



Cyber ESF 17 Overview

Jan 2025



Topics/Agenda

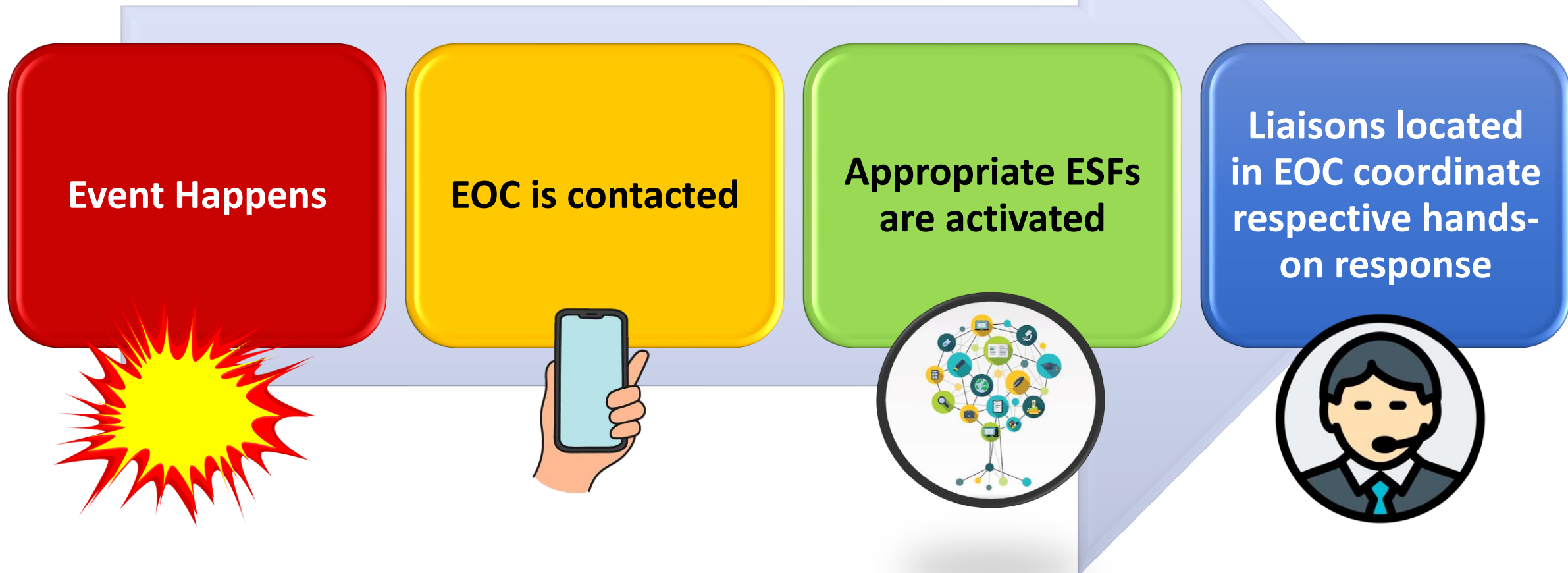
ESF?

How Does Cyber Fit Into EM?

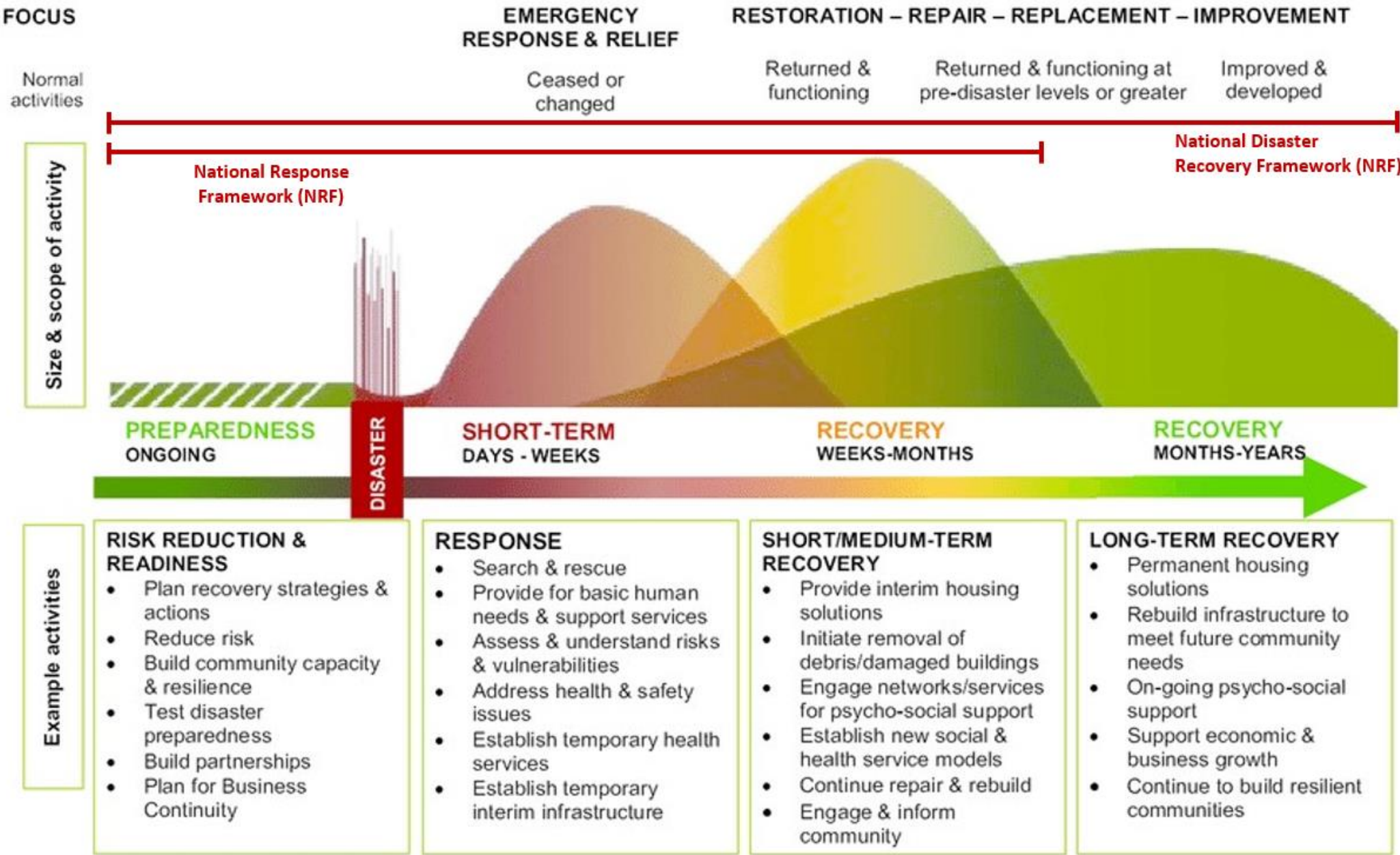
Honesty, The Best Policy

Most DANGEROUS scenarios and targets

EOC and ESF Activation Oversimplified



FEMA's Recovery Continuum (4 Phases)



Recovery is historically lengthier and more expensive than response.



Focus

Normal Activities

Emergency Response And Relief

Operations Ceased or Changed

Restoration – Repair – Replacement - Improvement

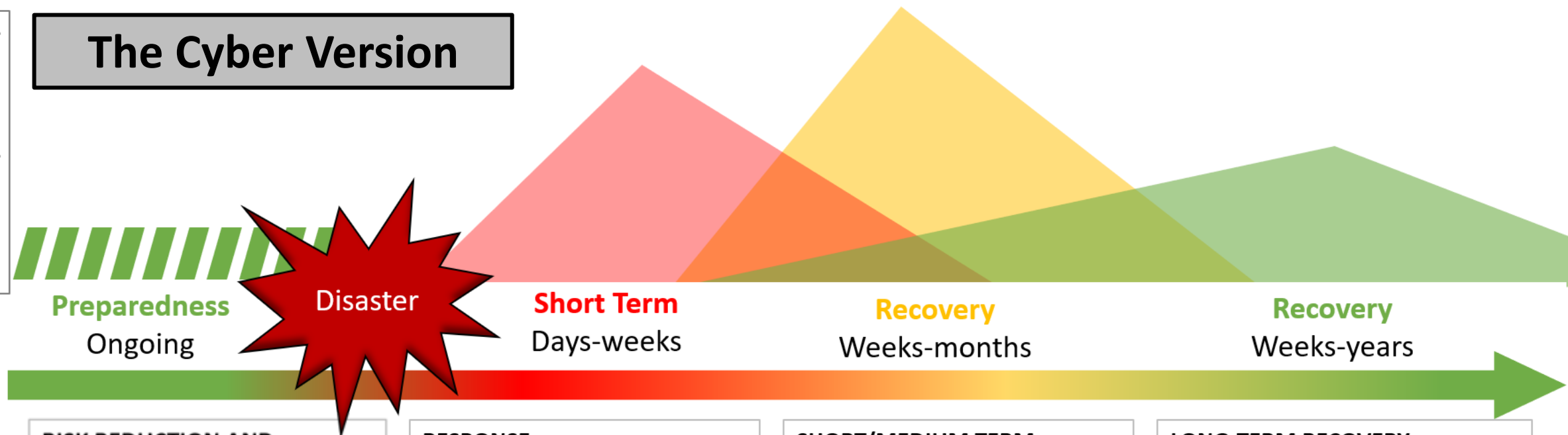
Restore Baseline Functionality

Returned and Functioning at Pre-Disaster Levels or Greater

Mature Cybersecurity Programs

The Cyber Version

Size and Scope of Activity



Example Activities

RISK REDUCTION AND READINESS

- Join MS-ISAC
- Utilize CISA tools
- Assess/reduce risk
- Build community resilience
- Test disaster preparedness
- Build partnerships (local/state/federal)
- Plan for business continuity
- Adopt best practices
- Apply for cyber grant(s)

RESPONSE

- Contain the infection
- Apply security patches
- Conduct forensics
- Identify the cause and cascading infrastructure impact(s)
- Restore backups
- Communicate early and often (local/state/federal)
- Share indicators of compromise within appropriate communities

