Policy Group. EOC members responded quickly and made substantial efforts to coordinate the University's response under rapidly evolving circumstances. The activation itself reflected a prompt good-faith response to a complex emergency.

The incident also exposed several implementation challenges involving EOC leadership, succession, delegation of authority, communications coordination, law enforcement representation, and situational awareness. These challenges were not primarily the result of individual performance. Rather, they reflected the difficulty of applying written EOC procedures during a fast-moving incident when several key leaders were away from campus, participating remotely, or managing competing responsibilities.

The University's Emergency Operations Plan designates Val Peterson, Vice President of Administration and Strategic Relations, as the Emergency Operations Center Manager. At the time of the shooting, Peterson was approximately 45 minutes from campus. He joined response discussions by speakerphone while traveling to UVU and remained actively engaged. However, his delayed arrival created a period during which EOC participants expressed uncertainty regarding leadership responsibilities, decision-making authority, and message approval processes. Interviews reflected broad confidence in Peterson's abilities and qualifications but also indicated that clearer succession and delegation procedures would have supported EOC operations more effectively during the initial phase of the response.

Peterson also had competing responsibilities during the response, including communications with the Governor's Office, preparation for a joint press conference, and assistance with public statements. These responsibilities required him to divide his attention between EOC management and external communications activities at critical moments, which led him to move in and out of the EOC during the incident.

The response was also affected by the physical absence of Robin Ebmeyer, UVU's Director of Emergency Management and Safety, who was out of state at the time of the incident. Ebmeyer engaged remotely by telephone and by the Microsoft Teams online meeting platform, and she worked diligently to support EOC operations. Her remote participation was valuable, but it also created coordination challenges because she had significant familiarity with the University's Rave emergency notification system and assumed a leading role in preparing and distributing emergency messages.

During the period when both the Vice President of Administration and Strategic Relations and the Director of Emergency Management and Safety were not physically present in the EOC, some Cabinet members believed that Jim Mortensen, Vice President of Finance and Auxiliary Services, was in charge. On September 5, the UVU President issued an email and memorandum designating Mortensen as the acting administrator and authorized signatory while she was traveling on September 10. That designation had not been communicated to all Cabinet members, which contributed to uncertainty regarding Mortensen's role.

The review also identified a potential inconsistency among the Emergency Operations Plan, the Campus-Wide Emergency Communication Plan, and UVU's Green Card succession process. The Project Team learned that UVU maintains a Green Card which documents EOC members' roles, contact information, and succession process on a wallet-sized green card. The succession process identifies the order of decision-making authority if the University President is unavailable. That succession order appeared to differ from the September 5 designation of Mortensen as acting administrator and authorized signatory. At least one version of the Green Card also reportedly listed personnel who were no longer with UVU (i.e., Police Chief Matthew Pedersen). These inconsistencies can create confusion during a fast-moving incident when personnel must quickly determine who has authority to approve emergency messages, direct EOC activity, coordinate with the Policy Group, and make operational decisions.

Law enforcement command presence in the EOC was also difficult to maintain. Chief Long and the limited UVUPD personnel assigned to the event were required to manage competing operational priorities in the field and in the Command Post. As the incident unfolded, Chief Long moved among operational responsibilities, which was understandable given the circumstances. However, this limited his ability to serve as a consistent law enforcement representative within the EOC and contributed to information-sharing challenges between field operations and University leadership. Several interviewees noted that there were periods during which no UVUPD command representative was physically present in the EOC.

UVU had previously identified related issues during its January 2023 active assailant tabletop exercise. The After-Action Report identified challenges involving communication and situational awareness between the EOC and Policy Group and recommended additional and ongoing EOC and Policy Group exercises. Several similar issues resurfaced on September 10, including challenges involving situational awareness, information sharing, communications coordination, and uncertainty regarding decision-making authority. The recurrence of similar issues suggests that corrective actions from the 2023 exercise had not been fully implemented or validated before September 2025.

In our assessment, UVU's written EOC framework was an important strength, and EOC activation occurred quickly. The primary opportunities for improvement involve succession planning, delegation of authority, role clarity, communications leadership, remote-participation protocols, information-sharing procedures, corrective-action tracking, and maintaining a consistent law enforcement command representative or liaison in the EOC during major incidents.

Recommendations related to the issues addressed in this section are included in Section 9.

4.4 Interagency Coordination and Mutual Aid Implementation

Recognized Practices

Major campus incidents often exceed the capacity of a university police department or require specialized resources not maintained by the institution. Interagency coordination and mutual aid provide access to additional personnel, equipment, specialized capabilities, investigative support, fire and EMS resources, emergency management support, traffic-control resources, tactical resources, and public information coordination.

Effective interagency coordination is built before an incident by establishing formal written agreements, working relationships, joint planning, shared training, practice exercises, and clear procedures for requesting and integrating outside resources. For planned events, external resources may be needed before an emergency occurs. For critical incidents, early integration of outside agencies can support field operations, campus searches, medical response, investigation, traffic control, emergency communications, EOC operations, and public information.

During major incidents, outside agencies may arrive quickly and assume or support different operational roles. Field command, investigative command, EOC coordination, public information, and executive decision-making may evolve as the incident expands. For that reason, effective interagency coordination depends on clear liaison roles, current contact information, resource-request procedures, command-

transition protocols, and a shared understanding of how outside agencies will be integrated into University operations.

UVU Application and Assessment

Project Team interviews with UVUPD and Orem Police Department leadership indicated that strong working relationships and longstanding informal cooperation existed between the agencies before September 10. Because much of UVU's student housing population resides within Orem's jurisdiction, officers from both agencies routinely collaborate on incidents involving UVU students. Interviewees described the relationship between UVUPD and OPD as positive, collaborative, and effective.

The September 10 response demonstrated the value of those relationships. The Orem Police Department, Orem Fire Department, Utah DPS, Utah Highway Patrol, Utah County Sheriff's Office, the FBI, and other responding local agencies provided critical support during a fast-moving and highly complex incident.

Orem Police Department personnel arrived quickly and helped organize resources from other responding departments. OPD command personnel supported campus searches intended to identify any additional victims and locate any suspect or suspects. Orem Police Chief B.J. Robinson also advised that OPD and UVU had operated under an informal mutual aid understanding and that, after the incident, he had taken steps to formalize that relationship through a written mutual aid agreement.

Utah DPS Commissioner Beau Mason also acted quickly after learning of the shooting. Commissioner Mason began mustering personnel from the State Bureau of Investigation, the SIAC, and the state Crime Lab, and then traveled to UVU. He coordinated with local law enforcement leaders, Utah County Sheriff Mike Smith, state leadership, and FBI representatives as the response transitioned into a state and federal investigative joint command structure. This transition was appropriate given the seriousness of the incident, the need for specialized investigative and forensic resources, and the involvement of both state and federal law enforcement interests.

Orem Fire Department also provided important support. Chief Marc Sanderson advised that fire personnel from multiple stations responded because the extent of medical need was not yet known. Orem Fire personnel supported medical response activity, provided information over the radio regarding the vehicle transporting Charlie Kirk, sent a fire captain to the UVU Command Post, and had paramedics assist on scene with searches for potential victims needing medical assistance.

The Utah Statewide Information and Analysis Center (SIAC)

SIAC is one of 80 fusion centers located throughout the U.S. that collaborates with local and federal public safety partners to create information-sharing networks. The SIAC, like other fusion centers, works as an integral conduit to the United States intelligence community, such as the Department of Homeland Security, the Federal Bureau of Investigation, the Drug Enforcement Agency, and others.

The SIAC supports Utah law enforcement with case support, criminal information reports, and threat assessments, focusing on crimes conducted in drug and human trafficking, criminal gangs, cyber threats, terrorism, mass threats of violence, and others. In addition to analyzing threats to Utah, the SIAC is focused on providing threat management and community engagement resources across the state.

The interview with Keith Stevenson, Emergency Management Director for the City of Orem, further illustrated the availability of external emergency management support. Stevenson offered assistance shortly after the shooting and remained at the Orem Emergency Operations Center when he was not asked to respond to UVU. Orem City officials coordinated fire operations from the Orem Emergency Operations Center and remained prepared to assist if requested.

Although these relationships were valuable during the response, the Project Team identified that they were largely informal before the incident. Formal written mutual aid agreements were not in place with key public safety partners, including OPD, Utah County Sheriff's Office, and Utah DPS. Written mutual aid agreements can help define how assistance will be requested, what resources may be available, how command coordination will occur, how communications will be managed, and how specialized capabilities may be integrated into major events and emergency incidents.

This is particularly important for major-event planning. External partners may be able to provide additional sworn personnel, tactical resources, traffic-control support, fire and EMS resources, emergency management personnel, investigative support, drones, and other specialized capabilities. For example, the Orem Police Department maintains drone capability that could support situational awareness during large outdoor events when legally permissible and operationally appropriate. Greater awareness and pre-event coordination regarding this capability would allow UVU to determine whether aerial observation should be requested or included in an Event Action Plan.

The incident showed that available external resources were not fully leveraged before the event or immediately as conditions changed. UVUPD did not initiate outreach to the Orem Police Department or other local public safety partners before the event to request potential additional security resources or specialized capabilities. Similar requests were not initiated after UVUPD and other UVU officials recognized the large crowd size gathering for the event. Given the nature of the event, the open outdoor venue, uncertainty regarding attendance, line-of-sight concerns, and expected protest activity, earlier coordination with external partners could have supported a more robust security posture.

The response also demonstrated the need for defined procedures for integrating outside agencies into Command Posts, EOC operations, field command, investigative command, emergency communications, and public information functions. As local, state, and federal agencies arrived, command and investigative responsibilities evolved quickly. The rapid arrival of outside agencies created significant operational benefits, but it also underscored the importance of defined liaison roles, clear information-sharing procedures, documented command transitions, and a common understanding of how the EOC will coordinate with field command and investigative command during a major criminal incident.

In the Project Team's assessment, UVU's relationships with external public safety partners were a significant strength during the September 10 response. Those partners responded quickly and demonstrated capability and professionalism. The primary opportunities for improvement involve formalizing mutual aid agreements, establishing clearer thresholds for requesting external support before major events, defining liaison and integration procedures, maintaining resource inventories, and conducting joint exercises so external partners can be incorporated effectively into UVU's command, EOC, Command Post, communications, investigative, and public information structures.

Recommendations related to the issues addressed in this section are included in Section 9.

5. Communications, Security Technology, and Protective Intelligence

5.1 Communications and Mass Notification

Recognized Practices

Clear, timely, and accurate communications are essential during emergency incidents, particularly during active-threat, large-crowd, or fast-moving events. Effective emergency communications require reliable internal coordination, interoperable communications with external responders, pre-approved message templates, clearly defined authority, and the ability to rapidly disseminate appropriate and accurate information to multiple audiences through multiple channels.

In a university environment, emergency communications involve several overlapping audiences and functions. Campus police, Dispatch, emergency management, University leadership, event personnel, local law enforcement, fire, EMS, students, employees, visitors, and the broader campus community may all need information at the same time, but not always the same information. Internal responders often need operational detail, while students, employees, and visitors need clear protective-action instructions that can be understood quickly under stress.

Illustration: Communications and Mass Notification Example



Recognized practices include maintaining a 24/7 dispatch or communications capability; establishing internal communications protocols among police, Dispatch, emergency management, leadership, event personnel, and operational stakeholders; ensuring interoperability with external public safety partners; using plain-language emergency terminology; developing pre-approved message templates; identifying message authority and backup authority; using multiple notification channels; regularly testing

emergency notification systems; and incorporating communications planning into major-event planning, tabletop exercises, drills, after-action reviews, and emergency management training.

Emergency messages are most effective when they are concise, action-oriented, and consistent. Public protective-action messages generally need to explain what is happening, what action to take, what areas to avoid, and when additional information will be provided. Messages issued during a fast-moving incident also need to account for uncertainty. When information changes, follow-up messages should make clear whether protective actions have changed and why.

UVU Application and Assessment

UVU has several important communications and mass notification capabilities in place. The UVUPD Dispatch Center operates 24 hours a day and serves as a central communications point for campus safety operations. UVU also uses multiple mass notification tools, providing the ability to communicate with students and employees through more than one channel during emergencies.

Dispatch staffing is a significant operational consideration. UVUPD Dispatch generally operates with one dispatcher per shift. During a major incident, one dispatcher may be required to manage simultaneous responsibilities, including incoming calls for service, radio traffic, officer assignments, external communications, emergency notifications, system monitoring, and incident documentation. On September 10, a senior administrative support person in the UVUPD office assisted as a second dispatcher. That support was valuable, but it was informal and did not reflect a planned event security or emergency staffing model.

Emergency communications were among the most significant challenges identified during the September 10 response. Interviews and document review indicate that multiple individuals participated in drafting, reviewing, approving, and disseminating emergency messages. However, no single individual was clearly functioning as the designated communications lead responsible for coordinating messaging strategy, managing approvals, and ensuring timely dissemination of accurate information.

This challenge was compounded by the fact that Robin Ebmeyer, UVU's Director of Emergency Management and Safety, was out of state at the time of the incident. Although she engaged immediately and supported EOC operations remotely, her physical absence created additional coordination challenges. Because she had significant familiarity with the University's Rave emergency notification system and assumed a leading role in preparing and distributing emergency messages, communications frequently required coordination among individuals operating in different locations under significant time pressure.

EOC personnel began communicating by telephone, text message, and Microsoft Teams to coordinate response activities. The first emergency notification to the broader campus community was distributed at approximately 12:42 p.m., approximately 19 minutes after the shooting. That message advised recipients that a single shot had been fired and that a suspect was in custody. Subsequent investigation revealed that the individual initially detained was not the shooter and that the actual assailant remained unidentified and at large.

EOC personnel faced the difficult challenge of balancing speed and accuracy while responding to a highly dynamic situation. Interviews reflected substantial discussion regarding the nature of the incident, whether it should be communicated as an active assailant event, and whether the campus community should be directed to leave campus, remain where they were, or follow police instructions.

These challenges became particularly evident as subsequent notifications provided changing guidance. Messages issued at approximately 1:19 p.m. and 1:20 p.m. directed individuals to leave campus immediately, while a subsequent notification at approximately 1:36 p.m. instructed those on campus to "secure in place" until law enforcement officers could escort them safely from campus. The situation was further complicated when an incomplete active shooter template message was inadvertently transmitted at approximately 1:51 p.m. and rescinded shortly afterward.

The delays, inaccuracies, and inconsistencies in emergency communications created confusion among students, faculty, staff, and visitors and were among the most frequently cited concerns identified during interviews. Emergency messaging on September 10 also highlighted the importance of using standardized protective-action terminology that is immediately understandable and consistently tied to specific actions.

Dispatch and Mass Notification Technical Context

The UVUPD Dispatch Center operates 24 hours a day and monitors or supports campus safety, communications, and physical security systems including access control, building and room lockdown systems, cell phone communications, elevator phones, emergency power systems, fire-life-safety annunciation and control panels, hardline phones, radio communications, license plate readers, Rave, Alertus, public address systems, remote lockdown, video surveillance, visitor management, and weather alerts.

Dispatch responsibilities include:

- Receiving any incoming requests for service from the Metro Dispatch center, which handles incoming 9-1-1 calls for UVUPD and the cities of Orem, Provo and Lindon
- Documenting calls for service
- Assigning officers and supervisors to calls
- Notifying UVUPD supervisors of significant calls for service
- Bookmarking video of security-related incidents
- Notifying environmental health and safety or facilities when appropriate
- Coordinating emergency drills
- Performing radio checks
- Supporting remote access control

UVU uses Rave as a multi-platform mass notification system to communicate with students and employees during emergencies and for controlled routine messages. UVU also uses Alertus, a network-based mass notification system that can send alerts to desktops, VoIP phones, digital signage, and other IP-based devices.

Potential future technology enhancements for Dispatch may include incident reporting and case management software, real-time alerting tools, social media monitoring tools, and travel-tracking tools for university-sponsored travel or off-site programs. Evaluation of these tools would involve operational need, staffing capacity, privacy considerations, legal requirements, cost, training requirements, and integration with existing systems.

UVU has begun incorporating the **Standard Response Protocol (SRP)**[27] into its emergency management program, consistent with its recent adoption within the Utah System of Higher Education. The SRP establishes five standardized protective actions — **HOLD, SECURE, LOCKDOWN, EVACUATE, and SHELTER** — with defined purposes and corresponding instructions. Under the SRP, SECURE generally directs people to get inside and restrict access because of a threat or hazard outside, an action similar to a reverse evacuation. LOCKDOWN, by contrast, is used when there is an active or imminent violent threat requiring occupants to lock or barricade rooms, get out of sight, and take other protective measures. SHELTER is reserved for hazard-specific protective actions, such as those associated with severe weather or hazardous materials.



HOLD	SECURE	LOCKDOWN	EVACUATE	SHELTER
Stay in your room or area.	*Get or stay inside. Lock outside doors.*	*Locks, lights, out of sight.*	*Get to a safer location.*	*Pay attention to the announced hazard and instructions.*
This may be used if emergency personnel are responding to a situation that doesn't pose a threat to others in the building.	Used when the threat is outside the building or in another area of campus. Lock outside doors and stay inside until the "all clear" is announced.	Used for immediate threats - typically inside the building. Lock or barricade individual rooms, turn off lights, and stay out of sight.	An evacuation order will direct you to a safer location. That could be outside or to another area in the building.	Instructions will be based on the situation – such as an earthquake or severe weather.

The Project Team noted that UVU used the emergency terminology "secure-in-place." However, this term is not located in UVU's EOP to describe locking or barricading classrooms and offices in response to an armed or hostile intruder — actions associated with LOCKDOWN under the SRP. The use of the term "secure-in-place" created confusion for numerous recipients interviewed. In the context of the 1:36 p.m. message, the direction functioned essentially as an instruction for individuals to remain inside and limit movement until police could safely escort them from campus. The same phrase therefore had the potential to convey different protective actions depending on context.

Feedback from student leadership reinforced this concern. The UVU Student Body President, who was present in the Command Post on September 10 just before the shooting, reported frustration with what he perceived as delayed and inconsistent emergency alerts, including changes in messaging about suspect status and protective actions. When asked to review several messages sent during the incident, he indicated that students may not have understood what action was expected from certain messages, particularly the direction to "secure-in-place." His feedback suggested that some messages may have been understandable in isolation but confusing in context, especially as students were hiding,

[27] https://iloveuguys.org/The-Standard-Response-Protocol.html

attempting to leave campus, sitting in traffic, or receiving changing information about campus closure and suspect status.

UVU's transition to the SRP provides an opportunity to establish a common emergency vocabulary across emergency plans, alert templates, training, exercises, classroom materials, and public-facing guidance. Consistent use of the five SRP actions, accompanied by clear hazard-specific instructions, should reduce ambiguity and help recipients more quickly understand what they are being asked to do during an emergency.



UVU's use of multiple emergency notification tools presents both benefits and challenges. Redundancy can strengthen emergency communications when each system has a defined role, activation protocol, failover procedure, and testing process. At the same time, overlapping systems can create operational complexity, cost, administrative burden, and uncertainty if personnel are not clear on which system to use, who activates it, how messages are coordinated across platforms, or how system performance is measured. This is particularly relevant given UVU's use of Rave, Alertus, and the fire suppression system. The red, yellow, and green emergency button system is used to activate an instantaneous campus-wide emergency alert via email, text and on-campus digital signage. In addition, separate emergency buttons are located in the fire suppression system panel that personnel use to activate the audible emergency alert through the speakers located throughout the campus. UVU should also determine whether any of the other public address systems that exist on campus facilities could be included in the automated emergency notification system.

While UVU had a system in place on September 10, 2025, to issue immediate campus-wide safety alerts to students, faculty, and administrators, nineteen minutes elapsed between the shooting and the first notification issued through UVU's Rave system. The delay was attributable in part to confusion in the EOC regarding whether the incident met the criteria for the type of text notification under consideration, as well as an initial report that a suspect was in custody. The individual who had identified himself as the shooter, however, was quickly determined not to be the assailant.

This uncertainty underscores the importance of disseminating available information and protective direction as quickly as possible to those who may be in harm's way. In the immediate aftermath of an on-campus shooting, critical facts are often unknown, including whether there are additional shooters, whether the assailant has moved to another location, or whether other potential victims remain at risk. Under these circumstances, it would have been appropriate for the UVU Incident Commander to ensure immediate activation of the red Alertus Active Shooter button in the UVU Dispatch Center, which would have initiated a Rave emergency alert stating: *"UVU Alert: Shooter/Violent Aggressor on Campus. If Shooter/Violent Aggressor is near Run-Hide-Fight! For more info @ www.uvu.info. Additional messages to come."* At the same time, activation of the fire suppression system panel switch would have broadcast the pre-recorded active shooter message over the campus fire alarm speaker system: *"Attention, attention, attention: There is an active shooter on the main campus. Run if it is safe, Hide and secure your location, Fight to survive."* The Project Team understands that UVU is taking steps to establish this as the protocol going forward.

Mass notification systems also depend on accurate contact data, user participation, system reliability, and clear activation protocols. UVU should regularly encourage students and employees to update contact information and evaluate whether message delivery rates meet institutional expectations. UVU documents indicate that on September 10, 2025, the campus had a population of approximately 35,176 students and employees, excluding enrolled high school students not present on campus. System records show 31,567 users were targeted to receive RAVE text and/or email notifications representing approximately 90% of the campus population targeted by email and 67% by text.

Post September 10, UVU has significantly strengthened its RAVE alert system coverage through a targeted campaign to increase mobile phone numbers on file. Subsequent testing on November 10, 2025, showed 98% of students and 98.6% of employees were receiving text alerts.

Communications planning was also an important event-security consideration. For higher-risk or large-scale events, communications roles, radio channels, contact numbers, message authority, notification pathways, public information coordination, and backup procedures are most effective when identified before the event. For September 10, the Project Team learned that UVU had communications tools available, but communications planning was not fully integrated into a written Event Action Plan, event-specific communications plan, or pre-event briefing process.

In the Project Team's assessment, UVU had important communications capabilities in place on September 10, including 24/7 Dispatch and multiple mass-notification platforms. The primary opportunities for improvement involve planned Dispatch surge capacity, clearer communications leadership, defined message issuance authority, plain-language emergency terminology, pre-approved templates, backup approval procedures, system coordination, responder interoperability, contact-data accuracy, and integration of communications planning into major-event preparedness. See **Appendix D.8: Announcements and Scripted Response Protocol Messages** for more information.

Recommendations related to the issues addressed in this section are included in Section 9.

