Maryland FFY202 SLCGP Subrecipient Funding Guide

Table of Contents

Overview

I. Maryland State and Local Cybersecurity Grant Program (SLCGP) Overview:
The goal of the State and Local Cybersecurity Grant Program (SLCGP) is to help states, local governments, rural areas, and territories address cybersecurity risks and cybersecurity threats to information systems. The program enables DHS to make

targeted cybersecurity investments in state, local, and territorial government agencies, thus improving the security of critical infrastructure and resilience of the services that state, local, and territorial governments provide to their communities.

The Cybersecurity and Infrastructure Security Agency (CISA) and Federal Emergency Management Agency (FEMA) are jointly managing the SLCGP. CISA will provide subject-matter expertise and determine allowable activities, while FEMA will conduct eligibility reviews and issue/administer the grant awards consistent with all applicable laws, regulations, and policies.

The SLCGP funds granted to the State of Maryland will be distributed by the Maryland State and Local Cybersecurity Grant Program Planning Committee ("the Committee''). The Committee will award subapplicants who demonstrate the ability to put forward the most competitive projects, in alignment with the project application, and maintain federal and state grant compliance.

The Maryland Cyber Planning Committee has developed a reimbursable Sub-grant program where eligible entities can apply for funding for their own projects.

II. Eligibility Criteria

The eligible applicants are Maryland "Local governments"[1] which include:

- A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments, regional or interstate government entity, or agency or instrumentality of a local government; or
- Rural as defined by FEMA which is, a rural community, unincorporated town or village, or other public entity. Per the Homeland Security Act of 2002, a "rural area" is defined in 49 U.S.C. § 5302 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 Commerce.
- Rural as defined by the Committee which is, any Maryland "Local Government" that can provide adequate evidence of their rural status such as a planning and zoning designation or mapping. Evidence should be submitted with the application package.

[1] "Local governments" defined in 6 U.S.C. § 101(13).

III. Award Information

Funding Amount & Federal Period of Performance:
The Federal Period of Performance is from December 1st, 2023 - November 30th, 2027, Maryland has been granted a total funding amount of $6,514,533.00.

Funding Instrument Type: Grant

Application Open & Submission Information

I. Application Open Date: September 3rd, 2024

II. Application Deadline: October 3rd, 2024, 11:59 PM EST

III. Project Completion Deadline: 30 September 2027
Projects are eligible for submission from the application open date to the application deadline date. All projects must be completed no later than 30 September 2027. The Committee will establish project-specific periods of performance in alignment with project needs and not to exceed the Project Completion Deadline (i.e., 30 September 2027)

IV. State Administrative Agency (SAA): The Maryland Department of Emergency Management (MDEM)

V. Award Notification: Will be sent by the State Administrative Agency (SAA) if a project has been approved.

VI. The performance period will start when the SAA notifies the subrecipient of project approval and the funds or services are released.

VII. Agreeing to Terms and Conditions of the Award
By submitting an application, applicants agree to comply with all federal, state, and local grant requirements to include, but not limited to, the SLCGP Notice of Funding Opportunity (NOFO), 2CFR200, FEMA Information Bulletins (IBs), and the Maryland FFY2023 SLCGP Funding Guide.

General Application Information

I. How to Apply & Receive Funding
Applying for this award is a multi-step process and requires time to complete. Please read the overview below on how to apply.

1. Review all information guides provided above.
2. Download & Complete the Following Documents:
    a. Maryland FFY2023 SLCGP Subrecipient Project Proposal Application
    b. Maryland SLCGP FFY2023 Additional Application Documents Packet
    c. Form W-9 *(if applicable)*
3. Email completed forms to slcgp.grant@maryland.gov. Subject Line must be in this format:
    a. FY[funding year] SLCGP - [Sub-recipient Name] [Project Title] Application Forms
    b. Example: FY[23] SLCGP - [MDEM]- [SLCGP Project] Application Forms
4. Committee submits projects to FEMA
5. FEMA approves/reject projects
6. Receive Committee Project Disposition
7. If approved, funds are awarded to the pass-through entity (MDEM) upon signature of the subrecipient subaward agreement.
8. Submit Letter of Intent to Accept or Reject Funding in 30 Days to slcgp.grant@maryland.gov. Subject Line must be in this format:
    a. FY[funding year] SLCGP - [Sub-recipient Name] [Project Title] Letter of Intent
    b. Example: FY[23] SLCGP - [MDEM]- [SLCGP Project] Letter of Intent

