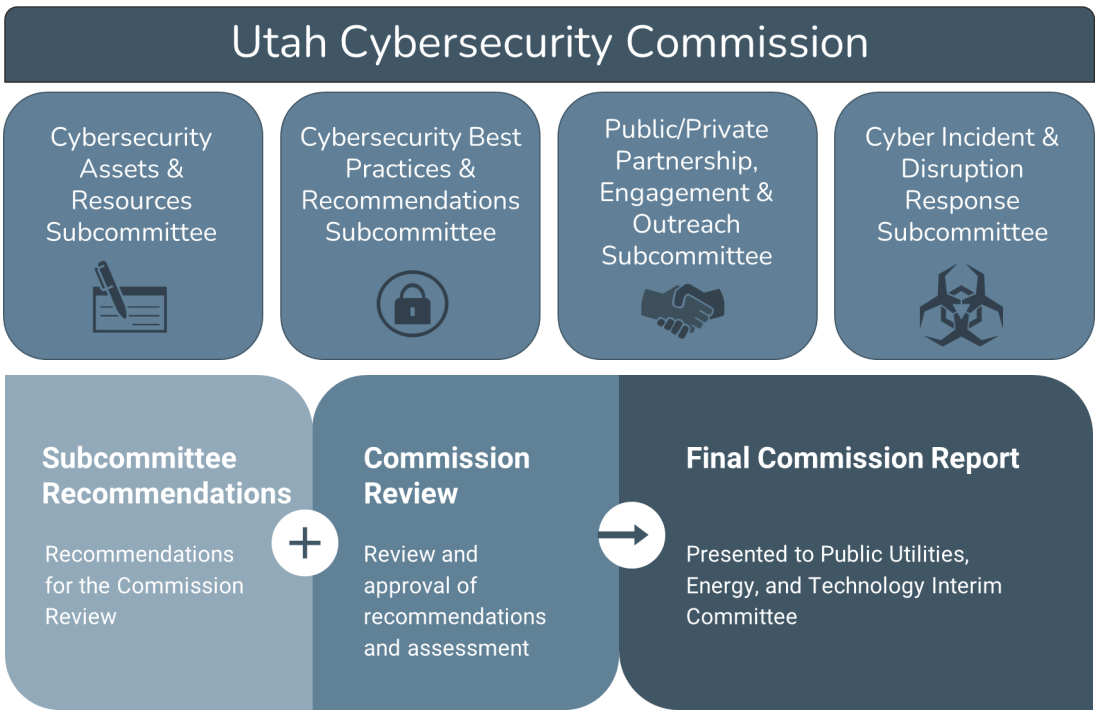
Utah Cybersecurity Commission

Executive Summary

The Utah Cybersecurity Commission was established through House Bill 280 during the 2022 legislative session and signed into law as 63C-27, Part 2. The Cybersecurity Commission is co-chaired by Governor Spencer J. Cox and Department of Public Safety (DPS) Commissioner Jess Anderson and consists of over 45 appointed and volunteer members, federal partners, and subject matter experts in critical infrastructure and cybersecurity.

After the formation of the Commission, the selected members were divided into four subcommittees to focus on how to fulfill different requirements specified in the bill to meet cybersecurity concerns in Utah. Each subcommittee held meetings to discuss ideas and recommendations for the Commission's annual report. Subcommittee findings include recommendations to follow existing best practices such as the NIST Cybersecurity Framework, improve information sharing, formalize and expand the Utah Cyber Center, update and develop cyber incident response plans, and develop ongoing funding sources to continuously improve Utah's cybersecurity.



Utah Cybersecurity Commission broken down by subcommittees and the process for final report recommendations

2022 First Year Accomplishments:

Beginning in August of 2022, the Cybersecurity Commission met for the first time after the members were appointed or selected based on expertise and experience in critical infrastructure and cybersecurity. The group divided into four subcommittees to focus on how to fulfill different requirements specified in the bill to meet cybersecurity concerns in Utah.

- Public/Private Partnership Engagement & Outreach
- Cybersecurity Assets and Resources
- Cybersecurity Best Practices and Recommendations
- Cyber Incident and Disruption Response

Each of the subcommittees elected a chair to facilitate and coordinate subcommittee meetings, and finalized each subcommittee's mission and goals. The Commission approved thirteen recommendations provided by each subcommittee. Subcommittee findings include recommendations to follow existing best practices such as the NIST Cybersecurity Framework, improve information sharing, formalize and expand the Utah Cyber Center, update and develop cyber incident response plans, and develop ongoing funding sources to continuously improve Utah's cybersecurity. It is expected that there will be additional discussion on current recommendations as well as new recommendations in the coming year.

