NATIONAL GOVERNORS ASSOCIATION

2022 CYBERSECURITY WEBINAR SERIES

State Support of Critical Infrastructure Cybersecurity

February 16, 2023

Introduction

Mikki Munson

Cybersecurity & Critical Infrastructure Protection Program Manager, Protected Critical Infrastructure Information Officer

Wyoming Office of Homeland Security

Katherine Chipman

Supervisory Intelligence Analyst,

Utah Statewide Information & Analysis Center

Mallorie Nielsen

Cyber Threat Intelligence Analyst,

Utah Statewide Information & Analysis Center

Cyber Assistance Response Effort (CARE) Team

CARE Team Overview and Cyber Incident Response Process

Mikki Munson

Cybersecurity & Critical Infrastructure Program Manager
Wyoming Office of Homeland Security (WOHS)
307.777.4939
Mikki.munson@wyo.gov

CARE TEAM Executive Summary

The State of Wyoming Cyber Disruption Response Plan was developed by the CARE Team to protect state and local jurisdictions by reducing the impacts of cyber related events, to include incidents and disruptions, through prevention, response, and recovery. Cyber events have the ability to severely impact the social, economic and physical welfare of state citizens and businesses through escalated or multiple simultaneously executed attacks on the state's most critical sectors. The plan provides a framework that enables the state emergency management and information technology to work seamlessly with public and private partners to rapidly respond to and minimize the impact of cyber events in Wyoming.

CARE TEAM Executive Summary

The CARE Team’s Cyber Disruption Response Plan provides a common framework for identifying and responding to technological threats at the state level, that mirrors the federal government model, with corresponding responses to address threats of increasing scope and severity. Cyber threats range from minor malware through specific attacks on targeted state networks and services, to severe attacks capable of catastrophic disruption to services and facilities of single or multiple sectors providing critical support to state and local jurisdictions. This plan enables closely integrated planning by providing for critical infrastructure entities and partnership use.

Purpose

The CARE Team's Cyber Disruption Response Plan provides the **Wyoming Office of Homeland Security (WOHS), Enterprise Technology Services (ETS), Wyoming Information Analysis Team (WIAT), Computer Crime Team (CCT)**, and other potential stakeholders within the state of Wyoming with a management framework to coordinate prevention, response and recovery activities related to cyber events within the state system. This framework is developed from the National Incident Management System (NIMS) and the Incident Command System (ICS) structure.

State Agencies Involved in Cybersecurity

Enterprise Technology Systems (ETS)

Chief Information Security Officer develops and implements a statewide information security program; including compliance goals, strategies, policies, and services designed to protect state technology resources from unauthorized access, use, disclosure, disruption, modification, or destruction of state technology resources.

Security Team implements, manages, maintains, and monitors a multi-layered security ecosystem, which protects the confidentiality, integrity, and availability of the state's technology systems and the data sources residing within it.

Cyber Assistance Response Effort (CARE) Team – WY Office of Homeland Security (WOHS)

CARE Team: The response team for cybersecurity incidents at the local/state level for critical infrastructure that is not privately owned. We can assist with private critical infrastructure in an advisory role.

WOHS Mission: Preparing Wyoming to respond to and recover from all hazards.

WY Information Analysis Team (WIAT) / Computer Crime Team (CCT)

CCT: Has jurisdiction over all computer crimes in the state pursuant to Wyo. Stat. § 9-1-618(b)(iv). They have digital forensics capabilities.

WIAT: The primary purpose of the Wyoming Information Analysis Team (WIAT) is to collect, analyze, and disseminate criminal intelligence and provide support to local, state, and federal law enforcement agencies pertaining to the state of Wyoming pursuant to Wyo.Stat. § 9-1-627 and 28 CFR Part 23. A major goal of WIAT is to identify, document, and disseminate criminal intelligence concerning persons involved in organized crime, terrorist groups, and those crimes involving multi-jurisdictional or serial crimes while protecting the privacy, civil rights, and civil liberties of the citizens we serve.

CARE Team Day-to-Day Members

WOHS
Homeland Security/ Emergency Management

ETS
Defensive Cyber Operations for WY State Network

CCT
Any criminal activity on computers in WY

WIAT
Information Analysis & Sharing

FBI
Technical Expertise and Unique Resources

DHS
Intelligence & Analysis Officer

National Guard Defensive Cyber Operations Element Support

CISA
Resources and guidance

Scope

Cyber events may be a single yet pertinent element of a larger incident that has the potential to threaten lives, property, and continued functionality for communities. Activities conducted pursuant to the CARE Team’s Cyber Disruption Response Plan work within the incident command structure, complement existing plans and procedures, and are consistent with the National Incident Management System (NIMS).

Roles and Responsibilities

The State of Wyoming through the **Wyoming Office of Homeland Security** coordinates federal, state, and local agencies to prevent, respond to, and recover from the effects of cyber events. The state promotes collaboration between the respective cyber functions and emergency management functions of these various entities. **During a cyber event, the Unified Command consists of members of the CARE Team and the specific agencies affected by the cyber event.**

Roles and Responsibilities

Enterprise Technology Services (ETS)

- ETS is directly aligned with the goals and objectives of the National Strategy to Secure Cyberspace. Working closely with federal, state, local and private sector partners, ETS actively gathers and analyzes information on cyber threats and vulnerabilities that present risk to the state's information systems or the critical information managed within.
- ETS is responsible for working with state agencies for security risk management to manage information security policies, security standards, onsets with agencies on technical matters, and manages enterprise projects to meet security requirements.
- ETS will be the decision maker for determining the appropriate reactive measures to a cyber event. ETS will notify WOHS through the WOHS Duty Officer, WIAT, and DCI through the Deputy Director of Operations and the Team Leader of the DCI Computer Crimes Team, at a Yellow/Level 2.

