



Cybersecurity for Critical Infrastructure

2026 Annual Report and Strategic Plan

Prepared by: Cybersecurity Advisory Council

Date: January 21, 2026



Executive Summary

Calendar Year 2025 built upon the previous work of the council. The Council met in January, March, May, July, and November with a change for 2026 to meeting quarterly.

The Council supported the State and Local Cybersecurity Grant program with a letter of endorsement for the matching funds request in the SFY 2026 budget.

The Council has made a pivot to have future work focused on individual Critical Infrastructure Sectors as each sector has different needs and continuing with a “one size fits all” approach will likely help none.

There continues to be interest from groups around the work of the Council, this year a recap of outreach is included.

The Council’s mission is to advance the cybersecurity readiness of Critical Infrastructure operators in the state of Vermont. To be effective, the Council needs representation from the core Critical Infrastructure Sectors. Included is a request to expand the membership to add two (2) additional sectors critical to making improvements. That request is detailed in the Legislative Recommendations Section of this report.

The goal of the strategic plan is to meet organizations where they are at currently, the strategic plan identifies three tiers of effort, one to match each of the three levels. Tier 1 is a training and planning path, Tier 2 is a risk management path, and Tier 3 is an information sharing and collaboration network. The program is designed so organizations can naturally move up the Tiers to the next level.

Details of each activity and the current Strategic Plan are included in this annual report.



Enabling Legislation

Summary

No. 71 (H. 291). An act relating to the creation of the Cybersecurity Advisory Council

Subjects: Executive; information technology; Agency of Digital Services; cybersecurity; critical infrastructure

This act creates the Cybersecurity Advisory Council to advise on the State's cybersecurity infrastructure, best practices, communications protocols, standards, training, and safeguards.

Sec. 1 of this act establishes the Council and relevant definitions in 20 V.S.A. chapter 208. The Council is composed of 11 members and the Chief Information Officer serves as Chair. Among other responsibilities, the Council is required to develop a strategic plan for protecting the State's public sector and private sector information and systems from cybersecurity attacks, evaluate statewide cybersecurity readiness, and conduct an inventory and review of cybersecurity standards and protocols for critical sector infrastructures. The Council is authorized to enter into executive session for certain reasons that are in addition to the considerations listed in 1 V.S.A. § 313 and also has a public records act exemption regarding cybersecurity standards, protocols, and incident responses, if the disclosure would jeopardize public safety.

Sec. 2 of this act amends the definition of "critical infrastructure" in 11 V.S.A. § 1701.

Sec 3. of this act requires the Council to include in its annual report due on January 15, 2024 any recommendations on whether to amend the definition of "essential supply chain".

Sec. 4 of this act sunsets the Council on June 30, 2028.

Link to Act 71

<https://legislature.vermont.gov/Documents/2024/Docs/ACTS/ACT071/ACT071%20As%20Enacted.pdf>



Membership

Membership for the Cybersecurity Advisory Council is identified in Act 71, in addition to those members a number of ADS staff are involved in supporting roles. Please see the Legislative Recommendations Section for requested changes.

Cybersecurity Advisory Council Membership as of January 1, 2026

Member Name	Role	Member Organization
Denise Reilly-Hughes	CIO/Co-Chair	State of Vermont, Agency of Digital Services
John Toney	CISO	State of Vermont, Agency of Digital Services
Erica Ferland	Director of Information Technology	Burlington Electric Department
Joe Duncan	General Manager	Champlain Water District
Mark Brisson	IT Risk and Resilience Manager	UVM Health Network
Eric Hillmuth	IT Director	Vermont Gas
Eric Forand	Director VEM	State of Vermont, Department of Public Safety
Ryan McLiverty	Homeland Security Advisor Designee	State of Vermont, Department of Public Safety
Lt. Col. Jason Galipeau	Vermont Adjutant General Designee	State of Vermont, Vermont National Guard
James Layman	Assistant Attorney General	State of Vermont, Attorney General
Sue Caswell	IT Director	Vermont Information Technology Leaders
Shawn Nailor	Director/Co-Chair	State of Vermont, Agency of Digital Services



Calendar Year 2025 Activities

Cybersecurity Advisory Council

Meetings were held bi-monthly from January to November. The Council has engaged with our Federal Partners, CISA and the FBI. Through these connections public attendance has expanded, and many are participating in sector specific working groups. The following are highlights from 2025.