Subcommittee Missions and Goals

Public/Private Partnership Engagement & Outreach

Mission: Establish recommendations to improve joint public and private mutual threat and mitigation information sharing and collaboration efforts with a proactive program of assessments, guidance, educational material, and MOUs.

Goal: Develop and foster key partnerships to improve information sharing, reduce information security risks, overcome sharing barriers, and to promote innovation and collaboration. Identify, facilitate, and make recommendations to develop successful cross-government and cross industry collaboration and coordination efforts to further cybersecurity within the State of Utah. Critical private sector entities including utilities should be included in cyber security planning, training, and exercising.

Cybersecurity Assets & Resources

Mission: Improve access and awareness to cybersecurity resources, funding, and grant opportunities throughout Utah.

Goal: Identify key needs and develop components for a holistic statewide strategic plan for advancing cybersecurity in the State of Utah. Identify, develop, or provide cybersecurity resources, funding sources, and grants. Ensure the state's technology and public safety communication infrastructures have resilient and secure cyber disaster recovery capabilities to support the continuity of critical services. Ensure continuous improvement and cybersecurity maturity.

Cybersecurity Best Practices & Recommendations

Mission: Develop and facilitate a whole-of-state cybersecurity initiative that will raise the security posture of all public and private critical infrastructure sectors throughout Utah organizations, through leadership, information sharing, resource development, and education.

Goal: Identify and share cybersecurity leading practices and recommendations available to all Utah government and critical infrastructure. Promote cybersecurity maturity and resilience throughout critical infrastructure in Utah.

Cyber Incident and Disruption Response

Mission: Provide incident response preparedness and resource awareness for critical infrastructure attacks and disasters, with a developed combination of a mutual aid structure of public and private partners and subject matter experts.

Goal: To build and extend a culture of awareness, preparedness, and resiliency throughout the state of Utah and to develop a mechanism for information and resource sharing; knowledge transfer, and skills development in both preparations for, response to, and recovery from major cybersecurity incidents. Mitigate risk to cyber attacks, and enhance preparedness and response. Utah should be able to effectively respond to cyber incidents involving public and private networks that affect the well-being of Utah residents, businesses, and the ability of the state to provide essential services.

State & Local Cybersecurity Grant Program (SLCGP):

In addition to providing recommendations for cybersecurity in Utah, the formation of the Cybersecurity Commission qualifies the State to receive federal funds to improve cybersecurity from the State and Local Cybersecurity Grant Program (SLCGP). Utah expects to receive $13 million over the next four years and will need to distribute those funds based on the grant program requirements. The Cybersecurity Commission will have a role in determining what cybersecurity projects Utah will provide under the SLCGP. The Division of Technology Services (DTS) manages the grant application, and the Cybersecurity Commission has approved four initial projects as starting points:

- Statewide Cybersecurity Plan/Assessments - determine gaps, needs, and incident response
- Training - Security Awareness, phishing, and professional courses
- Shared and managed services
- Local awards in key areas for specific cybersecurity projects

Assessment of Cyber Threats to Utah:

The Cybersecurity Commission also received an assessment of cyber threats to Utah, and some of the major concerns of that report include:

- Cryptocurrency crimes continue to increase, with scams involving cryptocurrency increasing from $991 thousand in 2020 to over $10 million in losses in 2021 in Utah alone.
- Phishing continues to be a major problem, especially for Utah businesses. Utah victims lost over $29 million in 2021 due to Business Email Compromise, where attackers target businesses with phishing emails to defraud them.
- Ransomware is still prevalent and still impacting Utah government and businesses.
- Cyber criminals, hacktivists, and nation state actors continue to target critical infrastructure in Utah, which includes the energy sector, defense industrial base, healthcare, food and agriculture sector and government facilities.
- Cyber threats, both the number of victims, reported losses, and damage and disruption to businesses will continue to increase.

