MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND
SAFETY INSTITUTE
LAW ENFORCEMENT BULLETIN

STRENGTHENING POLICY AND AWARENESS IN A HEIGHTENED GLOBAL THREAT ENVIRONMENT

Ongoing conflicts reinforce the importance of strong departmental policy, intelligence awareness, and disciplined preparedness during periods of elevated global instability. Ongoing tensions involving Iran and the broader Middle East underscore the need for local law enforcement agencies to remain vigilant, policy-driven, and informed about how international events may influence the local domestic threat environment.

The Department of Homeland Security (DHS) has consistently assessed that international conflicts and geopolitical crises can act as threat catalysts, increasing the likelihood of homegrown violent extremism (HVE), lone-actor violence, cyber activity, and other threats within the United States. The New Jersey Attorney General has also urged local residents and law enforcement agencies to be vigilant.[1]

The New Jersey Office of Homeland Security and Preparedness 2026 Threat Assessment also identified HVE and cyber intrusions as significant risks, especially in light of ongoing conflicts in the Middle East. Law enforcement agencies nationwide have historically observed increases in suspicious activity reporting, online rhetoric escalating toward action, and attempts to attack soft targets, critical infrastructure, or symbolic locations, such as religious institutions, during periods of international escalation.

During periods of elevated uncertainty, clear policy is a force multiplier. Well-defined and agency-specific policies provide operational consistency, legal protection, and professional accountability. They also assist in decision-making under pressure and align with constitutional principles and best practices. The policies and other resources in this bulletin will likely also be of benefit to agencies throughout the state as they prepare for the FIFA World Cup 2026 and Sail4th 250.

Chiefs of Police or their designees are urged to access the Law Enforcement Accreditation Plus Portal, review the policies below, and evaluate the necessity to implement these sample policies or modify existing agency polices:

- **Cyber Incident Response Plan:** The global threat environment has greatly enhanced the risk of cyber intrusion. This policy addresses essential actions that are not required for accreditation, including considerations that are consistent with the Municipal Excess Liability Insurance Fund Cyber JIF to minimize disruption and damage.

- **Artificial Intelligence:** The risk of cybersecurity involving artificial intelligence is substantial. This policy addresses essential actions that are not required for accreditation, including critical considerations concerning many aspects of artificial intelligence.

- **Computer Access Policy:** This sample policy addresses essential actions that are not required for accreditation, including security and policy considerations aimed at minimizing cyber-related incidents.

- **Hazardous Materials Incidents:** HVE events may involve hazardous materials, and having a policy dedicated to properly responding to and handling such incidents is essential. This policy includes standardized definitions, references to ICS, suspicious powder incidents, protective equipment, training, exposure, and more.

- **Persons not to have Weapons:** (Duty to Warn/ERPO): Persons who have been radicalized may sometimes be reported to law enforcement, and it is imperative that all agency members are aware of the protections available from the Extreme Risk Protection Order Act. This sample policy also includes policy considerations not required for accreditation, such as Duty to Warn legislation, essential definitions, initial and follow-up investigation procedures, and more.

- **Ambush Mitigation:** Domestic extremists may take steps to place officers at risk of an ambush. This sample policy addresses essential actions that are not required for accreditation, including establishing a system to address an advanced threat of officer ambushes or attacks against an officer.

- **Active Violent Event:** This sample policy addresses essential actions that are not required for accreditation, including initial dispatching considerations, swatting identification and mitigation, cross-referencing to agency policies, including Medical Care, Use of Force, Media, and more. This policy also addresses the training requirements for large venues and includes sample tables listing educational institutions and other critical locations.

- **Incident Command System:** This policy includes detailed essential function considerations, includes various resources, and a detailed definition of venues consistent with legislation.

- **Internal and External Intelligence Reporting:** Many contemporary threats are low-level, non-complex, and difficult to detect, relying on minimal planning and readily available means. This reality underscores the importance of early recognition of indicators, timely intelligence reporting, and supervisory review, rather than reliance on singular warning signs or assumptions about scale. This policy includes essential definitions, supervisor responsibilities, Violent Person File guidance, Suspicious Activity Reporting, Violent Criminal Apprehension Program (VICAP) guidance, NICS Denial resources, training considerations, and more.

- **Mutual Aid:** This sample policy addresses essential actions that are not required for accreditation, including standardized definitions and terminology, ICS consistency, staging practices, mutual aid response to other communities, criminal apprehension planning, and a detailed definition of venues consistent with legislation.

- **Bomb Threats and Suspicious Devices:** This sample policy addresses essential actions that are not required for accreditation, including dispatch and response procedures, evacuation protocols, investigation requirements, and applicable notifications.

Additional Considerations for the Chief of Police:

- Reinforce agency-specific policy guidance and ensure appropriate training of policy contents.
- Encourage reporting of suspicious activity, and promote reporting mechanisms to the community, including See Something Say Something.
- Maintain regular communication with partner agencies.
- Provide calm, consistent leadership that prioritizes professionalism over speculation, especially from social media platforms, which may not be accurate or even false.
- Support personnel by ensuring clarity of expectations during evolving conditions.
- Ensure that all personnel are aware of the importance of:
  - Maintaining situational awareness during routine duties, particularly around public spaces, critical infrastructure, soft targets, and special events. Review the Special Events Resource Page.
  - Observing and reporting suspicious behavior or activity consistent with agency-specific Intelligence Policy and their training.

- Rely on policy and training as the foundation for decision-making, and not to speculate or act outside established guidance.
- Treat all community interactions with professionalism and impartiality, recognizing that international events can heighten sensitivity.
- Prioritize officer safety, communication, and teamwork.

Please contact your Law Enforcement Risk Control Consultant with any questions or assistance with accessing the Law Enforcement Accreditation Plus Portal.

[1] *New Jersey Attorney General: Precautions Being Taken in State After Middle East Attacks*. (2026, February 28). Retrieved from The Monmouth Journal: https://themonmouthjournalwestern.com/nj-attorney-general-precautions-being-taken-in-state-after-middle-east-att-p17747-1.htm