



Cybersecurity Reporting & Response

Information Technology Oversight Committee

October 14, 2026

The Kentucky National Guard

MG Haldane Lamberton, The Adjutant General

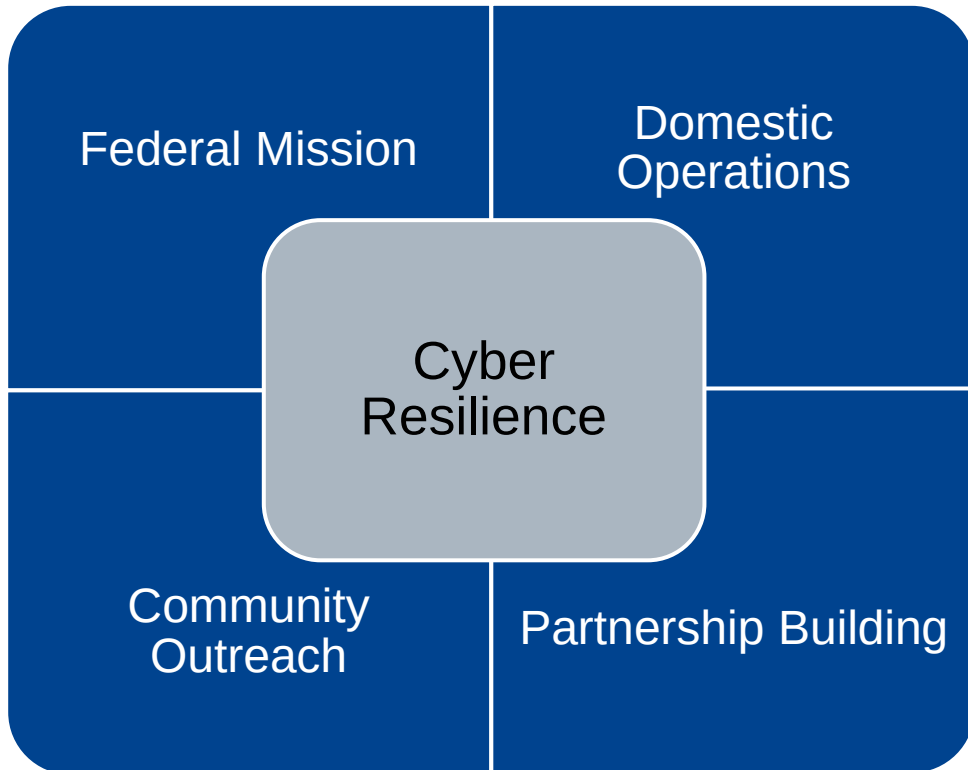
LTC Dayna Sanders, Cyber Program Manager



Kentucky National Guard Cyber Resilience Initiative

----- OVERVIEW

The Kentucky National Guard Cyber Resilience Initiative (KYNG-CRI) builds trust, cyber resiliency, and shared cyber capabilities and knowledge across public and private sectors through operating along four lines of effort:



"Together We Secure Kentucky"

- **Partnership & Community Centered:** Partnership building and community engagement remain the program's largest areas of focus. We have successfully completed 477 total engagements from 2024–2026, successfully maintaining our strong, trusted relationships across the entire enterprise.
- **Rapid Expansion of KY-CRI:** KY-CRI engagements continue to experience outstanding growth as the program expands. As of 1 October 2026, the program has successfully completed cyber hygiene assessments on 34 networks, conducted 2 incident responses, and executed 1 highly critical penetration test.
- **Explosive Growth in Technical Assessments:** Network Assessments have emerged as a premier success story, on track to reach a projected 36 completed assessments by the end of 2026—marking an exceptional 414% year-over-year expansion in technical verification capabilities.