II. Application Guidance

Please review the "Maryland FFY2023 SLCGP Project Application & Budget Narrative Instruction Manual" for complete guidance on the required application elements and documents. In general, all applications should:

- Clearly address the goals, audiences, and objectives of this notice.
- Address how the project will improve the overall cyber posture of your entity.
    - This can include both Information Technology and Operational Technology.
    - If the control you are requesting fund for would replace or enhance and existing control preforming a similar or identical function, explain why this new control and funds are needed.
- Enumerate specific outputs and outcomes to be achieved by the end of the grant period.
- Describe the involvement and expertise of relative partners, stakeholders, staff, contractors, and any other involved parties.
- Specify the groups that will benefit from the project and the geographic locations of project activities.

  - Proposed projects in multiple locations should explain how the project goals will be accomplished.
- Describe how elements of the project will be sustainable beyond the grant period.
- Address any impacts of the project on the general public and include a plan for how to disseminate information or facilitate public involvement, if applicable.
- Demonstrate competency to manage all financial and oversight aspects of the project through completion of the budget template, including costs and transparent arrangements of relationships with partner organizations, if applicable.
- Explain how the project objectives and milestones will be monitored, including developing performance indicators. Indicators should include baselines, targets, and information on how periodic updates will be reported to the Maryland State and Local Cybersecurity Grant Program Planning Committee during the life of the project.
- Pursuant to Section 504 of the Rehabilitation Act of 1973, recipients of FEMA financial assistance must ensure that their programs and activities do not discriminate against other qualified individuals with disabilities. If necessary, applicants should describe how the project will incorporate equity, inclusion, and accessibility in the projects design and implementation.
- Follow the guidelines outlined in this notice and include all mandatory forms.

III. Applicants must ensure:

- Budget narratives are in USD.
- The Maryland FFY2023 SLCGP Subrecipient Project Proposal Application has been signed by an approving authority. See the “Maryland FFY2023 SLCGP Project Application & Budget Narrative Instruction Manual ” for more information.

IV. Mandatory Application Forms

- Maryland FFY2023 SLCGP Subrecipient Project Proposal Application
- Maryland SLCGP FFY2023 Additional Application Documents Packet, which includes:
  - Budget Narrative and Justification Template
  - POETE Narrative and Justification
  - Appendix A: Cybersecurity Capabilities Assessment
  - Appendix E: Measurable Milestones

- Form W-9 (if applicable)

To Be Completed After Application Submission (slcgp.grant@maryland.gov will reach out to request these forms)**:**

Letter of Intent to Accept or Reject Funding (this form will be sent to you by the SAA after your application submission, if you are selected to receive funding)

V. Project Alignment with Maryland Project Categories

Through the collaborative efforts of the Maryland State and Local Cybersecurity Grant Program Planning Committee ("the Committee") and the provided SLCGP NOFO issued by the U.S. Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA)/Resilience/Grant Program Directorate (GPD), the Committee has identified 5 investment priorities (referred to as project categories) for Maryland. Your proposed project and project budget should align with at least one of these project categories.

The Committee's identified project categories are as follows:

1. **Project Category 1 (PC1): Adoption or enhancement of priority cybersecurity best practices -** The Maryland Cybersecurity Planning Committee has identified five baseline best practices that will significantly enhance the cybersecurity posture across the state. **Due to the limited amount of funding available, jurisdictions are encouraged to propose projects that enable or enhance these five priority best practices.**

   These best practices are: (1) Asset Discovery & Vulnerability Management; (2) Multi-Factor Authentication (MFA); (3) End-Point Detection and Response (EDR); (4) Email Security (such as Secure Email Gateway (SEG) solutions); and (5) Security Awareness Training.[2]

2. **Project Category (PC2): Adoption or enhancement of general cybersecurity best practices -** While not identified as Maryland's prioritized baseline cybersecurity best practices, jurisdictions can submit project proposals that support the adoption or enhancement of other general cybersecurity best practices.

[2] For definitions of the best practices listed in Project Category 1 (PC1), please review the Maryland SLCGP FFY2023 FAQs.