Outreach

Members from the Agency of Digital Services, representing the Council have presented to multiple groups this past year.

- May – a presentation to a regional meeting of National Guard and Reserve response coordinators.
- June - a presentation was provided on the work of the Council to the Governor's Emergency Preparedness Advisory Council.
- July – testify at the U.S. Senate on the renewal of the Cybersecurity Information Sharing Act (CISA).
- July – presentation to a delegation from the Department of State representing Brazil, Angola, the Philippines, and other countries on digital standards and the work of the Cybersecurity Advisory Council. This event was hosted by and coordinated with the Vermont Council on World Affairs.
- August – attended the Vermont Digital Summit, building connections between public and private sector organizations.
- September – Vermont Joint Information Technology Oversight Committee; a presentation on the work of the Council.
- October – a presentation to Vermont's electric utilities on the mission and work of the Council.

Budget Request Letter of Support

A related effort in Vermont is the use of Federal Funding through FEMA and CISA for the improvement of cybersecurity readiness for local government. The State and Local Cybersecurity Grant Program (SLCGP) has a matching fund component. The Council recognized the value of this funding and provided the appropriate legislative committees with a letter of support.



Critical Infrastructure Sector Specific Focus

The work in 2024, to assess the cybersecurity maturity of critical infrastructure operators, demonstrated that the operators are at different levels of maturity; this was a cornerstone of the Strategic Plan. This means no one solution, resource, or investment would benefit everyone; therefore, the Council has adopted a sector specific approach. The representatives have started working groups to assist with turning the strategies identified in the Strategic Plan into specific tactics to assist their sector.

Federal Executive Order

On March 18, 2025, Presidential Executive Order 14239 – Achieving Efficiency Through State and Local Preparedness, was issued. This order pushes many preparedness responsibilities to State and Local Government. The Council used this opportunity to collect information on the Federal resources used in the event the State needs to provide them.

IT Contracts for Municipal Use

One challenge for many small Critical Infrastructure operators is a lack of resources for contracts and where to turn in the event of a cyber incident. To help municipally owned Critical Infrastructure the State of Vermont is extending new Information Technology Retainer Contracts for use by local government. This will allow municipal government to take advantage of master agreements where the vendors have already agreed to Vermont's terms and conditions, know their expertise based on the State's categories, and engage with someone quicker.



Calendar Year 2026 Planned Activities

Cybersecurity Advisory Council

The Cybersecurity Advisory Council will change its meeting schedule for 2026; instead of meeting bi-monthly it will meet Quarterly (January, April, July, October). This will provide more time between meetings for the working groups to meet and focus on sector-specific activities.

Strategic Plan

Turning the Strategic Plan into action will require focus, effort and a sector specific approach. Sector specific implementation plans will focus on the 3 Rs, Resilience, Response, and Recovery. Each sector may have different applicable standards, if not the use of NIST, CIS and CISA will be applied as appropriate. Roadmaps will be developed that reflect local experience, the sector's risk profile, level of effort, and Vermont specific requirements to guide organizations improvements. Where applicable the State may develop specific services.



Legislative Recommendations

Council Membership

The Cybersecurity Advisory Council recommends that the Vermont State Legislature amend Act 71 of the 2023 session. The council would benefit from having membership expanded to include representatives from the telecommunications/internet service provider industries as well as a member from local government.

The telecommunications and internet service provider industries serve as the backbone for all digital services and are a critical foundational piece of the full critical infrastructure environment.

Many of the small, rural, critical infrastructure operators are owned by municipalities (water, wastewater, electric, emergency services, and transportation systems) and having representation will help to ensure efforts of the Council meet their needs.



Strategic Plan – established in 2025 Annual Report

Overview

The results of the Cybersecurity Advisory Council's survey showed that most Critical Infrastructure (CI) operators align to one of three levels of maturity. The three levels are 1) organizations that have yet to start any significant cybersecurity initiatives; 2) organizations that have started to address cybersecurity preparedness but may not have a dedicated program; and 3) organizations with an established cybersecurity program.

To meet organizations where they are at currently, the strategic plan identifies three tiers of effort, one to match each of the three levels. Tier 1 is a training and planning path, Tier 2 is a risk management path, and Tier 3 is an information sharing and collaboration network. The program is designed so organizations can naturally move up the Tiers to the next level.

