State of Vermont
Department of Finance & Management
109 State Street, Pavilion Building
Montpelier, VT 05609-0401
http://finance.vermont.gov/

[phone] 802-828-2376
[fax] 802-828-2428

Agency of Administration

Transmittal of External Audit Report

Instructions: Per Department of Finance & Management Policy #7.0: ***External Audit Reports***, departments are required to complete and submit this **coversheet** with a copy of the external audit report to the Commissioner of Finance & Management within 30 days of issuance of the final audit report. This coversheet must be submitted by the department's business office to ensure their awareness and acknowledgment of any potential financial impact. Official department responses to the audit report, including corrective action plans (*if required*), must also be submitted to Commissioner of Finance & Management upon completion.

Department	Department of Public Safety
Business Office Contact	Brenda Buker, Operations & IC Manager
Program/Activity Audited	State and Local Cybersecurity Program (SLCGP)
Audit Agency	FEMA and CISA
Audit Report Date	9/3/2024

1. **Does the audit report contain any findings or recommendations?**

   ☒ YES ☐ NO

   ➢ If YES continue to question #2; otherwise coversheet is complete.

2. **Does the report contain any repeat audit findings?**

   ☐ YES ☒ NO

3. **Please rate the findings and/or recommendations contained in the audit report using the following scale; for reports with multiple findings, this overall rating should be based on the most critical finding:**

   ☐ **Insignificant**: Nominal violation of policies, procedures, rules, or regulations. Corrective action suggested but not required.

   ☒ **Notable**: Minor violation of policies, procedures, rules, or regulations and/or weak internal controls; and/or opportunity to improve effectiveness and efficiency. Corrective action may be required.

   ☐ **Significant**: Significant violation of policies, procedures, rules, regulations or laws; and/or poor internal controls; and/or significant opportunity to improve effectiveness and efficiency. Corrective action required.

   ☐ **Major**: Major violation of policies, procedures, rules, regulations or laws; and/or unacceptable internal controls; and/or high risk for fraud, waste or abuse; and/or major opportunity to improve effectiveness and efficiency. Immediate corrective action required.

4. **Is the department required to develop a corrective action plan (*or similar*) to address the audit findings and/or recommendations?**

   ☒ YES ☐ NO

   ➢ If YES continue to next question; otherwise skip to question #8.

5. Has the corrective action plan been developed?

☐ YES ☒ NO [provide status below]

- ❖ Status of corrective action plan:

6. Does the department anticipate any inability or delay in implementing its corrective action plan?

☐ YES ☒ NO,

- ➢ If YES continue to next question; otherwise skip to question #8.

7. What fiscal and programmatic impact is this inability or delay likely to have?

8. Does the report contain any disallowed costs[1]?

☐ YES ☒ NO

- ➢ If YES list the amount(s) and page reference(s) below; otherwise skip to question #11.

Disallowed Amount $	Audit Report Page #

Disallowed Amount $	Audit Report Page #

9. Has the method and timing of repayment for all disallowed costs been agreed upon with the applicable organization?

☐ YES ☐ NO

10. Assess the impact this disallowance will have on the:

a. Program/Activity: ☐ Major ☐ Significant ☐ Minimal ☐ None
b. Dept Overall Budget: ☐ Major ☐ Significant ☐ Minimal ☐ None

11. Does the report contain any questioned costs[2]?

☐ YES ☒ NO

- ➢ If YES list the amount(s) and page reference(s) below; otherwise form is complete.

Questioned Amount $	Audit Report Page #

Questioned Amount $	Audit Report Page #

12. Assess the likelihood that the questioned costs will result in disallowances and/or reductions in future revenues:

☐ Very Likely ☐ Likely ☐ Somewhat Likely ☐ Not Likely

[1] Costs determined as unallowable under the applicable program/activity and not eligible for financial assistance; generally disallowed costs must be reimbursed to the awarding organization.

[2] Costs identified as potentially unallowable for financial assistance under the applicable program/activity.