These best practices include, but are not limited to: Enhanced logging; data encryption; end of use processes of software and hardware; strong password management; ability to reconstitute systems (backups); migration to .gov domain; implementing the NIST Cybersecurity Framework; implementing NIST cyber supply chain risk management practices; and making use of knowledge bases of adversary tools and tactics.[3]

3. **Project Category 3 (PC3): Cybersecurity policy and governance -** Jurisdictions may seek funding to support the development of cybersecurity policies and governance.

   Examples include, but are not limited to: cyber incident response plans; acceptable use policies; continuity of operations plans; technology modernization processes; risk and/or threat assessments.

4. **Project Category (PC4): Addressing specific jurisdictional cybersecurity needs -** Recognizing that some jurisdictions may have specific or unique cybersecurity needs, jurisdictions may propose projects to address those needs. For example: addressing gaps in cybersecurity critical infrastructure specific to your entity/jurisdiction.
5. **Project Category 5 (PC5): Cybersecurity workforce development -** Jurisdictions may seek funding to support workforce recruitment and development needs using the NICE Cybersecurity Workforce Framework[4].

For more information on the Project Categories, please review the "Maryland FFY2023 SLCGP Project Application & Budget Narrative Instruction Manual [5]".

Application Evaluation Criteria

Each application submitted under this announcement by the deadline will be evaluated by the Maryland State and Local Cybersecurity Grant Program Planning Committee and rated based on the criteria enumerated below. The criteria is designed to assess the quality of the proposed project, and to determine the likelihood of the project's success and long-term sustainment.

[3] For definitions of the best practices listed in Project Category 2 (PC2), please review the Maryland SLCGP FFY2023FAQs.
[4] For more information on the NICE Cybersecurity Framework view: https://niccs.cisa.gov/workforce-development/nice-framework
[5] Applicants are encouraged to review the FFY2022 State and Local Cyber Grant Program (SLCGP) NOFO from FEMA.

The criteria for evaluating proposals are as follows:

I. **Project Proposal & Project Management Plan Scoring (0-60 points awarded)**
   - ***Clarity & Quality:*** The project idea should be well developed, and include sufficient detail about how the project will be carried out. A clear and quality project plan will include the project's mission and vision, an appropriately and clearly defined project scope, and demonstrate that the applicant has a clear understanding of the underlying issue(s) that the project will address.
   - ***Feasibility****:* The project plan must demonstrate that the organization has sufficient expertise, skills, and human resources to implement the project.
   - ***Timeliness:*** The project plan must enumerate how all project outputs and outcomes will be achieved by the end of the grant period.
   - ***Monitoring and Evaluation:*** The proposal should provide a list of proposed project tasks, corresponding milestones, outcome indicators, and a timeline for completing all project objectives. The project plan must explain how these project objectives and milestones will be monitored, including developing performance indicators. Indicators should include baselines, targets, and information on how periodic updates will be reported to the Maryland State and Local Cybersecurity Grant Program Planning Committee during the life of the project.
   - ***Measurable Impact:*** The project should demonstrate a clear impact on the entity's cybersecurity posture with adequate evidence provided. Provide information on how the project will impact your entity beyond what would have happened if the project is not implemented in regards to your entity's cyber preparedness.
   - ***Sustainability:*** Describe how elements of the project will be sustainable beyond the grant period. In this section, you should also address any additional sources of funding that will be used to address the proposed challenges and how any additional funding will affect the long term sustainability of the project.

II. **Budget Narrative -** The budget narrative demonstrates competency to manage all financial and oversight aspects of the project through completion of the budget template, including an accurate summary of project costs and transparent arrangements of relationships with partner organizations, if applicable. Budget items must be reasonable, allowable, and allocable. If your entity has a financial management system that will assist in overseeing the funds, this will be

considered during scoring to determine the quality of the management system and its ability to meet management standards.[6] **(0-20 points awarded)**

III. **Cybersecurity Capabilities Assessment[7] -** The purpose of the Cybersecurity Capabilities Assessment is to establish an eligible entity's current cybersecurity capabilities relating to the listed cybersecurity elements in the assessment. This assessment should be filled out to the best of the applicant's ability. Having below an advanced level of capability will not impact the project proposal's overall score. This assessment is designed to help establish, strengthen, or further develop your cybersecurity capabilities by identifying elements that will be strengthened through your proposed project. **(0-5 points awarded)**