Roles and Responsibilities

Wyoming Information Analysis Team (WIAT)

- Analyze threat information, sharing best practices, investigative information, coordination of response and mitigation.
- Assist in attributing the source of cyber events through resources and the network of fusion centers.
- Work with and support the DCI Computer Crime Team as needed.
- Coordinate with federal partners to produce and -- as deemed appropriate and in accordance with relevant state policies -- disseminate intelligence reporting for use in mitigation efforts and intelligence analysis.

Roles and Responsibilities

Wyoming Division of Criminal Investigation (DCI) Computer Crime Team (CCT)

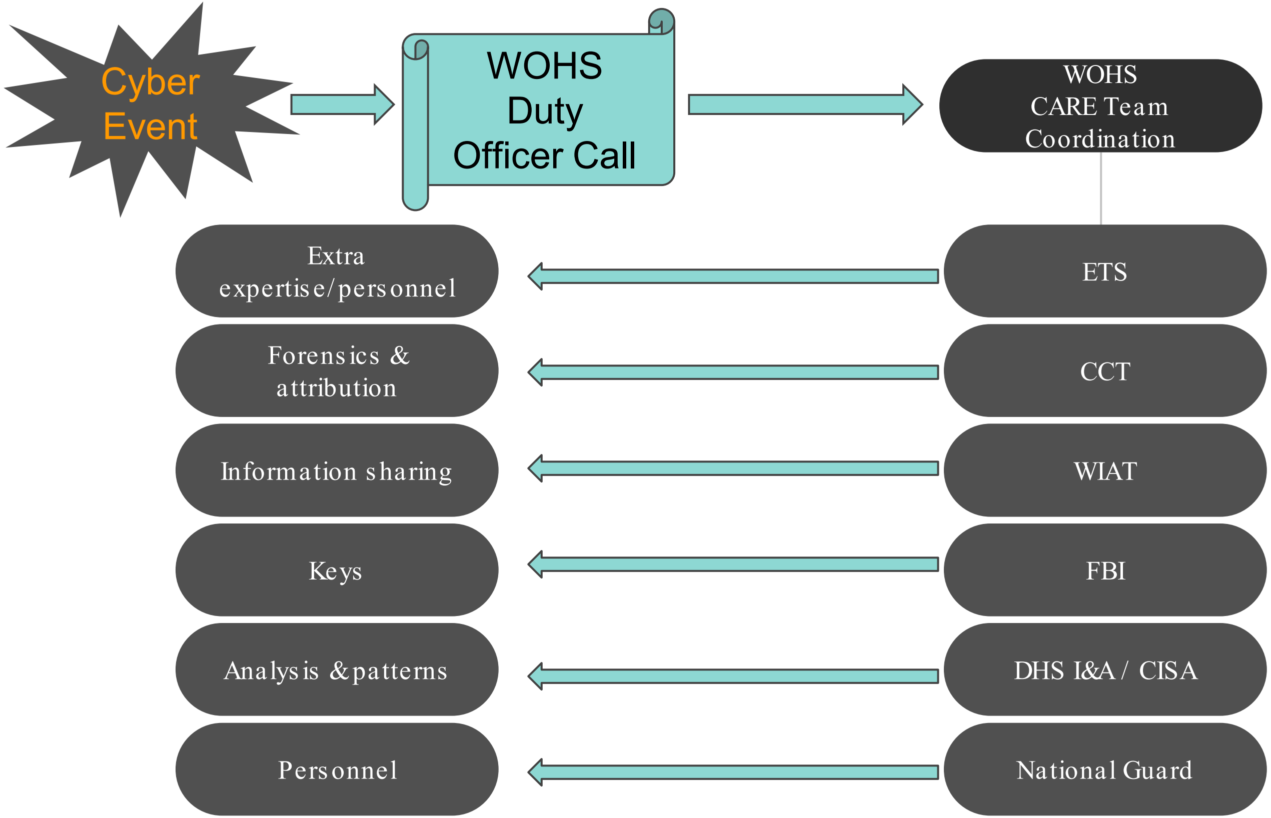
- Criminal Investigation
  - Wyo. Stat. 9-1-618(b)(iv) Suspected violations of computer crimes as specified in W.S. 6-3-501 through 6-3-507;
  - For example:
    Wyo. Stat. 6-3-507. **Computer extortion**; penalties.
    (a) A person is guilty of computer extortion if he knowingly and without authorization introduces, attempts to introduce or directs or induces another to introduce, any ransomware into a computer, computer system or computer network which requires the payment of money or other consideration to remove the ransomware or repair the damage caused to the computer, computer system or computer network by the ransomware.
    (b) Computer extortion is a felony punishable by imprisonment for not more than ten (10) years, a fine of not more than ten thousand dollars ($10,000.00), or both.
    (c) For purposes of this section:
    (i) "**Computer or data contaminant**" means any virus, worm or other similar computer program designed to encrypt, modify, damage, destroy, record or transmit information within a computer, computer system or computer network;
    (ii) "**Ransomware**" means a computer or data contaminant, encryption or lock that restricts an owner's access to a computer, computer data, computer system or computer network in any way. "Ransomware" does not include authentication required to upgrade or access purchased content.
- Forensic analysis and support as appropriate

Concept of Operations

In a cyber event, the WOHS Duty Officer should be notified through the appropriate channels for activation of the CARE Team.

- Complications from a cyber event may threaten lives, property, the economy, and security.
- Rapid identification, information exchange, investigation, and coordinated responses are critical in the consequence management of cyber events.