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.
    a. Examples of existing groups:
        i. Utah Cyber Center managed by the Division of Technology Services
        ii. Utah Statewide Information & Analysis Center (SIAC)
        iii. Information Sharing & Analysis Centers (ISACs)
        iv. Cybersecurity & Infrastructure Security Agency (CISA)
        v. Federal Bureau of Investigation (FBI) and InfraGard
        vi. Local government and business associations ex: Utah League of Cities and Towns, Utah Association of Counties, City Chambers of Commerce
        vii. Private sector trade and industrial associations ex: Rural Water Association, Utah Mining Association, Utah Hospital Association, etc.
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.
    a. Examples include:
        i. Formalize partnerships with Utah Valley University and Utah State University, specifically the Emerging Tech Policy Lab and the Intelligence, Industry and Security Consortium
        ii. Establish an online presence for the Utah Cyber Center and leverage partnerships mentioned through the DTS and City/County Government Outreach program
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.
    a. Examples of discussions/engagements that will enhance cybersecurity:
        i. Cybersecurity Awareness Month, Cyber Shield, Cyber Flag 20-2, Army Cyber Institute, Cyber Yankee Exercise, Jack Voltaic, etc.
        ii. Tabletop exercises with lifeline critical infrastructure sectors
        iii. Public service announcements & collaboration with the Association of Public Information Officers
4. Identify gaps in information sharing and assess the ability of public and private sector entities to share information by:
    a. Developing and adopting the goal to share as widely as possible
    b. Ensuring attack/compromise data is not shared outside of individual entities
    c. Identifying ways to share information between entities within Utah
        i. Formalize Utah Cyber Center as the Utah Sharing hub (Utah Cyber Center Information Sharing Analysis Center) and designate personnel to focus on public and private sector outreach
        ii. Create regulation and reporting requirements or legal restrictions through memorandum of understanding (MOU), sharing agreements, and non-disclosure agreements (NDA)
5. Develop and fund a website or 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).
    a. Develop an ongoing funding source to fund cybersecurity improvements for State and Local government, the Utah Cyber Center infrastructure, and staffing
    b. Develop an application process for local agency subrecipients to prioritize and distribute funds associated with the SLCGP
        i. Follow best practices outlined by the Utah Cybersecurity Commission
        ii. Agree to hold harmless agreements/joint aid agreements
        iii. Put forth incident reporting agreements, agree to use incident reporting framework as instituted by the Commission
2. Identify cybersecurity resource gaps and needs (hardware, software, personnel, and training) and available assets to fill those needs.
    a. Identify and compile various funding or resource opportunities such as free cybersecurity services for cybersecurity improvements
        i. Grant funding opportunities
        ii. Information Sharing & Analysis Center (ISAC) services
        iii. Cybersecurity & Infrastructure Security Agency (CISA) services
        iv. Utah Cyber Center - City & County Cybersecurity Outreach (public sector)
        v. Utah Statewide Information & Analysis Center (private sector)
    b. Create a hardware donation program
        i. Manage equipment lists with agreements that release ownership of donated items
        ii. Allow private and government entities to participate
            1. Defense Logistics Agency Disposition Services (formerly DRMO-Defense Reutilization Marketing Office)
            2. Utah DTS
            3. Local entities, etc.
        iii. Provide training and equipment configuration
3. Provide a framework for implementation and acquisition of cybersecurity assets and resources to fill resource gaps and needs.
    a. Invest in the cybersecurity workforce
        i. Offer paid for and volunteer cybersecurity training
            1. Identify professionals looking for recertification service hours that could provide training
        ii. Develop an internship program with local universities to provide students with experience in cybersecurity, and provide them opportunities to serve with state and local entities
        iii. Conduct market research on the cybersecurity workforce, including salary differences, job openings, demand, etc.
    b. Work with CISA, Utah Division of Emergency Management, and others to identify critical infrastructure/natural resources and dependencies
    c. Approve and/or develop a Statewide Strategic Cybersecurity Plan
    d. Create a Statewide Governance Program

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.
    a. Participate in Cybersecurity and Infrastructure Security Agency (CISA) free services and develop cybersecurity resilience and maturity by participating in CISA voluntary no-cost cybersecurity resources
    b. Participate in the Multi-State Information Sharing & Analysis Center (MS-ISAC) Nationwide Cybersecurity Review (NSCR) for government entities, or other yearly assessment programs
    c. Adhere to the NIST Cybersecurity Framework, and recommend CIS Critical Security Controls and Cyber Hygiene guide as a starting point for maturity models
        i. Develop online messaging and implementation guides for each control for various levels of audiences
2. Identify leading and varied ways to share and implement cybersecurity leading practice information.
    a. Develop online messaging and implementation guides for each control for various levels of audiences
    b. Expand and mature the Utah Cyber Center through statute as the premier entity for developing and sharing best practices
    c. Encourage private industries to participate in their respective Information Sharing & Analysis Center (ISAC) listed in the National Council of ISACs
    d. Where feasible, consolidate government entities to one network
    e. Require all government entities to use .gov domain