U.S. Department of Homeland Security
Washington, DC 20472
www.fema.gov

FEMA

September 3, 2024

Ms. Cally Audet
Homeland Security Program Manager
Vermont Department of Public Safety
45 State Drive
Waterbury, VT 05671

Re: State and Local Cybersecurity Grant Program (SLCGP) Post -Monitoring Letter

Dear Ms. Audet,

On July 9, 2024, the FEMA Grant Programs Directorate (GPD), Office of Grants Administration (OGA), National Programs Division (NPD), and the Cybersecurity and Infrastructure Security Agency (CISA), concluded a programmatic monitoring site visit for the Vermont Department of Public Safety FY 2022 State and Local Cybersecurity Grant Program (SLCGP) award (EMW-2022-CY-00088). I would like to thank you and your team for your assistance and cooperation throughout this process.

The monitoring included a review of the progress made towards implementing the Cybersecurity Plan and investments to be funded by the SLCGP grant program and the agency's compliance with applicable federal requirements and regulations. Our discussions during the site visit were valuable in providing FEMA and CISA with a status of the performance and compliance for your grant award.

The program, under Vermont Department of Public Safety, has made progress with establishment of the Vermont Cybersecurity Planning Committee and Charter, and the approval of the State of Vermont Cybersecurity Plan. However, the program implementation experienced delays due to staff turnover at both the Department of Public Safety's Homeland Security Unit and the Agency of Digital Services. Moreover, progress is limited due to a state statutory requirement the grant be reviewed and approved by the Governor's office.

Included below are the outstanding issues observed and discussed during the site visit. These are noted as monitoring results and include a required corrective action by your agency. Please provide a response that addresses each of the identified areas to your FEMA Preparedness Officer within 30 days of the date of this report. Both FEMA and CISA will evaluate the response and provide additional follow up, if needed.

SAA Compliance Review Results	
Corrective Action	**Response due to FEMA**
All SLCGP recipients and subrecipients are required to participate in a limited number of free services by CISA. These services include Cyber Hygiene Services and annual completion of the Nationwide Cybersecurity Review (NCSR). See Appendix G of the FY 2022 SLCGP NOFO for details.	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.
Changes in key personnel on Cybersecurity Planning Committee.	Submit current Cybersecurity Planning Committee member list.
The recipient was unable to provide the requested program specific documentation. The recipient has not established grant awards/local consent documentation or a grant closeout procedure. As the recipient is still in the planning stages of project implementation, attached are two examples of SLCGP Policy and Procedure manuals, shared with permission from the States of KY and MS, which include closeout procedures and details on required cyber memberships and services.	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.
As new staff is involved in the grant administration and program implementation, additional technical assistance is required. FEMA recommends monthly re-occurring meetings for status updates on project development.	The recipient will send FEMA proposed dates and times for re-occurring monthly meetings.

FEMA and CISA are available to assist you and your cybersecurity partners to ensure optimal management and implementation of grant programs and activities.

In addition, the following technical assistance resources are available to help your agency resolve the corrective actions and recommendations outlined above:

- FEMA GPD offers Fundamentals of Grants Management Course both online and in person for free. Please reach out to FEMA-GPD-Training@fema.dhs.gov for more information.

For questions related to the SAA Compliance Review Results please don't hesitate to contact your Preparedness Officer, Jocelyn Fykes at Jocelyn.Fykes@fema.dhs.gov or Elizabeth Koren, Cyber Branch Chief, at Elizabeth.Koren@fema.dhs.gov.

Sincerely,

Elizabeth J. Koren, Esq.
Cyber Branch Chief
FEMA National Program Division
Office of Grants Administration

cc: Official Grant File
Jennifer Morrison
Melissa Austin
Kaisa Lewia
Eric Forand
Bess Mitchell, CISA Stakeholder Engagement Division
Kim Chatman, CISA Stakeholder Engagement Division
Jim Fagan, CISA Integrated Operations Division

Stephanie Kerr, CISA Integrated Operations Division
Kerry Holmes, CISA Integrated Operations Division
Christian Cosans, CISA Supervisory Information Security Specialist
Cheri Ayoub, CISA Cybersecurity Advisor
Jocelyn Fykes, FEMA SLCGP Preparedness Officer