CARE Team Activation & Resources



Cyber Event

WOHS Duty Officer Call

WOHS CARE Team Coordination

ETS → Extra expertise/personnel

CCT → Forensics & attribution

WIAT → Information sharing

FBI → Keys

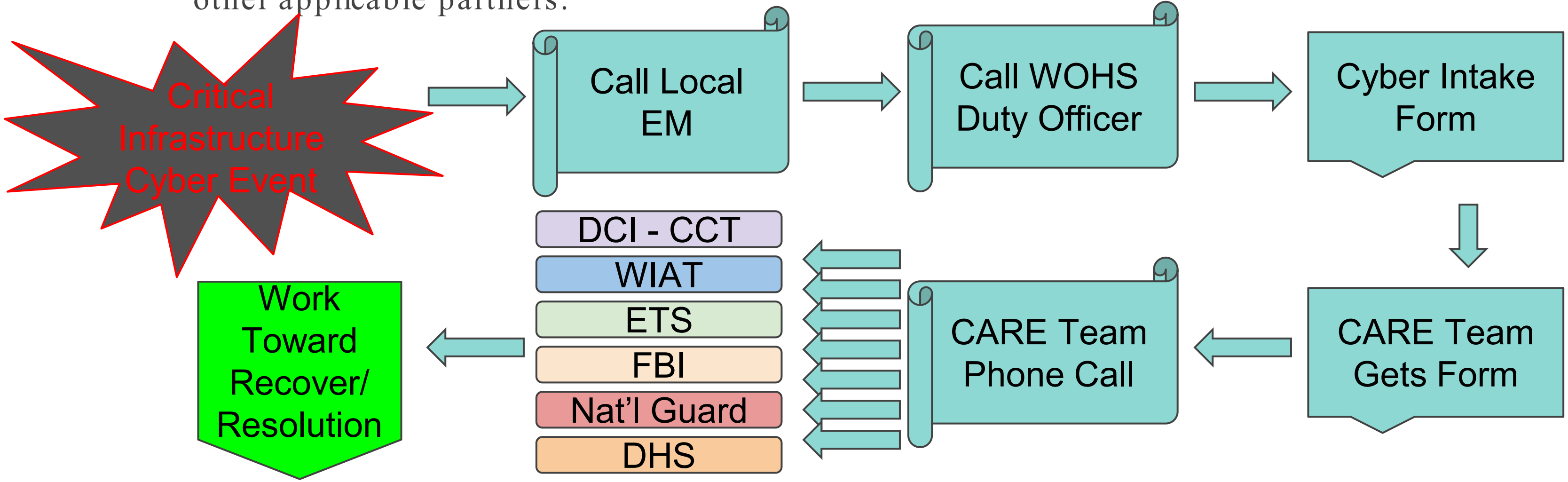
DHS I&A / CISA → Analysis & patterns

National Guard → Personnel

CARE Team Activation Procedures WOHS

Cyber Event on Critical Infrastructure (Public/Private Sector):

In the event of a cyber event/incident that may affect critical infrastructure, the initial call should come to the WOHS duty officer. The cyber event intake form will be completed and sent to the CARE team. WOHS will then work with the victim of the cyber event/incident and coordinate a call with: CCT/WIAT/ETS/FBI/NATIONAL GUARD, DHS I&A and CISA, and other applicable partners.



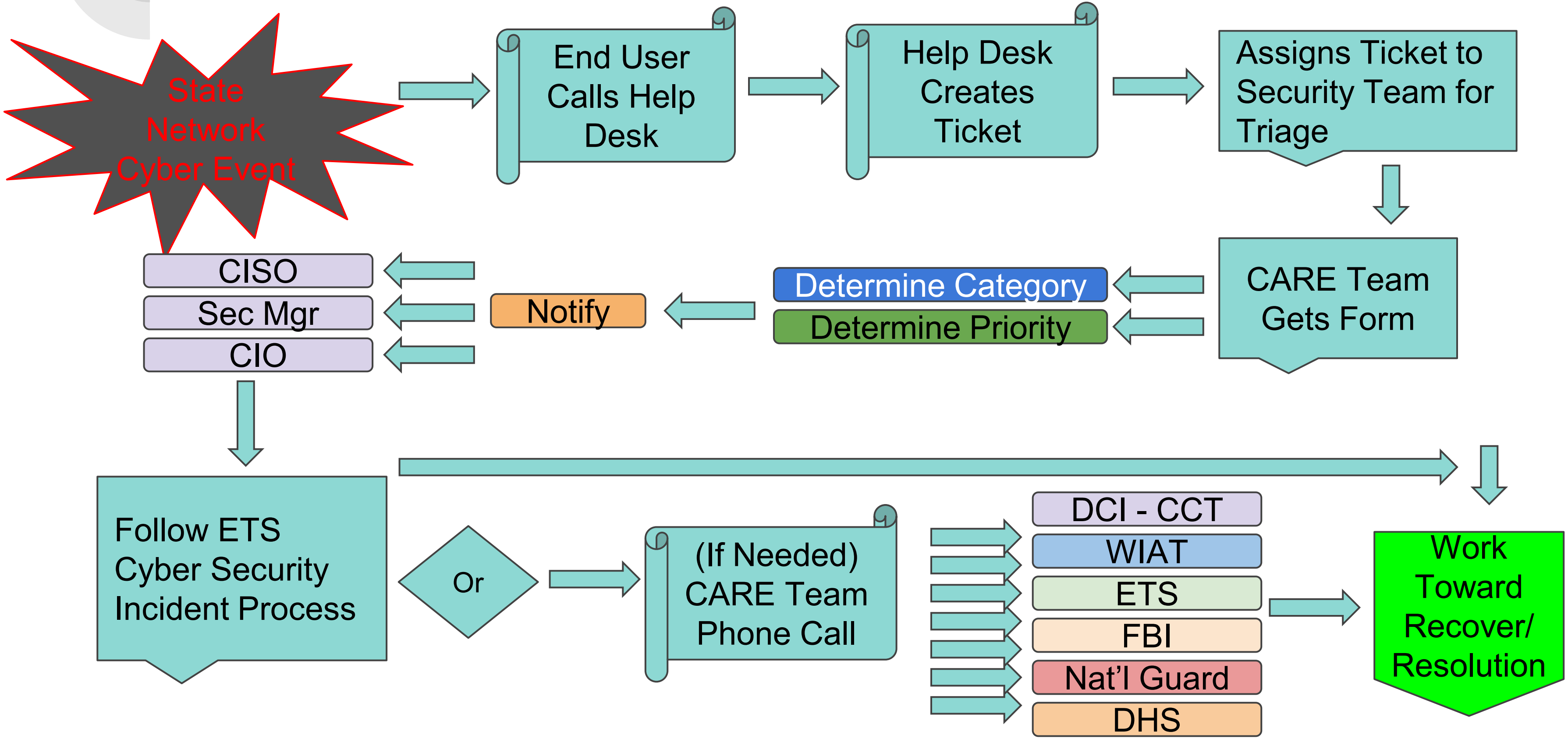
CARE Team Activation Procedures WOHS

Cyber Event on State Network:

The process for an event on the state network is when ETS receives an incident from an incident reporter, usually to the helpdesk. The helpdesk will create an incident ticket and assign it to the security team to triage. When a cyber security event is reported, specific steps must be taken. Items that enter this process are those that are potential security events/incidents and cannot be eliminated otherwise. The triage team will determine the initial incident category, internal priority and report all incidents to the CISO or CIO. From there, the security team will follow the cyber security incident process.