5.2 Physical Security Technology

Physical security technology can strengthen campus safety when systems are properly selected, maintained, integrated, monitored, and incorporated into operational planning. The value of these systems depends not only on the equipment itself, but also on how information is routed to Dispatch, field personnel, command staff, emergency management, and the Emergency Operations Center during routine operations, major events, and critical incidents. Additional technical considerations regarding access control, video surveillance, analytics, dispatch monitoring, panic and duress alarms, emergency call points, storage, and aerial observation are included in **Appendix D.9: Physical Security Technology Technical Considerations.**

Recognized Practices

Integrated Security Systems and Common Operating Picture

Physical security systems are most effective when access control, video surveillance, intrusion detection, duress alarms, panic alarms, public address systems, lockdown capabilities, and mass notification tools are connected through defined workflows. Integration allows an alarm, forced door, panic activation, or

other security events to trigger associated video, location information, mapping, and notification to the monitoring personnel responsible for incident response.

For campus environments, an integrated or unified security platform can help Dispatch and command personnel maintain a common operating picture. A single interface or coordinated set of interfaces can reduce the need to monitor multiple disconnected systems, improve response time, support incident documentation, and allow personnel to understand where an alarm occurred, what cameras are nearby, what access points are affected, and what resources should be dispatched.

These integrations can improve situational awareness, reduce the time needed to interpret alarms, and support a more coordinated response by Dispatch, field officers, the Command Post, and the Emergency Operations Center.

Access Control and Credential Management

Access-control systems support building security by limiting access to authorized individuals based on role, location, time, and operational need. Effective access-control programs include current credential records, defined approval authority, role-based access levels, timely deactivation of expired or unauthorized credentials, oversight of card issuance, and periodic audits of badge-holder information. For universities, access-control systems are most effective when they are connected to reliable Human Resources databases, student records, contractor, and visitor-management processes. These connections help ensure that access privileges change when a person's role, enrollment, employment, contractor status, or authorization changes.

Video Surveillance, Analytics, and Real-Time Monitoring

Video surveillance provides deterrence, situational awareness, investigative support, and documentation. Its operational value is strongest when camera placement is aligned with identified security concerns, event locations, access points, building entrances, parking areas, elevated positions, emergency routes, and areas where crowd activity may occur.

Video analytics can add value by identifying defined events or behaviors, such as weapons detection, perimeter crossing, unauthorized access, loitering, crowd-density changes, wrong-way movement, objects left behind, tailgating, falls, or movement in restricted areas. Virtual perimeter or video-geofencing tools may also be used to create a defined electronic boundary around a specific area and generate an alert when people or vehicles cross into or out of that area. These tools can reduce the burden on personnel when properly configured, tested, and monitored, but they require clear alert thresholds, trained users, privacy review, system maintenance, and integration with response procedures.

Dispatch Monitoring and Event Support

Dispatch is often the point where calls, alarms, radio traffic, video, access control, emergency communications, and response coordination converge. During major events or critical incidents, Dispatch may need to manage incoming calls, officer assignments, radio traffic, alarm monitoring, video review, notification systems, and documentation at the same time. Technology is most effective when Dispatch has sufficient staffing, programmed views, priority camera feeds, alarm workflows, and escalation procedures before an incident occurs.

Duress, Panic Alarm, and Emergency Call Capabilities

Duress and panic alarm systems can provide rapid notification when employees, students, visitors, or event personnel need immediate assistance. These systems may include fixed panic buttons, wireless or body-worn duress devices, emergency call boxes, or other assistance points. Their value depends on placement, reliability, monitoring, response protocols, location accuracy, training, testing, and integration with video or access-control systems where appropriate.

Aerial Observation and External Technology Support

Large outdoor events, demonstrations, and high-profile gatherings may benefit from aerial observation or other external technology support when legally permissible and operationally appropriate. Drone or aerial observation capabilities can provide situational awareness regarding crowd movement, pedestrian flow, perimeter concerns, elevated positions, and emergency response routes. If a university does not maintain this capability internally, mutual aid or interagency support may provide access to these resources.

UVU Application and Assessment

Integrated Security Systems and Common Operating Picture

UVU has multiple physical security and communications technologies in place, including access control, video surveillance, Rave, Alertus, public address capabilities, remote lockdown capabilities, radio communications, license plate readers, and other systems monitored or supported through UVUPD Dispatch. These systems provide important operational capabilities.

The Project Team identified opportunities to improve how systems work together. Some security-related technologies operate as separate systems rather than as part of a fully integrated common operating picture. When systems are not integrated, Dispatch or command personnel may need to move between platforms to understand what occurred, where it occurred, what video is associated with the event, and what response is needed. This can slow response, increase the burden on Dispatch personnel, and reduce situational awareness during fast-moving incidents.

A more integrated environment could allow alarms, forced doors, panic activations, or other defined events to call up associated video, display location information, support mapping, and assist Dispatch or command personnel in coordinating a response. This type of integration is particularly important during major events and active incidents, when multiple systems may be generating information at the same time.

Access Control and Credential Management

UVU uses an industry-recognized access-control system. Facilities or Physical Plant personnel assign access to employees, students, and contractors for specific buildings, rooms, days, and times, as well as manage activation and deactivation of access-control cards.

The access-control system provides an important foundation for managing access to campus buildings and restricted areas. The Project Team identified opportunities to strengthen governance of the access-control program, including credential audits, timely deactivation of expired or unauthorized badges, role-based access controls, oversight of card issuance, and integration with student or employee records where feasible.

Operational considerations related to when access-control systems are active were identified. Information provided during the review indicates that select access-control points may be turned off during business hours. While this may support ease of movement during normal operations, continuous access-control monitoring can strengthen awareness of doors that are forced open, held open, or accessed outside expected patterns. Decisions regarding 24-hour access-control operation should be based on building function, occupancy, security profile, operational needs, and emergency access requirements.

Video Surveillance, Analytics, and Real-Time Monitoring

UVU maintains an extensive network of security cameras throughout campus. During the September 10 TPUSA event, however, no individual had been specifically assigned to monitor camera feeds in real time for security purposes. UVUPD personnel were able to review recorded footage rapidly after the shooting to identify the suspect's apparent route of travel and obtain images of the suspect entering campus before the attack. This use of video was valuable to the post-incident investigation.

Cameras were used primarily as a post-incident investigative resource rather than as a real-time situational awareness tool. For high-profile outdoor events, active monitoring of camera feeds can support crowd management, identify suspicious activity, improve coordination of security resources, and provide earlier awareness of emerging concerns. Given the camera coverage already in place throughout campus, this represents an opportunity to leverage existing resources more effectively.

Information provided during the review indicated that video coverage does not extend to all interior and exterior areas of campus. Gaps in camera coverage can limit deterrence, delay detection, reduce available evidence, and impair response capabilities. Future camera planning should be guided by security considerations, event locations, access points, parking areas, building entrances, pedestrian pathways, elevated positions, and other priority areas.

Video analytics may also provide value for selected locations and events. For example, analytics could be configured to detect human activity on rooftops or in restricted areas, alert Dispatch when defined thresholds are met, support crowd monitoring, identify perimeter crossing in specific camera views, or create virtual boundaries around sensitive areas. These capabilities should be carefully configured and tested so alerts are meaningful, reliable, and actionable.

Dispatch Monitoring and Event Support

The UVUPD Dispatch Center operates 24 hours a day and serves as a central point for campus safety communications and system monitoring. Dispatch monitors or supports numerous campus safety and security systems, including access control, radio communications, video surveillance, emergency notification tools, public address capabilities, lockdown systems, panic alarms, and other technologies.

During major events, the volume of information available to Dispatch may exceed what a single dispatcher can reasonably monitor while also managing calls, radio traffic, officer assignments, emergency notifications, and documentation. This issue is addressed in Section 5.1, but it also has direct implications for physical security technology. Technology-enabled situational awareness depends on having trained personnel available to actively monitor relevant systems and communicate useful information to field personnel, command staff, the Command Post, and the EOC.

For the September 10 TPUSA event, UVUPD established a Command Post in a second-floor conference room within the Fugal Gateway Building. This location provided a strong vantage point over the event venue and allowed University personnel to observe much of the crowd, monitor protest activity, and maintain visual awareness of the event area before and during the incident. The selection of this location was a strength and reflected thoughtful use of an available observation point. Future major-event planning would benefit from pairing these types of physical observation points with assigned technology monitoring roles, priority camera views, and defined reporting procedures.

Duress, Panic Alarm, and Emergency Call Capabilities

UVU does not have a comprehensive interior or exterior panic alarm system. Panic alarms, duress devices, and emergency call points can provide another method for summoning assistance when a person is unable to call Dispatch directly or when a situation is escalating quickly.

These systems may be particularly useful in higher-risk public-facing offices, student service areas, event venues, parking areas, isolated exterior locations, or locations where employees regularly manage conflict, emotional distress, or volatile interactions. Their value depends on reliable location information, clear response protocols, regular testing, user training, and integration with Dispatch and video surveillance where feasible.

Aerial Observation and External Technology Support

The September 10 incident highlighted the potential value of aerial observation for large outdoor events. UVUPD did not possess unmanned aircraft systems capable of providing aerial surveillance during the event. Neighboring agencies, including the Orem Police Department, maintain drone capabilities that are available through mutual aid or interagency support arrangements.

Given UVU's campus layout, including multiple elevated vantage points overlooking major gathering areas, aerial observation may provide useful situational awareness during large outdoor events, demonstrations, and other high-profile activities when legally permissible and operationally appropriate. This capability could be incorporated into mutual aid planning, Security Assessments, and Event Action Plans for major outdoor events.

Recommendations related to the issues addressed in this section are included in Section 9.

5.3 OSINT, Web, and Social Media Monitoring

Recognized Practices

Effective campus safety, event security, and behavioral threat assessment programs increasingly rely on open-source intelligence (OSINT), web-based research, social media monitoring, and protective intelligence capabilities. These capabilities complement internal reporting, law enforcement records, behavioral threat assessment processes, event planning, and external intelligence resources.

For institutions of higher education, the purpose of these capabilities is not limited to monitoring general public sentiment or media coverage. Mature programs also include the ability to identify, assess, and monitor potential persons or groups of concern when there is a nexus to the institution, its people,

facilities, operations, or events. This may include students, former students, employees, former employees, contractors, vendors, parents, family members, visitors, online actors making threats toward the institution, or individuals who become fixated on a campus, employee, student, speaker, or event.

From a threat assessment perspective, the key issue is not whether someone is currently affiliated with the institution, but whether the individual or group may pose a potential threat to people, facilities, operations, or events associated with the institution.

Open-source and protective intelligence capabilities can help assess threatening communications, leakage[28] behaviors, grievances, fixation, target identification, escalation in rhetoric or behavior, relevant affiliations or networks, planning indicators, and other warning behaviors. These capabilities can also support event security planning by helping institutions understand the speaker profile, public discourse, protest activity, prior event history, and threat environment associated with high-profile or controversial events.

Mature programs typically establish documented procedures, trained personnel, defined workflows, legal and privacy guardrails, documentation standards, and escalation protocols for collecting, validating, analyzing, retaining, and disseminating relevant information. Information gathered through these efforts should be integrated into threat assessment, event planning, emergency management, and protective security decision-making when appropriate.

Social Listening and Subject-Focused OSINT Are Different

Social listening and media monitoring tools are useful for tracking public sentiment, media coverage, event-related discussion, reputational issues, and emerging topics of concern. These tools help institutions understand what is being said about the university, an event, or a broader issue.

Subject-focused OSINT and protective intelligence investigations serve a different purpose. They are used when a specific person, group, threat, or behavior of concern requires deeper assessment. These inquiries may involve review of publicly available online activity, prior communications, public records, litigation history, criminal justice information, affiliations, grievances, fixation, leakage, and other information relevant to assessing risk and informing intervention or protective measures.

Both functions are valuable, but they require different tools, training, procedures, documentation practices,

UVU Application and Assessment

UVU utilizes several resources to support social media monitoring, media awareness, open-source research, and intelligence collection activities. Campus Sonar serves as the University's primary social listening platform and is used to monitor publicly available online conversations, social media activity, sentiment trends, and event-related discussions.[29] During planning for the September 10 TPUSA event, Campus Sonar was used to monitor online discourse, protest activity, and public sentiment associated with the event.

---

[28] Leakage in the context of threat assessment is the communication to a third party of an intent to do harm to a target. Source: Meloy, J.R. & O'Toole, M. E. 2011. *The Concept cf Leakage on Threat Assessment*. Behavioral Sciences & the Law 29 (4), 513-517.

[29] Campus Sonar. Strategic engagement fuels fundraising. https://www.campussonar.com/our-work-uvu-fundraising?hsCtaTracking=8d2497dd-a9fb-43ca-b7b7-77dfe7ebb301%7C10a1e15f-9970-4183-aa9b-1a041bf49ae1.

The University also utilizes Sprout Social to support social media management and monitor engagement, reach, and traction associated with topics of interest to the institution. While Sprout Social contains certain social listening capabilities, Campus Sonar remains the University's primary platform for monitoring online conversations and sentiment related to emerging issues and events.

University Communications personnel also utilize Meltwater to monitor traditional and online media coverage, track news reporting, and identify developing issues receiving public or media attention. Collectively, Campus Sonar, Sprout Social, and Meltwater provide UVU with meaningful visibility into media coverage, social media activity, public sentiment, and event-related discussion. [30]

These tools are valuable, but they are not designed to serve as dedicated protective intelligence or subject-focused investigative platforms. They are better suited to understanding broader conversation, public sentiment, media activity, and institutional reputation than conducting comprehensive investigations of specific persons or groups of concern.

UVUPD personnel maintain access to criminal justice databases, law enforcement records systems, and calls-for-service information through the Utah County Spillman Flex system. These resources provide valuable investigative information regarding criminal history, prior law enforcement contacts, protective orders, and other indicators relevant to threat assessment and investigative activities.

A significant strength of UVU's current intelligence capability is its relationship with the Utah SIAC. SIAC provides threat assessments, suspicious activity reporting intake, criminal intelligence support, targeted violence prevention resources, and information sharing with federal, state, and local public safety partners. The SIAC Threat Management Unit also provides training, investigative consultation, and support to multidisciplinary threat assessment and management teams. [31] Interviews indicated that SIAC serves as the University's primary source of threat-related intelligence and protective intelligence support, with Chief Long and UVUPD acting as the primary conduit for intelligence sharing and coordination.

Intelligence-related activities currently occur across several functions, including UVUPD, Marketing and Communications, the Free Speech Committee, and members of the Behavior Assessment Team (BAT). Behavioral concerns may originate from multiple sources, including faculty and staff referrals, SafeUT submissions, Title IX reports, student concerns, law enforcement contacts, and BAT referrals. Information gathered through social media monitoring, media monitoring, open-source research, law enforcement records, and SIAC coordination may be shared with stakeholders involved in threat assessment, event planning, and campus safety decision-making.

While UVU possesses several valuable intelligence-related resources, current capabilities are primarily focused on social listening, media monitoring, law enforcement intelligence, and communications awareness rather than subject-focused protective intelligence investigations. When an individual becomes the subject of a BAT assessment or threat management inquiry, there does not appear to be a formalized process, dedicated capability, or specialized platform for conducting comprehensive open-source research regarding that individual.

---

[30] Meltwater. https://www.meltwater.com/en/our-story. Accessed June 13, 2026.

[31] The Utah Statewide Information and Analysis Center. https://siac.utah.gov/threat-management/. Accessed June 1, 2026.

Open-source information is gathered on an informal and case-by-case basis, often relying upon the initiative of individual BAT members, UVUPD personnel, or other stakeholders. Responsibility for collecting, analyzing, documenting, retaining, and integrating open-source information is distributed among multiple stakeholders without a clearly defined protective intelligence function responsible for supporting elevated-risk cases, event-security planning, or targeted violence prevention efforts.

The Project Team also identified instances where social media reviews of persons of concern were conducted using personal social media accounts. Although well-intentioned, this practice introduces unnecessary operational security, privacy, documentation, and investigative integrity concerns. Threat assessment-related inquiries should be conducted using authorized, agency-managed investigative accounts or approved investigative methods, with appropriate legal, privacy, documentation, and supervisory controls.

UVU has several meaningful intelligence and monitoring resources, including Campus Sonar, Sprout Social, Meltwater, Spillman Flex, and SIAC access. These capabilities provide important awareness of public discourse, media coverage, social media activity, criminal justice information, and threat-related intelligence. However, subject-focused protective intelligence requires different procedures, training, tools, and governance than general social listening or media monitoring. The primary opportunity is to create a more structured protective intelligence capability that defines when subject-focused OSINT is needed, who is authorized to conduct it, how legal and privacy issues are reviewed, how information is documented, how findings are shared with the BAT, UVUPD, Emergency Management, Event Services, Communications, legal counsel, SIAC, or other appropriate stakeholders, and how the information informs threat assessment, event planning, and protective decision-making.

Additional technical considerations regarding OSINT governance, investigative accounts, operational security, specialized platforms, analyst qualifications, documentation, retention, and dissemination are provided in **Appendix C: OSINT and Protective Intelligence Technical Considerations**.

Recommendations related to the issues addressed in this section are included in Section 9.

5.4 Information Sharing and Protective Intelligence

Recognized Practices

Effective prevention and response to targeted violence on a higher education campus depend on timely, accurate, and actionable information sharing across institutional and external partners. Institutions are increasingly expected to integrate campus-based intelligence efforts with broader local, state, and federal information-sharing ecosystems to identify emerging threats, assess risk, and coordinate protective actions.

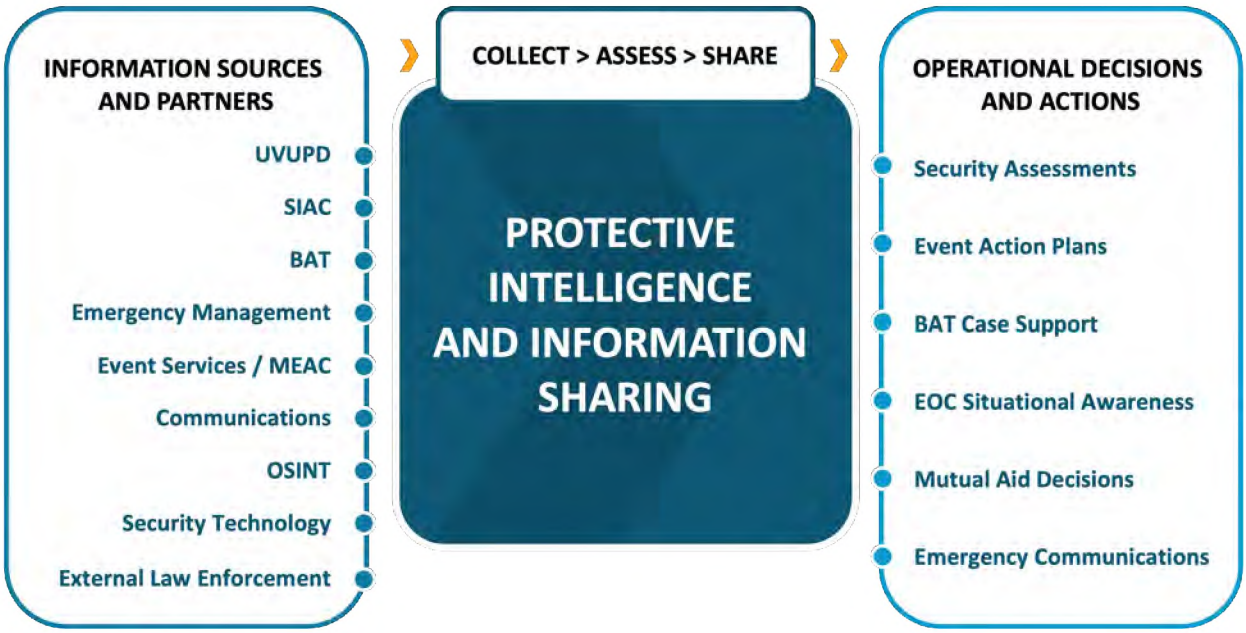
This section examines the institution's use of national platforms such as the Homeland Security Information Network (HSIN) and engagement with regional fusion centers and other intelligence-sharing mechanisms. It also evaluates the extent and effectiveness of collaboration with peer institutions, law enforcement agencies, and public-private partners to support threat awareness and mitigation.

Particular attention is given to how information is shared and operationalized before, during, and after critical incidents, including the clarity of roles, timeliness of communication, and integration of intelligence into decision-making processes. The review assesses both formal protocols and informal practices that support situational awareness and coordinated response.

Digital security considerations are also relevant to protective intelligence and event security when online activity creates risk to people, facilities, or events. For UVU, this may include monitoring for threatening online communications, doxxing or exposure of personal information, fixation on university leaders or high-profile guests, hostile event-related discourse, and online activity involving persons of concern. These issues should be distinguished from broader cybersecurity functions, such as network protection, wireless security, and system intrusion prevention, which are more appropriately addressed through UVU's information security program or a separate cybersecurity assessment.

A prime example of information sharing and protective intelligence dissemination with federal partners is the FBI InfraGard Program.[32] The Salt Lake City InfraGard Members Alliance[33] is a non-profit organization dedicated to the protection of our nation's critical infrastructure. Through a trusted partnership with the FBI, the InfraGard Program facilitates the sharing of intelligence, education, and security practices among the private and public sectors across Utah and Wyoming. Their mission is to enhance the collective security of the region and state through proactive communication and unified outreach.

Illustration: Protective Intelligence and Information Sharing Ecosystem



[32] InfraGard. Welcome to InfraGard. https://infragard.fbi.gov/

[33] Salt Lake City InfraGard Members Alliance. https://www.slcinfragard.org/

UVU Application and Assessment

The September 10 planning process illustrates the importance of documenting how threat-related information from SIAC, law enforcement partners, open-source research, event organizers, and University personnel is received, evaluated, assigned for follow-up, and incorporated into event-security decisions. When threat-related information is received before a major event, the planning record should identify what was received, who reviewed it, what follow-up occurred, whether the information was connected to the event, and whether it affected staffing, venue, access control, communications, or mutual aid decisions.

SIAC's existing intelligence and information-sharing capabilities also present an opportunity for UVU. Information provided to the Project Team indicates that SIAC uses Kaseware as part of its investigations, intelligence, and information-sharing environment. Rather than developing a wholly separate capability, UVU should explore whether and how SIAC's existing platform, analytical resources, and information-sharing workflows could support UVU's protective intelligence, suspicious activity reporting, major-event planning, and threat assessment needs.

This exploration should not be limited to technology acquisition. Any future capability should be evaluated as part of a broader governance model that addresses legal authority, privacy, data ownership, user access, auditability, information retention, investigative standards, and coordination among UVU, SIAC, UVUPD, the BAT, Emergency Management, and other appropriate stakeholders. Additional technical considerations regarding intelligence platforms, OSINT tools, and potential SIAC collaboration are included in **Appendix C: OSINT and Protective Intelligence Technical Considerations.**

Recommendations related to the issues addressed in this section are included in Section 9.