IV. **Inclusion of Relative Partners & Stakeholders -** Describe the involvement and expertise of relative partners and stakeholders. **(0-5 points awarded)**

V. **Compliance -** Describe how the project will follow grant compliance requirements, including how grant expenditures will be tracked and segregated from other expenditures, who will be responsible for completing and submitting programmatic and financial progress reports, and who will be responsible for managing the project. **(0-5 points awarded)**

Additional Evaluated Application Requirements

In addition to the criteria evaluated in the previous section, the following information must also be met as part of the application. Applications not submitted with this information will be considered incomplete and will not be reviewed by the Committee.

I. **Project Alignment with Maryland Project Categories -** The proposed project should align with at least one of the established Maryland Project Categories identified in the "Project Alignment with Maryland Project Categories" section of this funding guide. During the application process, you will be asked to identify which Project Category(ies) your proposed project will meet. Due to the limited amount of funding available, jurisdictions are encouraged to propose projects related to Project Category 1 (PC1).

[6] For more information on the budget narrative and allowable costs for this grant, review the SLCGP IJ Instruction Guidance Manual.
[7] See Appendix A: Cybersecurity Capabilities Assessment

For more information on the Project Categories, please review the "Maryland FFY2023 SLCGP Subrecipient Project Proposal & Budget Narrative Template Instruction Manual".

II. **Preventing Duplication of Effort -** To prevent duplication of effort, applicants will be required to certify, within their proposal, that there is/are no other entities in their jurisdiction applying for funds to conduct that same project other than to intentionally enhance each other's projects. Subsequently, while reviewing applicant projects, the planning committee will encourage collaboration between neighboring and/or integrated entities who are applying for similar projects.

III. **Itemized Quote for Vendor Services -** If the applicant intends to use a vendor for any services and/or any contractual work, said applicant must provide an itemized quote of the work to be performed, including vendor name, quote expiration date, price per item of good/service, labor costs (if applicable), total cost, etc.

IV. **Support of Equity, Inclusion, and Accessibility -** Pursuant to Section 504 of the Rehabilitation Act of 1973, recipients of FEMA financial assistance must ensure that their programs and activities do not discriminate against other qualified individuals with disabilities. If necessary, applicants should describe how the project will incorporate equity, inclusion, and accessibility in the project design and implementation.

Review Process of Submitted Applications

Each application submitted under this announcement by the deadline will be evaluated by the Committee and rated based on the criteria in the "Evaluation of Submitted Applications" section of this Funding Guide. The Committee will follow all applicable statutes, rules, and requirements, and will take into consideration all application materials to determine a recipient's eligibility.

The Committee reserves the right to request additional information or revisions from the applicant and request resubmission of the application with the requested revisions.

Grading Considerations

Because this is a competitive grant program, the committee has implemented a weighting system that ranks rural jurisdictions' applications highest by multiplying their final application score by:

- FEMA Rural Definition x 1.5
- Maryland Rural Definition x 1.4

The same practice will be applied to the project categories at the rates described below:

- Category 1 (Maryland's Priority Best Practices) x 1.3
- Category 2 (General Best Practices) x 1.1
- Category 3 (Cyber Security Governance) x 1
- Category 4 (Addressing specific needs) x 1
- Category 5 (Workforce development) x 1

Notice of Award

Before accepting the award, the recipient should carefully read the award package. The award package includes instructions on utilizing the grant award and the terms and conditions associated with responsibilities under federal awards. **Recipients must accept all conditions in this Funding Guide as well as any specific terms and conditions in the Notice of Award to receive an award under this program.**

Notification of award approval is made through the primary contact email designated in the Maryland FFY2023 SLCGP Subrecipient Project Proposal. The recipient should follow the directions in the notification to confirm intent to accept or decline the award.

Recipients must accept or decline their awards no later than 30 days from the award date. The recipient shall notify The Committee of its intent to accept and proceed with work under the award or provide a notice of intent to decline.

Funds will remain on hold until the recipient accepts the award through an acceptance letter sent to slcgp.grant@maryland.gov and all other conditions of the award have been satisfied or until the award is otherwise rescinded. Failure to accept a grant award within the 30-day timeframe may result in a loss of funds.

