

From: [Fykes, Jocelyn](#)
To: [Audet, Cally](#)
Cc: [Koren, Elizabeth](#); [Morrison, Jennifer](#); [DPS - Grant Notification](#); [Lewia, Kaisa](#); [Forand, Eric](#); [Elizabeth.Mitchell@mail.cisa.dhs.gov](#); [Kimberly.Chatman@mail.cisa.dhs.gov](#); [jim.fagan@mail.cisa.dhs.gov](#); [stephanie.kerr@mail.cisa.dhs.gov](#); [kerry.holmes@mail.cisa.dhs.gov](#); [christian.cosans@mail.cisa.dhs.gov](#); [cheri.ayoub@mail.cisa.dhs.gov](#); [patrice.perry@mail.cisa.dhs.gov](#); [FEMA-SLCGP](#); [Toney, John](#); [Kaiser, David](#); [Nailor, Shawn](#)
Subject: RE: VT Post monitoring summary letter: EMW-2022-CY-00088
Date: Thursday, September 26, 2024 4:10:26 PM
Attachments: [image002.png](#)
[image003.png](#)

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Good afternoon Cally,

Thank you for your detailed work on putting together the SLCGP Policy and Procedure Manual as well as the updates on the Committee and NCSR. Please accept this email as confirmation that the FY22 SLCGP monitoring corrective actions are now satisfied and closed.

Please let me know if you have any questions.

Many thanks,

Jocelyn

From: Audet, Cally <Cally.Audet@vermont.gov>
Sent: Wednesday, September 25, 2024 12:14 PM
To: Fykes, Jocelyn <jocelyn.fykes@fema.dhs.gov>
Cc: Koren, Elizabeth <Elizabeth.Koren@fema.dhs.gov>; Morrison, Jennifer <Jennifer.Morrison@vermont.gov>; DPS - Grant Notification <DPS.GrantNotification@vermont.gov>; Lewia, Kaisa <Kaisa.Lewia@vermont.gov>; Forand, Eric <Eric.Forand@vermont.gov>; Elizabeth.Mitchell@mail.cisa.dhs.gov; Kimberly.Chatman@mail.cisa.dhs.gov; jim.fagan@mail.cisa.dhs.gov; stephanie.kerr@mail.cisa.dhs.gov; kerry.holmes@mail.cisa.dhs.gov; christian.cosans@mail.cisa.dhs.gov; cheri.ayoub@mail.cisa.dhs.gov; patrice.perry@mail.cisa.dhs.gov; FEMA-SLCGP <fema-slcgp@fema.dhs.gov>; Toney, John <John.Toney@vermont.gov>; Kaiser, David <David.Kaiser@vermont.gov>; Nailor, Shawn <Shawn.Nailor@vermont.gov>
Subject: RE: VT Post monitoring summary letter: EMW-2022-CY-00088

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Please select the Phish Alert Report button on the top right of your screen to report this email if it is unsolicited or suspicious in nature.

Good afternoon Jocelyn,

Attached, please find the corrective action responses and documentation for the State of Vermont, as requested in the Post Monitoring Summary Letter received on September 3, 2024.

Please let me know if you have any questions or anything further is required from our team.

Thank you,

Cally

Cally Audet, MBA, MSC

Cally.Audet@vermont.gov

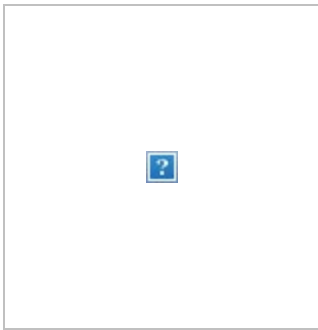
Homeland Security Program Manager
State of Vermont – Homeland Security Unit

45 State Drive

Waterbury, VT 05671

www.HSU.vermont.gov

Cell: (802) 585-5260



From: Fykes, Jocelyn <jocelyn.fykes@fema.dhs.gov>

Sent: Tuesday, September 3, 2024 4:27 PM

To: Audet, Cally <Cally.Audet@vermont.gov>

Cc: Koren, Elizabeth <Elizabeth.Koren@fema.dhs.gov>; Morrison, Jennifer <Jennifer.Morrison@vermont.gov>; DPS - Grant Notification <DPS.GrantNotification@vermont.gov>; Lewia, Kaisa <Kaisa.Lewia@vermont.gov>; Forand, Eric <Eric.Forand@vermont.gov>; Elizabeth.Mitchell@mail.cisa.dhs.gov; Kimberly.Chatman@mail.cisa.dhs.gov; jim.fagan@mail.cisa.dhs.gov; stephanie.kerr@mail.cisa.dhs.gov; kerry.holmes@mail.cisa.dhs.gov; christian.cosans@mail.cisa.dhs.gov; cheri.ayoub@mail.cisa.dhs.gov; patrice.perry@mail.cisa.dhs.gov; FEMA-SLCGP <fema-slcgp@fema.dhs.gov>

Subject: VT Post monitoring summary letter: EMW-2022-CY-00088

Some people who received this message don't often get email from jocelyn.fykes@fema.dhs.gov. [Learn why this is important](#)

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Good afternoon Cally,

Many thanks for your team's participation and cooperation with the FY2022 SLCGP monitoring site visit. Please find attached the post monitoring summary letter, as well as some examples of SLCGP policy and procedure manuals which are shared with permission from the states of KY and MS.

If you have any questions about the responses needed, please let me know!

Thank you,

Jocelyn Fykes, CGMS

Preparedness Officer | National Programs Division | Office of Grants Administration | Resilience

Mobile: (771) 208-9737

Jocelyn.Fykes@fema.dhs.gov

Federal Emergency Management Agency

fema.gov



This communication, along with any attachments, is covered by Federal and state law governing law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use, or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message.



State of Vermont
Department of Public Safety
45 State Drive
Waterbury, Vermont 05671-1300
<http://dps.vermont.gov/>

September 25, 2024

Ms. Jocelyn Fykes
SLCGP Preparedness Officer
U.S. Department of Homeland Security
Washington, DC 20472

Dear Ms. Fykes,

Please accept the following responses and attachments in response to the corrective action items outlined in the SLCGP Post Monitoring Summary Letter for the State of Vermont received on September 3, 2024.

Corrective Action Items:

- 1. The recipient shall submit evidence of compliance with 2023 NCSR for the Department of Public Safety or submit a corrective action plan to remedy compliance with required cyber memberships and Cyber Hygiene Services annually.**

As a department of the State of Vermont, the cybersecurity posture for the Department of Public Safety is included in the annual State of Vermont Nationwide Cybersecurity Review. The Agency of Digital Services, as the State's cybersecurity subject matter experts oversee cybersecurity relative to the state government as a whole and are tasked with submitting the NCSR on behalf of the State (and its Departments/Agencies) each year.

- 2. Submit current Cybersecurity Planning Committee member list.**

Please see the attached updated Cybersecurity Planning Committee member list.

- 3. The recipient shall update and submit to FEMA a copy of their current policies and procedures to include SLCGP grant closeout requirements, in compliance with 2 CFR 200.344 and the SLCGP NOFO.**

Please see the attached Vermont State and Local Cybersecurity Policy and Procedure Manual.





4. The recipient will send FEMA proposed dates and times for re-occurring monthly meetings.

Please see the following proposed dates and times for re-occurring monthly meetings:

- Any Monday of the month at 1:00 PM
- Last Wednesday of the month at 1:00 PM
- First or Last Friday of the month at 10:30 AM

We would like to thank you for the time and attention you have provided our team throughout this process. Please let us know if you have any questions.

Sincerely,

Vermont Department of Public Safety, Homeland Security Unit





VERMONT STATE AND LOCAL CYBERSECURITY GRANT PROGRAM POLICY & PROCEDURE MANUAL



Document created by the Vermont Homeland Security Unit on September 5, 2024.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

SECTION 1: STATE AND LOCAL CYBERSECURITY (SLCGP) OVERVIEW	3
<u>STATE AND LOCAL CYBERSECURITY (SLCGP) OVERVIEW</u>	4
<u>Program Objectives and Goals</u>	4
<u>Objective 1</u>	4
<u>Objective 2</u>	4
<u>Objective 3</u>	5
<u>Objective 4</u>	5
<u>Priorities</u>	5
<u>Eligibility Criteria</u>	6
<u>Cost Share or Match</u>	6
<u>Allowable Costs</u>	6
<u>Unallowable Costs</u>	8
<u>VERMONT STATE AND LOCAL CYBERSECURITY PLANNING COMMITTEE</u>	8
<u>STATE OF VERMONT CYBERSECURITY PLAN</u>	9
SECTION 2: GRANT MANAGEMENT	10
<u>PROJECT DEVELOPMENT & APPLICATION SUBMISSION</u>	11
<u>Step 1 – Gauging Local Interest</u>	11
<u>Step 2 – Contracted Services – Project Management</u>	11
<u>Step 3 – Local Consent</u>	11
<u>Step 4 – Project Development</u>	11
<u>Step 5 – Final Project Selection</u>	12
<u>Step 6 – Application Development</u>	12
<u>Step 7 – Obtain AOR Signature</u>	12
<u>Step 8 – Submit Application Materials</u>	12
<u>POST AWARD</u>	13
<u>Step 1 – Internal Award Setup</u>	13
<u>Step 2 – Notify Participating Eligible Local Units of Government</u>	13
<u>Step 3 – Complete Nationwide Cybersecurity Review</u>	13

<u>Step 4 – Procurement for Equipment/Service Offerings</u>	13
<u>Step 5 – Administer Services to Local Units of Government</u>	13
<u>Step 6 – Reporting</u>	14
<u>PROGRAMMATIC PROGRESS REPORTS</u>	14
<u>REQUEST FOR REIMBURSEMENTS</u>	14
<u>FEDERAL FINANCIAL REPORTING</u>	15
<u>SUBRECIPIENT MONITORING</u>	15
<u>CLOSEOUT</u>	15
<u>Internal Closeout</u>	15
<u>Federal Closeout</u>	16
<u>Record Retention</u>	16

APPENDIX A: 2022 VERMONT STATE AND LOCAL CYBERSECURITY GRANT
PLANNING COMMITTEE CHARTER

APPENDIX B: STATE OF VERMONT CYBERSECURITY PLAN

APPENDIX C: VERMONT HOMELAND SECURITY UNIT GUIDANCE ON
PROGRAMMATIC MONITORING GUIDELINES

SECTION 1: STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP) OVERVIEW

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP) OVERVIEW

The goal of the State and Local Cybersecurity Grant Program (SLCGP) is to help states and territories, specifically rural and local communities, address cybersecurity risks and cybersecurity threats. The SLCGP enables DHS to make targeted cybersecurity investments in state, local, tribal and territorial (SLTT) government agencies, thus improving the security of critical infrastructure and resilience of the services SLT governments provide to their community.