6. Behavioral Threat Assessment and Threat Management

This section addresses UVU's Behavior Assessment Team (BAT) structure, reporting and case management processes, information-sharing practices, use of open-source and protective intelligence, integration with security planning, training, intervention resources, and related institutional policies.

The Project Team notes that the BAT was not involved in the planning for, response to, or events surrounding September 10, 2025 because no internal credible threat had been identified. Accordingly, the observations and recommendations in this section are forward-looking and are intended to identify opportunities to strengthen UVU's behavioral threat assessment and management capabilities as part of its broader efforts to enhance campus safety and security.

Institutions of higher education play a critical role in identifying, assessing, and managing behaviors that may indicate an elevated risk of targeted violence or other harmful outcomes. Nationally recognized guidance from the U.S. Secret Service National Threat Assessment Center (NTAC), Federal Bureau of Investigation (FBI), National Association for Behavioral Intervention and Threat Assessment (NABITA), Association of Threat Assessment Professionals (ATAP), International Association of Campus Law Enforcement Administrators (IACLEA), and other professional organizations consistently emphasizes the importance of a formal multidisciplinary threat assessment and management capability.

Effective programs typically include:

- Clearly defined governance, authority, and operating procedures
- Multidisciplinary participation representing key institutional stakeholders
- Multiple reporting pathways and a strong reporting culture
- Structured assessment methodologies
- Centralized case management and documentation systems
- Appropriate information sharing practices
- Integration of behavioral assessment, intelligence gathering, and protective measures
- Access to mental health resources and intervention services
- Access to licensed clinical or forensic psychology expertise trained in violence risk assessment
- Ongoing training and professional development

Today's threat assessment programs focus not only on direct threats but also on patterns of concerning behavior, grievances, fixation, leakage, stalking, deterioration in functioning, and other pathway warning behaviors[34] that may precede violence.

6.1 Team Structure, Governance, and Case Management

UVU has maintained a multidisciplinary Behavior Assessment Team (BAT) for approximately 14 years and has established a mature behavioral intervention capability that aligns with many accepted higher education best practices.

[34] Reid Meloy, J. R., Hoffmann, J., Guldimann, A., & James, D. (2012). *The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology*. Behavioral Sciences & the Law, 30(3), 256–279. https://doi.org/10.1002/bsl.999.

The BAT's stated purpose is to promote the health, safety, well-being, and success of members of the university community through communication, collaboration, coordinated intervention, and case management. The BAT serves as the coordinating hub for violence prevention and early intervention efforts involving students, employees, faculty, and other members of the campus community. The BAT includes representatives from:

- Student Affairs
- UVUPD
- Employee Relations (HR)
- Student Health Services
- Accessibility Services
- Emergency Management
- Faculty
- Equity and Title IX
- General Counsel (advisory role)

UVU's BAT structure and operational model are generally consistent with accepted practices in higher education behavioral intervention and threat assessment. Interviews consistently described the BAT as a cohesive and collaborative team characterized by strong trust, open information sharing, and active participation by members. Team members emphasized the importance of relationship-building, annual training retreats, and maintaining team cohesion despite personnel turnover.

The BAT meets weekly and utilizes structured assessment methodologies, including the NABITA Risk Rubric and the U.S. Secret Service Key Investigative Questions,[35] to guide case assessment and intervention planning. Interviewees described a disciplined and methodical review process that leverages the collective expertise of the multidisciplinary team. Structured processes help institutions recognize these indicators before a crisis occurs. Without formalized processes, institutions may respond inconsistently, fail to connect fragmented information, overlook escalation, or intervene too late.[36]

Threat Assessment and Management Are Intertwined

Contemporary practice recognizes threat assessment and threat management as interdependent components of a continuous risk management process. The purpose of threat assessment is not simply to determine whether an individual presents a risk, but to inform management strategies designed to reduce risk, support the individual when possible, and protect potential targets and the broader community. The focus is prevention, not prediction.

In higher education settings, effective programs integrate behavioral assessment, information gathering, intervention planning, case management, mental health resources, employee support services, protective security measures, and ongoing monitoring. Risk is dynamic and may increase, decrease, or change over time based on evolving circumstances and interventions. Accordingly, this review evaluates both the University's assessment capabilities and its ability to implement coordinated management strategies intended to reduce risk and support members of the campus community.

[35] Fein, Robert A., Bryan Vosskuil, William S. Pollack, Randy Borum, William Modzeleski, and Marisa Reddy, *Threat Assessment in Schools: A Guide to Managing Threatening Situations and to Creating Safe School Climates* (2002).

[36] U.S. Secret Service National Threat Assessment Center. (2021). *Averting targeted school violence: A U.S. Secret Service analysis of plots against schools*; Deisinger, G., Randazzo, M., O'Neill, D., & Savage, J. (2008).

Governance Documentation

The Project Team reviewed the document entitled *Behavior Assessment Team (BAT): Behavior Intervention and Threat Assessment Utah Valley University*, which serves as the primary operating framework for the BAT. The document is comprehensive and reflects many best-practice principles related to team composition, referral processes, information sharing, assessment methodologies, intervention planning, and case management.

BAT leadership advised that the document remains in draft status because it is continually reviewed and updated to reflect evolving practices and institutional needs. While periodic review and revision are hallmarks of effective threat assessment and management programs, maintaining foundational governance documents in perpetual draft status may create ambiguity regarding institutional approval, authority, accountability, and operational expectations. Formal adoption of the document, coupled with a recurring review cycle, would provide greater clarity while preserving flexibility for future updates.

Threat Reporting, Intake, and Case Documentation

UVU has established multiple reporting pathways intended to encourage early identification and reporting of concerning behavior. Reporting mechanisms include:

- BAT online reporting portal
- EthicsPoint reporting system which includes anonymous reporting options
- "Report and Support" reporting website
- Maxient reporting form
- UVU tipline
- Direct reporting to university personnel
- UVU Police reporting channels

Interviewees reported significant increases in utilization of the "Report and Support" website, suggesting growing awareness of available reporting resources and increased willingness among UVU community members to report concerns.

The BAT utilizes Maxient as its centralized case management and documentation platform. Case files include referrals, supporting documentation, investigative information, risk assessments, intervention plans, and follow-up activities. The use of a centralized case management system supports continuity, accountability, historical review, and multidisciplinary coordination. UVU's documentation and case management practices are generally consistent with accepted higher education standards.[37]

Upon receipt of a referral, BAT members gather and review information from a variety of sources to develop a comprehensive understanding of the circumstances and behaviors of concern. Depending on the nature of the case, information may be obtained from incident reports, police reports, conduct records, prior BAT cases, faculty and staff observations, interviews with the individual of concern, family members, friends, and other relevant sources. Team members are expected to share pertinent information with the BAT and contribute relevant background information regarding cases under review.

[37] Maxient. Work Collaboratively. https://www.maxient.com/#1459304968060-3fec7f26-d472. Accessed June 6, 2026.

Following collection and review of available information, the BAT utilizes the National Association for Behavioral Intervention and Threat Assessment (NABITA) Risk Rubric — an evidence-based threat assessment tool — to assess the level of concern presented by the individual or situation and to guide appropriate intervention and management strategies. Risk determinations are documented in case records along with the factors that informed the assessment. This structured approach to information gathering, multidisciplinary review, documentation, and risk assessment is consistent with accepted higher education threat assessment and behavioral intervention practices.[38] The BAT appropriately utilizes the NABITA Rubric as a case prioritization and decision-support tool rather than as a clinical or predictive determination of future violence.

NABITA emphasizes:

- Early identification of concerning behavior
- Structured assessment of risk using evidence-based practices
- Documentation and information sharing within legal and ethical guidelines
- Development of individualized intervention and safety plans
- Ongoing monitoring until the concern has been resolved

For campus police departments and higher education institutions, NABITA's guidance complements standards from organizations such as International Association of Campus Law Enforcement Administrators (IACLEA) by focusing on behavioral intervention and multidisciplinary threat assessment rather than solely on law enforcement operations.[39]

6.2 Information Sharing, OSINT, and Protective Intelligence

Information sharing is central to effective behavioral threat assessment and threat management. Institutions are often required to evaluate fragmented information from multiple sources, including student affairs, human resources, faculty, campus police, mental health resources, conduct records, online activity, external law enforcement partners, and community reports. Effective programs rely on lawful and appropriate information sharing that allows multidisciplinary teams to identify patterns, evaluate context, and develop coordinated intervention and management strategies.

Interviews consistently described a culture of open information sharing among BAT members. Participants indicated that members trust one another and actively contribute information from their respective areas of responsibility. The BAT also benefits from strong relationships with UVUPD and external law enforcement partners, including access to information resources through the Utah SIAC.

The BAT appropriately utilizes established privacy exceptions, including the Family Educational Rights and Privacy Act (FERPA), U.S. federal law that protects the privacy of student education records, as well as health and safety provisions, when circumstances warrant information sharing for safety purposes. Team leadership demonstrated a strong understanding of the distinction between protected educational records and observable behaviors that may be relevant to safety assessments.

---

[38] Randazzo, M. R., & Plummer, E. (2009). Implementing behavioral threat assessment on campus. NABITA.

[39] National Behavioral Intervention Team Association. (2025). About NaBITA. https://www.nabita.org/

Integration of Open-Source Information

Threat assessment and management teams benefit from incorporating information from multiple sources, including institutional records, stakeholder reports, law enforcement information, and publicly available online content. Contemporary threat assessment research demonstrates that many individuals who engage in targeted violence may never communicate a direct threat. Instead, warning behaviors often emerge through grievances, fixation, leakage, stalking, target-focused communications, escalating anger, and online activity. As a result, effective threat assessment programs routinely consider both institutional information and relevant open-source information when evaluating elevated-risk cases.

Open-source research can be particularly valuable in cases involving alleged stalking, fixation, or targeted harassment. Publicly available information may help the team identify, document, and assess behavioral patterns such as repeated or escalating contact, efforts to gain physical proximity, surveillance or information gathering, use of multiple communication methods, rejection of requests to stop, threats or intimidation, underlying grievance or fixation, access to weapons, and any known history of violence or prior stalking behavior.[40] When documented and assessed appropriately, this information can strengthen risk evaluation, intervention planning, and protective decision-making.

UVU possesses several resources that support intelligence gathering and information awareness, including Campus Sonar, Sprout Social, Meltwater, law enforcement databases, and access to the Utah SIAC. These resources provide valuable visibility into media coverage, public sentiment, social media discussions, criminal justice information, and threat-related intelligence.

However, these capabilities are primarily designed to monitor broader conversations, media reporting, and institutional issues rather than conduct subject-focused protective intelligence investigations. When a specific individual becomes the focus of a BAT assessment, there is no formalized process, dedicated capability, or specialized platform for conducting comprehensive open-source investigations of that individual. Such investigations may include detailed reviews of publicly available social media activity, online communications, civil and criminal court records, litigation history, public records, prior law enforcement contacts, affiliations, and other information relevant to assessing risk and identifying warning behaviors.

Open-source information is gathered on an informal and case-by-case basis, often relying upon the initiative of individual BAT members or law enforcement personnel. Responsibility for collecting, analyzing, documenting, and integrating open-source information is distributed among multiple stakeholders without a clearly defined protective intelligence function supporting the BAT.

Although UVU's broader intelligence and OSINT capabilities are addressed elsewhere in this report, this issue is distinct because it relates specifically to subject-focused research in BAT cases. A more structured approach to subject-focused OSINT and protective intelligence investigations would strengthen risk evaluation, contextual understanding, case documentation, and intervention planning for elevated-risk individuals.

[40] Meloy, J. R., & Hoffmann, J. (Eds.). (2021). *International Handbook of Threat Assessment* (2nd ed.). Oxford University Press; Association of Threat Assessment Professionals. (2018). Risk factors for stalking and violence. ATAP.

6.3 Integration with Security Planning and Protective Measures

The BAT's primary focus is behavioral intervention, support, and conduct-related concerns rather than event security planning or protective security decision-making. This distinction is understandable from an organizational perspective. However, contemporary threat assessment and management programs increasingly emphasize the importance of connecting behavioral assessment findings to protective security planning when circumstances warrant.

The Project Team found limited evidence that threat assessment findings are routinely integrated into event security planning, security screening decisions, or other protective measures. This does not mean the BAT should become an event-security body or law enforcement operational unit. Rather, it means that when BAT cases, threat reports, or behavioral concerns intersect with major events, public gatherings, controversial or high-profile speakers, protective details, or identifiable targets, UVU would benefit from a defined process for ensuring that relevant information is shared with appropriate security, emergency management, and event-planning personnel.[41]

6.4 Training, Professional Development, and Continuous Improvement

Training represents one of the BAT's greatest strengths. The Project Team reviewed records demonstrating participation in numerous threat assessment, violence prevention, behavioral intervention, FERPA, Title IX, case management, suicide assessment, and higher education safety training programs over many years. In addition, UVU requires employees to complete annual compliance training covering topics such as:

- Workplace conduct
- FERPA
- Cybersecurity
- Free speech
- Harassment and discrimination
- Campus Security Authority responsibilities, as applicable

Importantly, completion of required training is tied to employee performance evaluations and merit pay considerations. This creates a meaningful incentive for participation and reinforces a culture of compliance and accountability.

The BAT has also demonstrated a commitment to professional development through participation in NABITA training programs, Stetson Law conferences, Utah Safety Summit programs, and other educational opportunities. While UVU's engagement with NABITA has been substantial and beneficial, the assessment identified an opportunity to broaden participation in training opportunities with external professional organizations and other subject matter experts focused specifically on threat assessment and threat management.

---

[41] Fein, R. & Vossekuil, B. (1998). *Protective Intelligence & Threat Assessment Investigations: A Guide for State and Local Law Enforcement Cjficials*. U. S. Department of Justice, Office of Justice Programs, National Institute of Justice: Washington, D.C. https://www.ojp.gov/library/publications/protective-intelligence-and-threat-assessment-investigations-guide0?

NABITA provides valuable guidance related to higher education behavioral intervention and case management. Association of Threat Assessment Professionals (ATAP)[42] — a multidisciplinary organization dedicated to threat assessment, protective intelligence, stalking, workplace violence, targeted violence prevention, and threat management — complements NABITA by providing exposure to a broader multidisciplinary community that includes law enforcement, mental health professionals, prosecutors, protective intelligence practitioners, workplace violence specialists, and threat management professionals. Participation in[43] both organizations would provide BAT members with access to emerging practices, current case studies, peer networks, and evolving threat assessment methodologies.[44]

In our assessment, UVU's investment in BAT-related training is a significant strength. Expanded participation in ATAP and similar multidisciplinary threat management organizations would supplement UVU's existing higher education-focused training and provide additional exposure to protective intelligence, stalking, workplace violence, targeted violence prevention, and threat management practices.

6.5 Intervention Resources and Related Policies

An effective threat assessment and management program depends not only on assessment capabilities, but also on access to intervention resources.[45] UVU maintains robust support services for both students and employees. Students have access to Mental Health Services that provide assessment and treatment for a variety of concerns, including anxiety, depression, trauma, grief, substance abuse, and relationship issues. Services include individual counseling, group counseling, and crisis support resources, along with free access to TimelyCare, a third-party mental health support service.

Employees have access to the Employee Assistance Program (EAP) through ComPsych, which provides counseling services, crisis support, referral services, and additional mental health resources for employees and their dependents. These resources provide the BAT with important intervention options and support prevention-focused case management strategies. They also reinforce the principle that threat assessment and management is often most effective when it incorporates support, treatment, conflict resolution, and resource referral in addition to traditional security measures. The Project Team also notes the importance of maintaining strong communication pathways between the BAT, Mental Health Services, and EAP providers when circumstances permit and legal obligations require coordination regarding safety concerns, threats, or duty-to-warn considerations.[46]

---

[42] Association of Threat Assessment Professionals. https://www.atapworldwide.org/page/desertswchapter, Accessed May 28, 2026.

[43] The BAT Chair has since joined ATAP, a positive step consistent with the Project Team's recommendation.

[44] International Association of Campus Law Enforcement Administrators. (2025). Operational readiness and threat mitigation in higher education. IACLEA; Okada, D. T., & Pollard, J. W. (2021). Community-based threat assessment and higher education. Journal of College Student Psychotherapy, 35(4), 406–417. https://doi.org/10.1080/87568225.2020.1753609; Michaelis, D. (2019). Notes from the field: The value of threat assessment teams. National Institute of Justice. National Institute of Justice.

[45] *UVU People and Culture. Benefits. EAP Program.* https://www.uvu.edu/peopleandculture/division/index.html.

[46] FBI. Making Prevention a Reality 2017. https://bn.knowledgebank.criminaljustice.ny.gov/system/files/documents/2021/06/making-prevention-a-reality-02_fbi.pdf. Accessed May 28, 2026; Utah Code § 78B-3-502.

Clinical and Forensic Psychology Consultation

One of the foundational principles of the U.S. Secret Service National Threat Assessment Center (NTAC) model is that threat assessment is a behavioral investigative process — not a mental health diagnosis or psychiatric evaluation.[47] A clinical diagnosis is a mental health condition identified by a qualified healthcare professional using established diagnostic criteria.[48] An individual is considered to be posing a threat when their behaviors, communications, or actions indicate an increased likelihood that they may engage in targeted violence or other harmful acts.[49]

Student Mental Health Services and the Employee Assistance Program provide important treatment, counseling, crisis support, and referral resources. These services are essential to a prevention-focused threat assessment and management program. However, counseling and EAP services are not the same as violence risk assessment or forensic consultation.

A licensed clinical or forensic psychologist trained in violence risk assessment can provide specialized consultation to the BAT when cases involve elevated concern, complex behavioral patterns, potential violence, stalking, fixation, return-to-campus decisions, or conditions for continued enrollment or employment. This type of expertise ensures objectivity and can help the team evaluate whether a threat appears transient or substantive, assess the likelihood of escalation, identify appropriate interventions, consider whether law enforcement involvement is warranted, and inform decisions regarding continued enrollment, employment status, campus access, or return to campus. The Project Team acknowledges that a NABITA-trained clinical mental health counselor is a member of the BAT. Access to an external evaluator is also recommended to ensure objectivity and clearly delineate the evaluator's role.

This role differs from counseling, which focuses primarily on symptom reduction, treatment, and client well-being. Threat assessment is fundamentally a risk-management and public safety function. While counseling centers and EAP providers may offer valuable support and treatment, a licensed clinical or forensic psychologist trained in violence risk assessment brings specialized expertise in evaluating threats, applying structured assessment tools, advising multidisciplinary teams, and supporting institutional decision-making.[50]

In the Project Team's assessment, UVU has strong counseling, mental health, and EAP resources, further strengthened by the presence of a NABITA-trained licensed clinical mental health counselor on the BAT. This provides the team with valuable clinical perspective and behavioral health expertise as part of its multidisciplinary assessment process. For elevated-risk or particularly complex cases, the BAT would also benefit from reliable access to an external clinical or forensic psychologist with specialized training in violence risk assessment. Such consultation can supplement the team's internal expertise by providing an independent perspective, specialized assessment capabilities, and additional support for

---

47 Fein, et al. *Threat Assessment in Schools a Guide to Managing Threatening Situations and Creating Safe School Climates.* United States Secret Service and the United States Department of Education. July 2024. https://www.ed.gov/sites/ed/files/admins/lead/safety/threatassessmentguide.pdf.

48 American Psychiatric Association. (2022). *Diagnostic and statistical manual of mental disorders* (5th ed., text rev.; DSM-5-TR). American Psychiatric Publishing.

49 National Behavioral Intervention Team Association. (2024). NABITA practice standards.

50 NABITA, Building an Individualized Threat Management Plan, notes that violence risk assessments should inform long-term threat management plans, risk mitigation strategies, and stakeholder engagement.

consequential decisions involving risk management, campus access, continued enrollment or employment, and return to campus.

Related Policies and Institutional Framework

The Project Team reviewed several policies and procedures that support UVU's violence prevention and behavioral intervention framework, including:

- Title IX Sexual Harassment Policy #162
- Discrimination and Harassment Policy #165
- Abusive Coaching Practices Policy #166
- Student Safety Intervention Protocol
- Workplace Conduct Policy #326
- Staff Grievance Policy #335
- Performance Management and Development for Full-Time Staff Employees Policy #371
- Faculty Sanction and Dismissal for Cause Policy #649

Collectively, these policies are comprehensive, well-written, and generally aligned with accepted higher education practices and applicable legal requirements. However, the BAT is referenced in only a limited number of these documents despite the broad range of behaviors routinely reviewed by the team. Greater integration of BAT referral pathways and consultation responsibilities across institutional policies would help reinforce awareness, improve reporting consistency, and strengthen multidisciplinary coordination.

In the Project Team's assessment, UVU has strong intervention resources and a supportive policy framework. The primary opportunity is to more fully connect those resources, policies, and referral pathways to the BAT's role so that community members and institutional partners understand when to consult the BAT, how to report concerns, and how multidisciplinary coordination will occur.

Recommendations related to the issues addressed in this section are included in Section 9.

7. Post-Incident Recovery, Corrective Actions, and Preparedness Enhancements

The September 10 incident required UVU to address immediate recovery needs, support affected students and employees, respond to public concern, identify lessons learned, and begin strengthening emergency preparedness systems. This section summarizes post-incident recovery measures and corrective actions initiated or proposed after the incident.

UVU and its partners took several meaningful steps after September 10, particularly in support of students, campus safety awareness, crisis communications planning, emergency preparedness training, and interagency coordination. At the same time, the Project Team identified opportunities to strengthen formal after-action processes, first responder wellness support, corrective-action tracking, and integration of post-incident lessons into sustained preparedness improvements.

7.1 Post-Incident Recovery and Community Support

Post-incident recovery is an important component of emergency management. Following a traumatic campus incident, effective recovery efforts typically include timely support for students, employees, families, first responders, dispatchers, witnesses, and others directly or indirectly affected. Recovery may involve reunification or temporary support locations, mental health resources, victim assistance services, trauma-informed communications, academic or workplace accommodations, and ongoing outreach after the immediate crisis has passed.

Following the September 10 incident, UVU and its partners took steps to support students and members of the campus community. The Alumni Building was opened as a temporary location for individuals who could not immediately leave campus or who needed a place to go, to include individuals needing transportation because their vehicles or other modes of transportation were locked down within the campus crime scene areas, and those who could not gain access to keys and other personal belongings left behind on campus as they fled the scene. The American Red Cross was contacted to support sheltering if needed, although a shelter was not activated because the need did not materialize.

Mental health support was also mobilized. UVU Mental Health Services made trained licensed therapists available to speak with students, and additional support was sought from community providers. Support included psychological first aid and post-trauma resources. Mental health support was active for approximately two weeks and then decreased as demand declined. The FBI Victim Assistance Program also became involved quickly after the incident and provided additional support resources.