Required, Encouraged, and Optional Services, Memberships, and Resources For Grant Awardees

Please be aware that all SLCGP grant recipients are required to participate in a limited number of free services by CISA. For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement. A list of required services and memberships is provided in Appendix B of this guide.

More information can also be found in the FEMA State and Local Cybersecurity Grant Program (SLCGP) NOFO[8], under NOFO Section F and NOFO Appendix G.

Support of Equity, Inclusion, and Accessibility

The following is a requirement for accepting FEMA financial assistance:
Pursuant to Section 504 of the Rehabilitation Act of 1973, recipients of FEMA financial assistance must ensure that their programs and activities do not discriminate against other qualified individuals with disabilities. Grant recipients should engage with the whole community to advance individual and community preparedness and to work as a nation to build and sustain resilience. In doing so, recipients are encouraged to consider the needs of individuals with disabilities into the activities and projects funded by the grant.

DHS expects that the integration of the needs of people with disabilities will occur at all levels, including planning; alerting, notification, and public outreach; training; purchasing of equipment and supplies; protective action implementation; and exercises/drills.[9]

Reporting

[8] Please view Required, Encouraged, and Optional Services, Memberships, and Resources For Grant Awardees in the FEMA SLCGP NOFO, NOFO Section F, Administrative and National Policy Requirements and NOFO Appendix H, Appendix F: Required, Encouraged, and Optional Services, Memberships, and Resources.
https://www.fema.gov/fact-sheet/department-homeland-security-notice-funding-opportunity-fiscal-year-2023-state-and-local

[9] For more information on how your project should incorporate Equity, Inclusion, and Accessibility. Please see the SLCGP FEMA FFY23 NOFO sections on Disability Integration in Section H.

Quarterly Reporting Requirements

Subrecipients are required to submit various financial and programmatic reports as a condition of award acceptance for projects. Future awards and funds drawdown may be withheld if these reports are delinquent. Records of these reports, along with any additional documentation supporting the financial expenditures for the project should be held for at least 3 years after the end of the project's period of performance.

I. **Subrecipient Quarterly Status Reports (QSRs)** - Subrecipients are required to report financial and programmatic information on a quarterly basis. The pass-through entity (MDEM) will provide a template for the subrecipients to utilize and will allow subrecipients to report on:
   - Expenditures and Obligations
   - 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 any additional Committee performance measure requirements.

The progress report is available here:

Reporting Period	Report Due Date
July 1 – September 30	October 15th
October 1 – December 31	January 15th
January 1 – March 31	April 15th
April 1 – June 30	July 15th

Closeout Reporting Requirements

I. **Closeout Reporting -** Subrecipients are required to complete a final QSR in alignment with closeout reporting requirements as stated in the NOFO. Subrecipients must utilize the final QSR to:
   - Provide a final progress report detailing all accomplishments, including a narrative summary of the impact of those accomplishments throughout the period of performance and

- Other documents as required by the Committee, or the pass-through entity (MDEM).

Additional Information

Appeals

If a project is not accepted, the applicant can appeal this decision. Applicants must complete an appeal request form and submit the form by the applicable deadline. All required documentation must be uploaded and submitted with the appeal request.

Appeals Process Overview:

1. Appeal form requested through slcgp.grant@maryland.gov
2. Appeal submitted to the Committee
3. Receive Committee Project Disposition
4. If approved, the project is resubmitted to FEMA
2. FEMA approves/reject projects
3. If approved, funds or services are awarded by the pass-through entity (MDEM) or the Maryland Department of Information Technology upon signature of the award agreement letter.

For more information on appeals, please email: slcgp.grant@maryland.gov.

Period of Performance (PoP) Extensions & Budget Change Requests

Any change in the scope of the project or request for additional funds must be brought to the committee for review and final determinations.

If an awardee requires information on PoP Extensions or Rebudgeting Requests, please email: slcgp.grant@maryland.gov.

Reimbursement Submissions

Reimbursements will be submitted in a timely and orderly fashion by subrecipients. All reimbursements must be submitted to slcgp.grant@maryland.gov. Failure to submit reimbursements to this email address may result in severe delays to failure in receiving reimbursement. Subrecipients are required to submit reimbursements for

expenditures no later than 90 days after that expenditure was incurred. Failure to abide by this requirement may result in the rejection of a reimbursement. For more information on reimbursements, please reference Appendix C.