Program Objectives and Goals

The FY 2022 SLCGP aligns with the 2020-2024 DHS Strategic Plan by helping DHS achieve Goal 3: Secure Cyberspace and Critical Infrastructure, Objective 3.3. Assess and Counter Evolving Cybersecurity Risks. The FY 2022 SLCGP also supports the 2022-2026 FEMA Strategic Plan which outlines a bold vision and three ambitious goals, including Goal 3: Promote and Sustain a Ready FEMA and Prepared Nation, Objective 3.2: Posture FEMA to meet current and emergent threats.

The goal of SLCGP is to assist SLT governments with managing and reducing systemic cyber risk. For Fiscal Year (FY) 2022, applicants are required to address how the following program objectives will be met:

- **Objective 1:** Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
 - Establish cybersecurity governance structures and implement a program to evaluate maturity of the cybersecurity program aligned to Cybersecurity Performance Goals established by CISA and the National Institute of Standards and Technology (NIST).
 - Participants have established and documented a uniform cybersecurity governance structure that is accountable to organizational leadership and works together to set the vision for cyber risk management.
 - Participants have identified senior officials to enable whole-of-organization coordination on cybersecurity policies, processes, and procedures.
 - Develop, implement, or revise, and test cybersecurity plans, including cyber incident response plans, with clearly defined roles and responsibilities.
 - Asset (e.g., devices, data, software) protections and recovery actions are prioritized based on the asset's criticality and business value.

- **Objective 2:** Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
 - Physical devices and systems, as well software platforms and applications, are inventoried.
 - Cybersecurity risk to the organization's operations and assets are understood.
 - Vulnerability scans are performed, and a risk-based vulnerability management plan is developed and implemented.

- Capabilities are in place to monitor assets to identify cybersecurity events.
- Processes are in place to action insights derived from deployed capabilities.
- **Objective 3:** Implement security protections commensurate with risk.
 - SLT agencies adopt fundamental cybersecurity best practices.
 - Reduce gaps identified through assessment and planning process and apply increasingly sophisticated security protections commensurate with risk.
- **Objective 4:** Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
 - Train personnel to have the fundamental knowledge and skills necessary to recognize cybersecurity risks and understand their roles and responsibilities within established cybersecurity policies, procedures, and practices.
 - Organization has adopted the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.

In FY 2023, The Federal Emergency Management Agency (FEMA) and the Cybersecurity and Infrastructure Security Agency (CISA) created a series of overarching goals and objectives for the SLCGP based on input from SLTT stakeholders and associations, and consideration of national priorities, frameworks, and the national cyber threat environment:

- Implement cyber governance and planning;
- Assess and evaluate systems and capabilities;
- Mitigate prioritized issues; and
- Build a cybersecurity workforce.

Priorities

The Homeland Security Act of 2002, as amended by the Bipartisan Infrastructure Law requires grant recipients to develop a Cybersecurity Plan, establish a Cybersecurity Planning Committee to support development of the Plan, and identify projects to implement utilizing SLCGP funding. To support these efforts, recipients are highly encouraged to prioritize the following activities using FY 2022 SLCGP funds, all of which are statutorily required as a condition of receiving a grant:

- Establish a Cybersecurity Planning Committee;
- Develop a state-wide Cybersecurity Plan, unless the recipient already has a state-wide Cybersecurity Plan and uses the funds to implement or revise a state-wide Cybersecurity Plan;
- Conduct assessment and evaluations as the basis for individual projects throughout the life of the program; and
- Adopt key cybersecurity best practices.

Eligibility Criteria

Entities eligible to receive funds or services under this grant program are:

- **State; and**
- **Local units of government:** The term “local government” means —
 - a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government;
 - an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and
 - a rural community, unincorporated town or village, or other public entity.

Entities not eligible to receive funding or services under this grant program are:

- **Nonprofit organization; and**
- **Private corporations.**

Other eligibility criteria include:

- Each eligible entity is required to submit a Cybersecurity Plan that aligns with the criteria detailed in Appendix C of the FY 2022 SLCGP Notice of Funding Opportunity (NOFO).
- Each eligible entity is required to establish a Cybersecurity Planning Committee comprised of the members summarized in Appendix B of the FY 2022 SLCGP Notice of Funding Opportunity (NOFO).

Cost Share or Match

Eligible entities, if applying as a single applicant, must meet a 10% cost share requirement for the FY 2022 SLCGP. The recipient contribution can be cash (hard match) or third-party in-kind (soft match). Eligible applicants shall agree to make available non-federal funds to carry out an SLCGP award in an amount not less than 10% of activities under the award. For FY 2022, in accordance with 48 U.S.C. § 1469a, cost share requirements are waived for the insular areas of the U.S. territories of American Samoa, Guam, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands.

The State of Vermont successfully submitted and received approval for a cost share waiver on the FY 2022 SLCGP award.

Allowable Costs

The FY 2022 SLCGP may support funding of the following items:

- Planning activities, such as those associated the development, review, and revision of the holistic, entity-wide cybersecurity plan and other planning activities that support the program goals and objectives and Cybersecurity Planning Committee requirements.
- Organizational activities to include:
 - Program management;
 - Development of whole community partnerships that support the Cybersecurity Planning Committee;
 - Structures and mechanisms for information sharing between the public and private sector; and
 - Operational support.
 - Personnel hiring, overtime, and backfill expenses are permitted under this grant to perform allowable SLCGP planning, organization, training, exercise, and equipment activities. Personnel expenses may include, but are not limited to training and exercise coordinators, program managers and planners, and cybersecurity navigators. The grant recipient must demonstrate that the personnel will be sustainable.
- Equipment costs intended to be used to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state and local governments.
 - Unless otherwise stated, all equipment must meet all applicable statutory, regulatory, and DHS standards to be eligible for purchase using these funds. Please refer to FEMA’s Authorized Equipment List. In addition, recipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment. Investments in emergency communications systems and equipment must meet applicable SAFECOM Guidance recommendations. Such investments must be coordinated with the Statewide Inoperability Coordinator (SWIC) and the State Interoperability Governing Body (SIGB) to ensure interoperability and long-term compatibility.
 - SLCGP funds may be used to purchase maintenance contracts or agreements, warranty coverage, licenses, and user fees in support of a system or equipment. These contracts may exceed the period of performance if they are purchased incidental to the original purchase of the system or equipment as long as the original purchase of the system or equipment is consistent with that which is typically provided for, or available through, these types of agreements, warranties, or contracts. When purchasing a stand-alone warranty or extending an existing maintenance contract on an already-owned piece of equipment system, coverage purchased may not exceed the period of performance of the award used to purchase the maintenance agreement or warranty, and it may only cover equipment purchased with SLCGP funds or for equipment dedicated for SLCGP-related purposes. As with warranties and maintenance agreements, this extends to licenses and user fees as well.
 - The use of SLCGP grant funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable, unless otherwise noted.

Except for maintenance plans or extended warranties purchased incidental to the original purchase of the equipment, the period covered by maintenance or warranty plan must not exceed the POP of the specific grant funds used to purchase the plan or warranty.

- Training costs to include the establishment, support, conduct, and attendance of training and/or in conjunction with training by other federal agencies.
- Exercise costs consistent with Homeland Security Exercise and Evaluation Program (HSEEP).
- Management and administration (M&A) activities directly relating to the management and administration of SLCGP funds, such as financial management and monitoring.
 - A maximum of up to five percent of SLCGP funds awarded may be retained by the state, and any funds retained are to be used solely for M&A purposes associated with the SLCGP award.
- Indirect costs are allowable under this program as described in 2 C.F.R. Part 200, including 2 C.F.R. § 200.414.

Unallowable Costs

- Spyware;
- Construction and renovations involving modifications to existing buildings or structures that would require attaching equipment to walls, ceilings, floors, or doors including but not limited to:
 - Drilling new holes in walls, ceilings, or floors to install cable.
 - Installation of new conduit on to existing walls, ceilings, or floors.
 - Floor raising to install new cabling.
 - Installation of electrical outlets.
 - Any activities that involve ground disturbance.
- To pay a ransom;
- For recreational or social purposes;
- To pay for cybersecurity insurance premiums;
- For any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the eligible entity that receives the grant;
- To supplant state or local funds; however, this shall not be construed to prohibit the use of funds from a grant under this NOFO for otherwise permissible uses on the basis that the SLT has previously used SLT funds to support the same or similar uses; and
- For any recipient cost-sharing contribution.

VERMONT STATE AND LOCAL CYBERSECURITY PLANNING COMMITTEE

In response to the requirements outlined in the 2022 State and Local Cybersecurity Grant Notice of Funding Opportunity, the Vermont State and Local Cybersecurity Grant Working Group (SLCG WG)

will assist in developing and advising on key cybersecurity activities within the state. Through representation of the whole community the SLCG WG will assist in developing a cybersecurity plan, building cybersecurity capabilities, and reviewing and scoring applications under the grant program.

Responsibilities, organization and membership details of the Committee can be found in the SLCGP Cybersecurity Grant Planning Committee Charter attached in Appendix A of this document.