These efforts reflected an appropriate recognition that students, witnesses, and other campus community members needed access to immediate and short-term support services. The involvement of UVU Mental Health Services, community providers, and the FBI Victim Assistance Program was a strength. To evaluate these efforts fully, UVU would benefit from compiling available utilization data, outreach records, after-action observations, and feedback from students, employees, and service providers regarding what support was used, what needs were unmet, and what resources may be needed in future incidents.

7.2 Support for UVUPD Personnel and First Responders



Post-incident support should include sworn personnel, dispatchers, emergency management staff, communications personnel, and other employees directly involved in the response. First responders may experience operational stress, trauma exposure, investigative constraints, public scrutiny, and difficulty decompressing after a major incident. These effects can be compounded when responders must continue working in the same environment where the incident occurred, respond to related protests or public activity, and avoid discussing investigative details while the criminal case remains active and judicial proceedings are underway.

Information provided during the review indicates that some peer-support activity occurred after the incident. However, the Project Team also identified concern that post-incident support for responding UVUPD personnel was less formalized and less visible than the support provided to students and the broader campus community. At least one responding officer described difficulty processing the incident, frustration with the absence of a formal internal department review process that could have provided some opportunity to process what personnel experienced, and a perception that institutional follow-up with officers was limited.

These observations should not be understood as criticism of any individual. Rather, they indicate that UVU's recovery framework would benefit from a more structured responder-support process after major incidents. Such a process should include timely wellness check-ins, peer support, access to confidential mental health resources, opportunities for facilitated decompression, supervisor follow-up, and a formal after-action process that allows responders to identify what worked, what was difficult, and what support is needed going forward.

In our assessment, responder support should be incorporated into UVU's post-incident recovery framework. Supporting responders is not only a wellness issue; it is also connected to employee retention, morale, operational readiness, organizational trust, and institutional learning. A comprehensive post-incident recovery plan should include the people who responded to the incident as well as the people affected by it.

7.3 Awareness, Training, and Preparedness Improvements

After the incident, UVU initiated or advanced several campus safety awareness and preparedness efforts. These efforts included updating classroom posters addressing active shooter, bomb threat, fire, medical emergency, and other emergency scenarios. UVU also developed new employee training through its learning management system focused on campus safety and active-threat preparedness. According to information provided during the review, UVU uses an active shooter training video originally developed by the University of Utah and provided for use in the Utah System of Higher Education.

UVU also continued updating emergency reference materials. The University's emergency flipchart was being updated in hard-copy and digital formats, and emergency information was being incorporated into the website and app environment. The website UVU.info was also being redesigned to improve access to emergency and campus safety information.

Additional preparedness efforts included the Building Marshal and Floor Captain program, continued training in areas such as CPR, bomb threat response, AED, Stop the Bleed, earthquake response, and civil disturbance, and more intentional campus safety tabling and outreach events. UVU has also begun transitioning to the Standard Response Protocol (SRP) terminology — HOLD, SECURE, LOCKDOWN, EVACUATE, and SHELTER — to provide more consistent and easily understood protective-action guidance across emergency communications, training, and public education. UVU personnel also described interest in developing a campus safety conference for employees and students. Collectively, these efforts reflect a recognition that students and employees want more practical information about what to do during emergencies.

The review also noted that the Utah System of Higher Education task force was evaluating a shift toward implementing *Avoid, Deny, Defend* terminology rather than *Run, Hide, Fight* for response to an active assailant incident. This type of terminology change should be incorporated carefully into training, signage, emergency messaging, and public education so students, employees, and visitors receive consistent protective-action guidance, and the Project Team notes that UVU and its Utah partner agencies are in the process of doing so. The Advanced Law Enforcement Rapid Response Training (ALERRT) Center[51] at Texas State University designed *Avoid, Deny, Defend*, and it has since been adopted and widely used by the FBI and law enforcement nationwide.



In the Project Team's assessment, UVU has made meaningful progress on emergency awareness and preparedness communications after September 10. These efforts should be sustained, measured, and tied to broader emergency management, EOC, communications, and event-planning improvements.

In the Project Team's assessment, UVU has made meaningful progress on emergency awareness and preparedness communications after September 10. These efforts should be sustained, measured, and tied to broader emergency management, EOC, communications, and event-planning improvements.

7.4 Crisis Communications Planning and Public Trust

Crisis communications planning was one of the most significant post-incident corrective actions initiated by UVU. Information provided during the review indicates that University leadership recognized the need for a more robust crisis communications framework after September 10, including clearer roles, faster message development, improved terminology, stronger media response protocols, and better coordination among Communications, UVUPD, Emergency Management, the EOC, the Policy Group, legal counsel, and senior leadership.

[51] Advanced Law Enforcement Rapid Response Training (ALERRT) Center. https://www.alerrt.org/.

The Project Team reviewed an in-progress draft of UVU's *Crisis Readiness Plan and Guidebook 2026*. The draft Guidebook is comprehensive and represents an important post-incident improvement. It establishes a crisis management framework, identifies emergency and crisis levels, addresses roles and responsibilities for life-safety alerts, includes coordination with external agencies, identifies major crisis categories, establishes media relations protocols, and includes procedures for lockdowns and post-crisis review. The inclusion of pre-drafted and legally reviewed "shelf statements" in a Digital Go Bag is also a meaningful improvement because it can help UVU communicate more quickly while verified facts are still being gathered.

As UVU finalizes the Guidebook, the University should consider cross-walking the crisis categories in the Guidebook with the broader incident categories identified in the Emergency Operations Plan and other foreseeable emergency scenarios that may require rapid institutional communication. This would help ensure that the Guidebook, Emergency Operations Plan, emergency communications templates, training materials, and operational response procedures are aligned across a full range of incidents.

UVU should also use the finalization process to clarify decision-making authority and standardize terminology across the Guidebook, Emergency Operations Plan, emergency alert templates, training materials, and public-facing instructions. The draft Guidebook appropriately emphasizes speed for life-safety alerts, but shared unilateral authority can create ambiguity if more than one person is authorized to act at the same level. UVU would benefit from identifying a primary decision-maker and designated backups for emergency notifications and crisis communications.

The Guidebook also reflects UVU's decision to use *Avoid, Deny, Defend, Aid* as its active-assailant response protocol. The University is in the process of updating its policy and protocol documents to reflect this, including the Emergency Operations Plan and related emergency management, crisis communications, training, exercise, and scripted message materials so they consistently use *Avoid, Deny, Defend, Aid* and align related terms such as "lockdown" and "shelter."

The value of the Guidebook will depend on implementation. Once finalized, UVU should train relevant personnel on the Guidebook, test it through realistic tabletop and functional exercises, integrate it with EOC procedures and emergency notification templates, and include crisis communications in after-action improvement tracking. Scenario-based exercises will be particularly important to ensure that the plan works under time pressure, with incomplete information, and during events involving competing operational, legal, reputational, and life-safety considerations.

7.5 Interagency Security and Preparedness Enhancements

Several important interagency security and preparedness enhancements were initiated or proposed after the September 10 incident. These actions are directly responsive to lessons identified during the assessment and should be sustained, formalized, and incorporated into UVU's future planning for major events and emergency response.

Commissioner Beau Mason of the Utah Department of Public Safety assigned a DPS member on the SIAC team responsibility to focus on locating and analyzing available information associated with safety concerns for Utah's institutions of higher education. Commissioner Mason also requested that each Utah institution of higher education designate at least one representative to participate in a new working group intended to support regular interaction, information sharing, and coordination among

institutions. These actions represent a meaningful enhancement to statewide situational awareness and should be incorporated into UVU's ongoing threat intelligence, event-planning, and emergency management processes.

The post-incident work initiated at the state level also reflects a broader opportunity to strengthen public safety coordination across Utah's public institutions of higher education. Regular interaction among campus police leaders, emergency management personnel, SIAC, Utah DPS, and institutional representatives can support information sharing, mutual aid planning, training coordination, threat intelligence, and consistency in major-event preparedness.

Commissioner Geoffrey T. Landward of the Utah Board of Higher Education reached out in January 2026 to Chief Safety Officer Keith Squires at the University of Utah to co-lead a Utah System of Higher Education (USHE) Campus Safety Task Force. Coupled with the efforts of Utah DPS Commissioner Mason and the SIAC, this commendable Task Force effort will assist UVU and other Utah public institutions benefit from a more formal statewide public safety coordination structure that supports collaboration among campus presidents, chiefs of police, emergency managers, and state public safety partners while preserving each institution's operational autonomy. Potential functions could include coordinating policy development, sharing best practices, supporting mutual aid, facilitating joint training, aligning emergency preparedness efforts, and improving information sharing across campuses. UVU's General Counsel is actively participating as a member of the Task Force. The Project Team learned the Task Force is nearing the completion of its initial work and will be releasing a report in the very near future.

IACLEA Accreditation

The International Association of Campus Law Enforcement Administrators (IACLEA) provides training, research, policy guidance, conferences, accreditation standards, and professional resources specifically focused on higher education public safety. IACLEA membership connects campus police leaders to a broad network of public safety professionals serving colleges and universities and provides access to emerging practices in campus safety, emergency preparedness, law enforcement operations, and community engagement.

IACLEA accreditation provides an externally validated framework for assessing campus police policies, operations, training, administration, accountability, and continuous improvement. Unlike general law enforcement accreditation programs, IACLEA standards are specifically designed for college and university environments. For UVU, pursuing IACLEA accreditation would provide a structured process for evaluating UVUPD against nationally recognized campus public safety standards, strengthening policy consistency, supporting risk management, improving operational effectiveness, and reinforcing trust with students, employees, parents, governing boards, and public safety partners.

IACLEA accreditation is not simply a one-time credential. The accreditation process requires documentation, compliance review, independent assessment, and periodic reassessment. This creates an ongoing mechanism for professional accountability and continuous improvement.

Chief Brian Redd of the Salt Lake City Police Department announced in March 2026 that his department is currently in the process of creating a Real-Time Crime Center to assist the department to leverage

new technologies that will enhance data integration and analysis capacities which, in turn, will help to improve situational awareness, improve response times, and enhance criminal case investigation effectiveness and social media monitoring. University of Utah Chief Safety Officer Squires advised he has already committed two University of Utah DPS staff members to join in the efforts of this center on a full-time basis. This promising move stands to assist not only both of their own departments to collaborate more effectively in their efforts to provide for public safety in Salt Lake City and at the University of Utah but also has the potential to provide an additional criminal intelligence resource for institutions of higher education throughout Utah.

The City of Orem Police Chief B.J. Robinson advised that OPD and UVU have taken steps to formalize their existing informal mutual aid relationship through a written mutual aid agreement. This agreement should define roles, request procedures, command coordination, resource sharing, specialized capabilities, communications expectations, cost-recovery protocols, and support for major events and emergency incidents.

OPD's aerial drone capability should also be considered as part of future event planning when appropriate and legally permissible. Chief Robinson advised that OPD would have provided drone support had the resource been requested and had OPD known more in advance about event details, including the specific location of the event. Future event planning should include early identification of specialized resources available from partner agencies, including drones, tactical teams, traffic-control assets, fire and EMS staging, emergency management personnel, and investigative support.

Orem Fire Chief Marc Sanderson advised that he had spoken with Chief Robinson about approaching UVU to conduct a joint active shooter training exercise. This proposed exercise should include UVUPD, OPD, Orem Fire, Orem Emergency Management, and other appropriate local partners. It should test the Incident Command System, unified command, emergency medical response, victim search and rescue, building sweeps, emergency communications, Command Post operations, Emergency Operations Center coordination, traffic control, and public information coordination.

Orem Emergency Management Director Keith Stevenson also advised that his office is willing to assist UVU with future emergency management policy development, training, and preparedness efforts. UVU should actively incorporate Orem Emergency Management into future planning, exercises, and after-action improvement tracking, particularly for major events with elevated security concerns or large public attendance.

As UVU continues post-incident preparedness enhancements, it should also consider whether no-cost CISA resources could support physical security review, cybersecurity preparedness, tabletop exercises, targeted violence prevention, and broader campus resilience planning.

In the Project Team's assessment, these local and statewide interagency efforts are a meaningful strength and provide UVU with important opportunities to enhance its own preparedness. The opportunity is not only to monitor these efforts, but to participate in them proactively, as UVU's General Counsel is doing, identify other appropriate UVU representatives who should become engaged as recommendations are ultimately being implemented statewide, and incorporate relevant tools, resources, intelligence-sharing practices, and lessons learned into UVU's Security Assessments, Event Action Plans, emergency management processes, threat assessment work, mutual aid planning, and corrective-action tracking.

7.6 Post-Incident Actions Taken or Initiated

The following table summarizes key post-incident actions taken or initiated by UVU and the Project Team's assessment of those efforts.

Area	Actions Taken or Initiated	Project Team Assessment
Event Planning and MEAC	▪ Hired a Police Sergeant for Public Safety/Event Security to focus on event-security staffing. ▪ Hired an Assistant Director for Campus Event Security to support event safety planning from pre-event risk assessment through post-event review; the Assistant Director supervises three part-time employees. ▪ Elevated MEAC leadership to the Associate Vice President for Student Life. ▪ Began developing a new MEAC Charter to define member roles, responsibilities, and expectations. ▪ Required MEAC members to attend SIAC training. ▪ Established a MEAC Security Subcommittee to coordinate and conduct threat and risk assessments for campus events. ▪ Developed MEAC Operating Procedures addressing Major Event identification, scheduling timelines, member roles, ticketing, security staffing, bag policies, signage, and capacity limits. ▪ Established a centralized Microsoft Team for MEAC information and documents. ▪ Created a tracking spreadsheet for MEAC event reviews and follow-up. ▪ Temporarily prohibited use of the Fountain Courtyard as an event venue. ▪ Initiated revision of Policy 425, Event Scheduling and Authorizing the Use of University Facilities. ▪ Developed a Threat and Risk Assessment tool to categorize events based on anticipated attendance and an established threat-evaluation matrix.	Substantial progress has been made in strengthening the structure, accountability, consistency, and security focus of the University's event-planning process. These actions are directly responsive to several of the principal event-planning issues identified during this review.
UVUPD Staffing and Event Security Resources	▪ Hired two additional police officers and is in the process of hiring six more. ▪ Increased police support from partner agencies following September 10, with the additional support reduced over time as appropriate.	These actions represent meaningful steps toward increasing UVUPD operational capacity and addressing staffing and Dispatch limitations

Area	Actions Taken or Initiated	Project Team Assessment
	▪ Improved event-response capability by assigning trained personnel to serve as a second dispatcher during events requiring expanded coverage.	identified during the review. The addition of dedicated event-security positions also provides greater institutional capacity for planning and managing complex events.
Student and Community Support	▪ Opened the Alumni Building as a temporary support location and contacted the Red Cross. ▪ UVU Mental Health Services, community providers, and the FBI Victim Assistance Program provided or supported services. ▪ Developed the Our Better Selves for a Better America initiative to encourage civil dialogue and constructive conflict engagement. ▪ Held two town halls for faculty and staff. ▪ Created an internal Q&A page for community questions and operational updates that reportedly received more than 8,000 views. ▪ Established a Memorial Committee.	Meaningful support was mobilized quickly for students and affected members of the University community. Subsequent outreach and engagement efforts demonstrate continued attention to recovery, communication, and strengthening constructive campus dialogue.
Emergency Awareness and Public Preparedness	▪ Initiated or expanded classroom posters, flipcharts, website and app updates, campus safety tabling, and other outreach activities. ▪ Promoted “See Something, Say Something” messaging through digital signage across campus following the incident. ▪ Began transitioning emergency guidance to the Standard Response Protocol (SRP) terminology of HOLD, SECURE, LOCKDOWN, EVACUATE, and SHELTER. ▪ Is developing uvu.edu/alert as a public location for emergency information and updates.	UVU has made strong progress in providing students and employees with more accessible, practical, and standardized information regarding emergency preparedness and protective actions. The transition to SRP terminology is an important step toward reducing ambiguity and establishing a common emergency vocabulary across the campus community.
Employee and Campus Safety Training	▪ Developed new LMS-based campus safety training. ▪ Adapted an active-threat training video for the University. ▪ Continued training in CPR, AED, Stop the Bleed, bomb-threat response, earthquake response, and civil disturbance.	These efforts reflect positive momentum toward expanding practical safety and preparedness education following the incident and increasing awareness of both emergency response and event-security responsibilities.

Area	Actions Taken or Initiated	Project Team Assessment
	▪ Retained security consultants to provide employee and student training in December 2025. ▪ Required MEAC members to participate in SIAC training.	
Crisis Communica-tions Planning	▪ Developed a comprehensive draft Crisis Readiness Plan and Guidebook 2026. ▪ Conducted a crisis-communications summit to improve coordination and messaging during future significant campus events.	These efforts represent significant post-incident improvement responsive to communications, coordination, and decision-making challenges identified during the review.
Mass Notification	▪ Conducted a targeted campaign encouraging current students and employees to provide text-capable phone numbers, using QR codes, direct links, and adoption tracking. ▪ November 20, 2025 testing reportedly showed that 98.6% of employees and 98% of students received the test text alert. ▪ Trained five additional employees to operate the Rave system. ▪ Reviewed and updated pre-scripted Rave messages. ▪ Tested the emergency "Active Shooter" red-button notification feature in December 2025. ▪ Rave and Alertus testing has reportedly demonstrated substantially improved delivery rates.	Significant progress has been made in improving notification reach, increasing redundancy among personnel capable of issuing alerts, and strengthening preparedness for emergency messaging.
Preparedness Roles	▪ Advanced the Building Marshal and Floor Captain program as part of broader campus preparedness efforts.	The program is a useful step toward distributing emergency-preparedness knowledge and responsibilities more broadly throughout campus buildings and departments.
Interagency Coordination and Mutual Aid	▪ An OPD/UVU mutual aid agreement is in development. ▪ Orem Emergency Management has offered additional support. ▪ A joint active-shooter exercise has been proposed. ▪ SIAC has increased its higher-education focus.	Meaningful interagency progress has occurred in areas directly related to staffing augmentation, emergency response, information sharing, and coordinated preparedness.

Area	Actions Taken or Initiated	Project Team Assessment
	▪ UVU relied on increased partner-agency law enforcement support following September 10.	
Physical Security and Access Control	▪ Constructed fencing on the Losee Center rooftop to prevent unauthorized access. ▪ Requires roof access to be reported to UVUPD Dispatch, which logs the roof accessed, staff member, and duration of access. ▪ Prohibited student roof access. ▪ Reviewed the physical key-access system to improve tracking and confirm individuals holding system-level access. ▪ Installed fixed bollards to restrict unauthorized vehicle access near buildings. ▪ Is working with the Utah Division of Facilities Construction and Management to evaluate additional facility-hardening measures, including improved rooftop security and potential bullet-resistant glazing in designated areas.	UVU has taken significant physical-security and access-control measures in response to vulnerabilities identified following September 10. These actions demonstrate increased attention to rooftop access, vehicle approaches, key control, and broader facility-hardening considerations.
Specialized Security Resources	▪ OPD drone capability was initially identified as a potential resource for major events. ▪ UVU has since established a drone coordinator and purchased drone technology to develop its own aerial observation capability.	Development of an internal drone capability represents meaningful progress and may enhance situational awareness during major outdoor events and other incidents when legally permissible and operationally appropriate.
External Security Expertise	▪ Retained security consultants to provide employee and student training. ▪ Engaged an expert security consulting firm to participate in meetings and provide guidance regarding broader security improvements.	The use of outside expertise provides UVU with additional specialized knowledge and independent perspective as it evaluates and strengthens its security programs and internal capabilities.
Statewide Public Safety Coordination	▪ SIAC added a higher-education focus. ▪ A statewide working group was initiated. ▪ The Utah higher-education campus safety task force is evaluating security across the state's public colleges and universities, with UVU participating. ▪ The University of Utah Department of Public Safety is participating in Salt Lake City Police Department's Real-Time Crime Center,	These initiatives reflect meaningful statewide efforts to strengthen intelligence sharing, multi-agency collaboration, training coordination, and campus public safety preparedness. UVU's participation provides an opportunity to remain

Area	Actions Taken or Initiated	Project Team Assessment
	providing another developing model for statewide and regional information sharing.	engaged in evolving systemwide practices and capabilities.
After-Action Learning and Independent Review	▪ Identified lessons through interviews, internal discussions, and post-incident review activities. ▪ Retained two outside firms to conduct an independent review and After-Action Report concerning the events surrounding September 10, 2025 and broader opportunities to strengthen campus event safety and security.	UVU's willingness to subject its actions, policies, systems, and practices to independent review reflects an institutional commitment to learning from the incident and identifying opportunities for continued improvement.

7.7 Overall Assessment

UVU's post-incident efforts reflect meaningful progress in several areas. The University and its partners provided support to students and the campus community, initiated significant crisis communications planning and operational improvements, advanced emergency awareness efforts, continued preparedness training, improved mass notification practices, and began important interagency coordination enhancements.

The post-incident process revealed areas requiring continued attention. Mental health support for responding UVUPD personnel and other first responders was less structured than the support provided to students and the broader campus community. Several corrective actions remain in development and will need to be finalized, trained, practiced, and tracked. UVU will benefit from this formal after-action improvement process that documents lessons learned and best practices. UVU should assign responsibilities, establish timelines, monitor implementation, and validate improvements through drills, exercises, and future event planning. See **Appendix D.10: Post-Event Review Considerations.**

In our assessment, UVU took meaningful steps to improve its safety and security policies and procedures after September 10, but the University should continue moving from response and recovery activity toward sustained institutional learning. The goal is not simply to complete individual improvement projects, but to build a durable preparedness system that improves unified and coordinated event planning and EOC operations that adhere to UVU's written policies, procedures and protocols; emergency communications; interagency coordination; first responder support; crisis response; and campus confidence over time.

Recommendations related to the issues addressed in this section are included in Section 9.

8. Legal Considerations

8.1 Legal and Regulatory Framework

The September 10 incident occurred within a legal and regulatory environment that imposes unique obligations and constraints on UVU. As a public institution of higher education in Utah, UVU must simultaneously comply with federal and state laws and safety requirements while safeguarding constitutional rights protected by the First and Second Amendments.

Several legal frameworks are relevant to this review. First, Utah law governs campus operations, public safety, firearms regulation, and the use of public university property. Second, UVU is subject to the Jeanne Clery Campus Safety Act ("Clery Act"), which establishes federal requirements related to campus safety, emergency notifications, crime reporting, and emergency preparedness. Finally, because UVU is a public institution, its decisions regarding speakers, events, demonstrations, and security measures are subject to federal and state constitutional scrutiny.

Legal Context Matters

Utah law imposes unique constraints on public universities that may not be familiar to readers outside the state. As a public institution, UVU must comply with First Amendment requirements protecting expressive activity, but unlike universities in many states, UVU is also subject to state laws that significantly limit its ability to prohibit firearms or implement certain weapons screening measures. These legal realities shaped the range of security options available before and during the September 10 TPUSA event.