The number of organizations that will benefit from this program is significant, to focus the effort we plan to make this program available in phases. Phase 1, planned to be start in calendar year 2025 and likely continue into calendar year 2026, will focus on those organizations that provide Critical Infrastructure and essential services to one of Vermont's hospitals.

Goals and Objectives

The goals of the program are the following, the ability to realize these goals will be dependent on available funding.

- 1) to increase awareness of cybersecurity risk to Critical Infrastructure operators and municipalities;
- 2) to improve Critical Infrastructure operators and municipalities cyber preparedness;
- 3) to build relationships and establish a Vermont Community of organizations working cooperatively for better cyber information sharing;
- 4) to develop a recommended Universal Incident Response Plan template and;
- 5) to establish a program that promotes continuous improvement.

Program objectives to support the goals are:

- 1) The initial objective is to successfully complete the pilot program and using the results of the pilot program to inform changes, refine services and better define future delivery metrics.

Program Strategies

The program has developed five core strategies to deliver the results outlined in the goals and objectives.



Strategy 1 – Outreach and Awareness

This strategy will focus on developing materials and a focused effort to engage the organizations in Phase 1. This will include direct communications, working with industry groups, and holding informational meetings.

Strategy 2 – Building Strong Partnerships

No one organization is prepared to deliver the three Tiers of this program without assistance. This strategy will focus on engaging and establishing relationships with organizations that have expertise in cybersecurity.

Partnerships will include local colleges and universities to provide the resources necessary to delivery both Tier 1 and Tier 2. This will provide students with real-world experience in helping establish cybersecurity programs at small to medium sized organizations.

Partnerships will also include recognized national cybersecurity leaders like the Cyber Readiness Institute (CRI). The CRI has developed, and makes available at no cost, cybersecurity fundamentals training and resources. This will ensure organizations will have access to cybersecurity resources being maintained in a timely manner.

Partnerships with Vermont based organizations to help in the delivery of the program. These organizations include the Vermont National Guard for planning and incident response preparedness. The Vermont League of Cities and Towns for coordination with municipal based organizations. Vermont industry specific organizations like the Vermont Rural Water Association and the Vermont Community Broadband Board.

Partnerships with Vermont based technology companies with a cybersecurity focus to provide secure communications, sharing and collaboration platforms. Along with preparing professionals to respond to cybersecurity incidents.

Strategy 3 – Multiple Tiers of Support

Tier 1 – Planning and Education is the primary entry point for the program. It will provide the basic resources for an organization to start a cybersecurity program. Utilizing the Cyber Readiness Institute materials, with coaching and support provided by local college students, organizations will develop playbooks, Incident Response Plans, and be provided training materials for staff so that they have a basic cybersecurity program.

Tier 2 – Risk Management is the middle tier of the program. Utilizing standardized tools like those available from CISA, organizations in this tier will receive risk assessments. In addition to the assessments prioritized improvement plans will be developed and student teams will stay engaged to ensure the mitigation efforts are successful. This will be the natural progression for organizations completing Tier 1.

Tier 3 – Information Sharing and Collaboration Network will be the most advanced offering of the program. This Tier will utilize secure



communications and analysis platforms to share routine cybersecurity threat discovery. This will provide a channel for mature organizations to work together with the intelligence community to develop a Vermont specific early warning system. Additionally this Tier will participate in cross-sector exercises. This is the progression from Tier 2.

Strategy 4 – Universal Incident Response Plan Template

The Universal Incident Response Plan is intended to help organizations on a number of fronts. It will provide a consistent manner to establish an Incident Response Plan, it will provide Vermont specific resources, it will address an organizations obligations in the event of a cybersecurity incident, and it will provide the steps on how to engage key organizations within Vermont. It will be based on the Cyber Readiness Institute model and reviewed annually to keep current.

Strategy 5 – Build a Community of Vermont Organizations sharing Cyber Information

Having a strong cybersecurity posture is not a one and done activity, it requires continuous monitoring, sharing, improving, and investment. A coalition of organizations that share information and support each other will magnify the benefits of the program. Routine meetings, communications, and relationship building will ensure these efforts continue.

Phased Implementation

There are many organizations that can benefit from this program but to assess its effectiveness and ensure the greatest impact the program will be implemented in phases. The first phase will be a pilot program and focus on the Critical Infrastructure and Essential Supply Chain organizations who support a Vermont hospital in one of the four regions of the state.