STATE OF VERMONT CYBERSECURITY PLAN

The approved Cybersecurity Plan for the State of Vermont as approved by FEMA/CISA can be found in Appendix B of this document.

SECTION 2: GRANT MANAGEMENT

PROJECT DEVELOPMENT & APPLICATION SUBMISSION

Step 1 - Gauging Local Interest

Members of the State of Vermont, Department of Public Safety and Agency of Digital Services continue to work together to gather information regarding interest from local units of government in receiving one or more of the three (3) cybersecurity offerings (multi-factor authentication, migration to .gov domain and/or cybersecurity training) set forth in the State of Vermont Cybersecurity Plan under the FY 2022 SLCGP award.

Through an initial survey sent to local representatives throughout the State, eleven communities have expressed interest in participating in the SLCGP program thus far. Through continued efforts of promoting the grant program both in written and verbal formats, we hope to gain additional interest in the coming months.

Step 2 - Contracted Services – Project Management

To assist staff with project planning and implementation, the State of Vermont has elected to hire a project management contractor to assist with community engagement activities to include coordinating, directing, administering, facilitating, monitoring, and reporting on all aspects of State and Local Cybersecurity Grant Program (SLCGP) projects.

A Request for Proposal was released in accordance with State of Vermont, Department of Buildings and General Services, Office of Purchasing and Contracting policies and procedures on behalf of the Agency of Digital Services on August 26, 2024. All Statement of Work Proposals are due no later than September 10, 2024, at 3:00 PM EST.

The selected resource(s) will be chosen in accordance with State of Vermont procurement policies and will be tasked with assisting in community outreach to gain additional interest from eligible entities.

Step 3 - Local Consent

Department staff and the contracted project manager(s) will work with eligible entities to obtain local consent signatures indicating acknowledgement that selected local entities will receive direct equipment/services in lieu of direct funding for one or more of the following three services offered by the State of Vermont:

- Multi-factor authentication;
- Migration to .gov domain; and/or
- Cybersecurity training.

Department staff and the project manager(s) will maintain copies of all signed documentation in the grant files and will provide a signed copy to all participating eligible entities.

Step 4 – Project Development

The project manager will work with staff to draft three (3) project proposals; one for each targeted objectives based on the number of interested local units of government. These proposals are to include projected costs, project narratives, investment strategies, impacts/outcomes and measurable milestones.

Step 5 – Final Project Selection

Final project proposals will be presented to the SLCGP Cybersecurity Planning Committee for final internal review and approval.

Step 6 – Application Development

The project manager will work with staff to draft the following FEMA application materials to be submitted for review and approval by FEMA and CISA:

- Initial Application:
 - SF-424: Standard Application for Federal Assistance Form
 - Grants.gov Lobbying Form, Certification Regarding Lobbying (if applicable)
 - SF-424A: Budget Information (Non-Construction)
 - SF-424B: Standard Assurances (Non-Construction)
 - SF-LLL, Disclosure of Lobbying Activities
 - Indirect Cost Agreement or Proposal (if applicable)
 - Cybersecurity Plan
 - Cybersecurity Planning Committee Membership List
 - Cybersecurity Planning Committee Charter
 - Cybersecurity Plan Submission Exception Request (if applicable)
 - Cost Share Waiver Request (if applicable)
 - SLCGP Investment Justification, for applicable grant year
 - SLCGP Project Worksheet

- Amendment - Project Development Stage:
 - SLCGP Investment Justification(s) – one for each objective
 - SLCGP Project Worksheet
 - Local Consent Forms

Step 7 – Obtain AOR Signature

The project manager will work with staff to obtain all necessary signatures prior to submitting.

Step 8 – Submit Application Materials

The Authorized Organization Representative will submit all applicable application materials to FEMA/CISA via the specified application portal (i.e. ND Grants, FEMA Go, etc.).

POST AWARD

Step 1 – Internal Award Setup

After receiving FEMA approval, the following internal steps are required to be completed prior to beginning the project:

- Homeland Security Unit to file award approval(s) and all correspondence in grant file.
- Financial Administrator finalizes internal working budget document
- Financial Administrator sets up funding task profile and PG code
- Financial Administrator drafts State of Vermont Financial Reimbursement Form (ADM-116a)
- Homeland Security Unit drafts internal Programmatic progress Report Template(s)

A file folder is created for each grant project. The grant project folder is labeled by the lead applicants name and the application project number. The file folder contains the following information:

- Federal Award Documentation
- Federal Application Materials
- Notice to Participate Confirmation email
- Local Consent Form, signed
- Monthly Programmatic Progress Reports
- Reimbursement Requests
- Correspondence
- Programmatic Monitoring
- Closeout Letter

Step 2 – Notify Participating Eligible Local Units of Government

Homeland Security Unit staff will email approval to participate notices to all local subrecipients selected during project planning to confirm they are still interested in being a recipient of one or more of the three offerings and reiterate intended scope of work as outlined in the signed local consent form.

Step 3 – Complete Nationwide Cybersecurity Review

Designated Agency of Digital Services staff will complete the Nationwide Cybersecurity Review on behalf of the State of Vermont annually.

Step 4 – Procurement for Equipment/Service Offerings

The project manager(s) and staff will work to begin necessary procurement procedures for equipment and/or service offerings in accordance with the State of Vermont and federal guidelines.

Step 5 – Administer Services to Local Units of Government

The project manager(s) will participate in the following activities to procure and facilitate equipment and/or services deliverables with participating local units of government and staff:

- Develop project implementation schedule with local participants
- Coordinate with equipment/service vendors to purchase authorized materials
- Participate in routine check-in meetings with Homeland Security and Agency of Digital Services staff to provide project updates
- Facilitate the delivery of equipment/services to local units of government

Step 6 – Reporting

The project manager(s) will complete the following reporting task(s):

- Provide monthly Programmatic progress Reports to Homeland Security Unit
- Track project expenditures, payments and request for reimbursements
- Submit monthly request for reimbursements
- Develop and submit necessary closeout documentation

PROGRAMATTIC PROGRESS REPORTS

The project manager will be responsible for submitting monthly programmatic progress reports to include updates on the following items for each of the three (3) project objectives:

- Reporting period;
- Project management step;
- Activity status in the report period (on schedule, ahead of schedule, behind schedule, no activity);
- Milestone progress;
- Project successes; and
- How the objective activities have helped achieved desired program outcomes.

Annually, no later than January 30th, the SAA is responsible for submitting updated Federal Programmatic Progress Reports to the federal awarding agency to include the following information:

- Brief narrative of overall project(s) status;
- Summary of project expenditures;
- Description of any potential issues that may affect project completion; and
- Data collected for DHS performance measures.

REQUEST FOR REIMBURSEMENTS

The project manager will be responsible for submitting monthly requests for reimbursement for expenses incurred. Reimbursement request submissions are to include the following items:

- Programmatic progress report;
- State of Vermont Financial Reimbursement Form (ADM-116a)
- Copies of invoices/purchase orders
- Copies of cancelled checks and/or proof of payment
- Homeland Security Property Records List (if applicable)

- Activity log detailing tasks completed during invoiced hours
- Proof of payment for hours worked (paystubs, etc.)
- Any other supporting documentation

The Financial Administrator is responsible for submitting monthly requests for reimbursement to federal awarding agencies through the Payment and Reporting System (PARS). Internal budget tracking documents must be updated on a monthly basis in coordination with the federal requests and payments received.

FEDERAL FINANCIAL REPORTING

The Financial Administrator is responsible for submitting quarterly Federal Financial Reports, with a final report due 120 days after the end of the period of performance.

Except for the final FFR due at 120 days after the end of the period of performance for purposes of closeout, the following reporting periods and due dates apply for the FFR:

Reporting Period	Report Due Date
October 1 – December 31	January 30
January 1 – March 31	April 30
April 1 – June 30	July 30
July 1 – September 30	October 30

SUBRECIPIENT MONITORING

Vermont Homeland Security Unit Guidance on Programmatic Monitoring Guidelines can be found in Appendix C of this document.

Programmatic monitoring for this program may be modified given that the State of Vermont has opted to pass through services to local units of government instead of awarding direct financial awards.

CLOSEOUT

Internal Closeout

The project manager will be responsible for submitting a final programmatic progress reports to include final updates on the following items for EACH of the three (3) project objectives no later than (90) calendar days after the end date of the period of performance:

- Reporting period;
- Project management step;
- Activity status in the report period (on schedule, ahead of schedule, behind schedule, no activity);
- Milestone progress;
- Project successes; and
- How the objective activities have helped achieved desired program outcomes.

The project manager will be responsible for submitting a final request for reimbursement for expenses incurred for EACH project. Final reimbursement request submissions are to include the following items no later than (90) calendar days after the end date of the period of performance:

- Final programmatic progress report;
- Final State of Vermont Financial Reimbursement Form (ADM-116a)
- Copies of invoices/purchase orders
- Copies of cancelled checks and/or proof of payment
- Homeland Security Property Records List (if applicable)
- Activity log detailing tasks completed during invoiced hours
- Proof of payment for hours worked (paystubs, etc.)
- Any other supporting documentation

Following completion of all necessary closeout actions, a formal closeout letter will be issued to signify the end of each project.

Federal Closeout

To complete federal closeout reporting, within 120 calendar days after the end of the period of performance for the prime award or after an amendment has been issued to close out an award before the original period of performance ends, recipients must liquidate all financial obligations and must submit the following:

1. The final request for payment, if applicable;
2. The final FFR (SF-425).);
3. The final progress report detailing all accomplishments, including a narrative summary of the impact of those accomplishments throughout the period of performance; and
4. Other documents required by this NOFO, terms and conditions of the award, or other DHS/FEMA guidance.

All closeout correspondence and documentation are to be filed in the respective grant files and retained for the duration of the designated record retention period.

Record Retention:

Financial records, supporting documents, statistical records, and all other non-federal entity records pertinent to a federal award generally must be maintained for at least three years from the date the final FFR is submitted. See 2 C.F.R. § 200.334. Further, if the recipient does not submit a final FFR and the award is administratively closed, FEMA uses the date of administrative closeout as the start of the general record retention period.