UVU policy 425 is also important from a regulatory standpoint. It governs the use of campus facilities and the conditions that may be imposed.

This legal review is intended to provide context regarding the legal environment in which UVU operated before, during, and after the September 10 incident. It is not intended to provide conclusions regarding civil liability or potential litigation. Rather, it identifies legal considerations that shaped institutional decision-making and should inform future policy and operational improvements.

8.2 Event Classification, External Use, and Fronting

UVU Policy 425 establishes important distinctions between University events, co-sponsored events, and external uses of University facilities. These distinctions are legally and operationally significant because they affect contracting requirements, insurance obligations, cost allocation, Event Services review, risk management review, and responsibility for event-related conditions.

Under UVU policy, external entities sponsoring external events are required to enter into a Use of Premises Agreement, provide proof of insurance, and defray various costs associated with the event, including security costs. These requirements help ensure that events involving external organizations are reviewed through appropriate University processes and that responsibilities for risk, insurance, facilities use, staffing, costs, and compliance are clearly documented.

Policy 425 also addresses the concern commonly referred to as "fronting." Section 3.4 defines fronting as "permitting or aiding an external use under the guise that the activity is a University or a cosponsored event for the purposes of avoiding contracts, risk management, or Event Services review, payments, or other requirements or conditions applicable to external events." This provision is intended to prevent external organizations from avoiding the procedural, financial, insurance, and risk-management requirements that apply to external events, including significant security fees that might be appropriately assessed.

The fronting provision is important because event classification affects how the University evaluates risk, assigns responsibilities, imposes conditions, coordinates with organizers, and documents obligations. If an external organization is effectively controlling or sponsoring an event, but the event is processed as a University or co-sponsored event without appropriate documentation, the University may lose the benefit of external-use agreements, insurance verification, cost recovery, indemnification provisions, and formal review procedures. At the same time, the entity that is being "fronted" may benefit from avoiding considerable costs associated with the event. The question is often whether an event is really being held at the request of a club or other internal university entity or whether an external organization is using the internal entity to avoid paying appropriate costs.

At the same time, event classification must be applied consistently and, in a content-neutral manner. A public university may not reclassify, burden, or deny an event because of disagreement with the speaker's viewpoint or anticipated public reaction. However, the University may apply neutral policy requirements related to sponsorship, facility use, contracting, insurance, cost allocation, risk management, and operational review when those requirements are grounded in objective criteria and applied consistently across events.

Key Legal Takeaways

Policy 425's fronting provision is an important risk-management and compliance tool. UVU should ensure that event classification decisions are documented, consistently applied, and based on objective criteria regarding sponsorship, control, facility use, and external involvement. Clear application of Policy 425 helps preserve constitutional neutrality while also ensuring that contracts, insurance, cost allocation, Event Services review, and risk-management requirements are not bypassed when external entities are involved.

8.3 First Amendment Considerations

Public University Obligations Regarding Free Speech

As a public university, UVU is required to protect lawful expressive activity regardless of the popularity or controversy of the viewpoint being expressed. UVU states its commitment to protection of First Amendment rights in its Policy 161, Freedom of Speech. The University's role is not to endorse or oppose particular viewpoints, but rather to provide a lawful environment in which protected speech may occur. These obligations become particularly significant when events involve political figures, controversial speakers, or issues that may generate strong public reactions. The September 10 TPUSA event presented many of the challenges public universities routinely face when balancing constitutional freedoms with safety and operational concerns.

Controversial Speakers

Public institutions generally may not deny access to facilities, cancel events, or impose burdens on speakers because of disagreement with the speaker's views or because others oppose those views. Anticipated controversy, public criticism, or the possibility of protests does not diminish First Amendment protections. Universities may, however, take reasonable steps to address legitimate safety concerns associated with an event, provided those measures are based on objective security considerations rather than the content of the speech itself.

Time, Place, and Manner Restrictions

Although public institutions must protect speech rights, they may impose reasonable, content-neutral restrictions concerning the time, place, and manner of expressive activities. Such restrictions must serve legitimate governmental interests, be narrowly tailored, and leave open alternative opportunities for expression. These principles are particularly relevant when evaluating venue selection, crowd management, protest activity, access-control measures, and event logistics. They are also reflected in Utah law, which recognizes outdoor areas of public university campuses as traditional public forums entitled to heightened constitutional protection. Section 4.2.2 of UVU Policy 161 provides for time, place, and manner restrictions.

Security Fees and Viewpoint Neutrality

Courts have consistently held that security-related decisions must remain viewpoint neutral. Institutions may not impose costs, restrictions, or conditions based upon the anticipated reaction to a speaker's message or the controversial nature of a viewpoint. As a result, universities must be able to demonstrate that security decisions are grounded in objective risk factors, documented planning considerations, and consistent institutional practices. Any security fee assessed must be based on objective, content-neutral criteria that eliminates arbitrary discretion by university officials.[52]

Key Legal Takeaways

The First Amendment significantly limits the ability of public universities to restrict speakers, deny event requests, or impose burdens based on anticipated controversy. Consequently, event planning processes must be capable of distinguishing between legitimate safety concerns and viewpoint-based considerations. Well-documented, objective, and consistently applied decision-making processes are essential to maintaining both constitutional compliance and public confidence.

8.4 Firearms and Security Screening Considerations

Utah Campus Carry Laws

While prohibition of firearms on college campuses is permissible under the Second Amendment,[53] Utah law broadly permits lawful concealed firearm possession on public college and university campuses. On September 10, 2025 an individual 18 years of age or older, with a concealed weapon permit, could carry

[52] Leadership Institute et al. v. Stokes et al., 2024 CV 01 87, U.S. District Court of New Mexico

[53] Wade v. Univ. of Michigan, 145 S.Ct. 1923, No. 24-773 (2025) (cert. denied).

a weapon on a Utah campus, either open or concealed.[54] At present, any individual 21 years of age or older, and not legally disqualified from possessing a firearm, can carry a concealed weapon on a Utah campus, with or without a concealed weapon permit.[55] Unlike many states, Utah does not provide public institutions with independent authority to prohibit lawful firearm possession on campus property. Accordingly, UVU's ability to regulate firearms during campus events is substantially more limited than that of institutions operating in jurisdictions with different statutory frameworks.

State Preemption

Utah maintains strong state preemption over firearms regulation. Public institutions generally may not adopt firearms restrictions beyond those authorized by state law. Decisions regarding firearm possession and regulation are largely reserved to the State Legislature. This legal framework limits the University's discretion to implement security measures that might otherwise be available in other states.

Weapons Screening Limitations

Because of Utah's statutory framework, the use of weapons screening measures presents unique legal and operational challenges. Security practices commonly employed at public events elsewhere—including temporary event-specific firearm prohibitions—may not be available to public universities in Utah. While screening may be used to identify who has a weapon, it may not result in prohibiting possession of the weapon inside the venue. As a result, readers from outside Utah should recognize that some security measures frequently discussed following high-profile incidents may not have been legally available to UVU.

Key Legal Takeaways

Utah's firearms laws significantly constrain the security options available to public universities. As a practical matter, institutions must rely more heavily on threat assessment, intelligence gathering, venue planning, staffing decisions, and other preventive security measures than universities operating in states that authorize broader firearm restrictions or screening programs.

8.5 Clery Act and Emergency Notification Considerations

Timely Warnings

The Jeanne Clery Campus Safety Act requires higher education institutions to issue timely warnings regarding certain crimes that pose a serious or continuing threat to the campus community. These warnings are intended to provide members of the campus community with information necessary to make informed decisions regarding their safety.

Emergency Notifications

The Clery Act separately requires emergency notifications when an institution confirms a significant emergency or dangerous situation involving an immediate threat to the health or safety of students or employees. These notifications are intended to be issued without unnecessary delay while considering

[54] HB 128, Utah Code § 76-11-205.5 (2025)

[55] HB 84, Utah Code § 76-11-205.5 (2026)

the needs of emergency response efforts. UVU's Annual Security and Fire Safety Report incorporates these requirements through its Emergency Operations Plan and Emergency Communications Plan.

Emergency Communications Obligations

Emergency notifications must provide timely, accurate, and actionable information to affected populations. In rapidly evolving incidents, institutions must make decisions based on incomplete information while balancing public safety concerns, operational realities, and evolving investigative facts. The events of September 10, 2025 demonstrate the challenges institutions face when communicating during a dynamic and uncertain incident. As circumstances evolve, maintaining consistency, clarity, and public understanding becomes increasingly difficult but remains critically important.

Documentation Requirements

The Clery Act and UVU policy require the institution to maintain records relating to emergency preparedness, emergency response procedures, testing, exercises, and after-action reviews. UVU's Emergency Operations Plan and Annual Security Report contain detailed provisions governing these responsibilities, including documentation of exercises, lessons learned, and corrective actions.

Key Legal Takeaways

The Clery Act does not merely require institutions to communicate during emergencies; it requires them to maintain policies, systems, training, and documentation capable of supporting effective emergency communications. The quality of emergency communications is often evaluated not only by the speed of notification, but also by the accuracy, consistency, and clarity of information provided throughout an incident.

8.6 Legal Review of Findings and Recommendations

Brownstein Hyatt Farber Schreck LLP reviewed the findings and recommendations contained in this report and determined that they are generally consistent with applicable federal and state law, including the Jeanne Clery Campus Safety Act, Utah statutory requirements applicable to public institutions of higher education, and relevant constitutional considerations governing free expression and public safety on university campuses.

Recommendations related to the issues addressed in this section are included in Section 9.

9. Recommendations

Recommendation Status Legend

#	Reported by UVU as Completed and Reviewed by the Project Team
#	Reported by UVU as In Progress and Reviewed by the Project Team
#	To Be Addressed by UVU

Status reflects information provided by UVU as of September 25, 2026

1	Recommendations for Organizational Alignment, Staffing, Training, and Professional Standards
1.1	Evaluate UVUPD's organizational placement and reporting structure to ensure the UVUPD Police Chief has appropriate visibility and access to senior University leadership.
1.2	Consider whether a senior campus safety leadership role, such as a Vice President or Associate Vice President for Campus Safety and Security, would improve coordination among UVUPD, Emergency Management, the Fire Marshal, physical security, event security, and related public safety functions.
1.3	Conduct a formal UVUPD staffing and pay analysis that considers University size, campus geography, call volume, event activity, patrol needs, investigative responsibilities, Dispatch capacity, emergency management support, and major-event security requirements.
1.4	Conduct an annual UVUPD public safety training needs assessment and develop a written UVUPD training plan aligned with the University's operating environment that prioritizes training for UVUPD in the Incident Command System, Event Action Plan development, active assailant response, major-event security, protective operations, emergency communications, crowd management, mutual aid, and higher education public safety practices.
1.5	Evaluate IACLEA accreditation as part of UVUPD's broader professional standards, policy development, accountability, training, and continuous improvement efforts.
1.6	Continue to ensure public safety leadership is routinely included in planning discussions involving major events, emergency preparedness, facilities use, communications, student affairs, and institutional risk management.
1.7	Evaluate no-cost CISA resources, including Protective Security Advisor support, physical security assessments, cybersecurity assessments, tabletop exercises, and targeted violence prevention resources, as part of UVU's broader public safety, emergency preparedness, and resilience improvement efforts.

2	Recommendations for Event Planning, Response, and Interagency Coordination
2.1	Ensure major events under Policy 425 § 3.5 undergo a documented MEAC-facilitated Security Assessment consistent with Policy 425 § 4.8.2 and MEAC review under Policy 425 § 5.2.1.

2	Recommendations for Event Planning, Response, and Interagency Coordination
2.2	Clarify MEAC procedures and decision authority for venue selection, security conditions, staffing expectations, ticketing requirements, access-control expectations, screening considerations, credentialing expectations, and event-specific restrictions or requirements.
2.3	Establish clear criteria for when events should be moved indoors or relocated to more controllable venues, including crowd size, line-of-sight concerns, high-ground vulnerabilities, access-control limitations, protest activity, or other security considerations and ensure criteria comply with Utah Code Ann. §53H-7-202 (Traditional Public Forums).
2.4	Require MEAC review to document event classification, venue selection considerations, external organizer responsibilities, legal considerations, unresolved security concerns, resource limitations, and leadership approvals.
2.5	Ensure co-sponsored events involving external organizers clearly define responsibilities consistent with Policy 425 §§ 3.7.1 and 4.1.5.
2.6	Coordinate event-security decisions with legal counsel when Policy 425 § 4.1.3 and UVU Policy 161 considerations intersect with security restrictions, access control, protest activity, signage, or conditions of entry.

3.1	Recommendations for Event Security Planning and Security Assessment
3.1.1	Require documented Security Assessments for major events which include high-profile events or speakers, large gatherings, outdoor events with security vulnerabilities, or events involving elevated security concerns.
3.1.2	Incorporate venue-specific vulnerabilities, speaker profile, anticipated attendance, protest activity, prior event history, intelligence reporting, SIAC information, OSINT, social media monitoring, and lessons learned from comparable events into Security Assessments when relevant.
3.1.3	Use Security Assessments to inform venue selection, staffing, access control, screening, credentialing, protective operations, communications, emergency response, emergency medical support, technology monitoring, and mutual aid needs.
3.1.4	Document key planning assumptions, mitigation options, rejected alternatives, unresolved concerns, resource limitations, and leadership approvals.
3.1.5	Develop criteria for implementing enhanced security measures when elevated security concerns are identified.

3.2	Recommendations for Event Security Operations
3.2.1	Establish process to create written Event Action Plan with operational plans for high-profile or elevated-risk events based on the Security Assessment that documents staffing assignments, command relationships, post responsibilities, communications procedures, and emergency response actions.

3.2	Recommendations for Event Security Operations
3.2.2	Establish ongoing process to update primary and backup personnel to fill key operational and decision-making roles, including Incident Command System positions and Emergency Operations Center leadership roles when applicable.
3.2.3	For events with an Event Action Plan, require formal pre-event briefings, site walk-throughs, and day-of briefings for UVUPD, event organizers, Emergency Management, local law enforcement, and any assigned private security or executive protection detail.
3.2.4	Assign responsibility for real-time video monitoring, relevant camera feeds, programmed event views, communications monitoring, video analytics, and situational awareness during high-profile, outdoor, or elevated-risk events.
3.2.5	Ensure major-event security planning addresses emergency medical support, including whether EMS personnel and an ambulance should be staged at or near the venue based on the results of the Security Assessment.

3.3	Recommendations for Access Control, Screening, and Credentialing
3.3.1	Develop event-specific access-control and credentialing plans for major events and elevated-risk events.
3.3.2	Require University-controlled ticketing for major events when attendance projections affect venue suitability, staffing, access control, emergency communications, or Event Action Plan development.
3.3.3	If for any reason University ticketing is not used, require event organizers to provide ongoing attendance projections and real-time access to ticketing data.
3.3.4	Establish written permitted and prohibited-items policies consistent with applicable law.
3.3.5	Develop written screening procedures for events where screening is legally permissible and operationally appropriate.
3.3.6	Train screening and event security personnel on prohibited-items policies, equipment use, ADA accommodations, escalation procedures, documentation requirements, and Utah firearms-law considerations.
3.3.7	Evaluate screening technologies based on the event's security profile, legal constraints, staffing capacity, privacy considerations, false alarm rates, and operational needs.
3.3.8	Develop written post orders for access control, screening, credentialing, perimeter security, roving patrols, crowd management, Command Post access, and emergency response posts.
3.3.9	Identify restricted areas, elevated positions, surrounding building access points, Command Post locations, media areas, VIP areas, and emergency response routes before major outdoor events.
3.3.10	Prepare attendee-facing information regarding access-control procedures, screening measures, prohibited items, bag restrictions, and legally applicable firearm-related requirements or limitations.

3.4	Recommendations for Protective Operations and Line-of-Sight Planning for Outdoor Events
3.4.1	Establish a written process for line-of-sight and elevated-position assessments for high-profile outdoor events.
3.4.2	Include arrival and departure routes, building access, rooftops, windows, balconies, elevated walkways, protest areas, crowd placement, emergency access, medical contingencies, and egress routes in protective operations planning.
3.4.3	Incorporate protective intelligence, prior event history, protest activity, and event-specific threat information into venue, staffing, and security decisions.
3.4.4	Ensure event staffing plans include both fixed-post coverage and mobile response capacity.
3.4.5	Establish control measures for buildings, rooftops, balconies, windows, access points, and other areas that may affect event security.

3.5	Recommendations for Traffic, Parking, and Perimeter Management
3.5.1	Develop traffic and parking plans for large-scale and elevated-risk events.
3.5.2	Coordinate traffic planning with local, county, and state law enforcement, transportation officials, parking vendors, emergency responders, and public works when appropriate.
3.5.3	Maintain emergency vehicle access and clearly designated arrival and departure routes.
3.5.4	Identify preferred emergency departure routes for attendees, students, employees, and visitors when a major event or critical incident may require rapid departure from campus.
3.5.5	Ensure emergency departure routes and traffic-control assumptions are available to Dispatch, the Command Post, the EOC, Communications, UVUPD, and partner agencies so emergency messages can provide accurate route or area-avoidance instructions when needed.
3.5.6	Incorporate parking operations into event security planning and assign responsibility for parking security functions.
3.5.7	Establish procedures for identifying, reporting, investigating, and removing unauthorized, unidentified, or suspicious vehicles within event parking areas or controlled perimeters.
3.5.8	Establish procedures for communicating parking, traffic, access-control, and emergency departure information before and during major events.

3.6	Recommendations for Fixed and Temporary Site Security Measures
3.6.1	Incorporate fixed and temporary site-security measures into planning for outdoor and elevated-risk events.
3.6.2	Evaluate fencing, gates, barricades, bollards, barriers, stanchions, signage, vehicles, planters, and other physical controls to manage access and movement.
3.6.3	Identify event boundaries, controlled-access areas, screening locations, restricted zones, adjacent building access points, and emergency routes before major events.

3.6	Recommendations for Fixed and Temporary Site Security Measures
3.6.4	Assign responsibility for staffing, monitoring, inspecting, and adjusting temporary barriers and other physical controls during event operations.
3.6.5	Test screening-support equipment, entry-flow procedures, temporary barriers, signage, and backup measures before major events.
3.6.6	Identify backup site-control measures in case equipment fails, crowd conditions change, or additional restrictions become necessary.
3.6.7	Establish layered security zones, such as outer, middle, and inner perimeters, with progressively stricter controls when appropriate.

4.1	Recommendations for Application of ICS and Event Action Planning
4.1.1	Develop a scalable Event Action Plan template for major events and elevated-risk events.
4.1.2	Require a written Event Action Plan or equivalent operational document for high-profile speakers or events, large gatherings, outdoor events with security vulnerabilities, and events involving outside organizers or private security teams.
4.1.3	Include event objectives, command roles, staffing assignments, post responsibilities, communications procedures, contingency plans, access-control decisions, mutual aid thresholds, emergency medical support, real-time monitoring responsibilities, and post-event review expectations in the Event Action Plan.
4.1.4	Conduct in-person pre-event briefings and site walk-throughs based on the written Event Action Plan so assigned personnel understand their roles, reporting lines, communications channels, and escalation procedures.
4.1.5	Incorporate Event Action Plans into post-event reviews and corrective-action tracking.

4.2	Recommendations for Implementation of the Emergency Operations Plan and Active Assailant Protocols
4.2.1	Develop practical Emergency Operations Plan implementation guides, staffing checklists, role cards for major incidents, and alternates for key positions, including EOC Manager, emergency management lead, communications lead, law enforcement liaison, and Policy Group coordination.
4.2.2	Clarify activation thresholds for the Emergency Operations Plan, Emergency Operations Center, Policy Group, and crisis communications team.
4.2.3	Incorporate active assailant protocols into training, practical exercises, event planning, and emergency communications templates.
4.2.4	Provide recurring training to students, employees, and event personnel on active assailant response, lockdown, evacuation, sheltering, emergency reporting, and protective actions.
4.2.5	Use plain-language terminology in public education and emergency messaging so protective actions are understood by students, employees, visitors, and event participants and attendees.

4.2	Recommendations for Implementation of the Emergency Operations Plan and Active Assailant Protocols
4.2.6	Ensure corrective actions identified through exercises and real incidents are entered into the post-incident improvement process.

4.3	Recommendations for EOC Activation, Situational Awareness, and Decision Support
4.3.1	Clarify Emergency Operations Center activation criteria for major events, active threats, mass-casualty concerns, major criminal incidents, and incidents requiring significant external agency support.
4.3.2	Establish an EOC monitoring posture for high-profile or elevated-risk events when full activation is not necessary but rapid escalation may be required.
4.3.3	Reconcile and continually update the Emergency Operations Plan, Campus-Wide Emergency Communications Plan, and Green Card succession process so leadership authority, succession, message approval, and EOC roles are consistent across documents.
4.3.4	Ensure the established line of succession and decision-making authority is followed during emergency operations, except where formally modified and clearly communicated before the incident or at the time of activation.
4.3.5	Clarify who has authority to approve emergency messages when designated leaders are unavailable, delayed, participating remotely, or assigned competing responsibilities.
4.3.6	Clarify how competing executive responsibilities, including Governor's Office coordination, press conference preparation, public statements, and EOC management, will be assigned during major incidents.
4.3.7	Assign a UVUPD command representative or designated law enforcement liaison to the EOC during major incidents to support situational awareness, operational coordination, and timely decision-making.
4.3.8	Establish procedures for regular briefings between field command, EOC leadership, Dispatch, Communications, Policy Group representatives, and external public safety partners.
4.3.9	Improve tools used to track incident status, resource requests, emergency notifications, decisions, unresolved issues, and follow-up assignments.
4.3.10	Clarify the relationship among field command, the Command Post, the EOC, the Policy Group, and University executive leadership.
4.3.11	Develop remote-participation protocols for key personnel who may need to support EOC operations by telephone, Microsoft Teams, or other remote platforms.
4.3.12	Conduct recurring EOC and Policy Group exercises that test situational awareness, decision-making authority, emergency message approval, communications coordination, public information, resource coordination, and leadership succession.