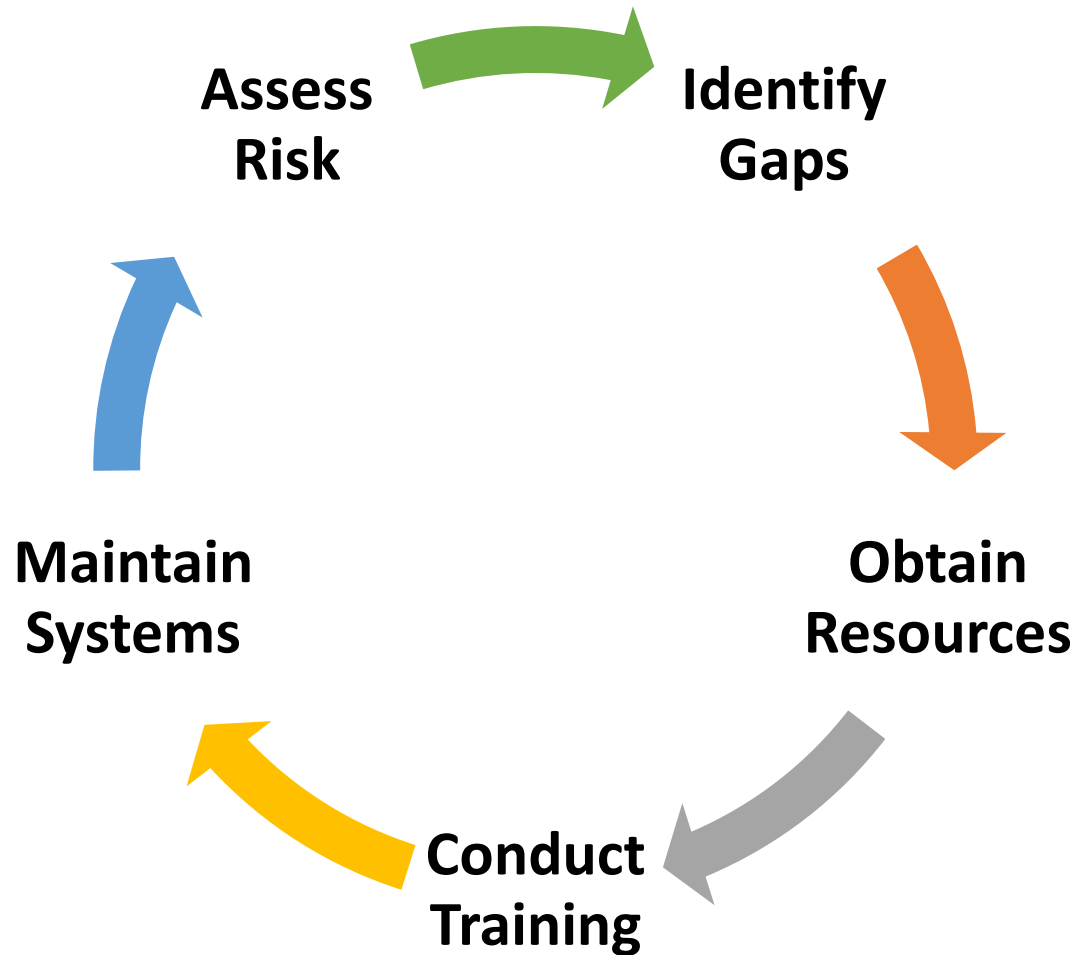
SHORT/MEDIUM TERM RECOVERY

- Restore primary functionality (i.e., water or energy distribution)
- Restore network functionality
- Document the incident thoroughly
- Review and revise plans
- Identify areas for network/system improvement
- Conduct recurring training

LONG-TERM RECOVERY

- Strengthen cybersecurity posture via implementation of best practices
- Establish continuous system monitoring
- Conduct annual risk assessment(s) via 3rd Party
- Conduct recurring training for IT staff and users
- Upgrade software/hardware
- Join cybersecurity groups

Cyber Recovery Continuum



Normal Operations/ Preparedness

Ongoing

RISK REDUCTION AND READINESS

- Join MS-ISAC
- Utilize CISA tools
- Assess/reduce risk
- Build community resilience
- Test disaster preparedness
- Build partnerships (local/state/federal)
- Plan for business continuity
- Adopt best practices
- Apply for cyber grant(s)

Cyber Recovery Continuum

Assess Situation

Does victim have:

- Response Plan
- Insurance
- IT/Cyber Staff

Report to EOC

What was impacted

Request Resources

Address Priorities
Fill Resource Gaps

Operations Ceased/Changed

Response

Days - Weeks

Event

RESPONSE

- Contain the infection
- Apply security patches
- Conduct forensics
- Identify the cause and cascading infrastructure impact(s)
- Restore backups
- Communicate early and often (local/state/federal)
- Share indicators of compromise within appropriate communities

Cyber Recovery Continuum

What do other locations need to know?

What would you want to know?

- What sector was targeted? (water, city/county, PSAP, etc...)
- What type of attack? (ransomware, DDoS, botnet, etc...)
- What system(s) were targeted?
- How was the network breached?
- How did the attacker get network admin?

Operations Ceased/Changed

Response

Days - Weeks

Event

RESPONSE

- Contain the infection
- Apply security patches
- Conduct forensics
- Identify the cause and cascading infrastructure impact(s)
- Restore backups
- Communicate early and often (local/state/federal)
- Share indicators of compromise within appropriate communities

Cyber Recovery Continuum

Nobody cares or wants to know:

- City/County/Organization Name
- Who was at fault

Operations Ceased/Changed

Response

Days - Weeks

Event

RESPONSE

- Contain the infection
- Apply security patches
- Conduct forensics
- Identify the cause and cascading infrastructure impact(s)
- Restore backups
- Communicate early and often (local/state/federal)
- Share indicators of compromise within appropriate communities

Cyber Recovery Continuum

Ask for help

- Updating or drafting plans
- Identifying areas for improvement
- Use cyber grants
- Training
- Exercises

Restore Functionality

Recovery

Weeks - Months

SHORT/MEDIUM TERM RECOVERY

- Restore primary functionality (i.e., water or energy distribution)
- Restore network functionality
- Document the incident thoroughly
- Review and revise plans
- Identify areas for network/system improvement
- Conduct recurring training

Cyber Recovery Continuum

Use State/Federal Resources

- Best practices
- CISA external monitoring
- CISA risk assessments
- Training and Exercises
- MS-ISAC
- Grants for upgrades

Mature the Program

Recovery

Months - Years

LONG-TERM RECOVERY

- Strengthen cybersecurity posture via implementation of best practices
- Establish continuous system monitoring
- Conduct annual risk assessment(s) via 3rd Party
- Conduct recurring training for IT staff and users
- Upgrade software/hardware
- Join cybersecurity groups

ESF 17 Alert Levels *(as of 2023)*

The alert level is determined using a threat severity formula: $\text{Severity} = (\text{Criticality} + \text{Lethality}) - (\text{System Countermeasures} + \text{Network Countermeasures})$

Level	Description	Actions
Low	No unusual activity exists beyond the normal concern for known hacking activities, known viruses, or other malicious activity.	Manage internally.
Guarded	The potential for malicious cyber activities exists, but no known exploits have been identified, or known exploits have been identified but no significant impact has occurred.	Manage internally.
Elevated	There are known vulnerabilities that are being exploited with a moderate level of damage or disruption, or the potential for significant damage or disruption is high.	Notify MS-ISAC, FBI IC3, and ESF 17 (activated? On call? Who specifically? Need internal SOPs) for awareness/sharing of information.
High	Vulnerabilities are being exploited with a high level of damage or disruption, or the potential for severe damage or disruption is high.	Notify MS-ISAC, FBI IC3, and ESF 17 for mobilization/consultation from KY ARNG DCOE team, CISA, FBI and IOC sharing across organizations similar to the victim organization. Notify other ESFs for awareness of possible cross-sector impact.
Severe	Vulnerabilities are being exploited with a severe level or widespread level of damage or disruption of Critical Infrastructure Assets.	Notify MS-ISAC, FBI IC3, and ESF 17 for mobilization/consultation from KY ARNG DCOE team, CISA, FBI and IOC sharing across organizations similar to the victim organization. Notify other ESFs for awareness and response.

As of now, there are no state-level cyber incident response resources to offer, other than coordinating with the federal agencies (if they respond).

ESF 17 Alert Levels *(as of 2023)*



Local

- Insurance or local IT has ability to address issue
- State/Federal resources also notified



State

- State has ability to address issue
- Federal resources also notified



Federal










- Federal resources address issue
- State also notified



Most common/LIKELY Scenarios & Targets

The majority of cyber criminals are financially motivated, prefer medium to low effort, low risk/high reward tactics.

FBI Reports 2021-2023 (National Data)

Threat		Frequency (2023, 2022, 2021)		Cost (2023,2022,2021)
Ransomware		2.8k, 2.4k, 3.7k		\$60m, \$34m, \$49m
Personal Data Breach		56k, 59k, 52k		\$744m, \$743m, \$514m
Phishing/Spoofing		299k, 321k, 342k		\$19m, \$160m, \$126m
Business Email Compromise		21k, 22k, 20k		\$3b, \$2.7b, \$2.4b
I'm gonna shut you down 'cause you're critical infrastructure and I'm gonna shut you down.			No data for that.	

Volt Typhoon and other APTs do target CI for both known and unknown purposes.