The record retention period **may be longer than three years or have a different start date** in certain cases. These include:

- Records for real property and equipment acquired with Federal funds must be retained for three years after final disposition of the property. See 2 C.F.R. § 200.334(c).
- If any litigation, claim, or audit is started before the expiration of the three-year period, the records must be retained until all litigation, claims, or audit findings involving the records have been resolved and final action taken. See 2 C.F.R. § 200.334(a).
- The record retention period will be extended if the non-federal entity is notified in writing of the extension by FEMA, the cognizant or oversight agency for audit, or the cognizant agency for indirect costs, or pass-through entity. See 2 C.F.R. § 200.334(b).
- Where FEMA requires recipients to report program income after the period of performance ends, the program income record retention period begins at the end of the recipient's fiscal year in which program income is earned. See 2 C.F.R. § 200.334(e).
- For indirect cost rate computations and proposals, cost allocation plans, or any similar accounting computations of the rate at which a particular group of costs is chargeable (such as computer usage chargeback rates or composite fringe benefit rates), the start of the record retention period depends on whether the indirect cost rate documents were submitted for negotiation. If the indirect cost rate documents were submitted for negotiation, the record retention period begins from the date those documents were submitted for negotiation. If indirect cost rate documents were not submitted for negotiation, the record retention period begins at the end of the recipient's fiscal year or other accounting period covered by that indirect cost rate. See 2 C.F.R. § 200.334(f).

All non-federal entities must maintain the following documentation for federally funded purchases:

- Specifications
- Solicitations
- Competitive quotes or proposals
- Basis for selection decisions
- Purchase orders
- Contracts
- Invoices
- Cancelled checks

Non-federal entities should keep detailed records of all transactions involving the grant. FEMA may at any time request copies of any relevant documentation and records, including purchasing documentation along with copies of cancelled checks for verification. See, e.g., 2 C.F.R. §§ 200.318(i), 200.334, 200.337.

In order for any cost to be allowable, it must be adequately documented per 2 C.F.R. § 200.403(g). Non-federal entities who fail to fully document all purchases may find their expenditures questioned and subsequently disallowed.

APPENDIX A:
**2022 VERMONT STATE AND LOCAL CYBERSECURITY
GRANT PLANNING COMMITTEE CHARTER**



State of Vermont
Department of Public Safety
45 State Drive
Waterbury, Vermont 05671-1300
<http://dps.vermont.gov/>

2022 State and Local Cybersecurity Grant Planning Committee Charter

Purpose: In response to the requirements outlined in the 2022 State and Local Cybersecurity Grant Notice of Funding Opportunity, the Vermont State and Local Cybersecurity Grant Working Group (SLCG WG) will assist in developing and advising on key cybersecurity activities within the state. Through representation of the whole community the SLCG WG will assist in developing a cybersecurity plan, building cybersecurity capabilities, and reviewing and scoring applications under the grant program.

Responsibilities:

The responsibilities of the SLCG WG are outlined below:

- Assisting and reviewing the development, implementation, and revision of the SLCG Cybersecurity Plan;
- Approving the SLCG Cybersecurity Plan;
- Assisting with the determination of effective funding priorities;
- Reviewing and scoring grant applications through the SLCG program for recommendation of funding to the Homeland Security Advisor and the Chief Information Security Officer;
- Coordinating with other committees and like entities with the goal of maximizing coordination and reducing duplication of effort;
- Creating a cohesive planning network that builds and implements cybersecurity preparedness initiatives using FEMA resources, as well as other federal, SLT, private sector, and faith-based community resources;
- Ensuring investments support closing capability gaps or sustaining capabilities; and
- Ensuring local government members, including representatives from counties, cities, and towns within the eligible entity provide consent on behalf of all local entities across the eligible entity for services, capabilities, or activities provided by the eligible entity through this program.

In addition to the above responsibilities, the SLCG WG, which is comprised of local units of governments and associations, may validate that funding held at the state level has a direct and tangible benefit to local jurisdictions in the state. Working group members may sign memoranda of understanding (MOUs) to validate the use of funds on behalf of local units of government which are not passed through to said units.

Organization:

Membership in the SLCG WG is maintained by the Department of Public Safety and abides by the requirements of the State and Local Cybersecurity Grant Program. Additional members may be identified and appointed by the Homeland Security Advisor (Commissioner of Public Safety) to reflect the evolving cybersecurity landscape. The Department of Public Safety, on behalf of the SLCG WG, should provide periodic updates to the Governor's Emergency Preparedness Advisory Council. Subcommittees and/or sub-working groups may be developed as needed.

VT Planning Committee Membership				
Representation	Name	Title	Organization	IT Experience (y/n)
Eligible Entity	Jennifer Morrison	Commissioner (HSA)	Department of Public Safety	No
CIO, CISO, Equivalent	Scott Carbee	CISO	Agency of Digital Services	Yes
Local Government	Cate Cross	Selectboard Member	Shelburne	Yes
Local Government	Jay Furr	Selectboard member	Richmond	Yes
Local Government Association	Ted Brady	Executive Director	VT League of Cities and Towns	No
Public Education	Emmanuel Ajanma	Technology Director	Barre Unified Union School District	Yes
Public Education	Mike Battig	Director, Cyber School	Norwich University	Yes
Public Health	Nate Couture	Network CISO	University of Vermont Health Network	Yes
Secretary of State's Office	Jon Welch	Technology Director	Secretary of State	Yes
Fusion Center	Ryan McLiverty	Cyber Intelligence Analyst	Vermont Intelligence Center	Yes
Attorney General	James Layman	Assistant Attorney General	Vermont Attorney General's Office	No

Governance:

The SLCG WG will be facilitated by the Department of Public Safety and the Agency of Digital Services. Administrative support will be provided by the Department of Public Safety.

Voting:

A formal vote will be utilized to make decisions. The voting procedures are as follows:

- Only official SLCG WG members can vote. Anyone else can be present but must abstain.
- A simple majority from the SLCG must be present to meet quorum.
- The vote will pass if it receives 50% plus one (majority).
- If a member has a real or potential conflict of interest, the member shall abstain from voting.

The SLCG WG may review applications that utilize a specific process as outlined in a Request for Proposal. The SLCG will follow any requirements in the specific Request for Proposal for scoring, reviewing, ranking, and approving projects as outlined in the Request for Proposal or the Department of Public Safety Granting Plan.

Meetings:

The SLCG WG will meet at least three times a year, or more or less frequently as determined by the Department of Public Safety. Administrative support is provided by the Department of Public Safety.

Limitations:

The SLCG WG is not permitted to make decisions relating to information systems owned or operated by, or on behalf of, the state.

Charter Adoption:

The SLCG WG will adopt the charter with the signatures of the original members as outlined below. Any new additional members will be required to adopt and sign the charter.

Name: James Layman **Agency:** Vermont Attorney General’s Office
Title: Assistant Attorney General **Email:** James.Layman@vermont.gov

DocuSigned by:
James Layman 11/7/2022

Name: Ryan McLiverty **Agency:** Vermont Intelligence Center
Title: Cyber Intelligence Analyst **Email:** Ryan.McLiverty@vermont.gov

DocuSigned by:
Ryan McLiverty 11/8/2022

Name: Jon Welch **Agency:** Vermont Secretary of State
Title: Technology Director **Email:** Jon.M.Welch@vermont.gov

DocuSigned by:
Jon Welch 11/7/2022

Name: Nathan Couture **Agency:** University of Vermont Health Network
Title: Network CISO **E-mail:** nathan.couture@uvmhealth.org

DocuSigned by:
Nathan Couture 11/7/2022

Name: Mike Battig **Agency:** Norwich University
Title: Director – Cyber School **Email:** mbattig@norwich.edu

DocuSigned by:
Mike Battig 11/7/2022

Name: Emmanuel Ajanma **Agency:** Barre Unified School District
Title: Technology Director **Email:** ejanbsu@buusd.org

DocuSigned by:
Emmanuel Ajanma 11/7/2022

Name: Ted Brady **Agency:** Vermont League of Cities and Towns
Title: Executive Director **Email:** tbrady@vlct.org

DocuSigned by:
Ted Brady 11/7/2022

Name: Jay Furr **Agency:** Town of Richmond
Title: Select Board Member **Email:** Jay.furr@richmondvt.org

DocuSigned by:
Jay Furr 11/7/2022

Name: Cate Cross **Agency:** Town of Shelburne
Title: Select Board Member **Email:** cateforvermont@gmail.com

DocuSigned by:
C. Cross 11/7/2022



Name: Scott Carbee

Title: CISO

Agency: Vermont Agency of Digital Services

Email: Scott.Carbee@vermont.gov

DocuSigned by:

Scott Carbee

11/8/2022

20CD5B84E3D241E...

Name: Jennifer Morrison

Title: Commissioner - HSA

Agency: Vermont Department of Public Safety

Email: Jennifer.Morrison@vermont.gov

DocuSigned by:

Jennifer Morrison

11/7/2022

6F59BEC42D84F2...

