

Cybersecurity Reporting & Response

presented by the Kentucky Office of Homeland Security
for the Information Technology Oversight Committee

October 14, 2026

Existing Laws & Authorities for Cyber Notifications & Responses

- ▶ **KRS 42.726** The Commonwealth Office of Technology (COT) coordinates incident response for the executive branch & submits an annual report of security breaches.
- ▶ **KRS 61.931-934** Ensures government agencies & third parties safeguard personal data, investigate breaches, & make notifications.
- ▶ **KRS 365.732** Requires any “information holder” to notify Kentucky residents when their unencrypted personal information is accessed by an unauthorized party.
- ▶ **KRS 367.110-305** The Kentucky Consumer Protection Act applies to trade or commerce, including online fraud, deceptive practices, or misleading conduct.
- ▶ **KRS 434.840-860** Criminalizes the unauthorized access, manipulation, interception, or destruction of data, computer systems, or networks.

Kentucky Office of Homeland Security

Role & Responsibilities

- ▶ **3/28/2002** – HB 258 established the Office of Security Coordination (OSC)
 - ▶ Placed under the Dept. of Military Affairs to “coordinate a comprehensive strategy to secure the Commonwealth of Kentucky from terrorist threats or attacks.”
- ▶ **5/27/2004** – EO 2004-530 established KOHS under the Governor’s Office
 - ▶ Responsibilities were expanded to include “other threats to public safety”
 - ▶ Appointed as the State Administrative Agency (SAA) for homeland security funds & primary liaison with U.S. Dept. of Homeland Security
- ▶ **6/12/2007** – EO 2007-453 established the Kentucky Intelligence Fusion Center
 - ▶ Intended to improve intelligence sharing & collaboration for “all crimes/all hazards”

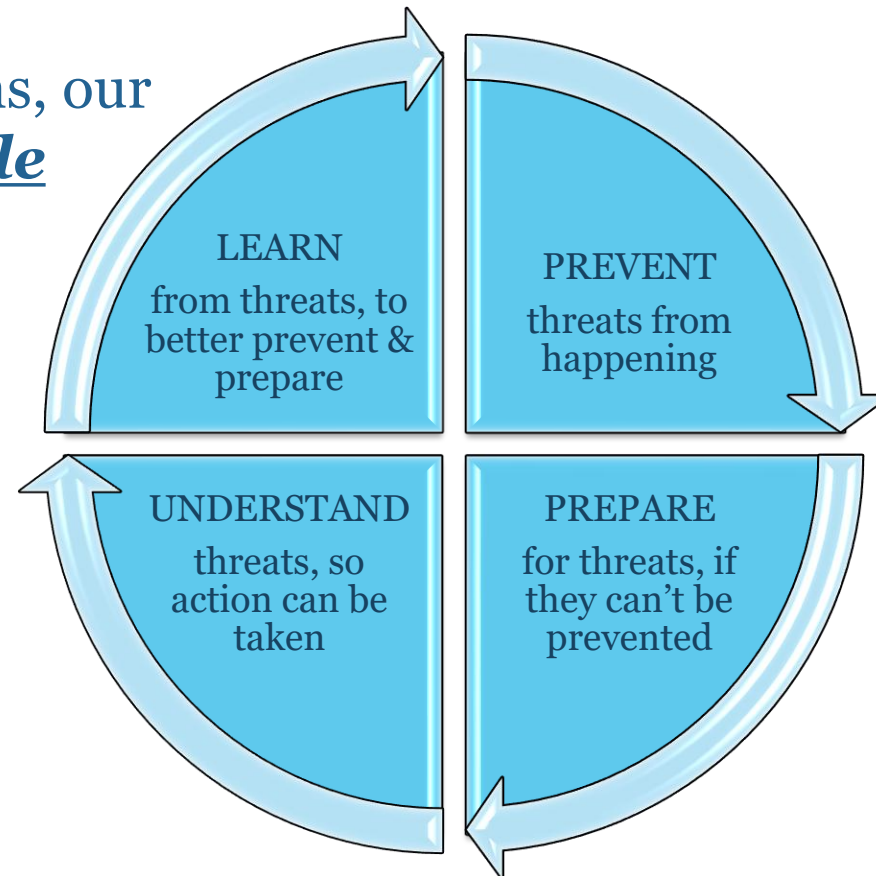
KOHS Components

Kentucky
Intelligence
Fusion Center

Grants
Administration

Kentucky 911
Services Board

In simple terms, our
job is to **enable**
others to:



KOHS' Role in Cyber

- ▶ No statutes or regulations explicitly tie KOHS to “cyber” beyond general references to terrorism
- ▶ EO 2024-728 – Kentucky Emergency Operations Plan
 - ▶ KOHS is designated as the Coordinating Agency for Emergency Support Function (ESF) 17: Cyber-Security
 - ▶ “...coordinate cyber critical response including the detection, mitigation, and information sharing related to statewide cyber-related events.”
 - ▶ Supporting agencies include the Commonwealth Office of Technology (COT), Kentucky National Guard, and Federal Agencies (e.g. FBI, DHS).
- ▶ Governor’s expectations for KOHS include:
 - ▶ staying abreast of threats & crisis events, with an emphasis on cybersecurity & interagency coordination
 - ▶ improving the management & impact of non-disaster FEMA grants for Kentucky