Cyber Bluegrass

OVERVIEW

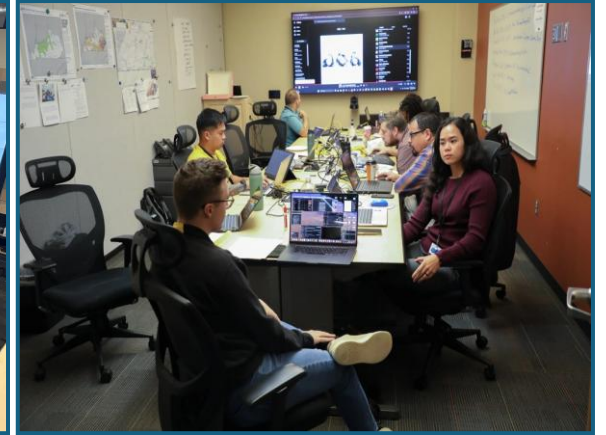
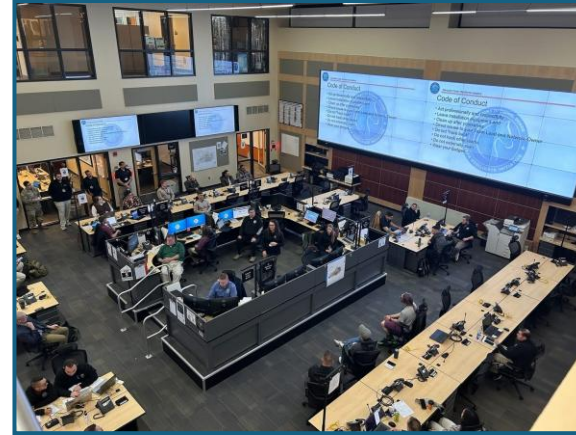


Mission

Cyber Bluegrass fortifies the security of the Commonwealth by preparing Kentucky's cyber defenders to protect and defend our state's critical infrastructure against its greatest threats. Through immersive, hands-on training and by strengthening partnerships between local industry, government, and communities, we enhance Kentucky's cyber resilience and build a premier defensive force.

October 27-29, 2026– Boone National Guard Center, KY, Murray State University Campus, and University of Louisville School of Engineering.

- Training: Training is available October 19-23
 - Topic: Incident Response & Assessment, Log Analysis and Threat Hunting, Operational Technology Fundamentals, Cyber Tools Training
- Cyber Summit (Optional): October 23
 - 15-30 min. briefings from industry experts, military leaders, and technology vendors on cybersecurity topics plus networking opportunities
- Distinguished Visitors Day: October 28
 - Media Round Table
- Lead Organizations: Murray State University, The University of Louisville, University of Kentucky, Defense Advanced Research Agency, Kentucky Office of Homeland Security, & KYNG
- **The goal of Cyber Bluegrass is to leverage** partners and resources across multiple public and private entities to establish a framework for cyber related disaster preparedness and response across FEMA Region 4 through building trust, cyber resiliency, and shared cyber capabilities and knowledge.
- Visit <https://kycrri.gov> for registration information.



2025 Exercise Snapshot



85 participants



44 DVs



9 states



2 Locations



36 Agencies/Companies



Army and Air Force



National Guard Capabilities Nationwide

----- HIGHLIGHTS

- **North Carolina:** The North Carolina **Joint Cybersecurity Task Force (JCTF)** coordinates National Guard, state agencies, and local IT strike teams to defend public-sector and critical infrastructure networks. In addition to providing on-site incident containment, malware eradication, and system reconstruction, the JCTF delivers proactive vulnerability assessments, penetration testing, and security scanning. This collaborative partnership actively secures county voting networks and conducts hands-on defensive training exercises like **Operation Tobacco Road** to maintain statewide readiness.
- **Minnesota:** Through the **Cyber Coordination Cell (C3)**, the Minnesota National Guard operates a full-time strategic planning and coordination office that prepares, trains, and equips the state's cyber forces. Operating under the state's military leadership and the Governor, the C3 manages readiness by training personnel for realistic scenarios, building vital interagency partnerships, and maintaining specialized "always ready" deployable forensic and network equipment.



National Guard Capabilities Nationwide

----- HIGHLIGHTS

- **Idaho: Operation Cyber Idaho** led by the Idaho Office of Information Technology Services in partnership with the Idaho National Guard and Boise State University. The initiative secures vulnerable municipal, county, school district, and tribal networks by providing free vulnerability scans, advanced endpoint security, and on-site incident response coordination. To address the state's technical workforce shortage, the program places fully funded, university-level cybersecurity apprentices directly with local public agencies, including the National Guard, to build long-term, decentralized defense capabilities. The Idaho National Guard hosts the annual Cyber Discovery exercise to promote readiness and coordination across all state agencies.
- **California: The California Cybersecurity Integration Center (Cal-CSIC)** centralizes state threat sharing and emergency response alongside the California National Guard's Computer Network Defense team. To enforce systemic readiness, California state law mandates that public agencies undergo independent security audits every two years. The state law designates the California Military Department to perform these technical assessments. This joint military-civilian team also secures local critical infrastructure, responds to active state emergencies, and hosts an annual multi-state cyber exercise, **Cyber Dawn**.



Questions