APPENDIX B:
STATE OF VERMONT CYBERSECURITY PLAN



STATE OF VERMONT CYBERSECURITY PLAN



January 2023

Approved by SLCGP Cybersecurity Planning Committee on September 22, 2023
Final Version

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

Letter from [cybersecurity planning committee]	1
Executive Summary	2
Background and context	2
introduction	3
Vision and Mission	6
Cybersecurity Program Goals and Objectives	6
Cybersecurity Plan Elements	6
Manage, Monitor, and Track	7
Monitor, Audit, and Track	7
Enhance Preparedness	7
Assessment and Mitigation.....	7
Best Practices and Methodologies	7
Safe Online Services.....	7
Continuity of Operations.....	8
Workforce	8
Continuity of Communications and Data Networks.....	8
Assess and Mitigate Cybersecurity Risks and Threats to Critical Infrastructure and Key Resources.....	8
Cyber Threat Indicator Information Sharing.....	8
Leverage CISA Services	9
Information Technology and Operational Technology Modernization Review	9
Cybersecurity Risk and Threat Strategies	9
Rural Communities	9
Funding & Services	9
Distribution to Local Governments	10
Assess Capabilities	10
Implementation Plan	10
Organization, Roles and Responsibilities	10
Resource Overview and Timeline Summary.....	11
Metrics	12
Appendix A: SAMPLE Cybersecurity Plan Capabilities Assessment	13
Appendix B: Project Summary Worksheet	16
Appendix C: Entity Metrics	16

Appendix D: Acronyms17

LETTER FROM CYBERSECURITY PLANNING COMMITTEE

Greetings,

The Cybersecurity Planning committee for the State of Vermont, Department of Public Safety (DPS) is pleased to present to you the State and Local Cybersecurity Grant Program FY2022 Cybersecurity Plan. The Cybersecurity Plan represents the State of Vermont’s continued commitment to improving cybersecurity and supporting our State, as well as cybersecurity practitioners across our local jurisdictions. In addition, this update meets the requirement of the current U.S. Department of Homeland Security guidelines for the State and Local Cybersecurity Grant Program (SLCGP).

Representatives from the Department of Public Safety and the Agency of Digital Services (ADS) collaborated with local municipalities, state agencies, and the private sector across multiple sectors including education, government, healthcare, and public safety to develop and update the Cybersecurity Plan with actionable and measurable goals and objectives that have champions identified to ensure completion. These goals and objectives focus on enhancing cybersecurity awareness, increasing cybersecurity protections, and enhancing the ability to respond to cybersecurity incidents. They are designed to support our state in planning for new technologies and navigating the ever-changing cybersecurity landscape. They also incorporate the SLCGP required plan elements.

As we continue to enhance cybersecurity, we must remain dedicated to improving our resilience within disciplines and across jurisdictional boundaries. With help from cybersecurity practitioners, we will work to achieve the goals set forth in the Cybersecurity Plan and become a model for cyber resilience.


Sincerely,

DocuSigned by:

49AF0B3D0CF84F4...

9/22/2023

David Kaiser, Acting Chief Information Security Officer
State of Vermont
Agency of Digital Services

DocuSigned by:

6F59BEC42D84F2...

9/22/2023

Jennifer Morrison, Homeland Security Advisor/Commissioner of Public Safety
State of Vermont
Department of Public Safety

EXECUTIVE SUMMARY



This Cybersecurity Strategy highlights the purpose and scope of the strategic plan, which aims to address the increasing cybersecurity challenges faced by the State of Vermont and local governments. The plan is guided by the vision, mission, and strategic guidance provided by the Cybersecurity Planning Committee. It focuses on managing and monitoring information systems, enhancing cybersecurity preparedness and resilience, adopting best practices, promoting safe online services, ensuring continuity of operations, and strengthening the cybersecurity workforce. The strategy emphasizes collaboration between various stakeholders, including public and private entities, neighboring states, and countries. Implementation and governance of the plan will be monitored by the Cybersecurity Planning Committee, ensuring continuous improvement and adaptation to the ever-evolving cybersecurity landscape. This strategy demonstrates a strong commitment to protect state and local governments' information systems, applications, and user accounts from cybersecurity risks and threats.

BACKGROUND AND CONTEXT

- A. The current cybersecurity landscape is characterized by rapidly evolving threats, increasingly sophisticated cybercriminals, and a growing reliance on digital technology. As a result, state and local governments face constant challenges in safeguarding their information systems and critical infrastructure.
- B. Key challenges and trends in cybersecurity include the rise of ransomware attacks, insider threats, supply chain vulnerabilities, and the increasing use of artificial intelligence in cyber-attacks. These challenges highlight the need for a robust and comprehensive cybersecurity strategy.
- C. A comprehensive cybersecurity strategy is crucial for protecting sensitive information, maintaining public trust, and ensuring the continuity of government services. It helps address the dynamic nature of cyber threats and establishes a proactive approach to risk management.

INTRODUCTION

The Cybersecurity Plan is a two-year strategic planning document that contains the following components:

Vision and Mission: To improve Vermont's cybersecurity and ensure a cyber secure and resilient Vermont that supports public safety, protects privacy, and fosters economic growth.

Organization, and Roles and Responsibilities:

State and Local Government in Vermont:

- Focus State government agencies on cyber prevention, protection, response and recovery.
- Establish a risk management framework to apply resources that are informed by an assessment of cybersecurity vulnerabilities and cybersecurity threats.
- Identify state and local cybersecurity gaps and develop mitigation strategies.
- Support continuing efforts relating to cybercrime interdiction and disruption as it affects Vermont by partnering with local, federal, and other state entities.
- Enhance the State's cyber threat intelligence network to support continued situational awareness and information-sharing for state, local, and private sector stakeholders in Vermont.
- Develop a cyber-awareness campaign to educate state and local government, the private sector businesses, and the citizens of Vermont.
- Build a cybersecurity education pipeline through increasing STEM programs in the K-12 educational system and providing support for K-12 cyber-focused extracurricular activities.
- Establish partnerships with Vermont's higher education community in creating certificate programs for cybersecurity education programs.
- Build marketing and economic development strategies to attract citizens into a cybersecurity workforce in support of Vermont government and industry.
- Develop a business plan for exporting these skills to other jurisdictions through telecommuting opportunities.

Critical Infrastructure Stakeholders in Vermont:

- Engage critical infrastructure owners and operators in cybersecurity strategies to enable continuity of operations and resource sharing.
- Foster continuous response and recovery improvement through state, local, and critical infrastructure exercises focusing on cyber incident consequence management capabilities.

Private Sector in Vermont:

- Initiate outreach programs to develop partnerships with Vermont businesses.
- Identify business cybersecurity needs and opportunities to share best practices.
- Coordinate prevention, response planning, information sharing and resiliency initiatives.
- Engage the private sector to develop solutions to risk management resource challenges.

- Develop strategies to increase cybersecurity business opportunities in Vermont.
- Engage private sector partners in continued cybersecurity emergency exercises and improvement planning.

Citizens of Vermont:

- Initiate outreach programs to educate Vermont citizens on cybersecurity protection principles and resiliency, cybersecurity awareness and best practices.

Funding:

- Growing complexity and reach of cyberattacks and events leave everyone vulnerable and as such the public and private sector must commit to fully growing and bolstering cyber defenses.
- The State of Vermont will utilize federal funding from the Department of Homeland Security State and Local Cybersecurity Grant Program and the Homeland Security Grant Program to support local and state jurisdictions in strengthening cyber defenses. In addition, other federal grant programs through the Department of Homeland Security passed through the Vermont Department of Public Safety will offer opportunities for nonprofit entities to enhance their cybersecurity postures.

Metrics:

- The State of Vermont will measure the implementation of this plan through several metrics outlined in **Appendix C**. These metrics will be tracked through collection of data by the Cybersecurity Planning Committee.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)¹, included in Figure 1, helps guide key decision points about risk management activities through various levels of an organization from senior executives to business and process level, as well as implementation and operations.

¹ <https://www.nist.gov/cyberframework/getting-started>

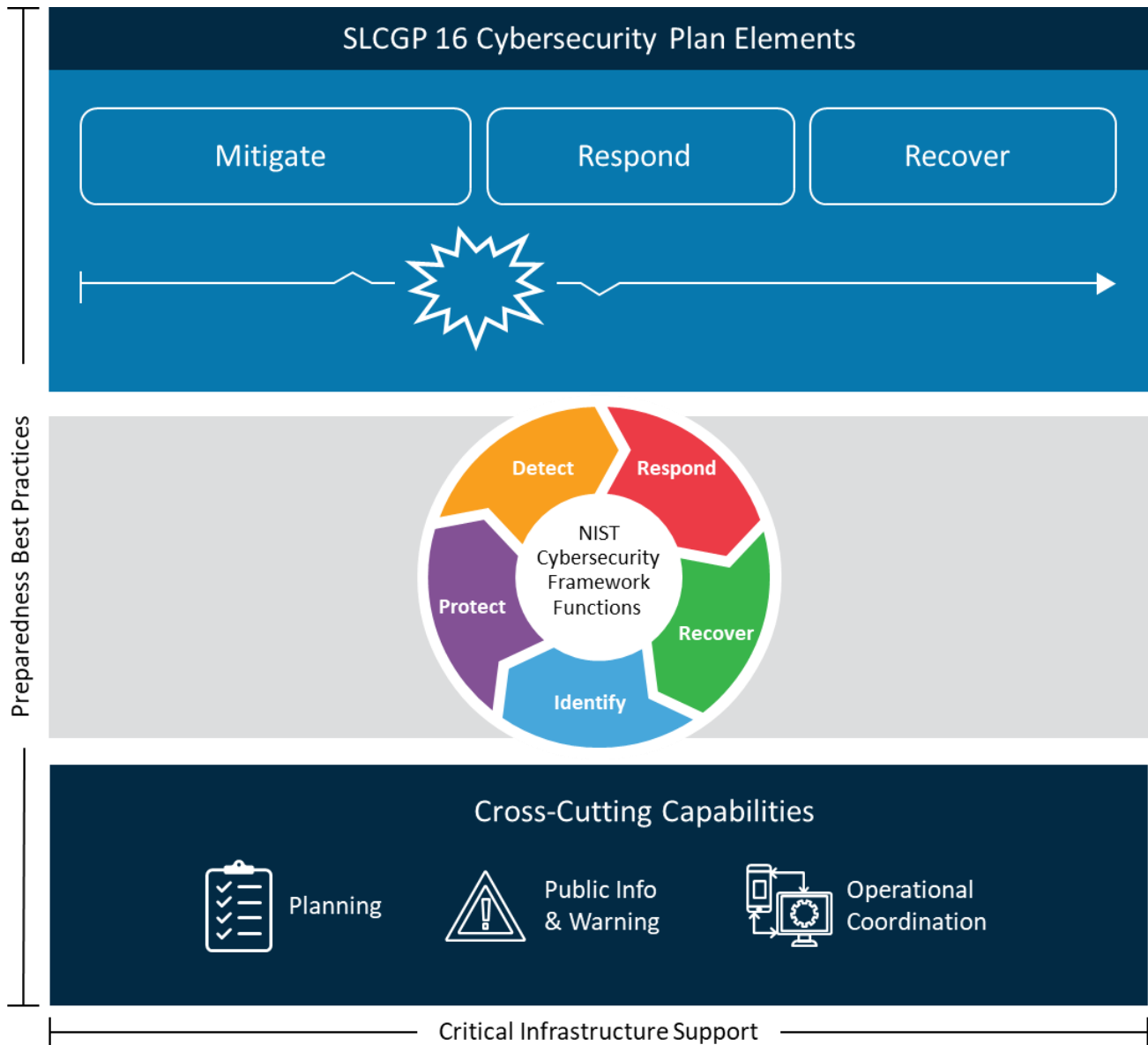


Figure 1: Achieving Cyber Resilience Through Comprehensive Cybersecurity Plans

Vision and Mission

This section describes the State of Vermont's vision and mission for improving cybersecurity:

Vision:

To improve Vermont's cybersecurity.