KOHS' Role in Cyber: Grants

- ▶ State & Local Cybersecurity Grant Program (SLCGP)
 - ▶ Purpose: To assist SLTT governments with managing & reducing systemic cyber risk
 - ▶ Applicants must address specific objectives in their proposed projects
 - ▶ No federal funding has been dispersed since the FFY25 grant cycle
 - ▶ This grant is an 80/20 pass-through (80% must be passed through to locals)
 - ▶ Requires a funding match, with incremental increases each FFY
 - ▶ Kentucky received match waivers for FFY22–FY24
 - ▶ Per FEMA & CISA, there will be no match waiver for FFY25

FFY	Federal Award Amount	Applications Received	Projects Funded	COT Projects	KOHS Cybersecurity	Grants Management (5%)
2022	\$3,658,555	29	19	\$235,857	\$79,000	\$182,928
2023	\$7,413,939	60	46	\$324,750	\$787,259	\$370,670
2024	\$5,564,421	42	24*	TBD	TBD	\$287,221
2025	\$1,830,332	0	0	TBD	TBD	\$91,016

**24 projects confirmed for FY24, but projects have not yet been awarded*

KOHS' Role in Cyber: Grants

▶ Homeland Security Grant Program (HSGP)

- ▶ Purpose: To help SLTT governments prevent, protect against, respond to, & recover from acts of terrorism & other major threats
- ▶ This grant is also an 80/20 pass-through
- ▶ “Enhancing Cybersecurity” is one of five (5) National Priority Areas
 - ▶ NPAs must account for 30% of total allocation, but there is no minimum for cybersecurity

FFY	SHSGP Cyber Applications	Total Requested	Awards	Amount Funded
2020	3	\$447,519	2	\$352,519
2021	5	\$348,800	5	\$348,800
2022	5	\$710,463	1	\$162,226
2023	2	\$202,406	1	\$127,200
2024	3	\$143,851	2	\$82,551
2025/2026	14*	\$1,125,292	TBD	TBD

**Includes 3 requests for Mobile Data Terminals (MDT) and a continuation of a program funded under FFY23 SLCGP*

KOHS' Role in Cyber: Fusion Center

- ▶ Focus on Prevention
 - ▶ Intelligence Products & Sharing
 - ▶ Education & Outreach
- ▶ Partnerships
 - ▶ CISA, FBI, COT
 - ▶ KYNG
 - ▶ Kentucky Cyber Resilience Initiative
- ▶ Training & Exercises
 - ▶ Blue Team Summit
 - ▶ Cyber Bluegrass
- ▶ Engaging Subject Matter Experts
 - ▶ 8/5/2026 “Brainstorming” Meeting
 - ▶ CISA, FBI, COT, KYNG
 - ▶ Murray State University
 - ▶ Kentucky Association of Government Technology Professionals
 - ▶ Louisville Metro Government
 - ▶ Kentucky Cyber Intelligence Information Initiative (KCI3)
 - ▶ UofL, public/private schools
 - ▶ Critical infrastructure entities
 - ▶ Private sector & vendors

Identifying Needs

- ▶ Needs identified from 8/5/2026 meeting & other interactions include:
 - ▶ **Risk Awareness**—You must understand your risk before action can be taken to mitigate it.
 - ▶ **Knowledge & Talent**—In many places, the “cyber” person may wear many hats & has not had relevant training or experience.
 - ▶ **Access to Funding**—Cybersecurity talent & tools are expensive & must be sustained.
 - ▶ **Building Trust**—Local agencies are sometimes reluctant to request or accept help from state or federal agencies.
 - ▶ **Awareness of Relevant Resources**—Entities are not sure what resources are applicable & available to them, or who to call in the event of an incident.
 - ▶ **Core Security Measures**—Insecure practices like weak access controls, outdated systems, & non-.gov email domains serve as single points of failure.
 - ▶ **Coordinated Response**—Operational priorities, legal/liability concerns, reporting mandates, & information sharing policies vary by jurisdiction & organization.
 - ▶ **Common Operating Picture**—Gaps in information can inhibit a statewide threat picture.
- ▶ A larger “needs assessment” meeting is tentatively scheduled for 10/26/2026

Other States: Reporting & Response

	North Carolina	Wisconsin	Georgia	Ohio
Mandatory Reporting	Yes	No statewide mandate	Yes	Yes
Covered Entities	State & local government (private sector voluntary)	N/A	Government & utilities	State agencies & political subdivisions
Reporting Timeline	24 hours	Voluntary	1-2 hours	≤ 7 days
Primary Report Recipient	NCDIT-ESRMO	WEM + WSIC (fusion center)	GEMA/HS + GTA	HS-Cyber Integration Center
State Cyber Response Team	Joint Cybersecurity Task Force (DIT, EM, NG, LGISA + Feds)	Cyber Response Team (volunteers led by EM)	ESF-17 Partners (GTA, GBI, NG, GEMA/HS)	OCIC + NG-Cyber Reserve
National Guard Role	Extensive	Supporting	Supporting	Extensive
Ransomware Restrictions	State/local govt. banned from paying or communicating; must consult with NCDIT	No explicit bans or consulting requirements	No explicit ban (focus on reporting)	State agencies banned; political subdivisions need formal resolution/ordinance

Questions?

Kentucky Office of Homeland Security

Amy Hess

Executive Director

200 Mero St.

Frankfort, KY 40622

amy.hess@ky.gov