Ransomware Map <https://www.comparitech.com/ransomware-attack-map/>

Total # of Attacks

2,970

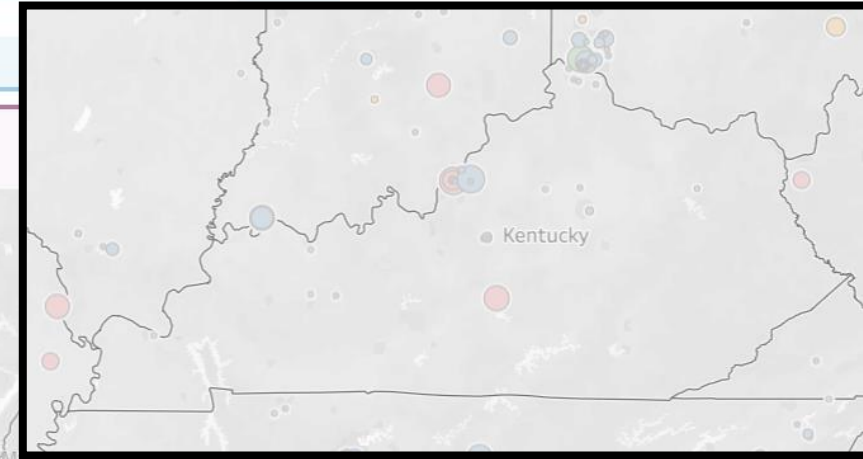
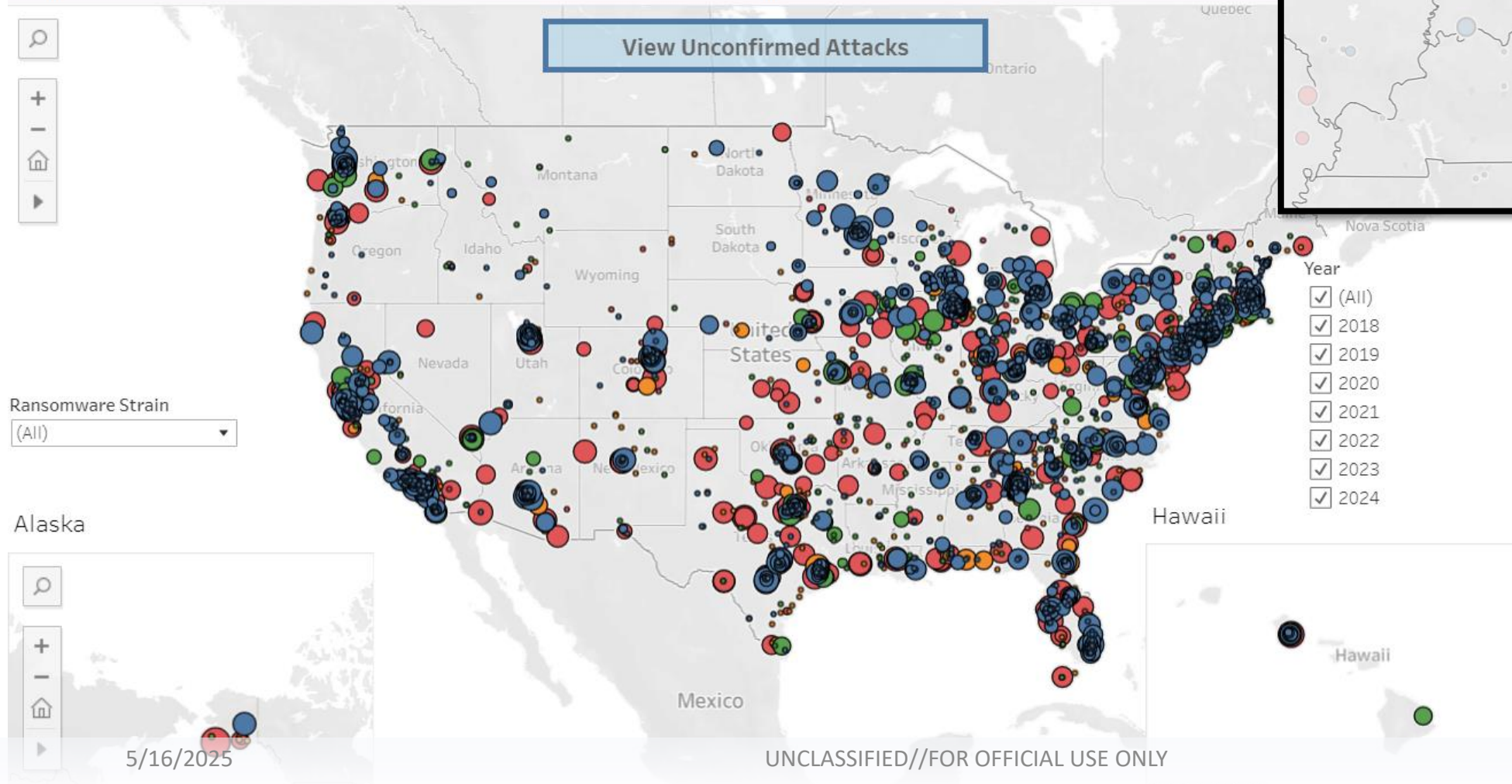
Average Ransom (\$)

2,363,722

Total Records Affected

293,113,062

Map of confirmed US ransomware attacks from 2018 to present



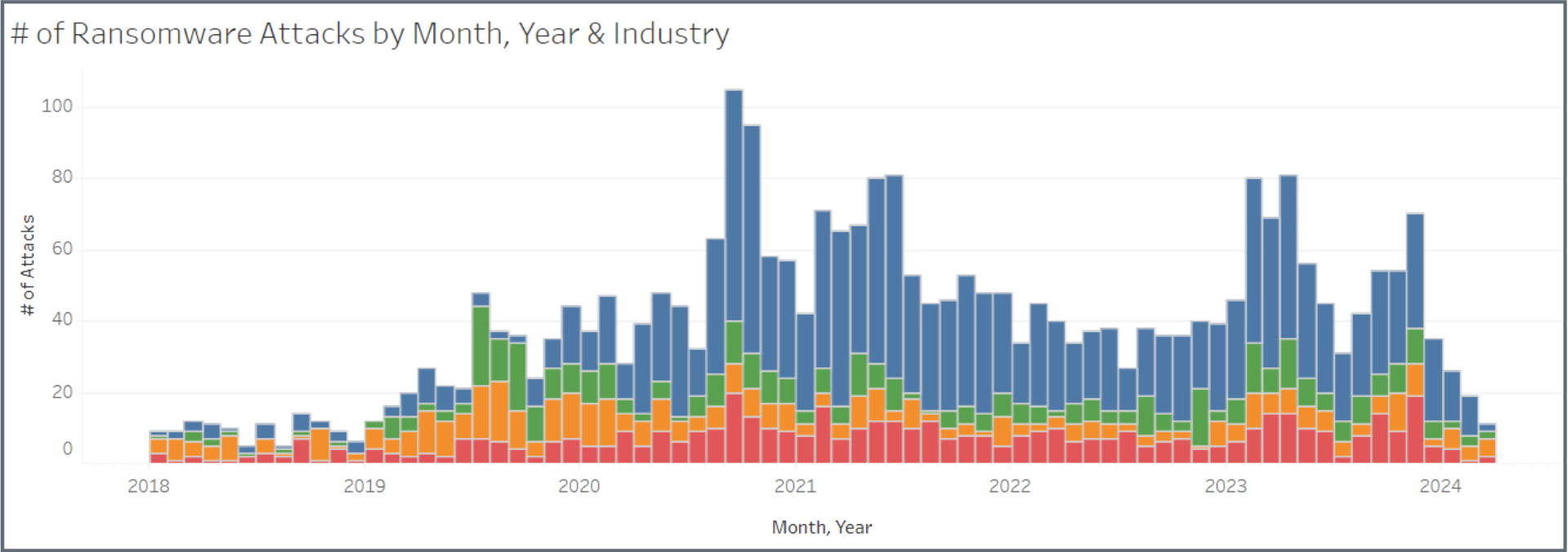
Rumors and hearsay:

KY “Agencies”
respond to appx one
ransomware event
and 2-3 BEC events
every week.

*That is not represented on
this map*

Ransomware by Sector

<https://www.comparitech.com/ransomware-attack-map/>



Remember:

Criminals are financially motivated, low risk/high reward, least effort. This is about money made vs time spent

Average Ransom by Industry (\$)

Business 6,035,438	Education 1,327,218	Government 541,956	Healthcare 1,369,470
-----------------------	------------------------	-----------------------	-------------------------

Average # of Records Affected

Business 258,235 5/16/2025	Education 41,265	Government 29,984	Healthcare 156,538
----------------------------------	---------------------	----------------------	-----------------------

Honestly, Can We Agree?

- The biggest “threat” in a major cyber event is **potential cascading effects** that are addressed by other ESFs. E.g., threat to life events such as: citizens don’t have water, shelter, climate control, emergency service dispatching, access to healthcare, etc.)
- Internal IT/Cybersecurity/Insurance – those with the budget for it, have it (or they self-insure). In an isolated incident, those entities *without* these resources are usually small enough that they would not require a large-scale response (cyber or otherwise).
- As with physical events, getting out of the response phase, and into the recovery phase as fast as possible is a good idea.

Honestly, Can We Agree?

If the Commonwealth remains standing despite the overwhelming threat of cyber-crime, can we assume there are already mechanisms in place that are being used to *successfully* manage these events?

- Internal IT/Cybersecurity – those with the budget for it, have it.
- Cybersecurity Insurance (most counties have it, major critical infrastructure has it, it's largely case-by-case after that)
- Federal Response – CISA, HSI, FBI, MS-ISAC. (available to most infrastructure)

The BIG Questions

Is the Cyber ESF expected to take the place of existing resources?

No.

Why report an incident that can be handled locally to the state EOC?

So others can avoid being victimized.

Will a local entity be punished after being the victim of a cyber attack?

No.