4.4	Recommendations for Interagency Coordination and Mutual Aid Implementation
4.4.1	Complete the written mutual aid agreement between UVUPD and the Orem Police Department and develop or update mutual aid agreements with other neighboring law enforcement, fire, EMS, emergency management, and public safety partners.
4.4.2	Establish criteria for requesting mutual aid from external public safety, emergency management, fire, EMS, traffic-control, investigative, tactical, and aerial-observation support before major or elevated-risk events, with a focus on identifying mutual aid needs when completing a Security Assessment and its associated Event Action Plan.
4.4.3	Include the Orem Police Department, Orem Fire Department, Orem Emergency Management, Utah County Sheriff's Office, Utah DPS, SIAC, SBI, and other relevant partners in pre-event planning when an event presents elevated security concerns.
4.4.4	Ensure UVUPD actively participates in statewide public safety coordination efforts involving Utah DPS, SIAC, SBI, Utah System of Higher Education representatives, the University of Utah Department of Public Safety, and other campus public safety agencies.
4.4.5	Develop written procedures for integrating external law enforcement, fire, EMS, emergency management, state, and federal partners into Command Posts, Emergency Operations Center operations, field command, investigative command, emergency communications, and public information processes.
4.4.6	Identify liaison roles to enhance coordination among the EOC, field command, investigative command, University leadership, and external agencies during major incidents.
4.4.7	Establish protocols for documenting command transitions, lead-agency decisions, resource requests, investigative handoffs, agency roles, and demobilization.
4.4.8	Maintain current contact lists and notification procedures for local, county, state, and federal response partners.
4.4.9	Clarify how investigative information, surveillance video, emergency notifications, public information, and operational updates will be shared between law enforcement agencies' leaders during a major incident, particularly when it involves a criminal investigation.
4.4.10	Ensure EOC activation procedures account for the rapid arrival of external agencies and the need to manage space, roles, communications, and decision-making.
4.4.11	Conduct joint training exercises with UVUPD, Orem Police Department, Orem Fire Department, Orem Emergency Management, Utah County Sheriff's Office, Utah Department of Public Safety, SIAC, SBI, fire, EMS, and other key partners.
4.4.12	Include mutual aid and interagency coordination in post-event reviews and after-action improvement plans.

5.1	Recommendations for Communications and Mass Notification
5.1.1	Evaluate need for additional Dispatch staffing and continuity for major events, high-risk periods, and major incidents, including second-dispatcher coverage, backup Dispatch procedures, alternate operations capability, and surge-support procedures.

5.1	Recommendations for Communications and Mass Notification
5.1.2	Designate a communications lead (PIO) for major incidents and define backup communications leadership when the primary lead is unavailable, remote, or assigned competing responsibilities.
5.1.3	Clarify emergency message issuance authority, including drafting, approval, update, correction, rescission, and backup approval procedures, with workflows for remote participation.
5.1.4	Adopt and consistently use the Standard Response Protocol terminology reflected in UVU's current Emergency Management guidance, including HOLD, SECURE, LOCKDOWN, EVACUATE, and SHELTER and the Avoid, Deny, Defend, Aid protocol. UVU should update emergency plans, alert templates, training materials, public-facing instructions, and exercise materials to use these terms consistently and eliminate or revise similar-sounding terms, such as "secure-in-place" or "shelter-in-place," where they may conflict with the Standard Response Protocol definitions.
5.1.5	Develop, test, and regularly update pre-approved message templates and scripted instructions for common emergency scenarios using Standard Response Protocol terminology and hazard-specific instructions. Templates should address active threat, lockdown, secure, hold, evacuate, shelter, campus closure, severe weather, fire, police activity, hazardous materials, medical emergency, and all-clear notifications.
5.1.6	Review emergency message templates and terminology with students, faculty, staff, and accessibility stakeholders for clarity and comprehension.
5.1.7	Evaluate and streamline UVU's mass notification systems, including Rave, Alertus, public address capabilities, desktop alerts, digital signage, and related activation protocols.
5.1.8	Ensure the Incident Commander is trained on the mechanisms for issuing immediate campus alerts that direct specific protective actions during an emergency.
5.1.9	Regularly test notification systems, public address coverage, radio communications, backup communications, contact-information accuracy, user enrollment, delivery rates, and all-clear procedures at the beginning of each semester.
5.1.10	Improve integration and interoperability among access control, security camera video feeds, panic alarms, public address, digital signage, radio communications, mass notification systems, and local responder communications.
5.1.11	Include communications planning, message testing, notification workflows, and public information coordination in Event Action Plans, major-event planning, drills, exercises, and after-action reviews.

5.2	Recommendations for Physical Security Technology
5.2.1	Develop a physical security technology roadmap that identifies system priorities, replacement needs, estimated costs, integration opportunities, maintenance requirements, and implementation timelines.

5.2	Recommendations for Physical Security Technology
5.2.2	Evaluate opportunities to integrate access control, video surveillance, intrusion detection, panic or duress alarms, public address systems, lockdown capabilities, mapping, and mass notification tools into a coordinated common operating picture for Dispatch, command staff, the Command Post, and the Emergency Operations Center.
5.2.3	Conduct an enterprise-wide audit of access-control credentials, deactivate expired or unauthorized badges, and establish recurring credential review procedures.
5.2.4	Strengthen access-control governance by defining role-based access levels, limiting card-issuance authority, and adding oversight from Human Resources, student records, or other authoritative data sources where feasible.
5.2.5	Evaluate whether select access-control points should remain active 24 hours a day based on building function, security profile, operational needs, emergency access requirements, and security considerations.
5.2.6	Expand and modernize video surveillance coverage based on security considerations, event locations, access points, parking areas, building entrances, pedestrian pathways, elevated positions, and investigative needs.
5.2.7	Establish camera standards for new installations to improve compatibility, maintenance, analytics capability, video quality, storage, and long-term system performance.
5.2.8	Configure priority camera views and selected analytics for major events, including rooftops, elevated areas, restricted zones, crowd areas, access points, emergency routes, and virtual boundaries around sensitive areas.
5.2.9	Establish procedures for communicating real-time video observations to Dispatch, field officers, command personnel, the Command Post, and the EOC.
5.2.10	Develop protocols for preserving, bookmarking, and sharing video during major incidents.
5.2.11	Evaluate panic alarm, duress alarm, and emergency call-point needs in public-facing offices, student service areas, event venues, parking areas, and other higher-risk locations.
5.2.12	Identify drone or aerial observation capabilities available internally or through partner agencies for major outdoor events when legally permissible and operationally appropriate.
5.2.13	Include physical security technology planning, monitoring assignments, programmed camera views, alarm workflows, and system testing considerations in Event Action Plans for major or elevated-risk events.

5.3	Recommendations for OSINT, Web, and Social Media Monitoring
5.3.1	Establish documented procedures governing OSINT collection, analysis, documentation, retention, dissemination, and legal or privacy review.
5.3.2	Designate responsibility for protective intelligence and OSINT functions supporting threat assessment, event planning, and targeted violence prevention efforts.
5.3.3	Define when subject-focused OSINT is required for BAT cases, event-security planning, threats, concerning communications, or other elevated-risk matters.

5.3	Recommendations for OSINT, Web, and Social Media Monitoring
5.3.4	Prohibit the use of personal social media accounts for official threat assessment, investigative, or protective intelligence activities.
5.3.5	Implement authorized investigative accounts, standardized documentation practices, and approved investigative methods for OSINT inquiries.
5.3.6	Evaluate dedicated protective intelligence and threat intelligence tools designed to support behavioral threat assessment, event security, targeted violence prevention, and subject-focused investigations.
5.3.7	Improve integration among intelligence collection activities, BAT processes, event planning, UVUPD operations, Emergency Management, and decision-making functions.
5.3.8	Establish procedures for documenting how intelligence information affects event classification, staffing, access control, venue decisions, communications, and mutual aid requests.
5.3.9	Provide training for personnel involved in OSINT, social media review, media monitoring, protective intelligence, and threat assessment-related investigations.

5.4	Recommendations for Information Sharing and Protective Intelligence
5.4.1	Continue leveraging SIAC for pre-event threat intelligence, suspicious activity reporting, protective intelligence, and post-incident information sharing.
5.4.2	Document threat-related information received before major events, including source, timing, follow-up, relevance, and operational impact.
5.4.3	Establish a process for incorporating intelligence and protective information into Security Assessments, Event Action Plans, staffing decisions, access-control decisions, venue decisions, communications planning, and mutual aid requests.
5.4.4	In collaboration with the university working group at SIAC, evaluate deep web and dark web monitoring tools or qualified external resources to identify adverse intelligence, threats, leaked information, or concerning online activity directed toward UVU, its people, facilities, operations, or events.
5.4.5	Evaluate services or programs designed to identify and reduce publicly available personally identifiable information for senior University leaders and other individuals who may face elevated exposure because of their roles.
5.4.6	Evaluate InfraGard membership for appropriate UVU personnel involved in campus safety, cybersecurity, emergency management, threat assessment, research security, or operations to strengthen information sharing with public- and private-sector security partners.
5.4.7	Ensure UVUPD takes a proactive role in participating in the new SIAC working group established to enhance interaction and collaboration with Utah's institutions of higher education to include exploring whether SIAC's existing intelligence and information-sharing platform, analytical capabilities, and related workflows can support UVU's protective

5.4	Recommendations for Information Sharing and Protective Intelligence
	intelligence, suspicious activity reporting, threat assessment, and major-event planning needs.

6	Recommendations for Behavioral Threat Assessment and Threat Management
6.1	Formally adopt the BAT Policies and Procedures document and establish a recurring annual review process.
6.2	Expand references to the BAT within relevant institutional policies to reinforce referral pathways, consultation expectations, and multidisciplinary coordination responsibilities.
6.3	Continue investing in annual BAT training and professional development, including expanded participation in ATAP and other multidisciplinary threat assessment organizations as external resources to supplement existing NABITA engagement.
6.4	Incorporate open-source research and publicly available information, and deep web and dark web searches more consistently into BAT assessment methodologies, particularly in elevated-risk cases and consistent with UVU's OSINT procedures and establish a more formal process for subject-focused OSINT and protective intelligence support in BAT cases involving elevated concern.
6.5	Strengthen integration between behavioral threat assessment activities, event security planning, Emergency Management, and protective measures when circumstances warrant.
6.6	Establish access to external clinical or forensic consultation for elevated-risk cases.

7	Recommendations for Post-Incident Recovery, Corrective Actions, and Preparedness Enhancements
7.1	Continue to conduct formal after-action reviews after major incidents, major events, emergency exercises, and significant security operations that identifies corrective actions, responsible owners, timelines, implementation status, and validation methods.
7.2	Establish a structured first responder-support process for UVUPD personnel, Dispatch, Emergency Management, Communications personnel, and other employees directly involved in major incidents that includes first responder wellness, peer support, confidential mental health resources, decompression opportunities, and supervisor follow-up in post-incident recovery planning.
7.3	Finalize the crisis communications plan and integrate it with Emergency Operations Center procedures, emergency notification templates, major-event planning, media response protocols, and Policy Group decision-making.
7.4	Conduct regular practice exercises for the crisis communications plan using realistic scenarios involving incomplete information, conflicting reports, active-threat messaging, campus closure, press conferences, and all-clear notifications.
7.5	Continue expanding campus safety awareness efforts, including posters, flipcharts, website and app resources, tabling, employee training, and student-facing preparedness education.

7	Recommendations for Post-Incident Recovery, Corrective Actions, and Preparedness Enhancements
7.6	Measure the effectiveness of campus safety training and communications through completion data, surveys, drills, message testing, and after-action feedback.
7.7	Use the post-incident corrective-action summary as a living document and update it regularly until items are completed, exercised, and validated.

8	Recommendations for Legal Considerations
8.1	Conduct a comprehensive legal review of Policy 425 and related event management policies to ensure continued compliance with First and Second Amendment requirements, Utah law, and evolving practices.
8.2	Develop formal guidance for planning and managing controversial-speaker events that integrates constitutional, operational, and security considerations and establish documented, viewpoint-neutral criteria for major event Security Assessments and venue-selection decisions.
8.3	Implement a campus speaking-event security fee policy that is based on narrow, objective, and content-neutral factors and that minimizes discretion of University officials.
8.4	Collaborate with other public colleges and universities in Utah to collectively consider how to conduct weapons screening at campus events in conformance with Utah law and advise the Utah Legislature of their concerns and recommendations regarding weapon possession policies on campuses.
8.5	Continue to review and update timely warning and emergency notification procedures to ensure continued alignment with Clery Act requirements and emerging practices.
8.6	Conduct periodic legal and policy reviews of campus safety, emergency management, and event planning procedures to ensure continued compliance with applicable law and regulatory requirements.

Appendices

Appendix A: Project Team Bios

Core Law Enforcement and Security Risk Management Team

Robert L. Davis, Project Manager, Law Enforcement Operations Specialist



President, Robert L. Davis, LLC; Former Chief of Police, San Jose, California; Former President, Major Cities Chiefs Association

Rob Davis brings more than 30 years of law enforcement leadership experience, including service as Chief of Police for the City of San Jose — one of the nation's largest municipal departments, along with 15 years of consulting experience. He is widely recognized for strengthening operational readiness and response, leading complex incident assessments, improving investigative processes, strengthening media interaction capabilities, and assessing training curriculums and methodologies. Rob has directed high-stakes assessments for public agencies and universities nationwide.

Matthew W. Doherty, Targeted Violence and Threat Assessment and Management Specialist



Founder and Managing Principal, Doherty Advisory

Matt Doherty is a nationally recognized authority in behavioral threat assessment and management, targeted violence, workplace violence prevention, and organizational security practices. He draws on more than four decades of distinguished service in both government and the private sector, including leadership of the U.S. Secret Service National Threat Assessment Center. Matt has led threat management practices for global consulting firms and continues to advise organizations seeking to strengthen violence-prevention programs and mitigate risk.

G. Michael Verden, Security Operations and Emergency Management Specialist



CEO and Founder, The Lake Forest Group

Mike Verden is a prominent security strategist with deep expertise in event security, protective intelligence, and emergency preparedness. As CEO and Founder of The Lake Forest Group and former operational leader within the Major Events Division, Dignitary Protection Division, and Presidential Protection Division of the U.S. Secret Service, he has directed complex risk assessments for NSSEs, major venues, universities, corporations, and government entities, and has also served as an expert witness reviewing security plans and threat intelligence for the Ben Shapiro event at the University of Minnesota. Mike brings extensive experience designing resilient security programs and plans that align operational needs with industry best practices.

Core Brownstein Team

John Suthers, Legal Counsel and Project Manager for the Brownstein Team



Shareholder, Brownstein Hyatt Farber Schreck, LLP; Former Mayor, Colorado Springs; Former Colorado Attorney General; Former United States Attorney

John Suthers brings nearly five decades of legal, public safety, government, and investigative experience to the project team. He has served as a Deputy District Attorney, Chief Deputy District Attorney, and elected District Attorney for Colorado's Fourth Judicial District. He also served as Executive Director of the Colorado Department of Corrections, United States Attorney for the District of Colorado, Attorney General of Colorado from 2005 to 2015, and Mayor of Colorado Springs from 2015 to 2023. Mr. Suthers has extensive experience conducting external and internal investigations, including matters involving school and campus safety. Following the 2007 shooting at Virginia Tech University, he served as co-chair of the National Association of Attorneys General Task Force on School and Campus Safety. As United States Attorney for Colorado, he conducted a review of the Columbine Commission report in response to a petition by parents of students killed at Columbine High School. In 2024, he was part of a Brownstein team that conducted an external review of a double homicide in a residence hall at the University of Colorado, Colorado Springs. Mr. Suthers earned his J.D. from the University of Colorado School of Law in 1977 and his B.A., cum laude, from the University of Notre Dame in 1974.

Jason Dunn, Legal Counsel



Shareholder, Brownstein Hyatt Farber Schreck, LLP; Former U.S. Attorney; Former Deputy Attorney General of Colorado

Jason Dunn has been practicing law for 25 years. He served as Deputy Attorney General of Colorado and as US Attorney for Colorado. As a seasoned counselor and litigator, he has led and advised on some of the most high-profile private and governmental investigations in Colorado. He is chair of Brownstein's Attorney General Practice and its Government Investigations and White Collar Defense Group. Mr. Dunn's extensive experience in conducting external and internal investigations includes work for the University of Colorado. He earned his J.D. from the University of Colorado Law School, his M.P.A. from the University of Colorado Graduate School of Public Affairs, and his B.S. from the University of Colorado College of Business.

Max Porteus, Legal Counsel



Max Porteus is a litigation associate whose practice focuses on handling complex disputes, including trial level and appellate litigation, internal and government investigations, and high stakes commercial matters. His work spans litigation strategy, complex briefing, and advising clients in investigations and disputes from inception through appeal. He previously clerked for Justice Carlos A. Samour, Jr. of the Colorado Supreme Court. He earned his J.D. from the University of Denver Sturm College of Law, Order of the Coif, and his B.A. from the University of Denver.

Advisory Board

Brent Herron, Subject Matter Expert: Campus Safety



Brent Herron is a nationally recognized expert in campus safety, emergency operations, and threat management with more than 30 years of experience in higher education and federal protective operations. He served as the University of North Carolina System's Senior Associate Vice President for Campus Safety and Emergency Operations, leading systemwide initiatives across 16 universities and directing major programs in policing, emergency management, and behavioral threat assessment. Prior to his higher education leadership role, Brent spent 21 years with the U.S. Secret Service, supporting and supervising technical security operations for multiple NSSEs. He currently advises the UNC System on policy, preparedness, major-incident response, and interagency coordination.

Chris Brenner, Subject Matter Expert: Open-Source Intelligence



Chris Brenner is an investigations and intelligence specialist with more than 15 years of experience applying advanced OSINT tools and methodologies to support complex investigations and threat assessments. As Associate Managing Director and Director of Technology at 221B Partners, he leads OSINT-driven research, deep and dark web analysis, and data visualization to support clients across corporate, government, and nonprofit sectors. He is Open-Source Certified (OSC) by the OSMOSIS Association, where he serves on the Board of Advisors, and is an active member of ATAP, InfraGard, and OSAC.

Heather Czyzewicz, Subject Matter Expert: Security Technology



Heather Czyzewicz is a security technology specialist with extensive experience helping organizations implement scalable, interoperable physical security solutions. She leverages strong industry partnerships, continuous technology research, and cross-market expertise to guide clients in selecting and deploying effective, budget-aligned systems. Heather currently serves as Business Development Manager for Sound Incorporated, where she advances integrated technology strategies and strengthens organizational readiness across diverse sectors.

James A. Konieczny, Subject Matter Expert: Counter Sniper Tactics



James Konieczny is a retired U.S. Secret Service Special Agent with 25 years of federal service and deep expertise in counter-sniper operations for high-risk environments. He spent two decades in the USSS Counter Sniper Unit — later serving as an instructor — where he trained agents in long-range precision shooting, weapons proficiency, and advanced counter sniper tactics. James has supported protective missions for four U.S. Presidents and led counter sniper teams during multiple NSSEs.

Michelle Hoy-Watkins, Psy.D., ABPP, Licensed Clinical Psychologist



Michelle Hoy-Watkins, Psy.D., ABPP is a Licensed Clinical Psychologist with more than 25 years of experience in clinical, forensic, and police and public safety psychology. She is Board Certified in Police and Public Safety Psychology and has provided psychological services, wellness programs, threat assessments, and consultative support to numerous law enforcement agencies, including the Chicago Police

Department, Illinois State Police, and Northwestern University Police. Dr. Hoy-Watkins previously led Northwestern University's threat assessment program and has extensive experience conducting forensic evaluations and working in federal and state correctional and mental health institutions. She currently serves as a consultant to state and national threat assessment teams and holds multiple leadership roles within the International Association of Chiefs of Police and the American Psychological Association.

John A. Gill, Subject Matter Expert: Crisis Communications and Public Affairs



John Gill is an accomplished crisis communications and public affairs leader with more than 30 years of experience guiding high-stakes messaging, media coordination, and stakeholder engagement at the highest levels of government and the private sector. His career includes senior roles in the White House and the U.S. Secret Service, where he led the agency's public affairs and crisis communications programs during the post-9/11 era. John has managed complex security, continuity, and executive communication efforts across global operations, bringing a steady, trusted voice to organizations facing sensitive or rapidly evolving events. He is known for his clarity, integrity, and ability to translate complex operational issues into decisive, credible communication strategies.

Communications Lead

Vicky Froderman, Senior Advisor, Research and Reporting



Vicky Froderman has a career rooted in communications, with long-standing expertise in writing, messaging, research, and producing high-quality materials for senior leaders and diverse audiences. For the past 20 years, her work has focused on security risk management and workplace violence prevention, where she has applied those skills to complex, high-stakes assessments and sensitive client matters. She has contributed to hundreds of assessments, including the Virginia Beach mass shooting review, supporting multidisciplinary teams through interviews, document review, report development, editing, quality control, and the organization and presentation of findings and recommendations. Vicky brings clarity, precision, and analytic discipline to complex engagements, helping ensure that conclusions are well-supported and communicated clearly and consistently.

Appendix B: Incident Command System (ICS) Roles and Responsibilities

The Incident Command System (ICS) is a standardized management framework used to coordinate personnel, resources, communications, and decision-making during emergencies and planned events. While the specific structure may expand or contract depending on the complexity of an incident, the following positions are commonly used within ICS-compliant organizations.

Incident Commander (IC)

The Incident Commander has overall responsibility for managing the incident and establishing incident objectives and priorities. The IC directs response activities, authorizes resource requests, approves strategic decisions, and serves as the primary decision-maker throughout the incident. Typical responsibilities include:

- Establishing incident objectives and priorities
- Approving operational strategies and response actions
- Requesting additional resources and mutual aid when necessary
- Coordinating with executive leadership
- Maintaining overall situational awareness
- Authorizing incident closure and "all clear" notifications

Public Information Officer (PIO)

The Public Information Officer serves as the official communications representative during an incident and is responsible for developing, coordinating, and disseminating information to internal and external audiences. Typical responsibilities include:

- Preparing public statements and media releases
- Coordinating communications with stakeholders and families
- Monitoring media coverage and public messaging
- Supporting emergency notification activities
- Ensuring consistent and accurate information is released

Liaison Officer (LNO)

The Liaison Officer serves as the primary point of contact for assisting agencies, partner organizations, and external stakeholders supporting incident operations. Typical responsibilities include:

- Coordinating with responding public safety agencies
- Facilitating information sharing between organizations
- Assisting with mutual aid coordination
- Participating in planning meetings
- Communicating resource needs and capabilities among partner agencies

Safety Officer (SO)

The Safety Officer monitors incident operations and advises leadership regarding safety concerns affecting responders, staff, students, visitors, and other stakeholders. Typical responsibilities include:

- Identifying and evaluating safety hazards

- Monitoring responder safety and operational risks
- Coordinating with law enforcement and emergency responders
- Assessing evacuation routes and assembly locations
- Recommending corrective actions when unsafe conditions exist

Operations Section Chief

The Operations Section Chief manages tactical activities and directs personnel engaged in incident response operations. Typical responsibilities include:

- Supervising operational resources
- Implementing incident objectives
- Coordinating field activities
- Monitoring operational progress
- Reporting status updates to command staff

Planning Section Chief

The Planning Section Chief is responsible for collecting, evaluating, and disseminating information needed to support incident management. Typical responsibilities include:

- Maintaining situational awareness
- Tracking incident status and resources
- Developing Incident Action Plans
- Documenting operational activities
- Supporting future operational planning

Logistics Section Chief

The Logistics Section Chief provides facilities, personnel, equipment, communications, and other resources necessary to support incident operations. Typical responsibilities include:

- Acquiring and distributing resources
- Coordinating communications systems
- Supporting personnel needs
- Managing facilities and equipment
- Tracking resource availability

Finance and Administration Section Chief

The Finance and Administration Section Chief manages financial, procurement, documentation, and administrative functions associated with incident operations. Typical responsibilities include:

- Tracking incident-related costs
- Managing procurement activities
- Documenting personnel time and expenses
- Supporting reimbursement processes
- Maintaining incident financial records

Appendix C: OSINT and Protective Intelligence Technical Considerations

This appendix provides additional technical considerations related to open-source intelligence, social media monitoring, subject-focused research, protective intelligence, and investigative governance. These considerations support the findings and recommendations in Section 5.3.