Mission:

Ensure a cyber secure and resilient Vermont that supports public safety, protects privacy, and fosters economic growth.

Cybersecurity Program Goals and Objectives

The State of Vermont cybersecurity goals and objectives include the following:

Cybersecurity Program	
Program Goal	Program Objectives
1. Improving Vermont's cybersecurity capabilities	1.1 Increasing cybersecurity knowledge statewide
	1.2 Enhancing cybersecurity workforce development
	1.3 Improving the technology to protect, defend against, and reduce the risk of cyber-attacks.
2. Increase Vermont's cyber resilience	2.1 Increase the ability to anticipate, withstand, respond to, and recover from cyber incidents.
3. Increase Vermont's cyber communication and information/intelligence sharing.	3.1 Expand the communication, coordination, and awareness between entities such as state and local government agencies, businesses, and citizens to improve an understanding of risk.
4. Increase Vermont's cyber education	4.1 Increase statewide partnerships with local, state, federal, nonprofit, and private sector organizations to enhance cyber education of Vermonters.

CYBERSECURITY PLAN ELEMENTS

This plan incorporates the following plans:

- State of Vermont, Cybersecurity Strategy, 2019.

Manage, Monitor, and Track

To effectively manage, monitor, and track information systems, applications, and user accounts, the strategy calls for the implementation of centralized monitoring tools and the establishment of clear access control policies. The specifics of monitoring tool design and implementation will be addressed in a follow-up plan; which will specifically include legacy systems.

Monitor, Audit, and Track

The strategy emphasizes the need to monitor, audit, and track network traffic and activity. This will be achieved through network security tools such as intrusion detection and prevention systems, firewalls, and security information and event management (SIEM) solutions.

Enhance Preparedness

Enhancing preparation, response, and resilience against cybersecurity risks and threats involves regular risk assessments, incident response planning, and continuous improvement of security controls. This will at a minimum consist of annual internal state exercises, with after action analysis and updates to Incident Response Planning and integration into state Emergency Response Planning.

Assessment and Mitigation

Continuous cybersecurity vulnerability assessments and threat mitigation practices will be implemented through periodic penetration testing, vulnerability scanning, and threat intelligence gathering.

Best Practices and Methodologies

Adopting and using cybersecurity best practices and methodologies will help strengthen the overall security posture of the state. The State of Vermont will continue to educate members of the whole community to work towards the adoption of best practices and methodologies which include:

- Implement multi-factor authentication.
- Implement enhanced logging.
- Data encryption for data at rest and in transit.
- End use of unsupported/end of life software and hardware that are accessible from the Internet.
- Prohibit use of known/fixed/default passwords and credentials.
- Ensure the ability to reconstitute systems (backups).
- Migration of local entities to the .gov internet domain.

Safe Online Services

Promoting the delivery of safe, recognizable, and trustworthy online services includes utilizing secure web protocols, implementing strong authentication measures, and ensuring secure data handling practices. Government organizations at the local and state level will be encouraged to adopt the .gov domain to ensure that regardless of the level of government, citizens will be ensured they are receiving safe, recognizable, and trustworthy services and information.

Continuity of Operations

Ensuring continuity of operations in the event of a cybersecurity incident requires comprehensive incident response plans, regular training, and exercises to validate and improve response capabilities. The State of Vermont will continue to develop, implement, and revise robust cybersecurity response plans at the State level and municipal level. These will be verified through regular training and exercises which will provide continuing opportunities for the State of Vermont to improve capabilities and plans.

Workforce

Using the NICE Workforce Framework for Cybersecurity will help identify workforce gaps, enhance recruitment and retention efforts, and improve the knowledge, skills, and abilities of cybersecurity personnel. The State of Vermont will continue to grow a pipeline of cybersecurity personnel while improving the cybersecurity knowledge of current personnel through training and information sharing.

Continuity of Communications and Data Networks

Ensuring continuity of communication and data networks in the event of an incident involves establishing redundant systems, backup communication channels, and robust disaster recovery plans. The State of Vermont will continue seeking to build future communications and data networks with redundancy and interoperability. Continuity operations will seek to integrate with already existing statewide response and interoperability plans which include the Vermont Statewide Communication Interoperability Plan.² Municipalities seeking to apply for communication funding through the Homeland Security Grant Program will be encouraged to coordinate with the Statewide Interoperability Coordinator to ensure that interoperability is being maintained.

Assess and Mitigate Cybersecurity Risks and Threats to Critical Infrastructure and Key Resources

Assessing and mitigating cybersecurity risks and threats related to critical infrastructure and key resources will involve close collaboration with relevant stakeholders, as well as the integration of security measures into the design and operation of these assets. In addition, the State of Vermont will seek to partner with CISA to utilize their services (through the Cybersecurity Advisor) to provide services to partners in the private sector.

Cyber Threat Indicator Information Sharing

Enhancing capabilities to share cyber threat indicators and related information entails creating secure communication channels, promoting a culture of information sharing, and fostering partnerships with relevant organizations.

The Vermont Intelligence Center (VIC) is the only fusion center in Vermont. As such they will assist in sharing cyber threat indicators and information sharing within the state and to federal partners. Information is also collected and shared through the MS-ISAC and other critical infrastructure sectors collect information through their respective information sharing and analysis centers.

² <https://rts.vermont.gov/sites/rts/files/documents/SCIP%202020%20Vermont%20FINAL.pdf>

Leverage CISA Services

Leveraging cybersecurity services offered by the Department includes utilizing CISA resources, required services, and membership to bolster the state's cybersecurity posture.

The State of Vermont will continue to utilize and partner with the services offered by CISA in coordination with the Cyber and Protective Security Advisor. Participation in cyber hygiene services including the Web Application Scanning and Vulnerability Scanning will be required in order to participate in the SLCGP program and marketed to municipalities and stakeholders throughout the state during meetings, conferences, and workshops.

The State of Vermont and entities receiving funding under the SLCGP program will complete the Nationwide Cybersecurity Review (NCSR) annually. In addition, entities seeking to enhance their cybersecurity programs will be required to complete the NCSR.

Information Technology and Operational Technology Modernization Review

Implementing an IT and OT modernization cybersecurity review process ensures that both information technology and operational technology systems align with cybersecurity objectives.

The State of Vermont's strategic approach to ensure alignment between information technology and operational technology cybersecurity objectives is that although much of the funding comes from different sources to protect the totality of these systems, a distinction is not made between controls applied to information technology and operational technology as the convergence of the (formerly) two technologies is almost complete. SLCGP participants may also replace end of life/outdated equipment found at this convergence, e.g., Windows XP and/or Windows 7 Machines if equipment purchases are approved by the SLCGP Planning Committee at some point in the future.

Cybersecurity Risk and Threat Strategies

Developing and coordinating strategies to address cybersecurity risks and threats requires ongoing collaboration with stakeholders, including local governments, associations, and neighboring entities. The Cybersecurity Planning Committee will continue to meet regularly to evaluate cybersecurity risks and threats to ensure that the strategies within this plan are addressing the evolving threat landscape.

Rural Communities

Ensuring adequate access to and participation in services and programs for rural areas involves providing resources, training, and support to these communities. As defined in 49 U.S. Code § 5302, rural areas are defined as "an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an ["urbanized area"](#) by the Secretary of the Agency of Commerce and Community Development." As such, this plan seeks to provide services to all Vermont communities and ensure that all Vermont communities receive access to the resources, training, and support necessary to improve Vermont's cybersecurity.

FUNDING & SERVICES

The State of Vermont SLCGP Planning Committee intends to focus on 4 key efforts to strengthen cybersecurity across the State.

These efforts include:

- Update and refine Cybersecurity Plan
- Provide Scholarships for Local IT Employees to achieve Security+ Certification
- Procure and Distribute Hardware Tokens for use by Local entities to implement Multifactor Authentication.
- Procure Professional Services for use by local entities to migrate to the .gov domain.

These efforts are detailed in **Appendix B: Project Summary Worksheet**

Distribution to Local Governments

The State of Vermont intends to use at least 80%, and most likely more, of the funding received through SLCGP to deliver services and capabilities to local government entities as described in Appendix B: Project Summary Worksheet. The State of Vermont does NOT intend to provide sub-grants or direct pass through of funds as part of this program. This approach, including ensuring that 25% of the Grant Funding is received as services to rural areas meets the requirement in the State and Local Cybersecurity Improvement Act: e.2.B.xvi. Individual local and rural recipients will enter an MOU acknowledging such per the Vermont SAA standard operating procedures.

ASSESS CAPABILITIES

The Vermont SLCGP Planning Committee used Appendix A: Cybersecurity Plan Capabilities Assessment to assess and document capabilities for the cybersecurity plan elements included in this plan.