Most DANGEROUS Least LIKELY Scenarios

- **Statewide 911**
- **Statewide Power**



Most DANGEROUS Least LIKELY

Statewide 911

117 PSAPs

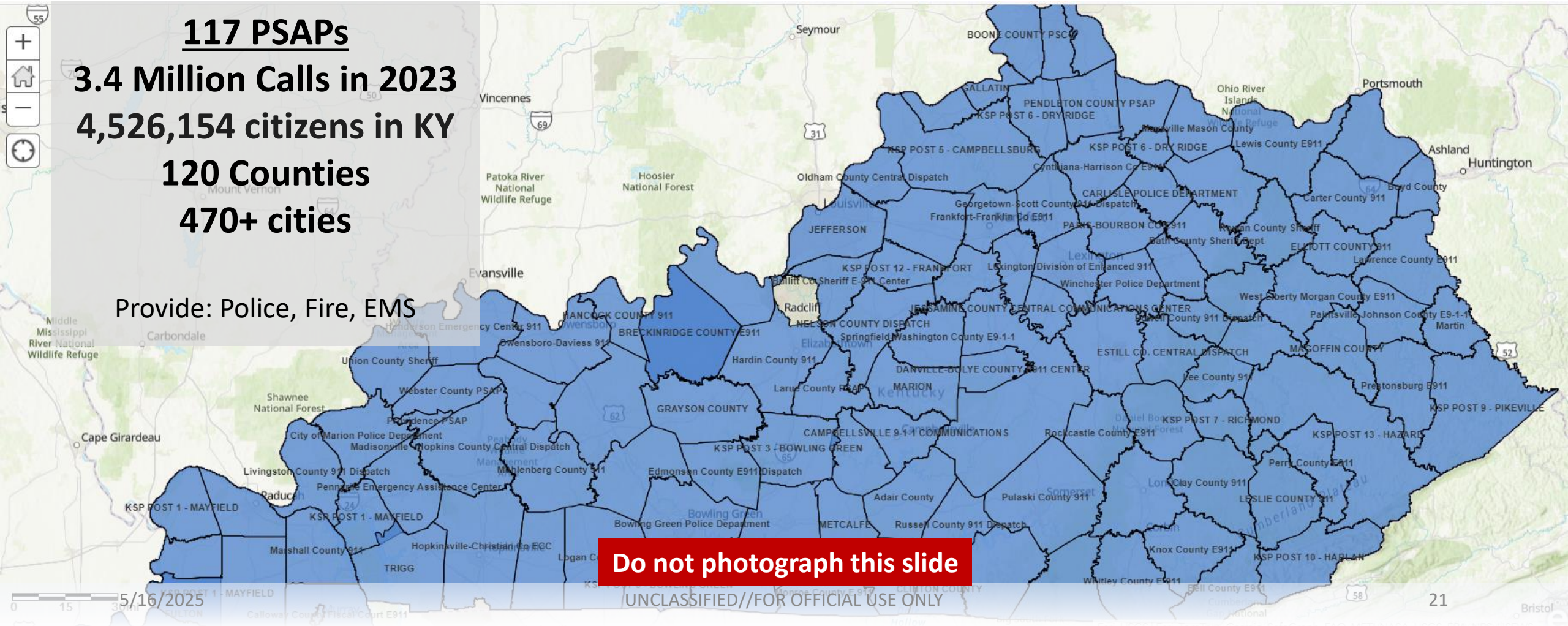
3.4 Million Calls in 2023

4,526,154 citizens in KY

120 Counties

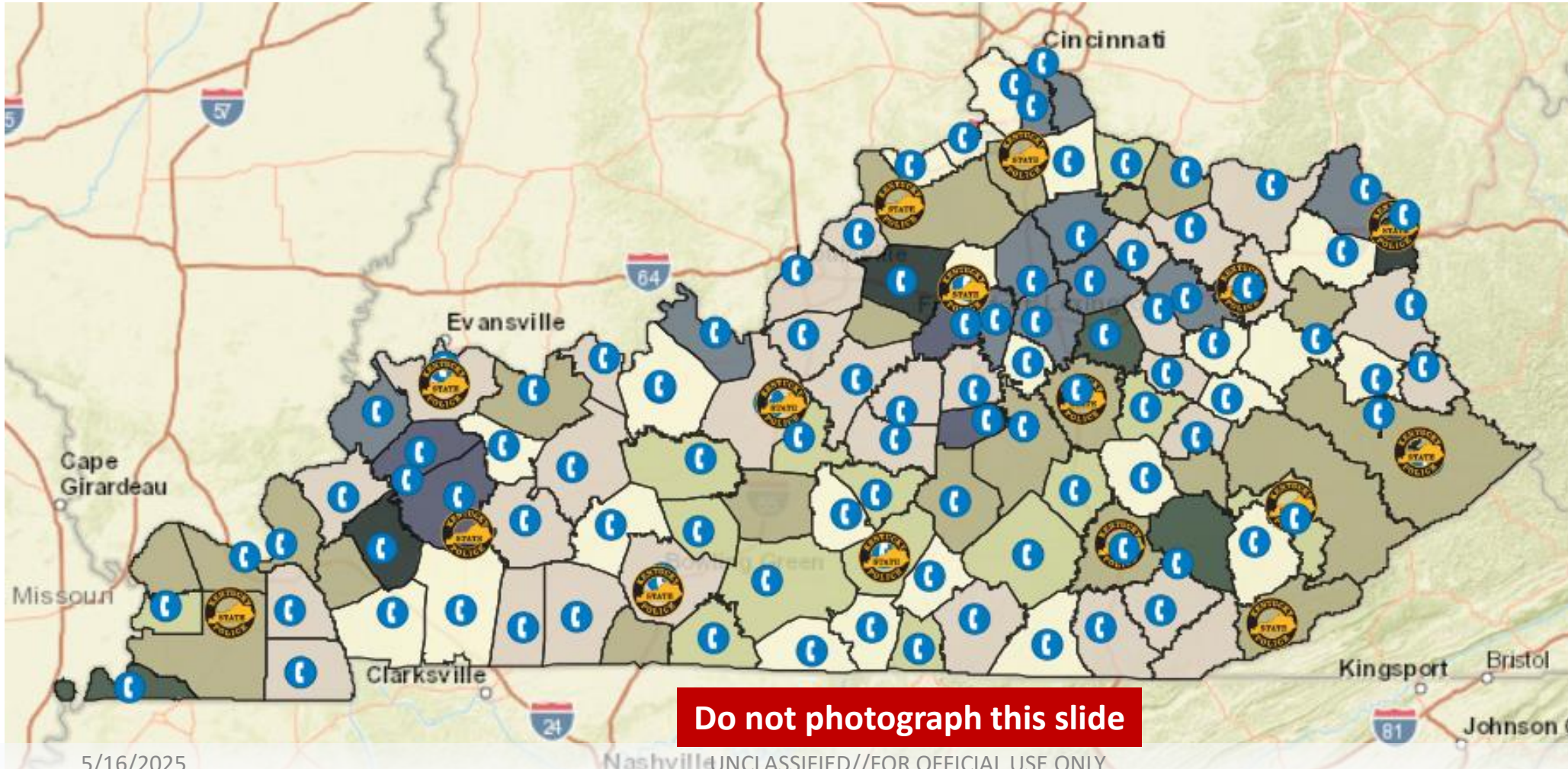
470+ cities

Provide: Police, Fire, EMS



Statewide 911

- PSAPs are currently decentralized but 1/3 are on regional networks



2020 Map

- ATT
- Spectrum
- Windstream
- KSP Post
- PSAP

Use several different dispatching (CAD) software vendors, call system vendors,

Statewide 911 ⇒ ESInet 2026

Oversimplified



1. Event happens
2. Call goes to cell tower. (may go to correct PSAP, may not)

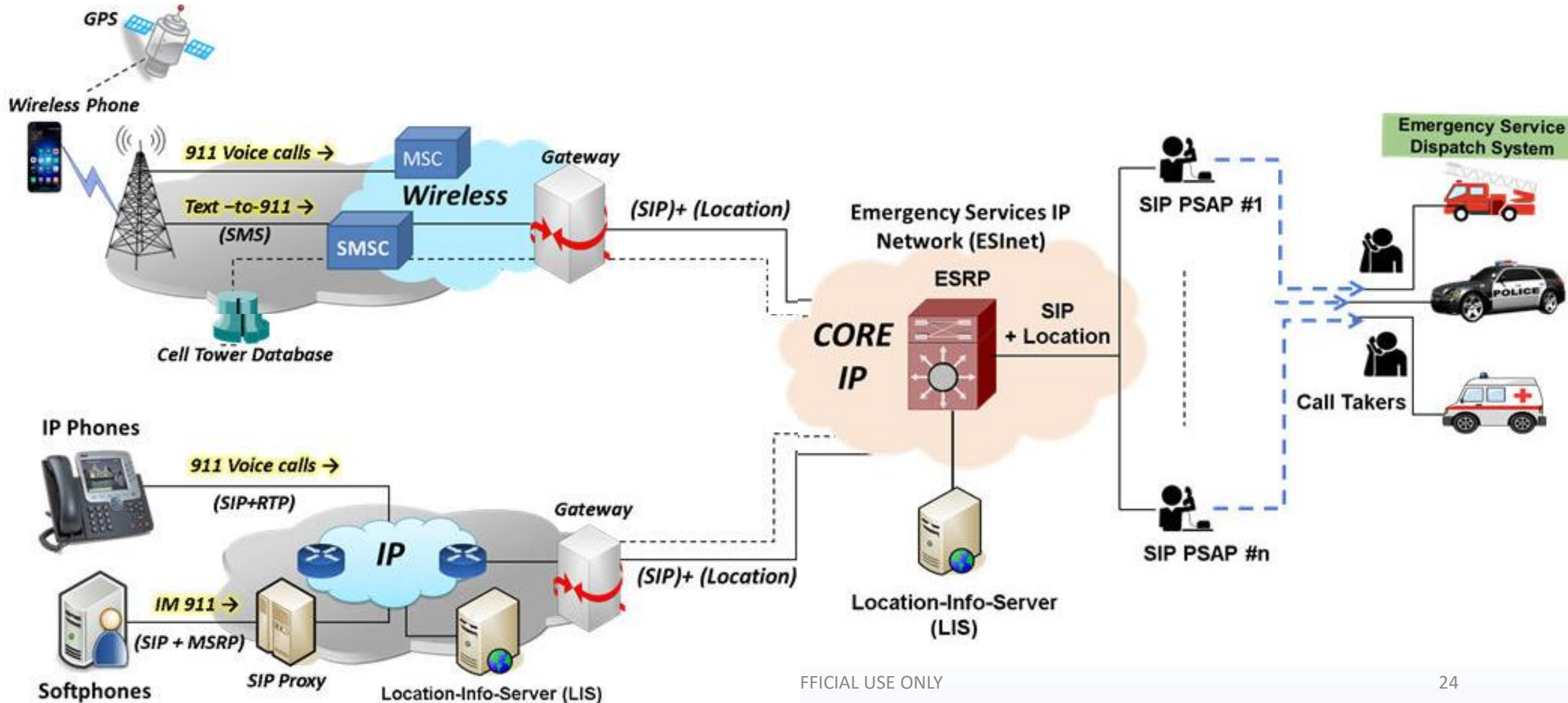
Old



1. Event happens
2. Call goes to state. Call is routed to correct PSAP.

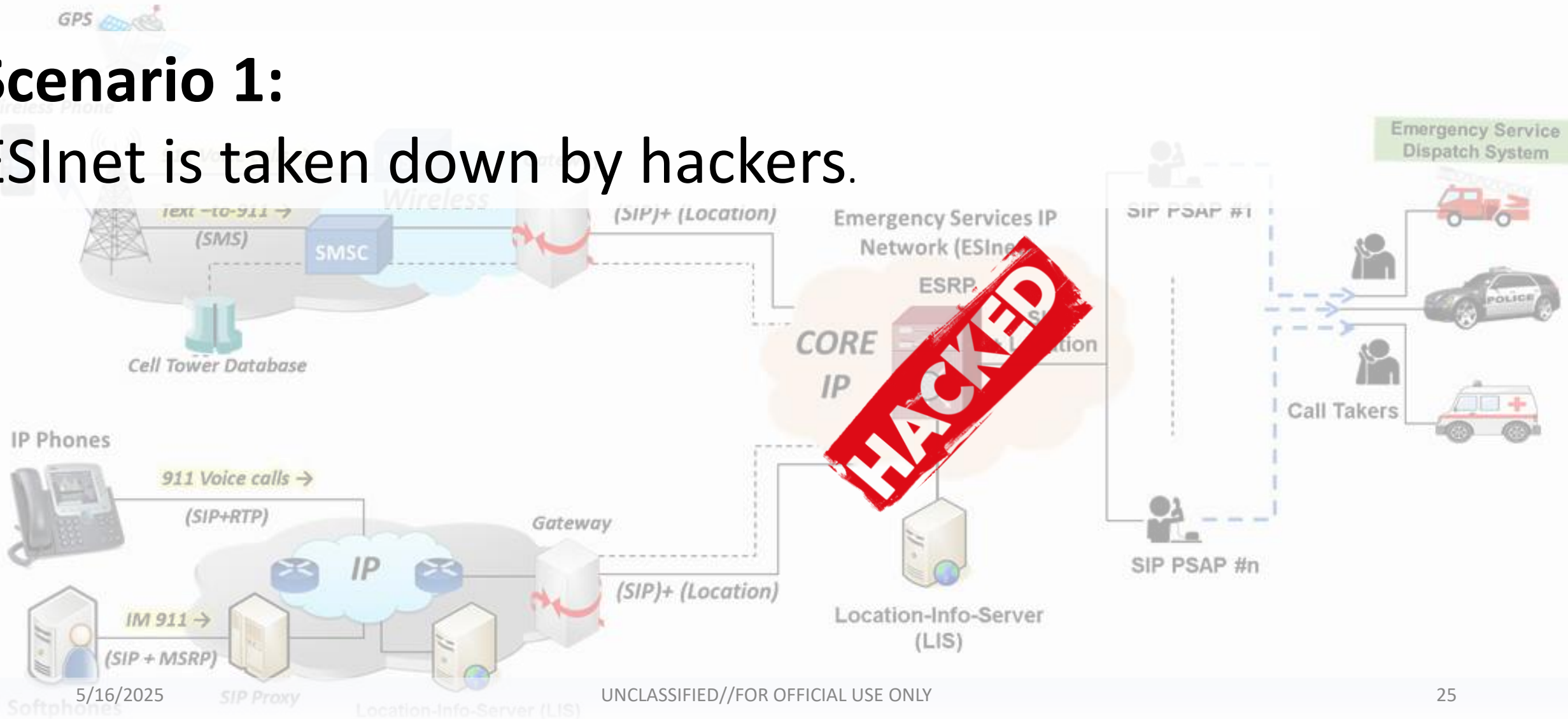
New

Statewide 911 ⇒ ESInet 2026



Statewide 911 ⇒ ESInet 2026

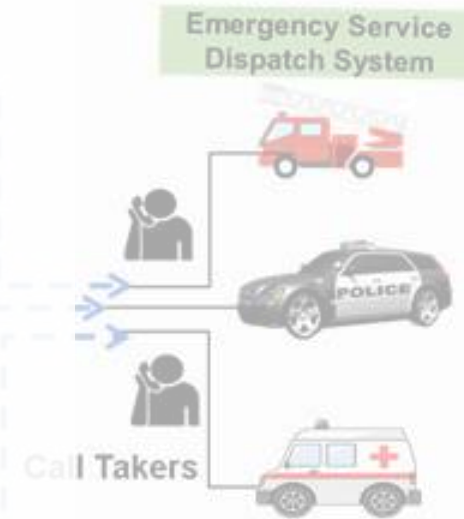
Scenario 1: ESInet is taken down by hackers.



Statewide 911 ⇒ Scenario 1

1. **Vendor manages NOC – Network Operations Center (Incident Commander)**