Monitoring/Site Visits

Per 2 C.F.R. § 200.337, subrecipients are subject to monitoring by FEMA and their authorized representatives, which in this case is the State Authorized Agency (SAA), MDEM. Grant-related records and information must be made available to FEMA and/or MDEM in a timely manner when requested.

Termination of Provisions

The subaward may be terminated in whole or in part by FEMA or the SAA (MDEM) if the subrecipient fails to comply with the terms and conditions of the award. FEMA and/or the MDEM will provide written notification of the termination including the reason for the termination. For more information on terms and conditions reference Appendix D: Termination of Provisions and Subaward Agreement Letter.

Contact Information

If you have questions about this grant or the submission process, please contact slcgp.grant@maryland.gov

Please Proceed to the Appendices on the Next Page.

Appendix A: Cybersecurity Capabilities Assessment[10]

The purpose of the Cybersecurity Capabilities Assessment is to establish an eligible entity's current cybersecurity capabilities relating to the cybersecurity elements listed in the "Cybersecurity Plan Required Elements" column. This assessment will help to establish, strengthen, or further develop your cybersecurity capabilities by identifying elements that require further development. The results of this assessment should be used to help justify the need for your proposed project. In your proposed project application, identify which gaps found in the assessment your project will address.

Eligible entities should provide a brief description of their current cybersecurity capabilities related to each element, and identify if these current capabilities are "Foundational, Fundamental, Intermediary, or Advanced".

Eligible entities can use the red "EVAL" column as a self-assessment tool. Entities with newly initiated programs could use this spreadsheet to track the status of their cybersecurity planning efforts. Similarly, entities with advanced programs could use this worksheet to evaluate their current cybersecurity posture for each element using "Met, Not Met, Partially Met, or N/A.

See the Appendix A Excel Sheet for a fillable template.

[10] Adapted from FEMA SLCGP NOFO, Appendix C: Cybersecurity Plan
https://www.fema.gov/fact-sheet/department-homeland-security-notice-funding-opportunity-fiscal-year-2022-state-and-local#a

Appendix B: Required Services and Compliance

Administrative and National Policy Requirements[11]

Please review the FEMA SLCGP NOFO for information on DHS Standard Terms And Conditions, Ensuring The Protection Of Civil Rights, Environmental Planning And Historic Preservation (EHP) Compliance, Safecom Guidance Compliance, and Requirement For Using CISA Services.

Required, Encouraged, and Optional Services, Memberships, and Resources[12]

All SLCGP recipients and subrecipients are required to participate in a limited number of free services by CISA. For these required services and memberships, please note that participation is **not required for submission and approval** of a grant **but is a post-award requirement.**

All SLCGP recipients are strongly encouraged to participate in other Memberships.

Additional, optional CISA resources are also available in this Appendix

Required Services and Memberships

Cyber Hygiene Services

---

[11] Please view Required, Encouraged, and Optional Services, Memberships, and Resources For Grant Awardees in the FEMA SLCGP NOFO, NOFO Section F, Administrative and National Policy Requirements and NOFO Appendix H, Appendix F: Required, Encouraged, and Optional Services, Memberships, and Resources. https://www.fema.gov/fact-sheet/department-homeland-security-notice-funding-opportunity-fiscal-year-2023-state-and-local

[12] Please view Required, Encouraged, and Optional Services, Memberships, and Resources For Grant Awardees in the FEMA SLCGP NOFO, NOFO Section F, Administrative and National Policy Requirements and NOFO Appendix H, Appendix F: Required, Encouraged, and Optional Services, Memberships, and Resources. https://www.fema.gov/fact-sheet/department-homeland-security-notice-funding-opportunity-fiscal-year-2023-state-and-local

1. Web Application Scanning is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards.
2. Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.

To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLGCP. For more information, visit CISA's Cyber Hygiene Information Page.

Nationwide Cybersecurity Review (NCSR)
The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC.

Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually.

For more information, visit Nationwide Cybersecurity Review (NCSR) (cisecurity.org).

