

Colorado Information Analysis Center (CIAC)  
Whole-of-State Critical Infrastructure Program  
Colorado Division of Homeland Security & Emergency Management  
February 24, 2026

Dear Senator Hester,

Thank you for your inquiry regarding Colorado's Whole-of-State (WoS) Critical Infrastructure Program and how our model operates to protect essential services and national security assets. We appreciate the opportunity to share our framework and operational approach.

Colorado's program was established in response to identified statewide gaps in critical infrastructure identification, interdependency awareness, and coordinated response planning. Following significant natural disasters and increasing nation-state targeting of U.S. infrastructure, Colorado recognized that fragmented coordination across sectors was insufficient to address modern, multi-domain risk. The result was the development of a unified, intelligence-led, whole-of-state framework administered through the Colorado Information Analysis Center (CIAC) and its 24/7 Watch Center.

Our structure is built on two concurrent and synergistic Lines of Effort, operating in parallel with unified governance, shared communications pathways, and an embedded Colorado National Guard executive partner working alongside CIAC leadership.

**Line of Effort 1: Critical Infrastructure Protection (Civilian-Led, Intelligence-Driven)**

This effort integrates all 16 critical infrastructure sectors into a coordinated statewide ecosystem. Six priority sectors—Energy, Water, Transportation, Communications, Healthcare, and Food & Agriculture—are fully operational, with additional sectors phased in through formalized onboarding, sector working groups, and standardized coordination protocols.

The CIAC 24/7 Watch Center functions as the central coordination hub. It validates incidents, applies tiered classification, issues rapid notifications, and maintains a shared Common Operating Picture (COP). The framework emphasizes proactive information sharing, sector equity, privacy protections, and interoperable communication spanning unclassified and classified environments.

**Line of Effort 2: Homeland Defense & Resilience Integration (National Guard Executive Partnership)**

Operating concurrently, this effort integrates the Colorado National Guard, U.S. Northern Command, and defense stakeholders into the broader whole-of-state ecosystem. A senior National Guard executive works alongside CIAC leadership to ensure seamless synchronization between civilian infrastructure protection and defense mission assurance.

This line of effort strengthens Defense Support to Civil Authorities (DSCA), defense installation resilience, cyber terrain defense, and continuity of operations. A Joint Coordination Cell (JCC) ensures lawful authority, appropriate classification handling, and disciplined integration between civilian and military equities during significant incidents. Civilian authority remains primary; the Guard operates in support while maintaining readiness for homeland defense contingencies.

### **Why This Model Matters**

Modern threats are systemic. A cyber intrusion targeting an energy provider can cascade into water distribution, healthcare delivery, transportation logistics, and defense readiness. Colorado's program applies systems engineering, interdependency mapping, and cascading impact analysis to anticipate and mitigate secondary effects before they compound.

Additionally, approximately 85% of defense-critical infrastructure supporting DoD missions outside military installations is privately owned and operated. Without structured public-private integration and disciplined civil-military coordination, continuity of essential services and mission assurance cannot be guaranteed.

Key outcomes of Colorado's model include:

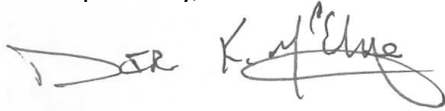
- Real-time, tiered incident notification across sectors
- Integrated cyber coordination between civilian and military domains
- Formalized sector governance and working groups
- Alignment with emergency operations and community lifelines
- Structured after-action review and continuous improvement cycles
- Sustainable funding and measurable risk reduction metrics

By 2030, Colorado intends to operate as a national model for state-level critical infrastructure integration—demonstrating that civilian leadership, private-sector engagement, and disciplined National Guard partnership can function as a unified homeland resilience architecture.

We believe this framework is scalable and adaptable to Maryland's infrastructure environment, particularly given the concentration of federal, defense, technology, and transportation assets within Howard and Montgomery Counties.

We would welcome the opportunity to provide a detailed briefing to your office to discuss implementation considerations, governance models, and lessons learned.

Respectfully,

A handwritten signature in black ink, appearing to read "Kevin McElyea". The signature is stylized with a large, sweeping initial "K" and a long, horizontal flourish at the end.

Kevin McElyea

Director

Colorado Information Analysis Center

Whole-of-State Critical Infrastructure Program

Colorado Division of Homeland Security & Emergency Management