2. KY will lose call routing capability throughout the state simultaneously
3. We would revert back to operations as they are now, decentralized.
4. Some PSAPs have maintained existing local connections (trunk lines) as a backup. They can restore capability.
5. All PSAPs have cellular connectivity via Cradle Point.
6. All PSAPs have failover agreements established.
7. Some PSAPs can route calls to admin lines.
8. Some PSAPs can route calls to a single cell #.
9. PSAPs have resources to continue with paper.
10. Map data is hosted by COT in the cloud and CAD systems store it locally.

Operations resume without ESF support.
Now Cybersecurity Issues are addressed.

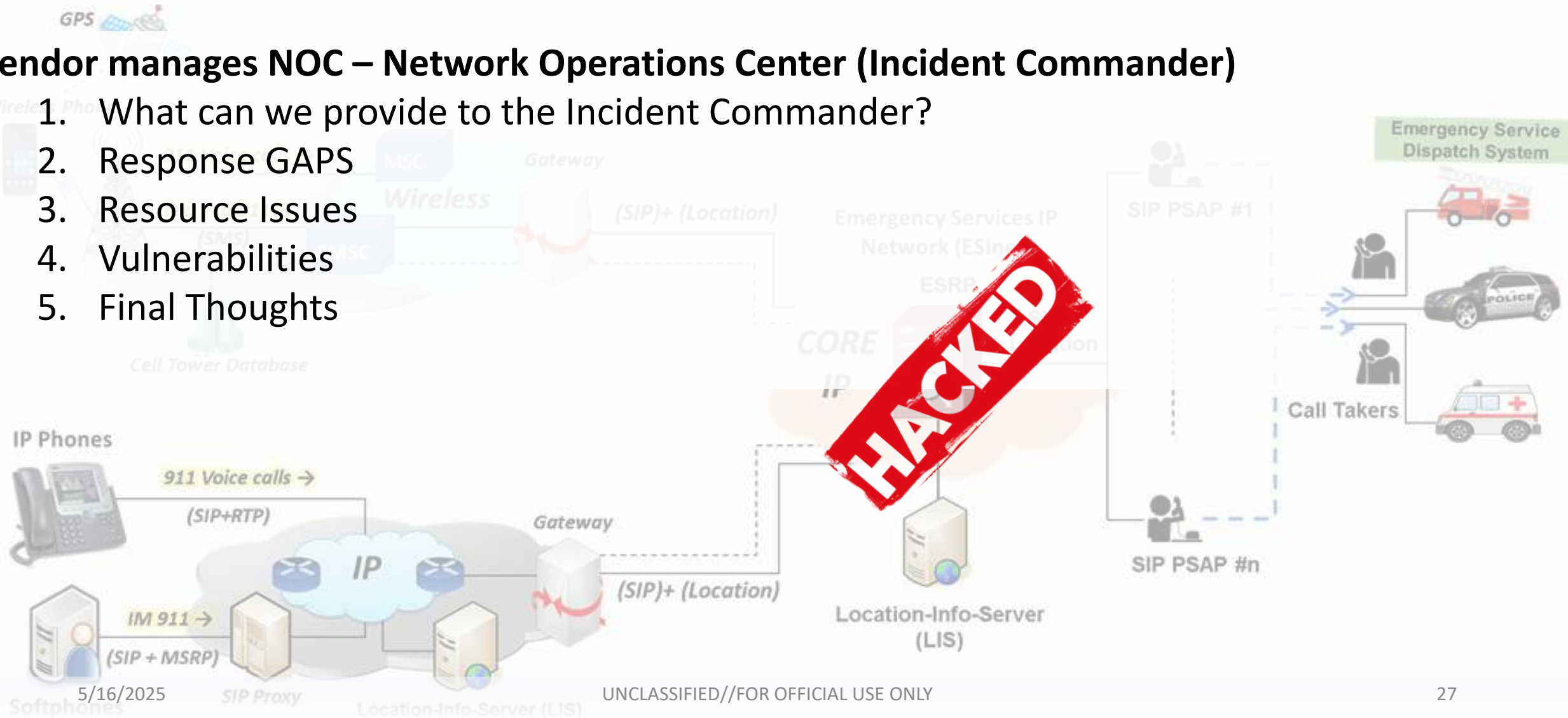


HACKED

Statewide 911 ⇒ Scenario 1

Vendor manages NOC – Network Operations Center (Incident Commander)

1. What can we provide to the Incident Commander?
2. Response GAPS
3. Resource Issues
4. Vulnerabilities
5. Final Thoughts



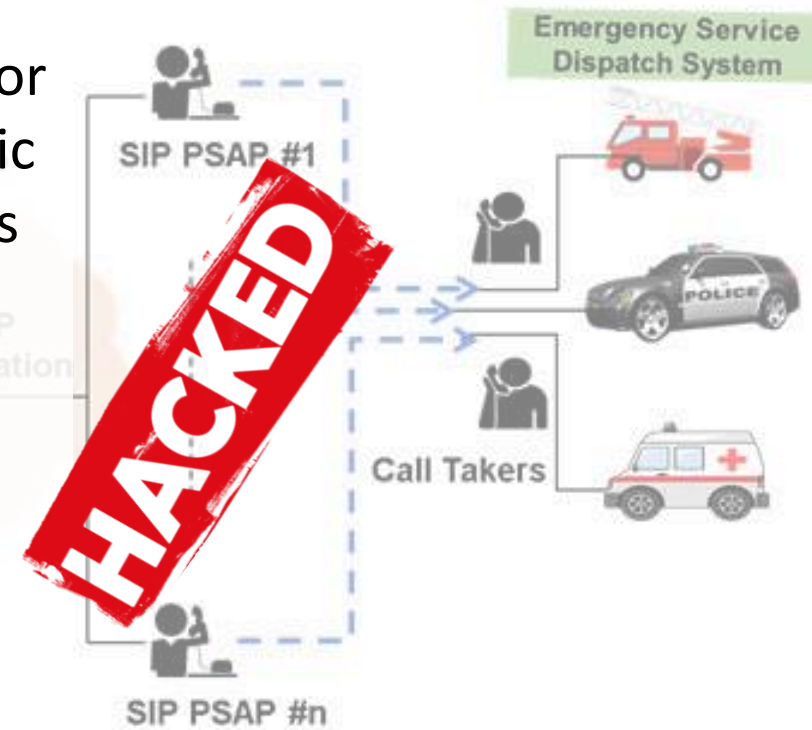
Statewide 911 ⇒ Scenario 2



Scenario 2:

Multiple PSAPs are infected with ransomware.