IMPLEMENTATION PLAN

Organization, Roles and Responsibilities

At the State Level, there are three individuals with primary responsibility and accountability under the Law for providing and maintaining the information technology infrastructure, including all aspects of cybersecurity for their respective branch of Government. For the Executive Branch of State Government, this individual is the Secretary of the Agency of Digital Services (Referred to as the State CIO.) For the Legislative Branch of State Government, this individual is the Legislative Director of Information Technology. For the Judicial Branch of State Government, this individual is the Vermont Judiciary Chief Technology and Innovation Officer. The State Chief Information Security Officer (CISO) reports to the State CIO. Additionally, there are CIOs and ISOs in various other State organizations depending on their size and complexity.

These individuals routinely collaborate and coordinate through two entities, The Tri-Branch IT Working Group and the Cybersecurity Advisory Council. **Appendix B: Project Summary Worksheet** provides a list of cybersecurity projects to complete that tie to each goal and objective of the Cybersecurity Plan.

Resource Overview and Timeline Summary

The following information is provided to meet the requirement in the **State and Local Cybersecurity Improvement Act: e.2.E**. This information represents the best estimation based on current reference material. It is subject to revision over time.

The resources in the following table will be required to implement the plan over the next four years:

Voting members if the Planning Committee and CISA Liaison to the Planning Committee

Representation	Name	Title	Organization	IT Experience (y/n)
Eligible Entity	Jennifer Morrison	Commissioner (HSA)	Department of Public Safety	No
CIO, CISO, Equivalent	David Kaiser	CISO	Agency of Digital Services	Yes
Local Government	Cate Cross	Selectboard Member	Shelburne	Yes
Local Government	Jay Furr	Selectboard member	Richmond	Yes
Local Government Association	Ted Brady	Executive Director	VT League of Cities and Towns	No
Public Education	Emmanuel Ajanma	Technology Director	Barre Unified Union School District	Yes
Public Education	Mike Battig	Director, Cyber School	Norwich University	Yes
Public Health	Nate Couture	Network CISO	University of Vermont Health Network	Yes
Secretary of State's Office	Jon Welch	Technology Director	Secretary of State	Yes
Fusion Center	Ryan McLiverty	Cyber Intelligence Analyst	Vermont Intelligence Center	Yes
Attorney General	James Layman	Assistant Attorney General	Vermont Attorney General's Office	No
Federal Govt	Cheri Ayoub	Cybersecurity Advisor	CISA	Yes

METRICS

Vermont - Cybersecurity Plan Metrics			
Program Objectives	Program Sub-Objectives	Associated Metrics	Metric Description (details, source, frequency)
1. Improve State and Local Entities capability and capacity to adopt and use best practices and methodologies to enhance cybersecurity	1.1 Improve and Refine SLGCP Cybersecurity Plan	Future plan(s) approved by CISA.	Email from CISA confirming approval of plan.
	1.2 Implement Multi-factor Authentication	Number of hardware tokens procured and distributed to local entities.	Integer, Report from Office of the CISO, quarterly
	1.3 Migrate Local entities to .gov domain	Number of new hardware and applications sending logs to collector	Integer, Report from Local Entity, quarterly.
	1.4 Increase knowledge and skills of local IT/Security Professionals	Number of Local employees that achieve Security + Certification through scholarships.	Integer, Report from Service Provider, quarter

APPENDIX A: SAMPLE CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

COMPLETED BY STATE OF VERMONT				FOR ASSESSOR
Cybersecurity Plan Required Elements	Brief Description of Current Capabilities of SLTT within the Eligible Entity	Select capability level from: Foundational Fundamental Intermediary Advanced	Project # (s) <i>(If applicable – as provided in Appendix B)</i>	Met
1. Manage, monitor, and track information systems, applications, and user accounts	Incomplete implementation across the totality of the State and Local Government entities.	Foundational	1,2,3	
2. Monitor, audit, and track network traffic and activity	Incomplete implementation across the totality of the State and Local Government entities	Foundational	1,2,4	
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts	Incomplete implementation across the totality of the State and Local Government entities	Foundational	2,3,4,5	
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk	Incomplete implementation across the totality of the State and Local Government entities. Different Processes used by State entities and other Local Entities	Foundational	2,4	
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)				
a. Implement multi-factor authentication	Incomplete implementation across the totality of the State and Local Government entities.	Foundational	3	
b. Implement enhanced logging	Incomplete implementation across the totality of the State and Local Government entities.	Foundational	1	
c. Data encryption for data at rest and in transit	Based on standard configurations of Microsoft and Network Devices this is addressed	Intermediary	None under this program	

d. End use of unsupported/end of life software and hardware that are accessible from the Internet	Incomplete implementation across the totality of the State and Local Government entities.	Foundational	6	
e. Prohibit use of known/fixed/default passwords and credentials	Incomplete implementation across the totality of the State and Local Government entities	Foundational	1,5	
f. Ensure the ability to reconstitute systems (backups)	Incomplete implementation across the totality of the State and Local Government entities	Intermediary	None under this program	
g. Migration of local entities to the .gov internet domain	Incomplete across the eligible entity	Intermediary	5	
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain	Incomplete across the eligible entity	Intermediary	5	
7. Ensure continuity of operations including by conducting exercises	Different processes are used across the various State and Local Government entities. Some are managed services, and some are inherent in State process and Procedure	Intermediary	None under this program	
8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity)	Different processes are used across the various State and Local Government entities. Some are managed services, and some are inherent in State process and Procedure	Intermediary	None under this program	
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks	Pretty solid at the State Level and for Local First Responders, but less than Advanced for many other local entities.	Intermediary	None under this program	
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which	Incomplete implementation across the totality of the State and Local Government entities.	Foundational	1,2,3,4,	

may impact the performance of information systems within the jurisdiction of the eligible entity				
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department	Will stick with current process and arrangement. No intent to expand information sharing agreements currently.	Intermediary	None under this program	
12. Leverage cybersecurity services offered by the Department	NOFO requires organizations receiving funding from the grant take MS-ISAC NCSR (membership/services paid by CISA) and CISA Vuln Scanning and Web App Scanning.	Foundational	1,2,3,	
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives	Replacement of end of life/end of support equipment used at the convergence of IT/IO systems.	Foundational	4	
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	This plan contributes to this required element	Advanced	1	
15. Ensure rural communities have adequate access to, and participation in plan activities	Inherent in the program administration. Many areas of Vermont qualify for this	Advanced	1,2,3,4	
16. Distribute funds, items, services, capabilities, or activities to local governments	Vermont has a mature SAA that routinely manages FEMA/DHS Grant programs.	Advanced	1,2,3,4	

APPENDIX B: PROJECT SUMMARY WORKSHEET

Purpose: The **Project Summary Worksheet** is a list of cybersecurity projects that the entity plans to complete to develop or improve any needed cybersecurity capabilities identified in **Appendix A: Sample Cybersecurity Plan Capabilities Assessment**.

Rank	1. Project Name	2. Project Description	3. Related Required Element #	4. Cost	5. Status	6. Priority	7. Project Type
1	Vermont Statewide Cybersecurity Plan Refinement	Additional planning by Cybersecurity Planning Committee to refine Cybersecurity Plan Submission for FFY2023	1,2,3, 4, 5, 7,9, 10	\$200K	Ongoing	High	Plan
2	Hardware Tokens for MFA	Procure and Distribute Hardware Tokens for use by Local entities to implement Multifactor Authentication	1,3,5a,5e,10	\$1M	Future	Medium	Equip
3	Migration of local entities to .gov Domain	Procure Professional Services for use by local entities to migrate to the .gov domain.	3,5g,8,10	\$1M	Future	High	Organize
4	Security Training Course	CompTIA Security+ is an entry level security certification, that validates knowledge of basic security concepts, communication security, infrastructure security, cryptography, and operational security. Local Government IT Employees will receive a “scholarship” to attend this training and receive certification	3, 4, 8, 10	\$100K	Future	Medium	Train

APPENDIX C: ENTITY METRICS

The below table should reflect the goals and objectives the Cybersecurity Planning Committee establishes.

Cybersecurity Plan Metrics			
Program Goal	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
1. The State of Vermont has an approved Cybersecurity Plan that meets the SLCGP requirements as defined in the NOFO	1.1 Draft the Plan	Draft Plan exists in Document Library	CISO confirms Draft Plan is in Document Library
	1.2 Committee Approves Plan	Signed Letter by CIO	Committee Meeting Minutes
	1.3 Submit the Plan to CISA	Confirmation of Receipt	Email from CISA
	1.4 CISA Approves Plan	Statement of Approval	Email from CISA
2. Receive Funding from SLCGP	2.1 Funding received to Execute approved projects	Receipt of funds	Accept and Expend approval from Governor and Council
3. Execute Procurement Process for Each Approved Project	3.1 Execute approved projects	Projects are invoiced and paid	Financial Reporting via SAA
	3.2 Closeout approved projects	Projects are terminated or renewed	Financial Reporting via SAA
4. Process services for Local Entities and Rural areas that request inclusion	4.1 Enroll Local Entities in Services	Number of entities enrolled in each approved project	Financial Reporting via SAA
5. Review, Revise and Update Plan for next FY as required.	5.1 Repeat Objectives for Goal 1 for subsequent FY	See Goal 1	See Goal 1

APPENDIX D: ACRONYMS

Acronym	Definition
VIC	Vermont Intelligence Center

APPENDIX C: VERMONT HOMELAND SECURITY UNIT GUIDANCE ON PROGRAMMATIC MONITORING GUIDELINES



Guidance on Programmatic Monitoring Guidelines

Definitions:

§200.328 Monitoring and reporting program performance.

(a) Monitoring by the non-Federal entity. The non-Federal entity is responsible for oversight of the operations of the Federal award supported activities. The non-Federal entity must monitor its activities under Federal awards to assure compliance with applicable Federal requirements and performance expectations are being achieved. Monitoring by the non-Federal entity must cover each program, function or activity. See also §200.331 Requirements for pass-through entities.