Depending on the details of a particular cyber incident, other actions may occur at any impact severity level, such as a larger security investigation to include nonfiction and potential assistance from WOHS, WIAT, CCT, or other state partners. The appropriate sharing of the cyber incident information with other stakeholders will be based upon agreed terms for the use of the information. This information could include submitting technical details to improve awareness and management of future cyber incidents.

CARE Team Activation Procedures WOHS



State Network Cyber Event

End User Calls Help Desk

Help Desk Creates Ticket

Assigns Ticket to Security Team for Triage

CARE Team Gets Form

Determine Category

Determine Priority

Notify

CISO

Sec Mgr

CIO

Follow ETS Cyber Security Incident Process

Or

(If Needed) CARE Team Phone Call

DCI - CCT

WIAT

ETS

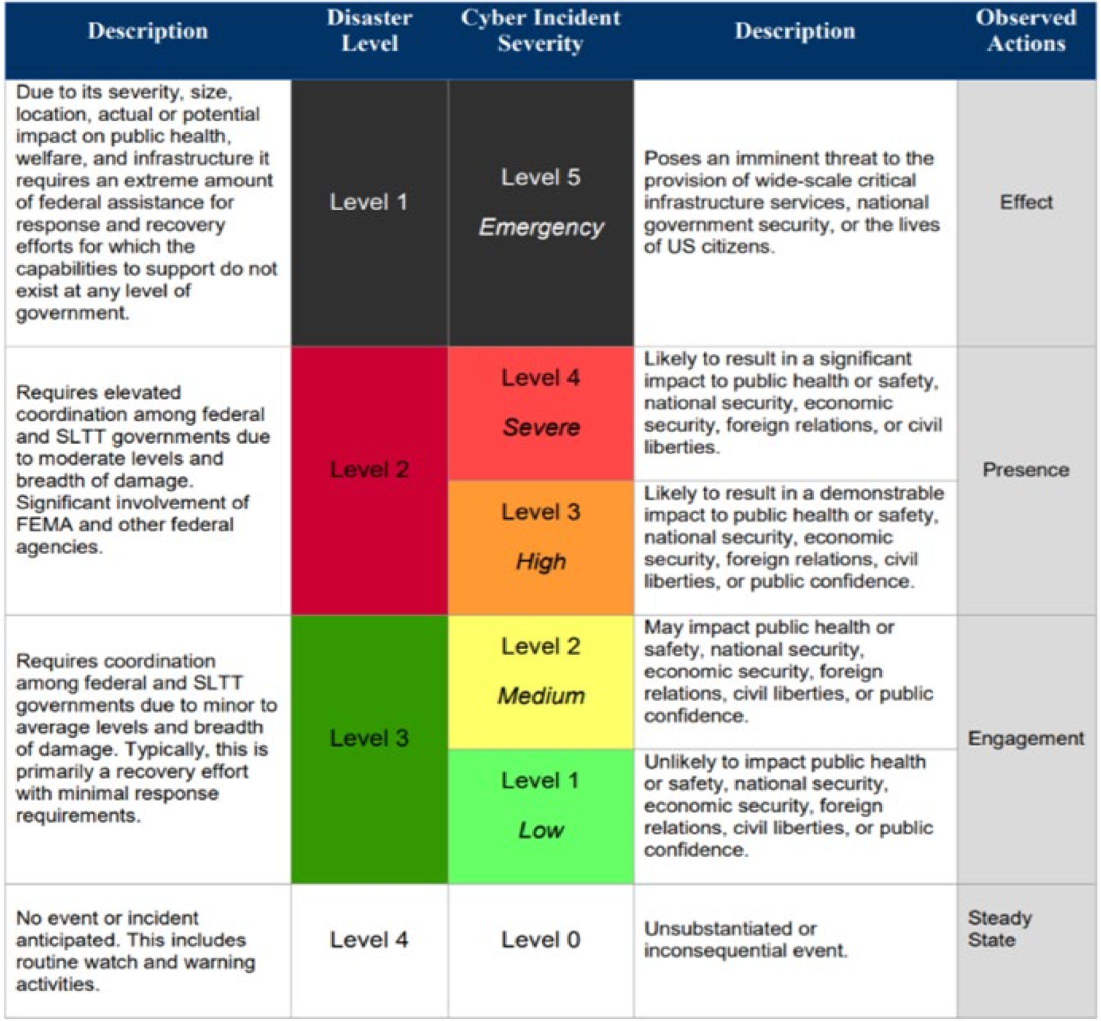
FBI

Nat'l Guard

DHS

Work Toward Recover/ Resolution

NGA Cyber Incident Severity Schema:



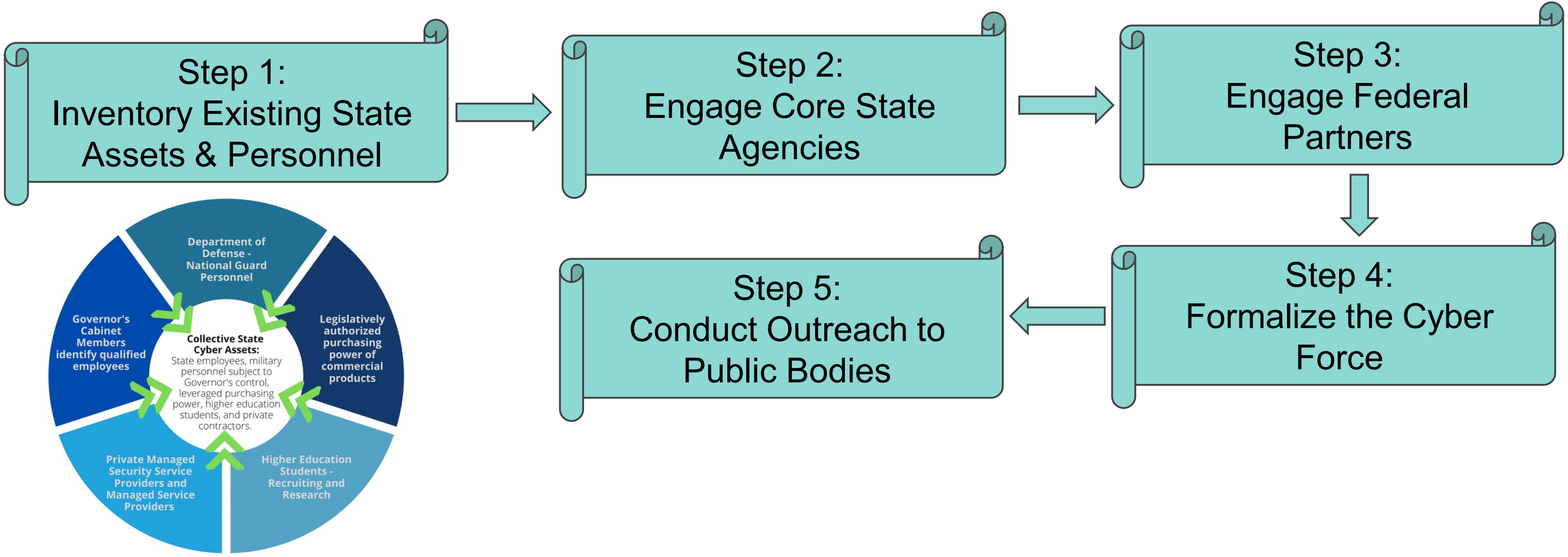
Description	Disaster Level	Cyber Incident Severity	Description	Observed Actions
Due to its severity, size, location, actual or potential impact on public health, welfare, and infrastructure it requires an extreme amount of federal assistance for response and recovery efforts for which the capabilities to support do not exist at any level of government.	Level 1	Level 5 *Emergency*	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens.	Effect
Requires elevated coordination among federal and SLTT governments due to moderate levels and breadth of damage. Significant involvement of FEMA and other federal agencies.	Level 2	Level 4 *Severe*	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	Presence
		Level 3 *High*	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
Requires coordination among federal and SLTT governments due to minor to average levels and breadth of damage. Typically, this is primarily a recovery effort with minimal response requirements.	Level 3	Level 2 *Medium*	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Engagement
		Level 1 *Low*	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
No event or incident anticipated. This includes routine watch and warning activities.	Level 4	Level 0	Unsubstantiated or inconsequential event.	Steady State

Source: Presidential Policy Directive 41, United States Cyber Incident Coordination.

National Governors Association – Council of Governors

2022-2023 CYBERSECURITY WORKING GROUP

Creating a Localized Cyber Force: 5 steps to creating a sustainable cyber force, for responses or preventative efforts, using existing resources:



Step 1: Inventory Existing State Assets & Personnel

Step 2: Engage Core State Agencies

Step 3: Engage Federal Partners

Step 4: Formalize the Cyber Force

Step 5: Conduct Outreach to Public Bodies

Department of Defense - National Guard Personnel

Legislatively authorized purchasing power of commercial products

Higher Education Students - Recruiting and Research

Private Managed Security Service Providers and Managed Service Providers

Governor's Cabinet Members identify qualified employees

Collective State Cyber Assets: State employees, military personnel subject to Governor's control, leveraged purchasing power, higher education students, and private contractors.

Questions?

Utah Cybersecurity Commission

February 2023

Statewide Information & Analysis Center (SIAC)

Fusion Center - facilitate information sharing between state, local, and federal public safety partners, as well as Critical Infrastructure

Maximize ability to **detect, investigate, apprehend**, and **respond** to criminal, terrorist, or other activity related to homeland security

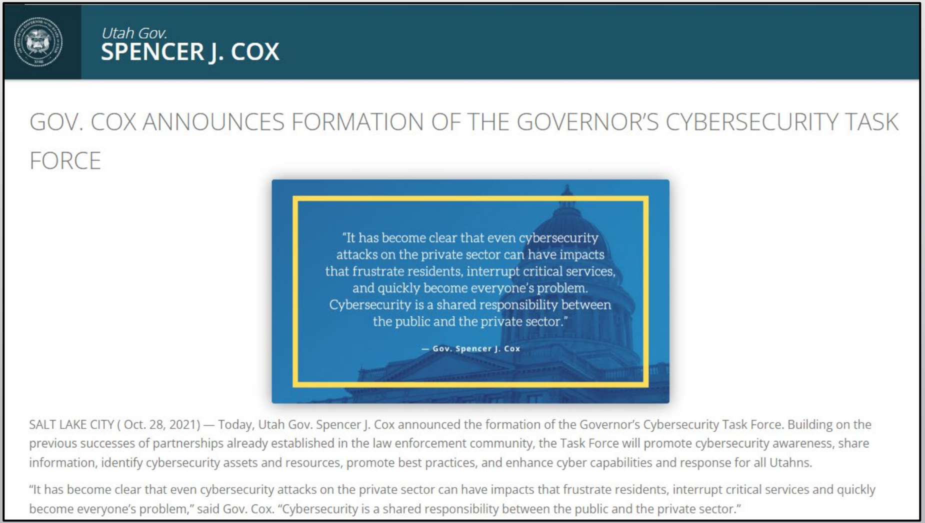
"A focal point within the state and local environment for the receipt, analysis, gathering, & sharing of threat-related information."

