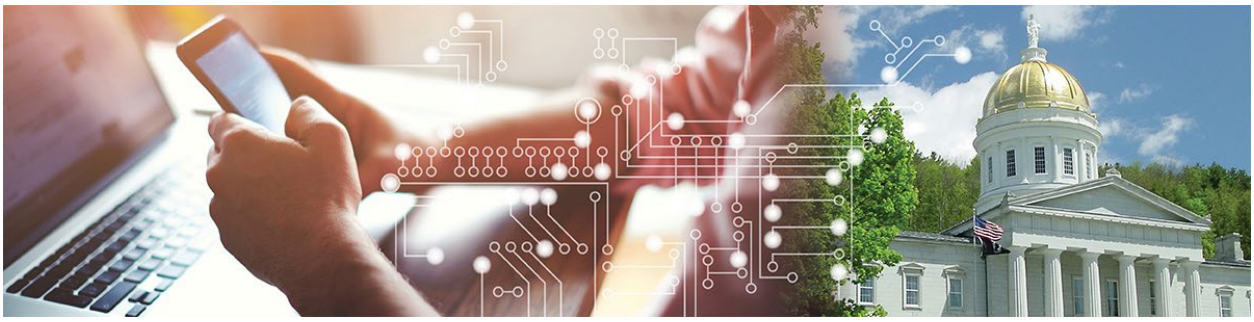

# Cybersecurity for Critical Infrastructure

## 2025 Annual Report and Strategic Plan

Prepared by: Cybersecurity Advisory Council

Date: January 15, 2025

VERMONT
CYBERSECURITY ADVISORY COUNCIL

# Executive Summary

Calendar Year 2024 was busy for the Cybersecurity Advisory Council. The Council first met in January and met every other month throughout the year. The council focused on the development of a survey to assess the maturity of Critical Infrastructure. The survey was then administered through June when the results were analyzed. Based on the results the Strategic Plan was developed.

Details of each activity and the full 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 suggested changes.

## Cybersecurity Advisory Council Membership as of January 1, 2025

| 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 |
| Nate Couture | Associate VP Information Security | UVM Health Network |
| Eric Hillmuth | IT Director | Vermont Gas |
| Eric Forand | Director VEM | State of Vermont, Department of Public Safety |
| Shawn Loan | Homeland Security Advisor Designee | State of Vermont, Department of Public Safety |
| Gregory C. Knight | Vermont Adjutant General | State of Vermont, Vermont National Guard |
| James Layman | Assistant Attorney General | State of Vermont, Attorney General |
| Sue Fritz | IT Director | Vermont Information Technology Leaders |
| Michelle Anderson | Legal Counsel | State of Vermont, Agency of Digital Services |
| Shawn Nailor | Director/Co-Chair | State of Vermont, Agency of Digital Services |

# Calendar Year 2024 Activities

## Cybersecurity Advisory Council

Meetings were held bi-monthly from January to November focused on delivering the items below. The first deliverable of the council was the 2024 Annual Report that included a review of the definition of Essential Supply Chain.

## Critical Infrastructure Survey

A survey was developed to assess the current maturity of Critical Infrastructure organizations. The survey is designed to not expose any organizations or vulnerabilities, this was done using generalized questions asking about maturity and not technical details. The survey was also administered in an anonymous format where the organizations had to identify as to which of the 16 Critical Infrastructure sectors, they are a part of. The survey design is also meant to be repeatable for the foreseeable future as the questions do not include time sensitive items like specific technology. We used multiple channels to broadcast the survey including the Vermont Intelligence Center, the Vermont League of Cities and Towns, the Vermont Community Broadband Board, and the Public Service Department. The survey consists of 39 questions and takes about 10 minutes to complete.

The survey was responded to by 119 organizations initially with 77 completing all 39 questions. The theme of the responses was that most organizations would fit into one of three categories. Category one is those who have not started a cyber program, category two are those who have started but may need assistance taking the next step, and category three are those organizations with an established cyber program. Distribution was relatively equal across the three categories.

## Strategic Plan

The Council also develop the first Cybersecurity for Critical Infrastructure and Essential Supply Chain Strategic Plan, please see the Strategic Plan Section of this document.

# Calendar Year 2025 Planned Activities

## Cybersecurity Advisory Council

The Cybersecurity Advisory Council will continue to meet on a bi-monthly basis. Its primary focus for 2025 will be the delivery of the work outlined in the Strategic Plan, developing the 2026 Annual Report, and updating the Strategic Plan based on lessons learned in the first year.

## Strategic Plan

Turning the Strategic Plan into action will require focus, effort and resources. The relationships need to be fully developed, inventories of Critical Infrastructure and Essential Supply Chain providers need to be completed, and the delivery of services needs to begin. First is to develop a detailed delivery plan for the services outlined in the Strategic Plan. Please refer to the Strategic Plan section for details.

# 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 and the internet provider industries.

These industries serve as the backbone for all digital services and are a critical foundational piece of the full critical infrastructure environment. This past year has shown that lacking representation it has been a challenge to communicate and engage with those communities.

Adding a representative from each industry will ensure their involvement and aid in the effective implementation of the strategic plan.

# Strategic Plan

## 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 organization's obligation in the event of a cybersecurity incident, and it will provide he 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.