1. Even under a unified ESInet, PSAPs use many different vendors for the variety of software required to function. PSAPs with 3 specific CAD vendors are victimized by ransomware. 43 out of 117 PSAPs are infected.
2. CAD systems no longer function, but call taking capability is restored quickly. (reference previous exercise).
3. All 43 PSAPs have reverted to manual, paper-based processes.
4. All 43 PSAPs have IT support either internally, or via MSP/MSSP
5. There are 43 local incident commanders attempting to identify patient zero, quarantine the infection, see if other city/county departments are impacted, contact insurance or other aid, and the list goes on...

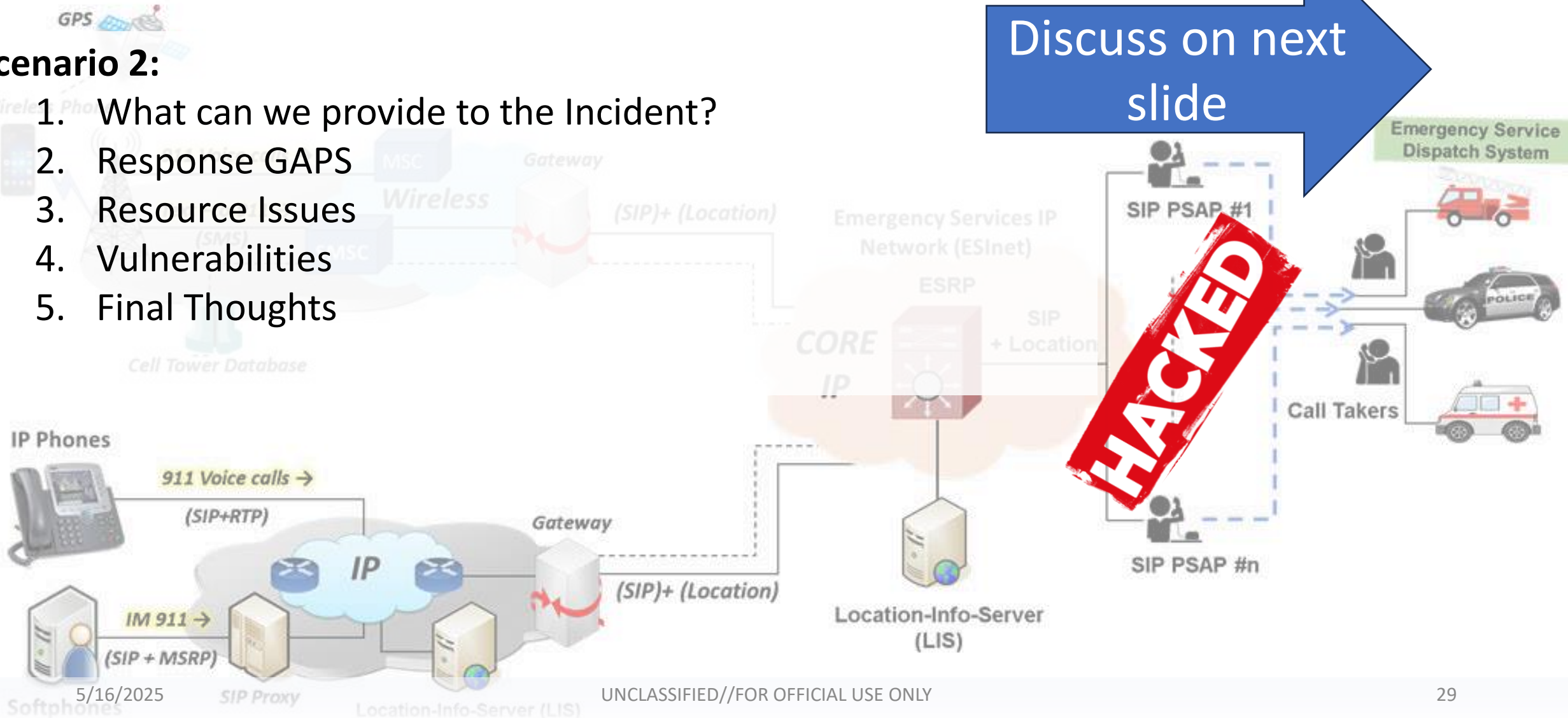


Statewide 911 ⇒ Scenario 2

Discuss on next slide

Scenario 2:

1. What can we provide to the Incident?
2. Response GAPS
3. Resource Issues
4. Vulnerabilities
5. Final Thoughts





Focus

Normal Activities

Emergency Response And Relief

Operations Ceased or Changed

Restoration – Repair – Replacement - Improvement

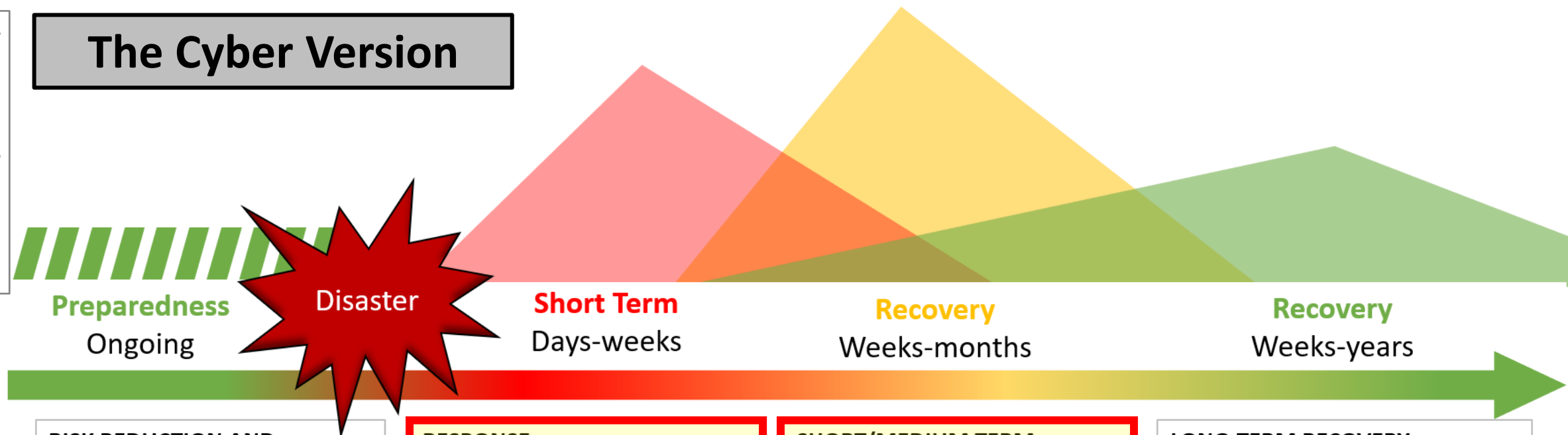
Restore Baseline Functionality

Returned and Functioning at Pre-Disaster Levels or Greater

Mature Cybersecurity Programs

The Cyber Version

Size and Scope of Activity



RISK REDUCTION AND READINESS

- Join MS-ISAC
- Utilize CISA tools
- Assess/reduce risk
- Build community resilience
- Test disaster preparedness
- Build partnerships (local/state/federal)
- Plan for business continuity
- Adopt best practices
- Apply for cyber grant(s)

Example Activities

RESPONSE

- Contain the infection
- Apply security patches
- Conduct forensics
- Identify the cause and cascading infrastructure impact(s)
- Restore backups
- Communicate early and often (local/state/federal)
- Share indicators of compromise within appropriate communities

SHORT/MEDIUM TERM RECOVERY

- Restore primary functionality (i.e., water or energy distribution)
- Restore network functionality
- Document the incident thoroughly
- Review and revise plans
- Identify areas for network/system improvement
- Conduct recurring training

LONG-TERM RECOVERY

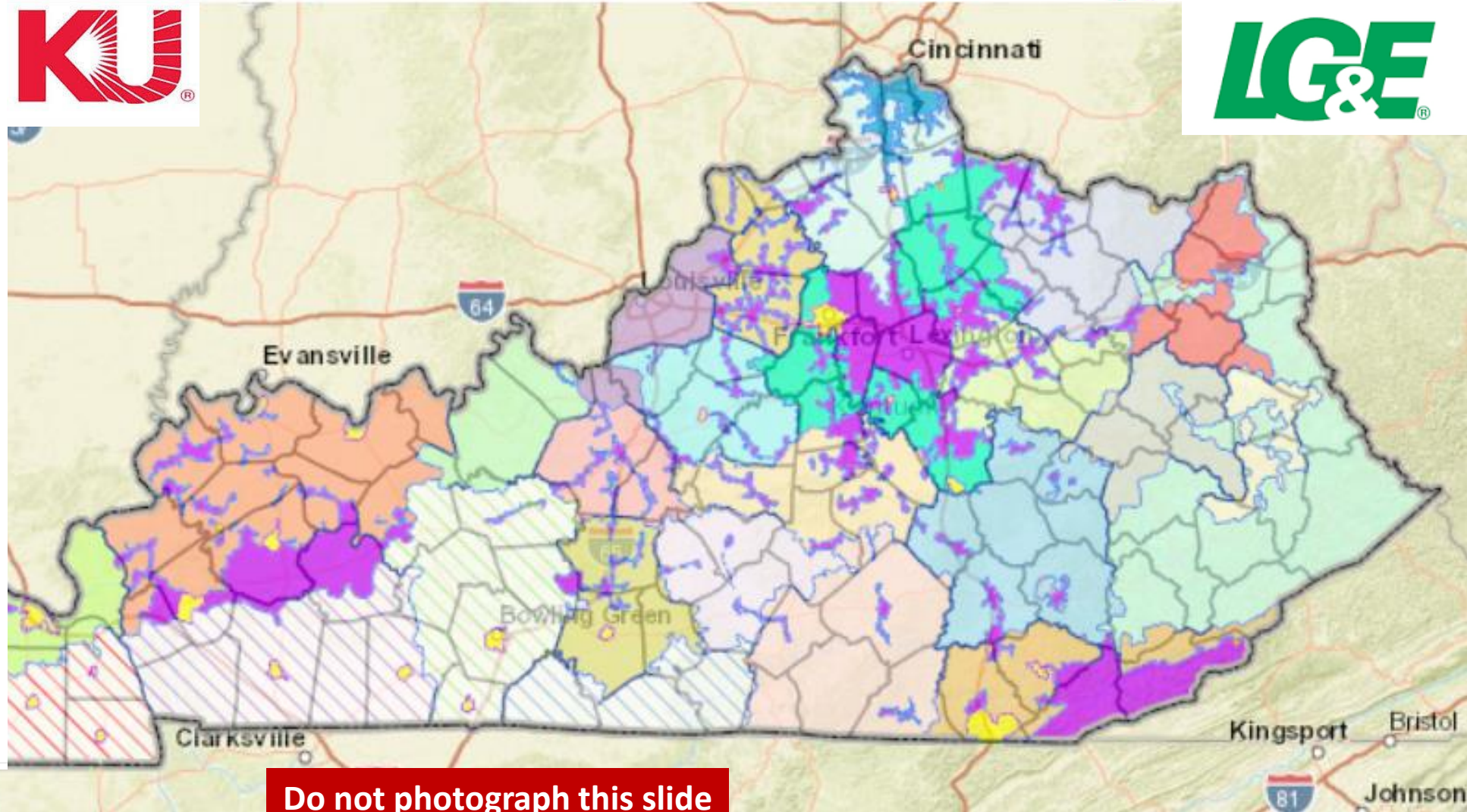
- Strengthen cybersecurity posture via implementation of best practices
- Establish continuous system monitoring
- Conduct annual risk assessment(s) via 3rd Party
- Conduct recurring training for IT staff and users
- Upgrade software/hardware
- Join cybersecurity groups