Utah Cybersecurity Commission

- How the Cybersecurity Commission was organized
- Commission
  - Duties
  - Membership
  - Division of Subcommittees
  - Subcommittee Recommendations
  - Annual Report
  - Plans for 2023

Utah Cybersecurity Commission

- Governor Cox announces the Governor's Cybersecurity Task Force October 2021
  - Protect the state CI from cybersecurity attacks
  - Bring together resources from both public and private sector, and critical infrastructure
- HB0280 proposed and passed in 2022, now 63C-27, Part 2
- Creates the Cybersecurity Commission
  - Supported by the SIAC
  - Chaired by Governor & Public Safety Commissioner



Utah Gov.
SPENCER J. COX

GOV. COX ANNOUNCES FORMATION OF THE GOVERNOR'S CYBERSECURITY TASK FORCE

"It has become clear that even cybersecurity attacks on the private sector can have impacts that frustrate residents, interrupt critical services, and quickly become everyone's problem. Cybersecurity is a shared responsibility between the public and the private sector."

— Gov. Spencer J. Cox

SALT LAKE CITY (Oct. 28, 2021) — Today, Utah Gov. Spencer J. Cox announced the formation of the Governor's Cybersecurity Task Force. Building on the previous successes of partnerships already established in the law enforcement community, the Task Force will promote cybersecurity awareness, share information, identify cybersecurity assets and resources, promote best practices, and enhance cyber capabilities and response for all Utahns.

"It has become clear that even cybersecurity attacks on the private sector can have impacts that frustrate residents, interrupt critical services and quickly become everyone's problem," said Gov. Cox. "Cybersecurity is a shared responsibility between the public and the private sector."

Utah Cybersecurity Commission

- Commission duties:
  - Identify and inform the governor of cyber threats, vulnerabilities to critical infrastructure, cyber assets and resources, and analysis of incident response capabilities
  - Provide cyber best practices, education, and mitigations
  - Promote cybersecurity awareness
  - Collaborate with public/private sector organizations
  - Share cyber threat intelligence with Utah's critical infrastructure
- Members consist of both government and private sector representatives

Cybersecurity Commission Membership

➔ **Voting Members:**

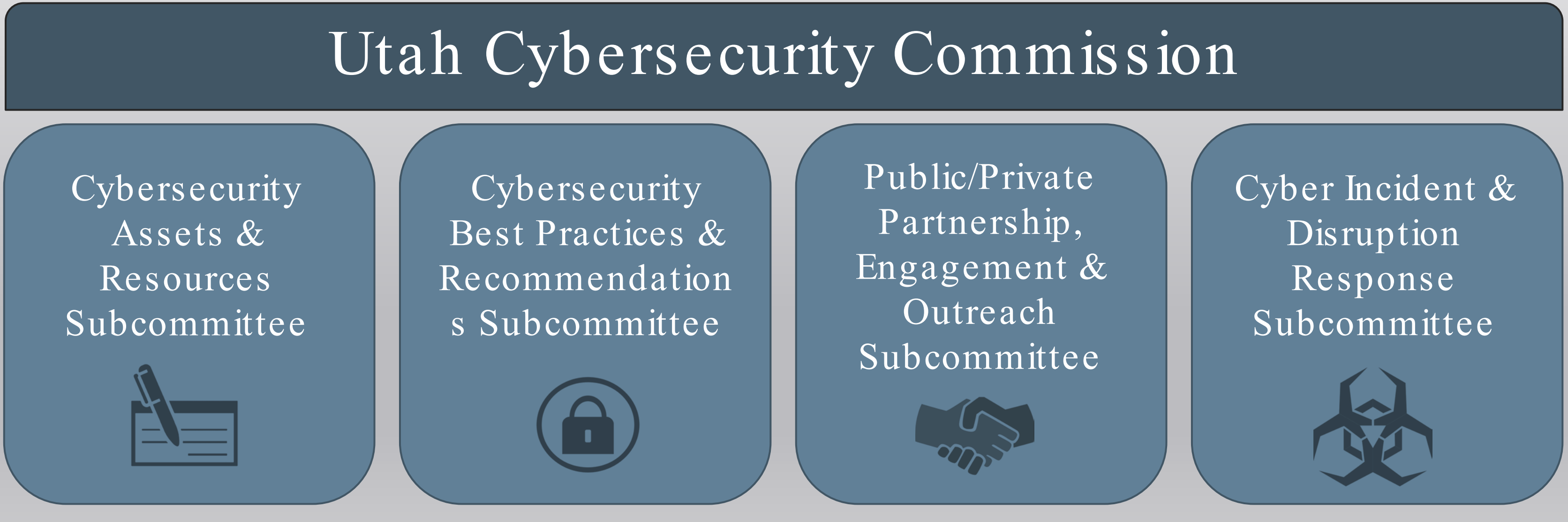
- ***Governor*** *- Chair*
- ***Utah Department of Public Safety*** *- Chair*
- Lieutenant Governor's office
- Attorney General's office
- Utah state CIO & CISO
- State Agencies:
  - Transportation, Tax Commission, Finance, Health, Indian Affairs, Environmental Quality, Natural Resources, Judicial Council, Utah Board of Higher Education, State Board of Education
- League of Cities and Towns, Association of Counties
- Utah National Guard
- Governor's Office of Economic Opportunity
- Utah Senator
- Utah House of Representatives

➔ **Advisory Members:**

- CISA
- FBI
- Critical Infrastructure Sectors:
  - Energy
    - Electricity
    - Natural Gas
  - Chemical
  - Healthcare
    - Utah Hospital Association
  - Commercial
    - Venues/Convention Center
  - Water/Wastewater
  - Communications

Cybersecurity Commission Subcommittees

- Commission comprised of subcommittees to focus on different aspects of cybersecurity