1. Social Listening, Media Monitoring, and Protective Intelligence

Universities may use several types of tools and processes to support safety, communications, and threat assessment functions. These capabilities overlap but are not interchangeable.

Social listening tools help monitor public online discussion, sentiment, event-related activity, and institutional reputation. Media monitoring tools help track traditional and online media coverage. Law enforcement databases support criminal justice and public safety inquiries. Protective intelligence and OSINT investigative tools support deeper research into specific persons, groups, threats, or behaviors of concern.

A mature program defines the purpose, owner, workflow, documentation requirements, and escalation path for each capability.

2. Subject-Focused OSINT

Subject-focused OSINT may be appropriate when a specific individual, group, communication, or behavior of concern requires additional assessment. Depending on the circumstances, this may include review of:

- Publicly available social media activity
- Online communications
- Public records
- Civil and criminal court records
- Litigation history
- Prior law enforcement contacts
- Publicly available affiliations or networks
- Grievances, fixation, leakage, or target-focused communications
- Event-related threats or concerning statements
- Information from law enforcement, fusion center, or intelligence-sharing partners

The purpose of subject-focused OSINT is to support risk assessment, case management, intervention planning, event security, and protective decision-making. It should not be conducted casually, inconsistently, or without appropriate documentation and oversight.

3. Governance and Documentation

OSINT-related procedures should address:

- Who may conduct OSINT research.
- What circumstances justify subject-focused OSINT.
- What sources may be reviewed.

- What approvals are required.
- How findings are documented.
- How information is validated.
- How screenshots or other records are preserved.
- How irrelevant or sensitive information is handled.
- How long information is retained.
- Who receives findings.
- How findings are incorporated into BAT, UVUPD, emergency management, or event-planning decisions.
- How legal, privacy, and institutional policy issues are reviewed.

4. Investigative Accounts and Operational Security

Threat assessment-related OSINT should not be conducted using personal social media accounts. Use of personal accounts may create operational security, privacy, documentation, attribution, and investigative integrity concerns.

Where OSINT research is authorized, institutions should consider approved investigative accounts, controlled research environments, standardized documentation practices, and supervisory oversight. Policies and procedures may address operational security practices, preservation of content, authorized platforms, account management, and methods for preventing inadvertent exposure of personal or institutional information.

More advanced operational security considerations may include controlled workstations, approved internet environments, virtual research environments, attribution management, and specialized investigative tools. These capabilities should be implemented only with appropriate legal, privacy, cybersecurity, procurement, and supervisory review.

5. Specialized OSINT and Protective Intelligence Platforms

UVU may evaluate dedicated OSINT, protective intelligence, or threat intelligence platforms designed to support subject-focused investigations, identity resolution, monitoring, case documentation, and intelligence reporting. Platform evaluation should be based on institutional need, legal requirements, privacy considerations, cybersecurity, data retention, auditability, integration with existing case-management systems, training needs, and cost.

Examples of industry-recognized enterprise platforms used in OSINT, protective intelligence, or threat intelligence contexts include Ontic,[56] Liferaft,[57] Babel Street,[58] Flashpoint,[59] Fivecast,[60] Skopenow[61] and other similar tools. This list is not a recommendation or endorsement of any vendor. Any vendor

[56] https://ontic.co/

[57] https://liferaftlabs.com/

[58] https://www.babelstreet.com/

[59] https://flashpoint.io/

[60] https://www.fivecast.com/

[61] https://www.skopenow.com/

evaluation should be conducted through UVU's normal procurement, legal, privacy, and cybersecurity review processes.

6. Deep Web, Dark Web, and Alternative Platforms

Some protective intelligence inquiries may require awareness of information outside mainstream social media or traditional web searches. Depending on the matter, relevant information may appear on alternative social media platforms, online forums, message boards, encrypted or semi-private communities, deep web sources, or dark web environments.

These sources present heightened legal, ethical, operational security, cybersecurity, privacy, and safety considerations. They should be accessed only by trained personnel or qualified external resources using approved methods, documented procedures, and appropriate legal, cybersecurity, privacy, and supervisory oversight.

Operational security policies and investigative procedures should address, as appropriate, the authorized use of VPNs or proxies, Tor[62] and other dark web access methods, virtual machines, controlled or segregated internet connections, so-called "dirty" internet connections, air-gapped workstations, agency-managed investigative or "sock puppet" accounts, enterprise-managed attribution tools, and forensic preservation methods. The level of technical control should be based on the nature of the inquiry, the sensitivity of the matter, the risk to personnel or the institution, and applicable legal and policy requirements.

UVU should not rely on ad hoc searches, personal devices, personal social media accounts, or informal access methods for official protective intelligence inquiries involving deep web, dark web, or alternative-platform research. Any use of these sources should occur within a defined governance framework that addresses authorization, training, documentation, retention, evidence preservation, source validation, reporting, and dissemination of findings.

7. Analyst Qualifications and Training

Personnel conducting OSINT or protective intelligence work should receive training in lawful and ethical collection, source evaluation, documentation, reporting, privacy, operational security, and threat assessment integration.

When evaluating internal OSINT analyst staffing or external vendors, UVU may consider recognized training and certification programs. The OSMOSIS Association's Open-Source Certification is one example of a credential that evaluates OSINT-related knowledge across core areas such as critical thinking, tradecraft, reporting, and laws and ethics.[63] Certification should not be the only qualification considered, but it may help identify baseline expertise.

8. Integration with BAT, Event Planning, and Emergency Management

OSINT and protective intelligence are most valuable when integrated into decision-making. Procedures should clarify how relevant information is shared with:

---

62 https://www.torproject.org/

63 https://osmosisassociation.org/certifications/

- Behavioral Assessment Team members
- UVUPD
- Emergency Management
- Event Services
- Communications
- Legal Counsel
- SIAC or other law enforcement partners
- Event security planners
- Executive leadership when appropriate

For elevated-risk events, protective intelligence findings may inform venue selection, staffing, access control, screening, credentialing, protest management, communications planning, mutual aid requests, and Event Action Plans. For BAT cases, findings may inform risk assessment, intervention planning, monitoring, outreach, documentation, and protective measures.

9. Relationship with SIAC and External Partners

SIAC is an important resource for threat-related intelligence, suspicious activity reporting, criminal intelligence, targeted violence prevention, and information sharing. UVU should continue leveraging SIAC for pre-event threat assessments, threat management consultation, training, information sharing, and support for elevated-risk cases.

UVU should also define when and how SIAC, local law enforcement, state partners, or qualified external OSINT resources may be engaged to support specific cases or events.

10. Leveraging SIAC's Existing Intelligence and Information-Sharing Platform

A potential opportunity exists for UVU to leverage SIAC's existing intelligence and information-sharing technology to support threat management, protective intelligence, suspicious activity reporting, major-event planning, and information sharing. SIAC currently uses Kaseware as part of its investigations, intelligence, and information-sharing environment. Because SIAC already has this capability in place, UVU may not need to develop or procure a wholly separate platform to improve access to certain intelligence workflows, analytical support, or information-sharing processes.

This appendix does not recommend or endorse a specific vendor. Rather, the relevance of Kaseware is that SIAC already uses the platform in support of its fusion center mission. UVU should explore whether SIAC's existing environment can support appropriate collaboration involving threat information, suspicious activity reports, investigative leads, intelligence products, event-related intelligence, and other information relevant to campus safety.

A structured discovery process involving UVU, SIAC, UVUPD, Emergency Management, the Behavior Assessment Team, Legal Counsel, and other appropriate stakeholders would help determine the most appropriate operating model. That process should evaluate whether UVU would benefit from direct platform access, a dedicated tenant, a shared collaborative environment, a SIAC-managed workflow, or another structure that supports operational needs while preserving appropriate access controls, auditability, data ownership, privacy protections, and organizational independence.

The discovery process should address, at a minimum:

- What types of threat, suspicious activity, event-security, or protective intelligence information UVU would submit to or receive from SIAC.
- Which UVU personnel, if any, should have direct access to the platform.
- Whether UVU should operate within a dedicated tenant, a shared collaboration space, or a SIAC-managed process.
- How access controls, audit logs, role-based permissions, retention rules, and data ownership would be managed.
- How sensitive student, employee, law enforcement, and behavioral threat assessment information would be protected.
- How information-sharing procedures would be documented through memoranda of understanding, operating procedures, or other agreements.
- How intelligence products or investigative leads would be incorporated into Security Assessments, Event Action Plans, BAT processes, Emergency Operations Center operations, and public safety decision-making.
- How legal, privacy, cybersecurity, procurement, and records-retention requirements would be reviewed before implementation.

UVU and SIAC may also wish to evaluate whether specialized OSINT tools, such as OSINT Combine's NexusXplore or similar platforms, should be deployed through SIAC, UVU, or a hybrid model. A SIAC-supported model may allow UVU to benefit from SIAC's existing intelligence mission, analytical personnel, public safety relationships, and information-sharing processes without requiring UVU to independently develop and sustain a specialized OSINT capability. A UVU-based or hybrid model may be appropriate if UVU determines that it needs more direct control over intake, documentation, event planning, or case-support workflows.

Any use of OSINT tools should remain subject to the governance principles described in this appendix, including clear authorization, trained users, approved investigative methods, documentation standards, privacy review, legal review, cybersecurity review, retention rules, and supervisory oversight.

In the Project Team's assessment, UVU should explore whether SIAC's existing Kaseware environment, SIAC's analytical capabilities, and appropriate OSINT tools can support a more collaborative and intelligence-informed approach to campus safety. The goal should not be technology acquisition for its own sake, but improved information sharing, better threat awareness, stronger documentation, more coordinated investigations, and more informed decision-making for threat assessment, major-event planning, and incident response.

Appendix D: Event Security Planning and Protective Measures Reference Guide

D.1: Event Security Planning Framework for High-Profile Events

The level of security planning associated with an event should be commensurate with the event's risk profile, anticipated attendance, venue characteristics, public visibility, and threat environment. While every event does not require the same degree of planning, the following elements are commonly incorporated into comprehensive event security programs.

Security Assessment

Event planning begins with identifying potential threats, assessing vulnerabilities, evaluating potential consequences, and determining appropriate mitigation measures. Factors often considered include anticipated attendance, protest activity, speaker profile, venue characteristics, historical incidents, and intelligence information.

Security Planning and Coordination

Effective event security planning integrates venue management, law enforcement, security personnel, emergency management, communications personnel, event organizers, and executive protection representatives. Planning activities commonly include coordination meetings, site visits, communications planning, contingency planning, and assignment of responsibilities.

Executive Protection Considerations

For high-profile speakers and guests, planning often includes advance site assessments, protective intelligence reviews, secure arrival and departure procedures, route planning, communications protocols, medical contingencies, and emergency evacuation procedures.

Access Control and Credentialing

Depending on the event's risk profile, organizations may implement ticketing systems, staff and contractor credentialing procedures, controlled access points, prohibited-items policies, screening procedures, and guest verification processes.

Screening Operations and Staffing Considerations

When screening operations are implemented, organizations should clearly define roles and responsibilities for security personnel, event staff, and law enforcement officers. Screening personnel should receive training on prohibited-items policies, screening procedures, ADA accommodations, de-escalation techniques, communications protocols, and escalation procedures.

In many event environments, primary screening functions are performed by trained security personnel or event staff, with law enforcement personnel available to provide supervisory support, respond to incidents, address prohibited or illegal items, and manage enforcement actions when necessary. This approach allows law enforcement resources to remain available for incident response, crowd management, intelligence functions, and other security responsibilities while maintaining effective screening operations.

Security Staffing and Deployment

Security plans typically identify staffing levels, supervisory responsibilities, fixed posts, mobile patrols, crowd management personnel, emergency response resources, and command personnel. Staffing requirements should be informed by the event's size, complexity, and risk profile.

Intelligence and Situational Awareness

Event planning may incorporate intelligence gathering, social media monitoring, open-source intelligence (OSINT), law enforcement information sharing, protective intelligence activities, and real-time situational awareness measures.

Emergency Response Planning

Security plans should identify emergency procedures for medical emergencies, fires, severe weather, disturbances, active assailant incidents, evacuations, shelter-in-place situations, and other foreseeable contingencies.

Traffic and Perimeter Management

Planning may include arrival and departure routes, emergency vehicle access, parking management, pedestrian flow, temporary barriers, road closures, and perimeter control measures.

Command and Communications

Events benefit from clearly defined command structures, communications plans, coordination procedures, and incident escalation protocols. Larger events may warrant the establishment of a command post or integration with emergency management structures.

Post-Event Review

Following significant events, organizations should conduct structured debriefings to identify lessons learned, evaluate operational effectiveness, document challenges, and capture opportunities for future improvement, including an After-Action Review.

D.2: Event Screening Operations Planning Considerations

For major events, high-profile speakers, controversial events, or events with elevated security concerns, UVU should consider developing written screening procedures that address attendees, bags, containers, vendors, deliveries, equipment, vehicles, staff, VIPs, officials, emergency responders, and event participants. Screening procedures should be tailored to the event's risk profile, venue, expected attendance, crowd flow, legal constraints, staffing levels, and available equipment. Written screening procedures should address:

- Screening authority and conditions of entry
- Permitted and prohibited items
- Bag and container restrictions
- Entry-point layout and queuing
- Staffing assignments and supervisory roles
- Law enforcement support and escalation procedures

- Equipment selection, testing, calibration, and backup methods
- Signage and pre-event communications
- Medical, ADA, VIP, official, vendor, delivery, staff, emergency responder, and participant exceptions
- Documentation, incident reporting, and post-event review

For bag and container screening, UVU should consider:

- Clearly posting signage regarding bag checks and prohibited items.
- Communicating bag restrictions, including size, before the event through websites, ticketing language, social media, email, and event materials.
- Using clear-bag policies for selected events when legally permissible and operationally appropriate.
- Inspecting bags and containers before entry to the venue.
- Using tables or other screening stations to support efficient screening.
- Providing appropriate tools, lighting, and protective measures for screening personnel.
- Establishing express lanes for attendees with no bags or items requiring inspection.
- Creating designated lanes for medical devices, mobility devices, diaper bags, staff, vendors, participants, and equipment.

If hand-held metal detectors, walk-through magnetometers, X-ray screening, weapons-detection systems, or other screening equipment are used, UVU should ensure that personnel are trained on equipment use, alarm resolution, secondary screening, calibration, and escalation procedures. Sufficient equipment and staffing should be provided to reduce entry delays and avoid crowding at screening points.

If pat-downs are used, UVU should develop written procedures in consultation with legal counsel. Procedures should address privacy, dignity, consent or conditions of entry, gender-related considerations, witness procedures, semi-private screening locations, refusal procedures, documentation, and law enforcement support. Personnel conducting pat downs should receive specialized training, including sensitivity training and instruction on respectful, nondiscriminatory screening practices.

Screening procedures should be tested before major events. Testing may include equipment checks, staffing rehearsals, tabletop exercises, entry-flow simulations, and controlled penetration testing or red-team exercises designed to evaluate whether screening procedures are understood and effective. Results should be documented and used to improve procedures, staffing, equipment deployment, communications, and training.

D.3: Access Control, Ticketing, and Credentialing Considerations

Access control, ticketing, and credentialing are core components of event security planning. These functions help determine who may enter an event, where individuals may go once inside the event footprint, what restrictions apply, and how event organizers, security personnel, and law enforcement will manage authorized and unauthorized access.

Access-control planning should be based on the event's risk profile, anticipated attendance, venue configuration, public visibility, speaker or guest profile, threat environment, legal considerations, and operational capacity. For elevated-risk events, planners should evaluate whether the venue can support controlled entry, ticket verification, credentialing, screening, designated entry and exit points, restricted-access areas, and controlled movement between public and non-public spaces.

Access-control measures may include:

- Defined event boundaries
- Designated entry and exit points
- Ticket verification
- Credentialing procedures
- Restricted-access zones
- Staff and vendor check-in points
- Media check-in areas
- VIP or speaker access controls
- Emergency responder access points
- Controlled delivery areas
- Re-entry rules
- Late-entry procedures
- Conditions of entry
- Prohibited-items policies
- Screening procedures, when legally permissible and operationally appropriate

Access-control plans should address both normal operations and exceptions. Exceptions may include medical needs, ADA-related accommodations, emergency responder access, credentialed media, staff and vendor access, VIP movement, late-arriving participants, and emergency conditions. Plans should also identify how unauthorized access, fraudulent credentials, refusal to comply with conditions of entry, prohibited items, disruptive behavior, or suspicious activity will be handled.

Ticketing should be treated as a security and planning tool, not solely as an administrative or attendance-management function. Ticketing systems can support crowd management, occupancy control, staffing decisions, access-control planning, emergency egress planning, fraud prevention, accountability, and real-time situational awareness. For major or elevated-risk events, ticketing data should help planners evaluate expected attendance, peak arrival times, crowd-density concerns, venue suitability, staffing requirements, and emergency response needs.

When outside event organizers manage ticketing or registration, UVU should consider requiring advance and continuing access to ticketing or registration data. This may include projected attendance, total registrations, ticket distribution, VIP or special-access lists, staff and volunteer lists, vendor lists, media lists, waitlist information, and expected arrival patterns. Access to this information supports more accurate planning and reduces uncertainty regarding crowd size, staffing, screening, credentialing, and emergency operations.

Credentialing provides an additional layer of access control by allowing planners to distinguish between public areas, restricted areas, controlled-access zones, VIP areas, media areas, technical areas, back-of-house spaces, command posts, emergency operations areas, and other secure locations. A credentialing plan should define who is authorized to access each area, how credentials will be issued and verified,

what access levels are permitted, and how unauthorized access will be handled. Credentials may include:

- Staff badges
- Contractor or vendor passes
- Media credentials
- Law enforcement or emergency responder credentials
- VIP or speaker access passes
- Volunteer credentials
- Digital tickets or passes
- Parking credentials
- Technical or production credentials
- Command post or operations credentials

Credentialing plans should identify access levels, credential design, issuing authority, verification procedures, expiration times, replacement procedures, lost-credential protocols, and procedures for revoking or denying access. For larger or elevated-risk events, planners should consider whether credentials need to be color-coded, role-specific, date-specific, zone-specific, or integrated with electronic access-control systems.

Access-control and credentialing personnel should receive clear instructions before the event. Written post orders should identify the purpose of each access point, who is authorized to enter, what credentials or tickets are valid, what exceptions apply, how issues should be escalated, and who has authority to resolve disputes. Personnel should also be trained to recognize suspicious behavior, fraudulent credentials, tailgating, unauthorized attempts to enter restricted areas, and conditions requiring law enforcement support.

Event access-control plans should also address late gate opening, re-entry, and any circumstances in which screening or ticketing operations may be modified. If screening, ticketing, or credential verification is part of the security plan, those controls should not be discontinued simply to expedite entry unless the change has been reviewed and approved through the event command structure. If re-entry is restricted, exceptions should be defined in advance for medical, ADA-related, childcare, operational, or emergency circumstances.

Because access control, screening, prohibited-items policies, firearms issues, bag restrictions, and conditions of entry may raise legal considerations, UVU should coordinate with legal counsel when developing event-specific access control and credentialing procedures for events held on public University property.

D.4: Common Event Security Posts and Functions

Effective event security operations rely on clearly defined security posts, assigned responsibilities, established reporting relationships, and coordinated communications. The specific number and type of posts should be based on the event's risk profile, venue characteristics, attendance, threat environment, and operational objectives.

Supervisory Posts

Supervisors provide leadership, oversight, and operational coordination for designated areas of responsibility. Supervisors monitor personnel performance, respond to incidents requiring additional authority, coordinate resource deployment, and serve as the primary link between field personnel and command staff. Common practice is to assign supervisors responsibility for defined geographic zones or functional areas to ensure timely response and effective span of control.

Access Control and Screening Posts

Access-control personnel regulate entry into controlled or restricted areas and help ensure compliance with event security procedures. Responsibilities may include validating tickets, credentials, badges, or passes; monitoring entry points; enforcing access restrictions; screening for prohibited items; managing attendee queues; and reporting suspicious behavior or security concerns. These posts often serve as the first layer of event security and may incorporate personnel, technology, physical barriers, or screening equipment depending on the event's risk profile.

Crowd Management Posts

Crowd-management personnel monitor attendee behavior, crowd density, and pedestrian movement patterns. These personnel help facilitate orderly ingress and egress, identify congestion points, assist with wayfinding, intervene in minor disturbances, and support emergency evacuation procedures when necessary. Crowd management positions are particularly important in high-density areas, event entrances and exits, gathering locations, and areas where protests or demonstrations may occur.

Stage and VIP Protection Posts

Stage and VIP protection personnel are responsible for protecting speakers, performers, executives, dignitaries, and other protected individuals. These posts help maintain secure buffer zones, monitor audience behavior near the stage, control access to restricted areas, coordinate with executive protection personnel, and respond to disruptions or security concerns involving protected individuals.

Perimeter Security Posts

Perimeter security personnel monitor the boundaries of the event area and help prevent unauthorized access. Depending on the venue, these posts may monitor fencing, barricades, gates, pedestrian access points, parking areas, natural barriers, or designated protest areas. Perimeter personnel also help identify vulnerabilities, detect suspicious activity, and provide early warning of emerging issues outside the primary event footprint.

Roving Patrol Posts

Roving patrol personnel provide mobile security coverage throughout the event area. These personnel may patrol on foot, bicycle, vehicle, or other authorized means and are often responsible for monitoring conditions, identifying hazards, responding to minor incidents, and providing visible deterrence. Roving personnel also support situational awareness by identifying developing issues before they escalate into larger incidents.

Parking and Traffic Posts

Parking and traffic personnel assist with vehicle access, pedestrian safety, traffic flow, emergency vehicle routes, parking management, and ingress and egress operations. These positions help reduce congestion, improve safety, and facilitate emergency response access when necessary.