Most DANGEROUS Least LIKELY 2

Statewide Power

Statewide Power



Legend

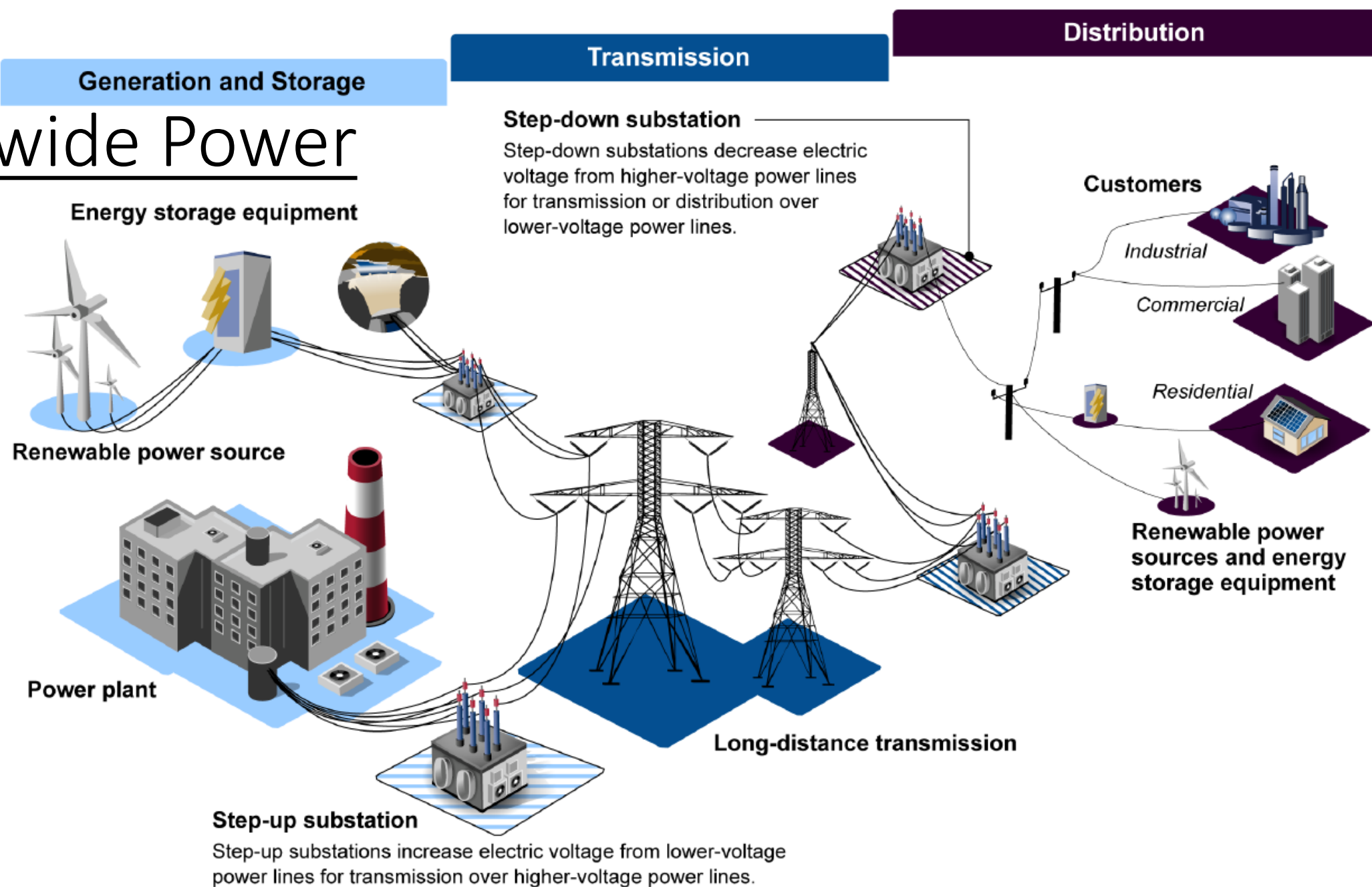
Electric Service Areas

- Municipal Utilities
- Kentucky Power Company (KPC)
- Duke Energy Kentucky, Inc.
- Kentucky Utilities Company (KU)
- Louisville Gas and Electric Company (LG&E)
- Jackson Energy Cooperative & KU
- Meade County RECC & LG&E
- Big Sandy RECC
- Blue Grass Energy Cooperative
- Clark Energy Cooperative
- Cumberland Valley Electric
- Farmers RECC
- Fleming-Mason Energy Cooperative
- Grayson RECC
- Inter-County Energy Cooperative
- Jackson Energy Cooperative
- Jackson Purchase Energy Corporation
- Kenergy Corporation
- Licking Valley RECC
- Meade County RECC

Do not photograph this slide

Three "Phases"...

Statewide Power



Statewide Power

The U.S. electric grid comprises three distinct functions:

Generation and Storage. Power plants generate electric power by converting energy from other forms—chemical, mechanical (hydroelectric or wind), thermal, radiant energy (solar), or nuclear—into electric power. Energy storage, such as batteries or pumped hydroelectric, can improve the operating capabilities of the grid while also regulating the quality and reliability of power.

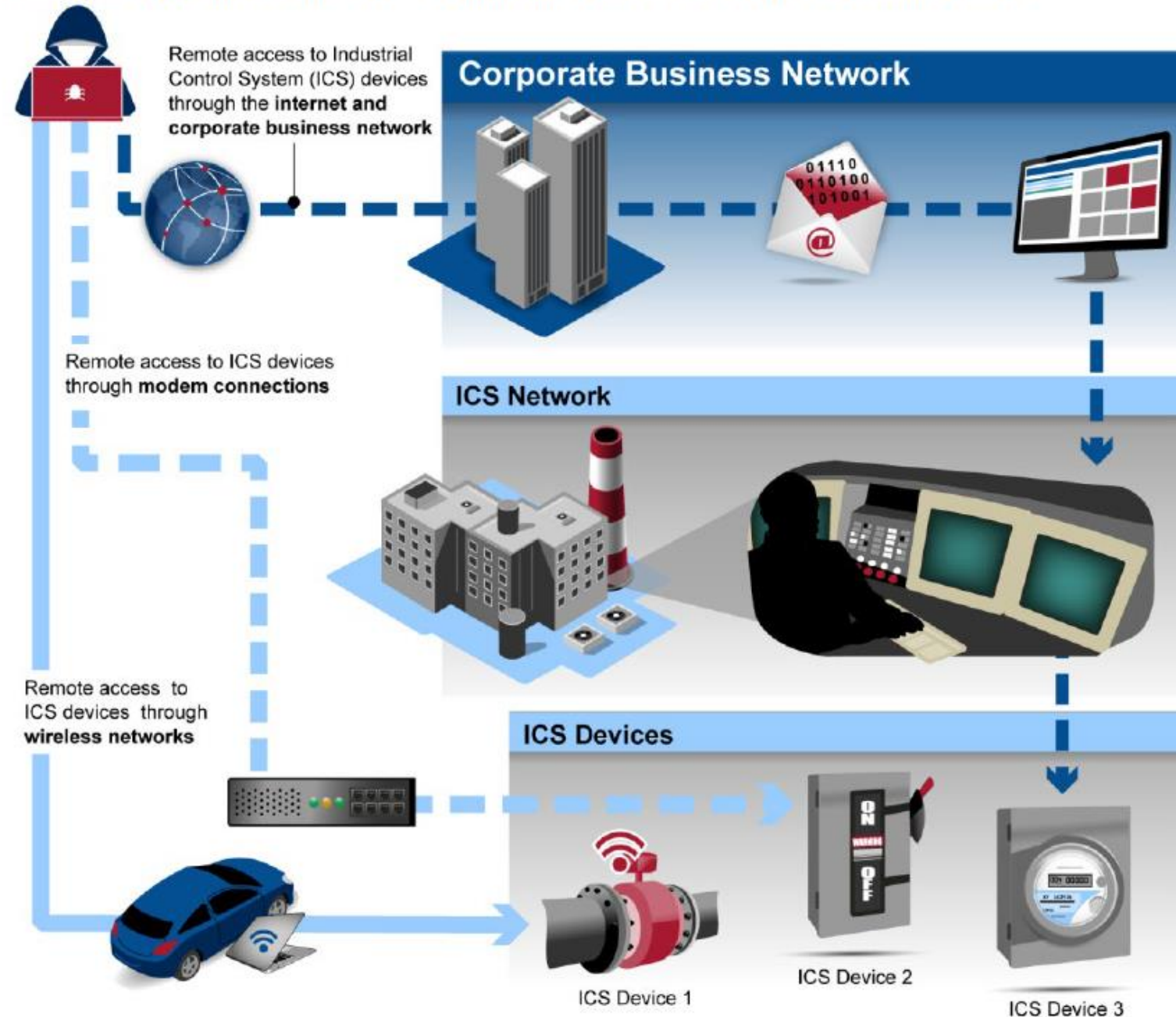
Transmission. The power transmission system connects geographically distant power plants with areas where electric power is consumed. Substations are used to transmit electricity at varied voltages and generally contain a variety of equipment, including transformers, switches, relays, circuit breakers, and system operations instruments and controls.