Utah Cybersecurity Commission

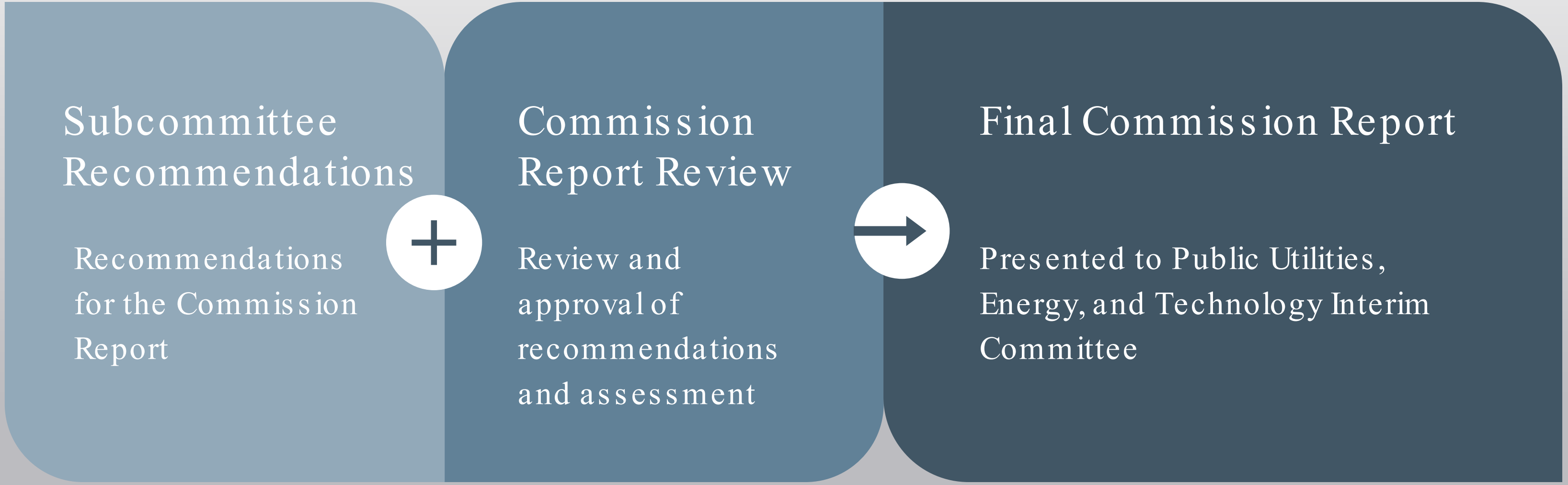
Cybersecurity Assets & Resources Subcommittee

Cybersecurity Best Practices & Recommendations Subcommittee

Public/Private Partnership, Engagement & Outreach Subcommittee

Cyber Incident & Disruption Response Subcommittee

Cybersecurity Commission Reporting



Subcommittee Recommendations

Recommendations for the Commission Report

+

Commission Report Review

Review and approval of recommendations and assessment

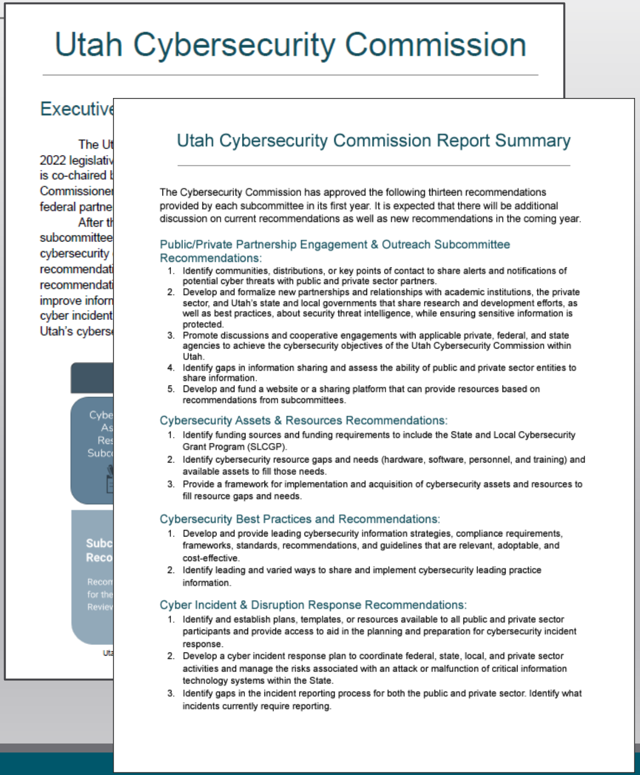
→

Final Commission Report

Presented to Public Utilities, Energy, and Technology Interim Committee

Commission Report Recommendations

- Develop and fund a website or a sharing platform that can provide resources based on recommendations from subcommittees.
- Identify funding sources and funding requirements to include the SLCGP
- Identify cybersecurity resource gaps and needs (hardware, software, personnel, and training) and available assets to fill those needs (hardware donation program)
- Develop and provide leading cybersecurity information strategies
- Identify gaps in the incident reporting process for both the public and private sector. Identify what incidents currently require reporting
    - SB 127



Utah Cybersecurity Commission

Executive

The Ut
2022 legislativ
is co-chaired b
Commissioner
federal partne
After th
subcommittee
cybersecurity
recommendati
recommendati
improve inforn
cyber incident
Utah's cyberse

Cybe
As
Res
Subc
Subc
Reco
Recom
for the
Review
Uta

Utah Cybersecurity Commission Report Summary

The Cybersecurity Commission has approved the following thirteen recommendations provided by each subcommittee in its first year. It is expected that there will be additional discussion on current recommendations as well as new recommendations in the coming year.

Public/Private Partnership Engagement & Outreach Subcommittee Recommendations:

1. Identify communities, distributions, or key points of contact to share alerts and notifications of potential cyber threats with public and private sector partners.
2. Develop and formalize new partnerships and relationships with academic institutions, the private sector, and Utah's state and local governments that share research and development efforts, as well as best practices, about security threat intelligence, while ensuring sensitive information is protected.
3. Promote discussions and cooperative engagements with applicable private, federal, and state agencies to achieve the cybersecurity objectives of the Utah Cybersecurity Commission within Utah.
4. Identify gaps in information sharing and assess the ability of public and private sector entities to share information.
5. Develop and fund a website or a sharing platform that can provide resources based on recommendations from subcommittees.