Command Post Personnel

Command post personnel provide operational oversight, resource coordination, communications support, intelligence sharing, and incident management functions. These personnel maintain situational awareness, coordinate field resources, document significant activities, and support decision-making throughout the event.

Emergency Response Teams

Emergency Response Teams (ERTs) provide surge capacity and rapid response capabilities for incidents requiring additional personnel. These teams may respond to disturbances, medical emergencies, crowd-control issues, evacuations, suspicious activity, or other security concerns requiring immediate intervention. The use of designated response teams can improve operational flexibility and help event organizers manage incidents without disrupting broader event operations.

Key Principles

Regardless of the specific security model employed, effective event security operations generally incorporate three foundational principles:

- Clearly defined posts with assigned responsibilities and accountability.
- Appropriate supervisory oversight and span of control.
- Integration with the Incident Command System (ICS), Event Action Plan (EAP), and emergency response procedures.

D.5 Protective Operations Considerations for Outdoor Events

This appendix provides operational considerations for outdoor events involving high-profile speakers, controversial events, large crowds, or other circumstances that may require enhanced protective planning. These details should be treated as sensitive security information and distributed only to personnel with a need to know.

Pre-event planning should include a coordinated walk-through involving UVUPD, event organizers, emergency management, local law enforcement partners, and any executive protection detail assigned to the speaker or VIP. The walk-through should address:

- Arrival and departure points
- Line-of-sight concerns
- Elevated positions and rooftops
- Building, room, and window access
- Potential protester locations
- Security post locations
- External law enforcement support

- Communications capabilities
- Emergency access and egress routes
- Protective movement routes
- Crowd placement and barriers
- Contingency plans for relocation, evacuation, lockdown, or shelter-in-place

When an outdoor event presents line-of-sight or elevated-position concerns, UVUPD should evaluate whether the event can be moved indoors or whether the identified risks can be reasonably mitigated. If the event remains outdoors, security planning should include control or monitoring of buildings, rooftops, windows, stairways, ladders, parking structures, tree lines, and other areas that overlook the event site. Where staffing is limited, UVU should consider physical screening, line-of-sight obstruction, restricted access areas, or mutual aid support to reduce exposure.

Arrival and departure areas for speakers, VIPs, and other protectees should be planned to minimize public visibility and unnecessary exposure. When appropriate, protective planning may include controlled entry points, screened movement routes, vehicle placement, temporary barriers, canopies or tents, parking structures, or other measures that reduce visibility and improve control of the area.

UVUPD should also consider whether staffing plans provide sufficient fixed-post coverage and mobile response capacity. Fixed posts may be needed to control key access points, while mobile officers may be needed to respond to incidents without leaving critical posts unattended. Staffing limitations should be addressed through advance planning, mutual aid agreements, and coordination with nearby law enforcement partners or university police agencies.

Training for UVUPD and partner agencies should address protective operations for high-profile outdoor events, including line-of-sight assessment, elevated-position concerns, site control, access control, coordination with executive protection details, communications, and event-specific response planning. Joint training with local agencies and nearby university police departments would support a more coordinated response during major events.

D.6: Traffic, Parking, and Perimeter Security Considerations

Traffic, parking, and perimeter security are important components of event security planning, particularly for outdoor events, large gatherings, controversial speakers, and events involving elevated security concerns. Effective planning helps facilitate safe movement of people and vehicles, maintain emergency access, reduce congestion, establish event boundaries, and mitigate security risks associated with unauthorized access or vehicle-related threats.

Traffic Management

Traffic management plans should address the movement of vehicles and pedestrians before, during, and after an event. Planning considerations may include:

- Arrival and departure routes
- Traffic-control points
- Road closures and detours
- Shuttle operations
- Rideshare pick-up and drop-off locations

- Accessible parking and ADA accommodations
- Loading and delivery access
- Emergency vehicle routes
- Post-event departure operations
- Coordination with local law enforcement, transportation agencies, parking vendors, and public works departments may be necessary for larger events.

Parking Operations

Parking areas are often the first and last points of interaction attendees have with an event and should be considered part of the overall security footprint. Parking plans may address:

- Parking-lot capacity and overflow procedures
- Alternate parking locations
- Pedestrian routes from parking areas to the venue
- Lighting and visibility
- Parking-lot patrols
- CCTV coverage
- Suspicious-activity reporting procedures
- Vehicle access controls
- Emergency response access

Depending on the event's risk profile, parking areas may warrant dedicated staffing, roving patrols, temporary surveillance measures, or periodic security inspections.

Perimeter Security

Perimeter security measures establish the boundaries of the event and help control the movement of attendees, staff, vendors, media personnel, and vehicles. The objective is to create a secure and manageable environment while maintaining safe access and emergency egress. Perimeter security measures may include:

- Temporary fencing
- Barricades
- Gates
- Designated entry and exit points
- Controlled-access zones
- Restricted areas
- Vehicle-control points
- Security staffing
- Signage and wayfinding

The level of perimeter security should be proportional to the event's risk profile, venue characteristics, attendance, and threat environment.

Vehicle Mitigation and Protective Barriers

For outdoor events, planners may consider physical measures designed to reduce the risk of unauthorized vehicle access or vehicle-related attacks. Depending on the venue and threat assessment, these measures may include:

- Bollards
- Planters
- Jersey barriers
- Water-filled barriers
- Vehicle barricades
- Temporary fencing systems
- Crash-rated gates
- Vehicle-control points
- Heavy vehicles positioned as protective barriers

When evaluating protective barriers, planners should consider vehicle approach routes, vehicle speed, pedestrian density, emergency access requirements, and appropriate standoff distances from attendees, structures, and critical infrastructure. The selection of barrier systems should balance security requirements, operational needs, emergency access, aesthetics, and the overall attendee experience.

Parking and Perimeter Patrols

Parking areas and perimeter zones should be incorporated into security patrol plans. Depending on the size and nature of the event, patrol resources may include:

- Law enforcement personnel
- Security officers
- Roving foot patrols
- Bicycle patrols
- Vehicle patrols
- CCTV monitoring
- Drone or aerial observation resources where legally permissible

Patrol personnel can help identify suspicious activity, monitor crowd movement, detect perimeter vulnerabilities, respond to incidents, and provide visible deterrence.

Signage and Wayfinding

Signage serves both operational and security functions. Effective signage helps reduce confusion, improve crowd flow, communicate security procedures, and support emergency operations. Signage considerations may include:

- Parking directions
- Shuttle locations
- Designated entrances and exits
- Accessible routes
- Emergency exits
- Restricted access areas
- Prohibited items notifications
- Screening requirements
- Emergency contact information
- Suspicious-activity reporting information

Information should be communicated through multiple channels whenever practical, including websites, social media, event communications, parking areas, transit points, pedestrian routes, and venue entrances.

Key Planning Considerations

Traffic, parking, and perimeter planning efforts are most effective when they:

- Support safe and efficient movement of attendees.
- Maintain emergency vehicle access and operational flexibility.
- Integrate with event security, access control, and emergency-response plans.
- Provide clear communication and wayfinding.
- Establish reasonable protection against foreseeable risks.
- Balance security needs with the overall event experience.

D.7: Fixed and Temporary Site Security Measures

Fixed and temporary site security measures help define event boundaries, control movement, support screening operations, protect pedestrian areas, reduce unauthorized access, and improve emergency response coordination. These measures should be selected based on the event's risk profile, venue characteristics, anticipated attendance, crowd movement, traffic patterns, public visibility, threat environment, and emergency response needs. Site security measures may include:

- Temporary fencing
- Gates
- Barricades
- Stanchions
- Concrete barriers
- Water-filled barriers
- Bollards
- Planters
- Vehicles used as protective barriers
- Signage
- Access-control points
- Screening areas
- Controlled delivery points
- Restricted access zones
- Vehicle-control points
- Lighting
- Cameras or temporary surveillance measures

For outdoor events, physical controls should help establish a clear and manageable event footprint. These measures can direct attendees to approved entrances, separate pedestrians from vehicles, protect screening areas, create buffer zones between the event site and adjacent roads, and help personnel identify unauthorized access or perimeter breaches.

Temporary fencing and barricades should be used in a way that supports both security and life safety. Barriers should not obstruct emergency exits, emergency vehicle access, evacuation routes, ADA-

accessible paths, or responder staging areas. Any fencing or barricade plan should be reviewed for crowd-flow, emergency egress, accessibility, and operational feasibility.

When roads remain open near an event site, planners should evaluate whether temporary barriers are sufficient or whether additional measures are needed, such as law enforcement staffing, road closures, traffic-control points, vehicle screening, or alternate pedestrian routing. If temporary barricades are used to control roads or vehicle access points, they should be staffed, monitored, or otherwise incorporated into the security plan.

Vehicle-related risk should also be considered for outdoor events, high-density pedestrian areas, and venues adjacent to active roadways. Depending on the Security Assessment and venue configuration, planners may consider bollards, planters, Jersey barriers, water-filled barriers, concrete barriers, gates, vehicle-control points, or strategically positioned heavy vehicles. Barrier selection should account for vehicle approach routes, potential vehicle speed, pedestrian density, standoff distance, emergency access, aesthetics, and the overall attendee experience.

Physical controls should be coordinated with access control, screening, traffic, parking, communications, and emergency response plans. For example, a fencing plan should align with designated entry points, screening queues, credentialing locations, emergency exits, command post access, delivery routes, and responder access points. Similarly, vehicle barriers should be placed in a way that protects attendees while preserving the ability of emergency vehicles to reach the venue.

Site security measures should also account for vendors, deliveries, staff, event participants, media, VIPs, emergency responders, and people requiring ADA-related accommodations. Designated entry points, delivery checkpoints, staff lanes, equipment routes, and accessible paths should be identified in advance and communicated to personnel responsible for access control.

Temporary measures should be inspected before, during, and after the event. Personnel should check for gaps, damaged barriers, unsecured gates, blocked exits, unstaffed access points, unauthorized movement through restricted areas, and changes in crowd behavior or traffic patterns that require adjustments. Any changes to the site-security layout during an event should be communicated through the event command structure.

D.8: Announcements and Scripted Response Protocol Messages

HOLD

PA, phone, text, email, signage, and voicemail: **HOLD, HOLD, HOLD!** THIS IS NOT A TEST! We are responding to a report of (problem) at (location). Calmly and quickly clear the hallways and remain in your current room, office, classroom, or general area. Continue normal activity unless otherwise directed. Remain in your location until given the **ALL CLEAR**. Watch for additional information and updates. (Send message three times, two minutes apart.)

PA, phone, text, email, signage, and voicemail: **ALL CLEAR, ALL CLEAR, ALL CLEAR**. The incident at (location) has been resolved and it is safe to return to normal activity. (Send message three times, two minutes apart.)

LOCKDOWN

PA, phone, text, email, signage, and voicemail: **LOCKDOWN, LOCKDOWN, LOCKDOWN!** THIS IS NOT A TEST! We are responding to a report of (problem) at (location). The facility will be in **LOCKDOWN**. Calmly and quickly move to the nearest Safe Room,[64] lock the door, and remain there until given the **ALL CLEAR**. Watch for additional information and updates. (Send message three times, two minutes apart.)

PA, phone, text, email, signage, and voicemail: **ALL CLEAR, ALL CLEAR, ALL CLEAR**. The incident at (location) has been resolved and it is safe to return to normal activity. (Send message three times, two minutes apart.)

EVACUATE

PA, phone, text, email, signage, and voicemail: **EVACUATE, EVACUATE, EVACUATE!** THIS IS NOT A TEST! Calmly and quickly **EVACUATE** the building using all available exits. Move away from the building to your designated Assembly Area and remain there until given the **ALL CLEAR**. Watch for additional information and updates. (Send message three times, two minutes apart.)

PA, phone, text, email, signage, and voicemail: **ALL CLEAR, ALL CLEAR, ALL CLEAR**. The incident at (location) has been resolved and it is safe to return to normal activity. (Send message three times, two minutes apart.)

SECURE[65]

PA, phone, text, email, signage, and voicemail: **SECURE, SECURE, SECURE**! THIS IS NOT A TEST! We are responding to a report of (problem) at (location). Calmly and quickly **SECURE** inside the building using all available entrances. Move to the nearest Safe Room and lock the door. Remain there until given the **ALL CLEAR.** Watch for additional information and updates. (Send message three times, two minutes apart.)

PA, phone, text, email, signage, and voicemail: **ALL CLEAR, ALL CLEAR, ALL CLEAR**. The incident at (location) has been resolved and it is safe to return to normal activity. (Send message three times, two minutes apart.)

SHELTER

PA, phone, text, email, signage, and voicemail: **SHELTER, SHELTER, SHELTER**! THIS IS NOT A TEST! We are responding to a report of (problem) at (location). Please **SHELTER** and take precautions until given the **ALL CLEAR**. Watch for additional information and updates. (Send message three times, two minutes apart.)

PA, phone, text, email, signage, and voicemail: **ALL CLEAR, ALL CLEAR, ALL CLEAR**. The incident at (location) has been resolved and it is safe to return to normal activity. (Send message three times, two minutes apart.)

---

[64] A safe room refers to a designated place of refuge that offers enhanced security during an armed-intruder event; where storm protection is intended, FEMA defines a safe room as a hardened structure designed to meet FEMA criteria and provide near-absolute protection during extreme wind events.

[65] Secure is the rapid and safe movement of people from outdoor areas into a facility or other safer indoor location when the source of danger is outside. FEMA states that Secure (also known as Reverse Evacuation) is used "to rapidly and safely move people inside a facility when it would be dangerous to remain outside," such as when people are on playgrounds, sports fields, or at an outdoor event and the danger is outside.

ACTIVE ASSAILANT

PA, phone, text, email, signage, and voicemail: **ACTIVE ASSAILANT, ACTIVE ASSAILANT, ACTIVE ASSAILANT!** THIS IS NOT A TEST! A subject with a weapon is in the building. Calmly and quickly move to the nearest Safe Room, lock the door, and remain there until given the **ALL CLEAR**. If you are not in the building, stay away and wait for the **ALL CLEAR** notification. Watch for additional information and updates. (Send message three times, two minutes apart.)

PA, phone, text, email, signage, and voicemail: **ALL CLEAR, ALL CLEAR, ALL CLEAR**. The incident at (location) has been resolved and it is safe to return to normal activity. (Send message three times, two minutes apart.)

D.9: Physical Security Technology Technical Considerations

This appendix provides additional technical context regarding physical security technologies referenced in Section 5.2. These considerations are intended to support future planning, budgeting, system evaluation, and implementation decisions.

Integrated Security Management

A mature campus security technology environment may integrate access control, video surveillance, intrusion detection, panic alarms, lockdown capabilities, public address systems, mapping, and mass notification tools. Integration can allow defined events, such as a forced door, panic alarm, duress activation, or intrusion alarm, to trigger associated video, location information, maps, automated alerts, and response workflows.

An integrated or unified platform can help Dispatch and command personnel view relevant alarm and video information through a common graphical user interface. This can reduce the need to monitor multiple disconnected systems and improve response coordination.

Access Control System Considerations

UVU uses an industry-recognized access-control system. Future access-control planning may include:

- Enterprise-wide credential audits
- Deactivation of expired or unauthorized badges
- Role-based access by building, room, day, time, and operational need
- Defined approval authority for card issuance and access levels
- Oversight by Human Resources, student records, or other authoritative systems
- Integration with student records, employment records, contractor records, or visitor-management systems where feasible
- Automated updates or deactivation when student, employee, contractor, or visitor status changes
- Cardholder image capture and verification at selected critical access points
- Evaluation of whether select access points should remain controlled 24 hours a day
- Use of visible visitor or contractor badges where appropriate
- Evaluation of turnstiles or other access-control measures for selected high-control areas

Any consideration of biometric authentication, facial recognition, or advanced identity verification should include legal review, privacy review, accessibility considerations, cybersecurity evaluation, data governance, retention policies, and community impact considerations.

Access Control and Video Integration

Integration between the access-control system and video management system can allow alarms, door-forced events, door-held-open events, or access-denied events to call up associated video. This can help Dispatch or authorized personnel confirm what occurred, identify who was present, and determine what response is needed.

If UVU retains separate access-control and video platforms, integration between those systems may be pursued through available manufacturer tools or application programming interfaces. If UVU evaluates replacement platforms in the future, unified systems may be considered as part of a broader technology roadmap. Any vendor-specific decision should be based on operational requirements, lifecycle cost, cybersecurity, integration capability, maintenance burden, training needs, procurement requirements, and long-term support.

Video Surveillance Coverage and Modernization

Information provided during the review indicated that camera coverage does not extend to all interior and exterior campus areas. Future expansion should be guided by risk and operational need, including:

- Building entrances and exits
- Major pedestrian pathways
- Event venues and outdoor gathering areas
- Parking areas and vehicle access points
- Elevated areas, rooftops, balconies, and terraces
- Public-facing service areas
- Emergency routes and staging areas
- Areas with prior incidents or recurring security concerns

A camera standard for new installations can simplify maintenance and improve system performance. Standards may address manufacturer compatibility, camera type, resolution, low-light capability, field of view, on-board analytics, cybersecurity, environmental rating, retention needs, and compatibility with the video management system.

Video Analytics

Selected video analytics may support security operations when properly configured, tested, and monitored. Potential analytics include:

- Perimeter or virtual-fence detection
- License plate recognition in vehicle areas
- Restricted-area or rooftop intrusion detection
- Object-left-behind detection
- Anti-tailgating detection
- Fall detection
- Occupancy or crowd-density detection
- Traffic-flow or pedestrian-flow monitoring

- Wrong-way movement detection
- Speed monitoring
- Loitering detection
- Crowd detection thresholds
- Weapons-detection analytics where legally permissible, operationally justified, and actively monitored

Analytics should be evaluated based on reliability, false alarm rates, privacy impact, legal requirements, monitoring capacity, integration with response workflows, and usefulness to Dispatch or command personnel.

Video Storage, Retention, and Resilience

Video surveillance planning should account for server capacity, storage needs, retention periods, system performance, and resilience. Potential considerations include:

- Replacement planning for aging cameras and servers.
- Storage expansion to support added cameras or higher-resolution video.
- Retention policies aligned with operational, investigative, legal, and privacy requirements.
- Off-site or cloud-based backup where appropriate.
- Protection against natural disasters, theft, cybersecurity incidents, and site-specific system failures.

Dispatch Monitoring and Event Views

For large campus events, programmed camera views can help Dispatch and command personnel monitor priority areas. These may include:

- Event site overview
- Speaker or stage area
- Crowd entry and exit points
- Protest areas
- Rooftops and elevated positions
- Parking areas and vehicle routes
- Emergency response routes
- Command post access points
- Restricted areas
- Building entrances near the event

Event Action Plans should identify who will monitor these feeds, how observations will be communicated, what conditions require escalation, and how video will be preserved during or after an incident.

Panic Alarms, Duress Devices, and Emergency Call Points

Panic alarms, duress devices, and emergency call points may be considered for selected locations based on risk and operational need. Potential locations include:

- Public-facing administrative offices
- People and Culture or Human Resources offices
- Student Life and student service areas

- Event venues
- Cash-handling locations
- Isolated exterior locations
- Parking areas
- Areas with recurring conflicts or safety concerns

These systems should include clear location information, Dispatch monitoring, defined response procedures, regular testing, user training, and integration with video where feasible.

Emergency Call Boxes

Exterior emergency call boxes may be considered in selected areas where direct emergency communication is needed. Common features include visible blue lights, emergency call buttons, direct connection to Dispatch, and associated camera coverage where feasible. Placement decisions should be based on lighting, pedestrian routes, parking areas, isolated locations, call volume, mobile-phone coverage, accessibility, maintenance, and integration with Dispatch response procedures.

Aerial Observation and Partner Agency Support

Drone or aerial observation capabilities may support situational awareness during large outdoor events, demonstrations, searches, or major incidents when legally permissible and operationally appropriate. If UVU does not maintain this capability internally, mutual aid agreements or interagency procedures may identify partner agencies that can provide aerial observation support.

Planning considerations include legal authority, privacy, flight restrictions, operator certification, request procedures, command integration, video sharing, evidence preservation, and public communications.

D.10: Post-Event Review Considerations

Post-event review is an important component of continuous improvement. Following significant events, elevated-risk events, incidents, or events involving unusual operational challenges, UVU should conduct a structured review to identify lessons learned, evaluate operational effectiveness, document challenges, and capture opportunities to improve future planning.

Post-event reviews may range from a brief hotwash to a formal after-action review, depending on the event's size, complexity, risk profile, and whether incidents occurred. Reviews should be conducted soon enough after the event that participants can provide accurate observations, but with enough structure to ensure the review is useful, documented, and tied to corrective action.

A post-event review may examine:

- Pre-event planning and coordination
- Risk assessment and intelligence information
- Venue selection and site layout
- Access control, ticketing, credentialing, and screening
- Staffing levels and post assignments
- Supervisory structure and span of control
- Command structure and decision-making

- Communications among event personnel, UVUPD, university leadership, and external responders
- Emergency notification and public messaging
- Crowd management and attendee behavior
- Protest activity or counter-event activity
- Traffic, parking, shuttle, and rideshare operations
- Emergency vehicle access
- Perimeter security and barrier placement
- Medical response
- Fire, EMS, and law enforcement coordination
- Vendor, media, VIP, and delivery access
- ADA-related accommodations
- Incident documentation
- Technology performance
- Public feedback, student feedback, and stakeholder concerns
- Post-event departure and site closure

Reviews should include the personnel and stakeholders most directly involved in planning and operations. Depending on the event, participants may include UVUPD, emergency management, event organizers, facilities, communications personnel, legal counsel, student affairs, parking and transportation, local law enforcement, fire, EMS, contracted security, venue staff, and representatives from the sponsoring organization. The review should distinguish between:

- What was planned
- What actually occurred
- What worked well
- What created challenges
- What should be changed before future events

The process should include both operational observations and attendee-facing issues, such as confusion about entry points, prohibited items, emergency messaging, parking, crowd movement, or event closure.

When incidents or significant disruptions occur, UVU should preserve relevant records before they are overwritten, deleted, or dispersed. Records may include event plans, staffing rosters, post orders, radio audio and logs, Dispatch records, emergency messages, surveillance video, photographs, incident reports, ticketing data, credentialing records, public communications, social media monitoring summaries, and correspondence with external partners.

Post-event reviews should result in documented corrective actions. Corrective actions should identify the issue, recommended improvement, responsible owner, priority level, target completion date, resource needs, and follow-up process. Items that require policy changes, training, technology investment, mutual aid coordination, legal review, or budget approval should be tracked until resolved.

For recurring events or future events involving similar risks, lessons learned should be incorporated into event templates, planning checklists, training materials, post orders, emergency message templates, access-control plans, and tabletop exercises. This helps ensure that lessons are institutionalized and not dependent on individual memory or informal knowledge.