Distribution. The distribution system carries electric power out of the transmission system to industrial, commercial, residential, and other consumers.

Statewide Power

Volt Typhoon and other APTs do target CI for both known and unknown purposes.

Potential Ways an Attacker Could Compromise Industrial Control System Devices



Statewide Power

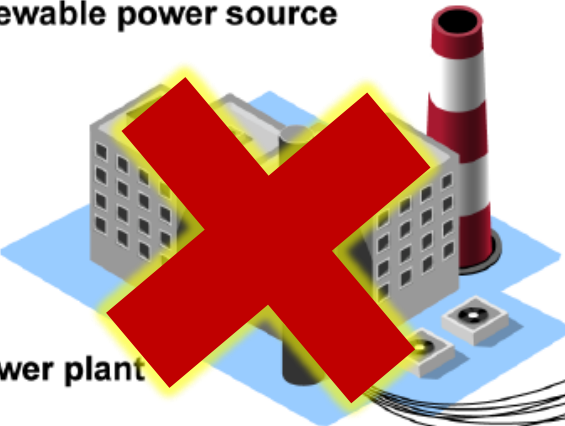
Step-down substation

Step-down substations decrease electric voltage from higher-voltage power lines for transmission or distribution over lower-voltage power lines.

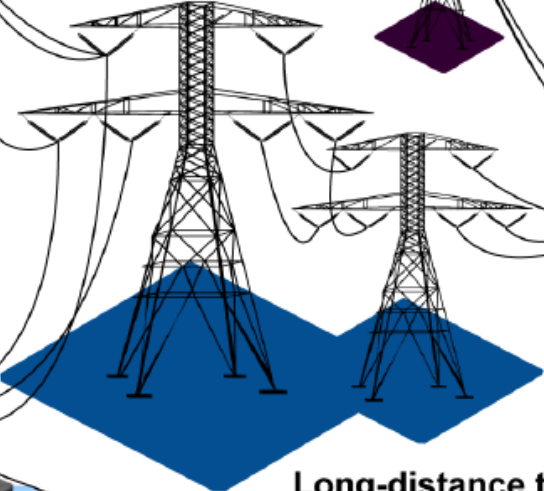
Energy storage equipment



Renewable power source



Power plant



Long-distance transmission

Step-up substation

Step-up substations increase electric voltage from lower-voltage power lines for transmission over higher-voltage power lines.

Customers

Industrial

Commercial

Residential

Renewable power sources and energy storage equipment

What happens if...??

Statewide Power

- KY's other ESFs have been responding to power outages for many years, it may be safe to assume physical needs/response remains the same regardless the cause (flood, winds, ice, cyber, etc.)
- How will the cyber ESF fit in?
 - Do power centers have internal resources (or cyber insurance) to respond to cyber attacks?
 - Do they want external help from state government/EOC?
 - Have they established relationships with Federal resources?
 - What do we (or will we) be able to offer?



Focus

Normal Activities

Emergency Response And Relief

Operations Ceased or Changed

Restoration – Repair – Replacement - Improvement

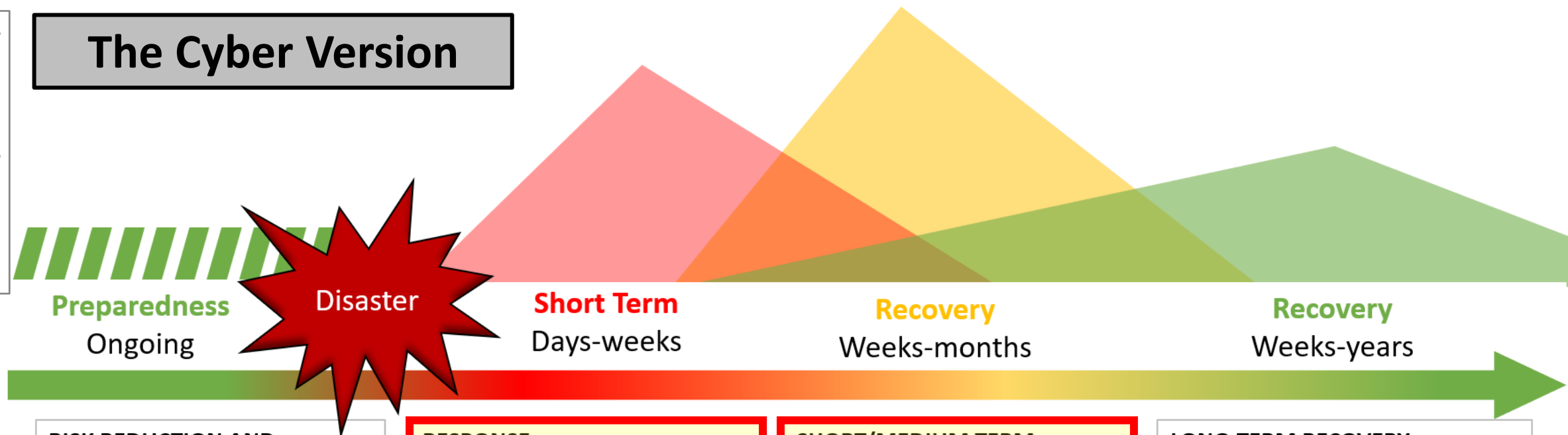
Restore Baseline Functionality

Returned and Functioning at Pre-Disaster Levels or Greater

Mature Cybersecurity Programs

The Cyber Version

Size and Scope of Activity



Example Activities

RISK REDUCTION AND READINESS

- Join MS-ISAC
- Utilize CISA tools
- Assess/reduce risk
- Build community resilience
- Test disaster preparedness
- Build partnerships (local/state/federal)
- Plan for business continuity
- Adopt best practices
- Apply for cyber grant(s)

RESPONSE

- Contain the infection
- Apply security patches
- Conduct forensics
- Identify the cause and cascading infrastructure impact(s)
- Restore backups
- Communicate early and often (local/state/federal)
- Share indicators of compromise within appropriate communities

SHORT/MEDIUM TERM RECOVERY

- Restore primary functionality (i.e., water or energy distribution)
- Restore network functionality
- Document the incident thoroughly
- Review and revise plans
- Identify areas for network/system improvement
- Conduct recurring training

LONG-TERM RECOVERY

- Strengthen cybersecurity posture via implementation of best practices
- Establish continuous system monitoring
- Conduct annual risk assessment(s) via 3rd Party
- Conduct recurring training for IT staff and users
- Upgrade software/hardware
- Join cybersecurity groups

Statewide Power

From CISA website: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>




ACTIONS TO TAKE TODAY TO MITIGATE VOLT TYPHOON ACTIVITY:

1. Apply patches for internet-facing systems. Prioritize patching critical vulnerabilities in appliances known to be frequently exploited by Volt Typhoon.
2. Implement phishing-resistant MFA.
3. Ensure logging is turned on for application, access, and security logs and store logs in a central system.
4. Plan “end of life” for technology beyond manufacturer’s supported lifecycle.




Scenario 4: Small to Medium Infrastructure

We've looked at the big, "statewide exercise" events, we may know how to prepare for them, but does ESF 17 and its partners have anything to offer to dealing with the 1 ransomware a week and 2 BEC events a week? These events are already happening.



Vulnerabilities For Small- Medium Infrastructure

- 
1. Vulnerabilities are finite but seem infinite.
 2. Lack of IT/Cybersecurity personnel
 3. Not using .gov
 4. Needing and not leveraging MS-ISAC, CISA, Grants, and free tools
 5. Not using MFA
 6. Legacy Systems
 7. No awareness of external/internal vulnerabilities
 8. No awareness of resources (cyber ESF & partners)
 9. No backups

Alert Levels

The alert level is determined using a threat severity formula: $\text{Severity} = (\text{Criticality} + \text{Lethality}) - (\text{System Countermeasures} + \text{Network Countermeasures})$

Level	Description	Actions
Low	No unusual activity exists beyond the normal concern for known hacking activities, known viruses, or other malicious activity.	Manage internally.
Guarded	The potential for malicious cyber activities exists, but no known exploits have been identified, or known exploits have been identified but no significant impact has occurred.	Manage internally.
Elevated	There are known vulnerabilities that are being exploited with a moderate level of damage or disruption, or the potential for significant damage or disruption is high.	Notify MS-ISAC, FBI IC3, and ESF 17 for awareness/sharing of information.
High	Vulnerabilities are being exploited with a high level of damage or disruption, or the potential for severe damage or disruption is high.	Notify MS-ISAC, FBI IC3, and ESF 17 for mobilization/consultation from KY ARNG DCOE team, CISA, FBI and IOC sharing across organizations similar to the victim organization. Notify other ESFs for awareness of possible cross-sector impact.
Severe	Vulnerabilities are being exploited with a severe level or widespread level of damage or disruption of Critical Infrastructure Assets.	Notify MS-ISAC, FBI IC3, and ESF 17 for mobilization/consultation from KY ARNG DCOE team, CISA, FBI and IOC sharing across organizations similar to the victim organization. Notify other ESFs for awareness and response.

Capabilities Matrix (2024)

Cyber response is :

1. Voluntary (for the victim and resource)
2. Non-regulatory

Organization	Federal/State	Capability
KOHS	State	Preparedness only. Grants, training and exercises.
CISA	Federal	Limited Response, consultation, risk assessment security services.
FBI	Federal	Financial fraud killchain, limited response, investigation
KY ARNG DCOE	State	Working to enact taskforce and executive order for response and other capabilities.
MS-ISAC	Federal	24/7 SOC - remote response, forensics, consultation, security tools.
COT	State	Consultation

Cyber ESF 17 Overview

January 2024

Phillip.Ross@KY.gov

Dayna?

Colin?