Encouraged Services, Membership and Resources

Membership in the Multi-State Information Sharing and Analysis Center (MS-ISAC) and/or Election Infrastructure Information Sharing and Analysis Center (EI-ISAC):
Recipients and subrecipients are strongly encouraged become a member of the MS-ISAC and/or EI-ISAC, as applicable. Membership is free.

The MS-ISAC receives support from and has been designated by DHS as the cybersecurity ISAC for SLT governments. The MS-ISAC provides services and information sharing that significantly enhances SLT governments' ability to prevent, protect against, respond to, and recover from cyberattacks and

compromises. DHS maintains operational-level coordination with the MS-ISAC through the presence of MS-ISAC analysts in CISA Central to coordinate directly with its own 24x7 operations center that connects with SLT government stakeholders on cybersecurity threats and incidents. To register, please visit https://learn.cisecurity.org/ms-isac-registration. For more information, visit MS-ISAC (cisecurity.org).

The EI-ISAC, is a collaborative partnership between the Center for Internet Security (CIS), CISA, and the Election Infrastructure Sub-Sector Government Coordinating Council. The EI-ISAC is funded through DHS grants and offers state and local election officials a suite of elections-focused cyber defense tools, including threat intelligence products, incident response and forensics, threat and vulnerability monitoring, cybersecurity awareness, and training products. To register, please visit https://learn.cisecurity.org/ei-isac-registration. For more information, visit https://www.cisa.gov/election-security.

CISA Recommended Resources, Assessments, and Memberships (not mandatory)

The following list of CISA resources are recommended products, services, and tools provided at no cost to the federal and SLT governments, as well as public and private sector critical infrastructure organizations:

- Ransomware Guide (Sept. 2020)
- Cyber Resilience Review
- External Dependencies Management Assessment
- EDM Downloadable Resources
- Cyber Infrastructure Survey
- Validated Architecture Design Review
- Free Public and Private Sector Cybersecurity Tools and Services

CISA Central: To report a cybersecurity incident, visit https://www.us-cert.gov/report.
For additional CISA services visit the CISA Services Catalog.
For additional information on memberships, visit Information Sharing and Analysis Organization Standards Organization

Appendix C: Termination of Provisions and Subaward Agreement Letter

Termination of an award in whole or in part may be done for one of the following reasons outlined in 2 C.F.R. § 200.340[13]. If the award is terminated, the recipient must still comply with closeout requirements even if an award is terminated in whole or in part.

I. **Noncompliance -** If a recipient fails to comply with the terms and conditions of the award, the Committee may terminate the award in whole or in part. If the noncompliance can be corrected, the Committee may first attempt to direct the recipient to correct the noncompliance.
If the noncompliance cannot be corrected or the recipient is non-responsive, the Committee may proceed with a Remedy Notification, which could impose a remedy for noncompliance per 2 C.F.R. § 200.339[14], including termination. Any action to terminate based on noncompliance will follow the requirements of 2 C.F.R. §§ 200.341-200.342[15].

II. **With The Consent Of The Recipient -** An award may also be terminated in whole or in part with the consent of the recipient, in which case the parties must agree upon the termination conditions, including the effective date, and in the case of partial termination, the portion to be terminated.

III. **Notification By The Recipient -** The recipient may terminate the award, in whole or in part, by sending written notification to the Committee setting forth the reasons for such termination, the effective date, and in the case of partial termination, the portion to be terminated. In the case of partial termination, the Committee may determine that a partially terminated award will not accomplish the purpose of the federal award, so the Committee may terminate the award in its entirety. If that occurs, the Committee will follow the requirements of 2 C.F.R. §§ 200.341-200.342 in deciding to fully terminate the award.

---

[13] View 2 C.F.R. § 200.340:
https://www.ecfr.gov/current/title-2/subtitle-A/chapter-II/part-200/subpart-D/subject-group-ECFR86b76dde0e1e9dc/section-200.340
[14] View 2 C.F.R. § 200.339:
https://www.ecfr.gov/current/title-2/subtitle-A/chapter-II/part-200/subpart-D/subject-group-ECFR86b76dde0e1e9dc/section-200.339
[15] View 2 C.F.R. § 200.342:
https://www.ecfr.gov/current/title-2/subtitle-A/chapter-II/part-200/subpart-D/subject-group-ECFR86b76dde0e1e9dc/section-200.342