Cybersecurity Assets & Resources Recommendations:

1. Identify funding sources and funding requirements to include the State and Local Cybersecurity Grant Program (SLCGP).
2. Identify cybersecurity resource gaps and needs (hardware, software, personnel, and training) and available assets to fill those needs.
3. Provide a framework for implementation and acquisition of cybersecurity assets and resources to fill resource gaps and needs.

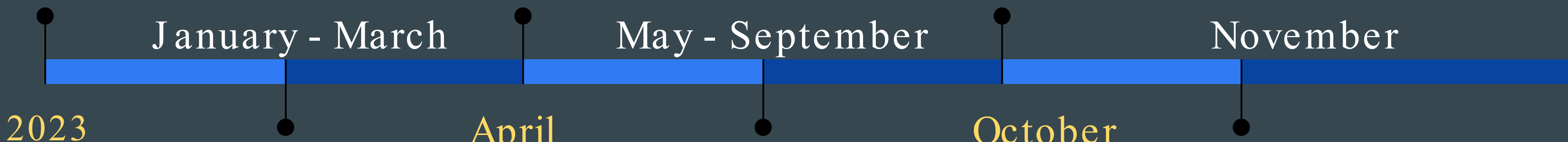
Cybersecurity Best Practices and Recommendations:

1. Develop and provide leading cybersecurity information strategies, compliance requirements, frameworks, standards, recommendations, and guidelines that are relevant, adoptable, and cost-effective.
2. Identify leading and varied ways to share and implement cybersecurity leading practice information.

Cyber Incident & Disruption Response Recommendations:

1. Identify and establish plans, templates, or resources available to all public and private sector participants and provide access to aid in the planning and preparation for cybersecurity incident response.
2. Develop a cyber incident response plan to coordinate federal, state, local, and private sector activities and manage the risks associated with an attack or malfunction of critical information technology systems within the State.
3. Identify gaps in the incident reporting process for both the public and private sector. Identify what incidents currently require reporting.

Proposed Cybersecurity Commission Timeline



2023

January - March

2023 Legislative session

- Track state cyber legislation
- Plan April commission meeting
- Confirm subcommittee chairs and membership, & fill vacancies
- Conduct research for subcommittee needs

April

Commission Meeting
(Utah Capitol)

- Legislative updates
- Research updates
- Gartner report
- Commission goals 2023

May - September

Subcommittee Meetings
(Virtual)

- Finalize legislative recommendations
- SIAC to compile all recommendations into report

October

Commission Meeting
(Utah Capitol)

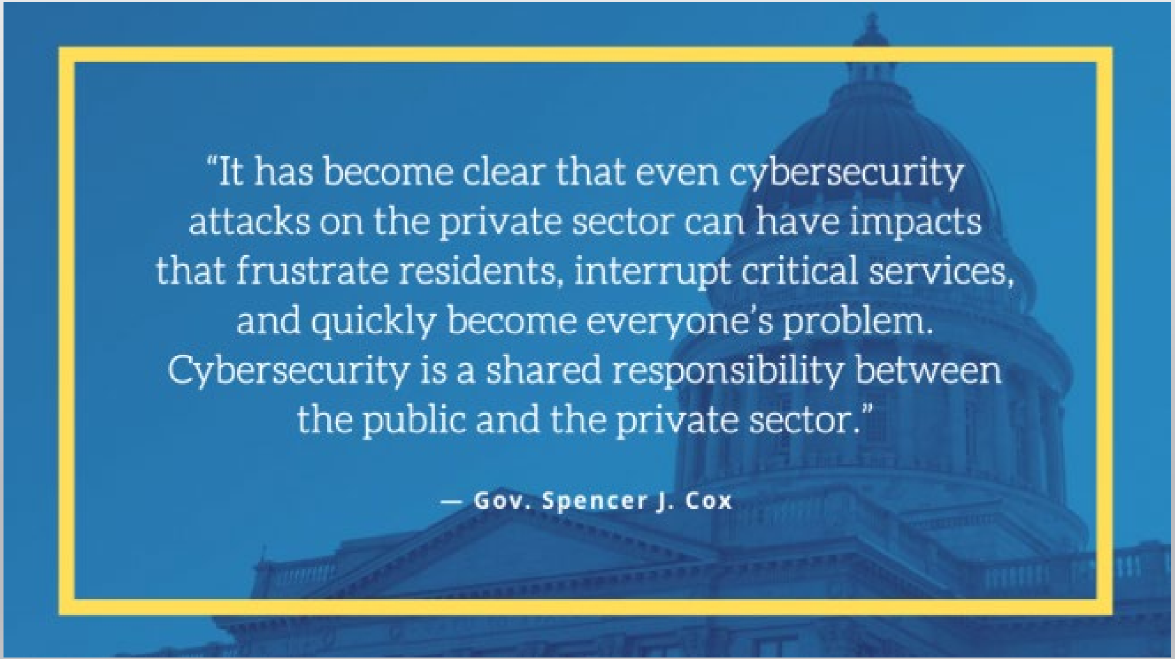
- Final commission report from each subcommittee
- Assessment of cyber threats to Utah
- SLCGP grant requirements or updates

November

Finalize Commission Report

- Present to legislative committee

Cybersecurity Commission



"It has become clear that even cybersecurity attacks on the private sector can have impacts that frustrate residents, interrupt critical services, and quickly become everyone's problem. Cybersecurity is a shared responsibility between the public and the private sector."

— Gov. Spencer J. Cox

(U) Questions

cyber@utah.gov

Audience Q&A

Thank You

For questions, additional resources, or to be put in contact with any of our speakers, please contact:

Casey Dolen

Senior Policy Analyst, Cybersecurity
National Governors Association

cdolen@nga.org

Please visit https://www.nga.org/statecyber/ for more updates from NGA's cybersecurity division