General Rule/Decision:

Introduction & Purpose

The State of Vermont, Department of Public Safety (DPS), Homeland Security Unit (HSU), as the federal grantee, is responsible for monitoring grant sub-recipients and ascertaining that all compliance and programmatic responsibilities are fulfilled.

State and local sub-grants are monitored in order to (1) track the progress and alignment of agencies towards the State Preparedness Report (SPR) and Core Capabilities, (2) track the support HSU is providing to local and State agencies for implementation of the SPR and Core Capabilities, and (3) determine whether funds designated for planning, equipment, training and exercises are being obligated and expended in accordance with DPS/HSU and FEMA Grants and Programs Directorate guidelines.

Monitoring provides a comprehensive picture of how Core Capabilities are progressing statewide. Monitoring assists HSU in identifying areas of need for subrecipient support, provides feedback on ways to improve its services to subrecipients, and illuminates the strengths and areas for improvement in subgrantees programs. Both forms of monitoring require written documentation.

Programmatic monitoring, executed either through an office based (“desk”) assessment or an on-site visit, focus on two areas:

1. Statutory and regulatory compliance with procurement, planning, inventory control, training and exercise actions, and
2. Goal and Objectives achievement focused on subrecipient stated operational targets, including equipment deployment.

The programmatic monitoring program places a high value on consistent, fair, transparent, and reasonable reporting and accountability by subrecipients.



Grant programs subject to HSU programmatic monitoring efforts include but are not limited to State Homeland Security Program (SHSP), Operation Stonegarden Program (OSGP), and Nonprofit Security Grant Program (NSGP) federal awards that are currently open.

The metrics, requirements, and guidelines used to conduct programmatic monitoring are found in, though not limited to, the following core documents:

- 2CFR (Grants and Agreements)
- OMB Circular A-102 (Administrative Requirements)
- OMB Circular A-133 (Audit Requirements)
- The relevant FY Funding Opportunity Announcement/Program Guidance
- Certifications and Assurances
- Subrecipient Grant Award Agreement
- VT NIMS Implementation Plan

On-Site Monitoring

The HSU On-Site Monitoring process is aligned with and designed to ensure compliance with 2CFR, among other guidance documents. The HSU personnel utilize an interview template designed to comprehensively address the spectrum of content.

The Monitoring Form is the driving engine of a monitoring visit, and subrecipients ought to be familiar with all aspects of the document in order to properly prepare. Specifically, the visit matrix is categorized into 7 sections:

- A- Overall/General Assessment
- B- Recordkeeping
- C- Equipment, with accountability and inventory control as per 2CFR, being focus areas
- D- Plans and Training
- E- NIMS Requirements
- F- Vehicle Purchases Only
- G- Operation Stonegarden Only

At least 6 subrecipients will be selected for a programmatic monitoring review each year. The determination for which entities are monitored is based upon several possible criteria:

- New subgrantee (to be monitored within the first performance year)
- Periodic routine review of subrecipient projects
- Review of specific items of interest
- Response to perceived problems or issues (i.e. not meeting goals or on the high-risk list)
- Response to financial audit or programmatic monitoring exceptions
- Response to requests for assistance from subrecipients

Visits will be communicated to subrecipients via multi-media dissemination of a long-term monitoring visit calendar, which will be developed annually.



A pre-monitoring analysis of the subrecipient will be conducted. This is done by monitoring personnel to determine which items should be reviewed during the site visit. The signed grant agreement(s), including Attachment B of the grant agreement, vendor invoices and correspondence, Financial Report Forms, Subgrant Progress Reports, audit findings, amendment requests, rate of expenditures, reimbursement requests, and any additional compliance requirements should all be reviewed during the pre-monitoring analysis. The HSU personnel should also request a copy of the subgrantees mandated asset inventory, based on grant awards and reimbursement requests. At this time, the HSU personnel should note any file irregularities or problems that are discovered.

A pre-visit phone call or email, to schedule a date and time for the monitoring visit, should be made two to three weeks in advance. The initial contact should outline for the subrecipient the items that will be reviewed during the site visit and any preparation the subrecipient should make prior to the visit. The phone call should be followed up by a pre-visit confirmation letter (Attachment A), preferably the same day, detailing the agreed to date and time, and items to be reviewed. It should include an agenda for the visit, a copy of the Monitoring Report Form (interview matrix) (Attachment B), and a sample Property Records List.

The visit involves discussions about project implementation such as milestones, timeline, rate of fund expenditure, project operations, performance measures, and evaluation. The visit includes interviews with key agency members, a review of documentation and equipment, and an exit interview to discuss findings and address questions or concerns. The exit interview will clarify future corrective action items for the subrecipient and highlight what will be included in the post-visit letter to the subrecipient. If any outstanding issues are identified, the subrecipient is required to submit a Corrective Action Plan within the allotted time identified in the post-visit letter, typically 45 days, identifying what steps the subrecipient is taking to resolve the issues.

The process for the site visit is as follows:

- HSU Authorized Personnel arrives on time, presents identification
- Introductions with key agency members
- Conducts interview(s)
 - Establishes proper contact person, working space, subrecipient working hours, parking, security
 - Authorized personnel details the monitoring process
- Reviews the Monitoring Report Form with sub-recipient
- Authorized Personnel takes notes throughout the visit on the Monitoring Report Form
- Authorized Personnel reviews equipment takes pictures of valuable, serialized equipment and records on photo log (Attachment C).
- Conducts exit interview used to:
 - Address Findings
 - Detail follow-up requirements with deadline for compliance – Corrective Actions
 - Q&A Session with Subrecipient (Outreach). Items to cover include:



- Proper filing of Financial Report Forms
- Progress reporting
- NIMS
- VCOMM
- New policies and procedures
- Vehicle policy
- Other funding sources
- Training
- Exercise
- FAQ's
- MOU templates
- Amendment requests
- Grant application

Upon completion of the visit, the HSU personnel should review the file and follow up with a post-visit results/corrective action letter (Attachment D). Findings and Corrective Action requirements will be included in this letter. If results warrant, HSU may place the subrecipient on the Department of Public Safety High-Risk list. All notes and forms should be typed. The visit should be reviewed with the HSU Homeland Security Program Manager and Deputy Homeland Security Advisor, advising of critical issues found, corrective actions, and best practices. The VTHSU personnel, at which time the report should be finalized, will follow up

corrective action requirements and the file closed. Hardcopy files should be archived with relevant grant history paperwork, while electronic data should be stored within the HSU SharePoint Site Programmatic Monitoring folder.

Proper Conduct for HSU Authorized Personnel

Monitoring personnel should be professional at all times. They must always display the attributes of objectivity, courtesy, reason, focused engagement, and receptivity. If HSU personnel note improper conduct by a subrecipient, they should document the issue and immediately address with supervisory personnel. Interviews can be conducted in an informal manner. HSU personnel should be courteous, good listeners, flexible, reasonable and knowledgeable.

Desk Monitoring

When it is not possible to complete on-site visits, a desk monitor may be completed. The documentation remains the same.

Progress Reporting

All subrecipients are required to submit Progress Reports as outlined below in the grant agreements. VTHSU personnel is responsible for receiving and reviewing progress reports addressing overall successes, technical assistance needs, and updates on progress success.



- a. A completed Program Progress Report Form must be submitted each time reimbursement is requested or bi-annually, at a minimum. The reporting periods are July 1 - December 31 (due January 15), January 1 – June 30 (due July 15). If the due date falls on a weekend or holiday, please submit the following business day. A final report is due within 30 days of the end date of this grant agreement. Program Progress Report Form is required even if no activity has been performed on the project.
- b. Program Progress Report Form is required even if no activity has been performed on the project.
- c. The Program Progress Report Form shall be completed to the best of the grantees' ability. Blank, incomplete, or insufficient Program Progress Report Forms will not be accepted.
- d. The State reserves the right to withhold part or all grant funds if the State does not receive timely documentation of the successful completion of grant deliverables.

List of Attachments:

- Attachment A- Pre-Visit Confirmation Letter
- Attachment B- Monitoring Interview Matrix
- Attachment C- Photo Log
- Attachment D- Post-Visit Results/Corrective Action Letter

Exceptions: There are currently no exceptions.

Resources:

State of Vermont, Department of Public Safety, [Granting Plan Part 4](#)
 §200.328 Monitoring and reporting program performance.
 §200.331 Requirements for pass-through entities

Drafted By:	Natalie Elvidge, Homeland Security Program Manager
Original Issue Date:	July 28, 2020 Initials:
Revision Date:	
Location Saved	https://vermontgov.sharepoint.com/:f:/r/sites/DPS/vsp/hsu/Shared%20Documents/HSU%20Operations/Decision%20Tracker/Decisions/2020-02_Guidance%20on%20Programmatic%20Monitoring%20Guidelines?csf=1&web=1&e=np7yWd
Decision Number	2020-02

VT Planning Committee Membership				
Representation	Name	Title	Organization	IT Experience (y/n)
Eligible Entity:	Jennifer Morrison	Commissioner (HSA)	Department of Public Safety	No
CIO, CISO, Equivalent	John Toney	CISO	Agency of Digital Services	Yes
Local Government	Cate Cross	Equity Committee Member	Shelburne	Yes
Local Government	Jay Furr	Selectboard Member	Richmond	No
Local Government Association	Ted Brady	Executive Director	VT League of Cities and Towns	No
Local Government Association	Emmanuel Ajanma	Director of Technology	VT League of Cities and Towns	Yes
Public Education	Peter Drescher	Director of Technology and Innovation	Essex Westford School District	Yes
Public Education	Mike Battig	Director, Cyber School	Norwich University	Yes
Public Health	Nate Couture	Network CISO	University of Vermont Health Network	Yes
Secretary of State's Officer	Jon Welch	Technology Director	Secretary of State	Yes
Fusion Center	Ryan McLiverty	Cyber Intelligence Analyst	Vermont Intelligence Center	Yes
Attorney General	James Layman	Assistant Attorney General	Vermont Attorney General's Office	No

Updated September 18, 2024