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.
    a. Develop workflow for incident management
        i. Include recommendations on how to track and document the incident
        ii. Outline requirements vs. incident response suggestions or best practices
            1. Define procedure to keep this workflow up-to-date
    b. Identify, develop, and share recommended incident response plans including those that determine critical components, identify and address points of failure, and include a workforce continuity plan
    c. Develop memorandum of understanding (hold harmless agreements), joint aid agreements or other legal documents needed for engagement during an incident
    d. Stand up a State Incident Response Hotline/Platform as centralized intake and response to cyber incidents that would also allow for centralized reporting
    e. Identify possible incident responders and experts and hold multi-agency information forums to assess incident response capabilities
        i. Advertise contacts and resources available in an incident
        ii. Identify needed and recommended training for incident responders
            1. Explore credentialing responders and partnering with universities
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.
    a. Identify critical resources and scope of State incident response
        i. Include Federal Resources (Utah National Guard & FBI) and how they are activated and deployed and the level of support they provide
    b. Update State Cyber Annex and State Incident Response Plan (last updated August 2016)
        i. Hold regular multi-agency exercises ex: tabletop incident response plan, statewide cyber event similar to Great Utah Shakeout
    c. Establish a Cyber Threat Schema that identifies threat levels, workflows, and follow-up actions to assist with triage in response to cybersecurity incidents
3. Identify gaps in the incident reporting process for both the public and private sector. Identify what incidents currently require reporting.
    a. Consider legislation for reporting incidents to Utah Cyber Center or law enforcement which are non-punitive and non-regulatory
        i. Protection of information from disclosure such as GRAMA/FOIA
        ii. Ability to anonymize reporter information once reported
    b. Identify other federal/state requirements and protections in place for reporters, consider legislation for legal protection for aiding in incident response
    c. Legislation for the acquisition of funds for software, hardware,and personnel that can be used in incident response for critical infrastructure.

Acknowledgements:

The Cybersecurity Commission would like to thank the dedicated members of each of the subcommittees volunteering their time and expertise, as well as the Department of Public Safety (DPS) Statewide Information & Analysis Center (SIAC) staff for coordinating and facilitating the Cybersecurity Commission.

Governor Spencer J. Cox, Cybersecurity Commission Chair
DPS Commissioner Jess Anderson, Cybersecurity Commission Co-Chair

Public/Private Partnership Engagement & Outreach	***Cybersecurity Assets and Resources***	***Cybersecurity Best Practices and Recommendations***	***Cyber Incident and Disruption Response***
Chair: Nathan Lee	*Chair: Phil Bates*	*Chair: Julissa Garfias*	*Chair: Mayor Tamara Tran*
Austin Tsosie	*Alan Fuller*	*Ben Mehr*	*Brody Arishita*
Ty Howard	*Patrick Hawkins*	*Bobette Phillips*	*Curtis Mansfield*
Yvonne Hogle	*Stephen Hess*	*Bryan Farnsworth*	*Erick Wiedmeier*
Matthew Beaudry	*Wade Kloos*	*David Sonnenreich*	*Mark Mitchell*
Dennis Rice	*Rep. Jon Hawkins*	*Matt Ceniceros*	*Rebecca Brown*
Joe Masnica	*Albert Gonzalez*	*Sen. John Johnson*	*Troy Jessup*
Blake Larsen	*John Coker*	*Jason Hoyt*	*Zachary Posner*
Annette Newman		*Sean Stalzer*	*Brent Robertson*
Matt Miller			*Michael Pickett*
Tara Thue			*Derrek Spencer*

Thank you to the individuals who contributed to several or each of the subcommittees:

Richard Gardner, Travis Scott, Ken Wheeler, Brandon Amacher, Captain J. Tanner Jensen, Hanna Bennett, Katherine Chipman, Mallorie Nielsen, Erin Mortensen, Daniel Mealy, & Tyson Jarrett.