Fiscal Year 2023 State and Local Cybersecurity Grant Program (SLCGP) Guidance for the State of West Virginia

Program Overview and Grant Priorities for 2023

The goal of the State and Local Cybersecurity Grant Program is to assist governmental entities with managing and reducing systemic cyber risk. The four overarching federal objectives of the program are to:

- Establish appropriate governance structures
- Evaluate and assess current cybersecurity posture
- Implement security protections commensurate with risk
- Ensure personnel are trained commensurate with responsibility

For the FY 23 grant cycle, our state priorities will focus on best practices in the areas of:

- Implementing Multi-Factor Authentication
- Enhanced Logging
- Data Encryption
- Ending the use of unsupported/end of life software and hardware that are accessible from the internet
- Prohibiting the use of known/fixed/default passwords and credentials
- Ensuring the ability to reconstitute systems (backups)
- Migration to the .GOV internet domain
- Endpoint Detection and Network Security
- Vulnerability Assessment and Penetration Testing
- Cybersecurity Awareness Training

Eligible Applicants

An eligible subrecipient includes local governments and **does not include nonprofit and for-profit organizations**. Section 2(13) of the Homeland Security Act of 2002 (codified as amended at 6 U.S.C. § 101(13)) defines a local government as:

- A county, municipality, city, town/village, 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.
- A rural community, unincorporated town or village, or other public entity.

- A public educational institution (e.g., elementary school, secondary school, or institution of higher education) is generally eligible to receive assistance under SLCGP if it is an agency or instrumentality of a state or local government under state and/or local law. In contrast, a private educational institution would **not** be eligible to receive SLCGP assistance because it is not an agency or instrumentality of a state or local government.

Allowable and Unallowable Costs

All costs charged to federal awards (including both federal funding and any non-federal matching or cost sharing funds) must comply with applicable statutes, rules and regulations, policies, the federal NOFO, and the terms and conditions of the federal award. They must also comply with the Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2 C.F.R. Part 200 unless otherwise indicated in the NOFO or the terms and conditions of the federal award. This includes, among other requirements, that costs must be incurred, and products and services must be delivered within the budget period. 2 C.F.R. § 200.403(h). The following identifies a list of activities for which a recipient may **not** use federal funds and any cost sharing or matching funds under federal awards:

- Matching or cost sharing requirements for other federal grants and cooperative agreements (see 2 C.F.R. § 200.306).
- Lobbying or other prohibited activities under 18 U.S.C. § 1913 or 2 C.F.R. § 200.450.
- Prosecuting claims against the federal government or any other government entity (see 2 C.F.R. § 200.435).
- Spyware.
- Construction.
- Renovation.
- Paying Ransoms.
- For recreational or social purposes.
- Cybersecurity Insurance Premiums.
- To acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building.).
- 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 or a local government within the jurisdiction of the eligible entity.

- 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.
- For any recipient or subrecipient cost-sharing contribution.

Though construction and renovation projects are not permissible, some projects will involve minor modifications. In these instances, an Environmental and Historic Preservation (EHP) screening will be required. The Homeland Security State Administrative Agency will follow up with all approved applicants to assist with this process.

Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services

Recipients, subrecipients, and their contractors must comply with the prohibitions set forth in Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 (2018) (FY 2019 NDAA) and 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200. The FY 2019 NDAA and these regulations, as they apply to recipients, subrecipients, and their contractors and subcontractors, provide for two distinct prohibitions: (1) prevent the use of federal award funds to procure or obtain covered telecommunications equipment or services; and (2) prevent the use of federal award funds to contract with an entity that uses such covered telecommunications equipment or services.

Guidance is available at FEMA Policy #405-143–1 - Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services

Additional guidance is available at Contract Provisions Guide: Navigating Appendix II to Part 2–0 - Contract Provisions for Non-Federal Entity Contracts Under Federal Awards (fema.gov).

FEMA recipients and subrecipients **may not** use any FEMA funds under open or new awards to:

- Procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system.
- Enter, extend, or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system.

- Enter, extend, or renew contracts with entities that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

Procurement Standards

All procurement activity must be conducted in accordance with federal procurement standards at 2 C.F.R. §§ 200.317 – 200.327. Subrecipients must comply with all requirements, even if they are not listed in this guidance.

All subrecipients must have and use their own documented procurement procedures that reflect applicable state laws and regulations, provided that the procurements conform to applicable federal law and the standards identified in 2 C.F.R. Part 200. These standards include, but are not limited to, providing for full and open competition consistent with the standards of 2 C.F.R. § 200.319 and the required procurement methods at § 200.320.

The recognized procurement methods in 2 C.F.R. § 200.320 have been reorganized into informal procurement methods, which include micro-purchases and small purchases; formal procurement methods, which include sealed bidding and competitive proposals; and noncompetitive procurements. The federal micro-purchase threshold is currently $10,000, and non-state entities may use a lower threshold when using micro-purchase procedures under a FEMA award. If a non-state entity wants to use a micro-purchase threshold higher than the federal threshold, it must follow the requirements of 2 C.F.R. § 200.320(a)(1)(iii)-(v). The federal simplified acquisition threshold is currently $250,000, and a non-state entity may use a lower threshold but may not exceed the federal threshold when using small purchase procedures under a FEMA award. *See* 2 C.F.R. § 200.1 (citing the definition of simplified acquisition threshold from 48 C.F.R. Part 2, Subpart 2.1).

Competition and Conflicts of Interest

Among the requirements of 2 C.F.R. § 200.319(b) applicable to all non-federal entities other than states, in order to ensure objective contractor performance and eliminate unfair competitive advantage, ***contractors that develop or draft specifications, requirements, statements of work, or invitations for bids or requests for proposals must be excluded from competing for such procurements***. FEMA considers these actions to be an organizational conflict of interest and interprets this restriction as applying to contractors that help a non-federal entity develop its grant application, project plans, or project budget. This prohibition also applies to the use of former employees to manage the grant or carry out a contract when those former employees worked on such activities while they were employees of the non-federal entity.

Under this prohibition, unless the non-federal entity solicits for and awards a contract covering both development and execution of specifications (or similar elements as described above), and this contract was procured in compliance with 2 C.F.R. §§ 200.317 – 200.327, federal funds cannot be used to pay a contractor to carry out the work if that contractor also worked on the development of those specifications. This rule applies to all contracts funded with federal grant funds, including pre-award costs, such as grant writer fees, as well as post-award costs, such as grant management fees.

Additionally, some of the situations considered to be restrictive of competition include, but are not limited to:

- Placing unreasonable requirements on firms for them to qualify to do business.
- Requiring unnecessary experience and excessive bonding.
- Noncompetitive pricing practices between firms or between affiliated companies.
- Noncompetitive contracts to consultants that are on retainer contracts.
- Organizational conflicts of interest.
- Specifying only a "brand name" product instead of allowing "an equal" product to be offered and describing the performance or other relevant requirements of the procurement.
- Any arbitrary action in the procurement process.

Under 2 C.F.R. § 200.318(c)(1), non-federal entities other than states are required to maintain written standards of conduct covering conflicts of interest and governing the actions of their employees engaged in the selection, award, and administration of contracts. No employee, officer, or agent may participate in the selection, award, or administration of a contract supported by a federal award if he or she has a real or apparent conflict of interest.

Cost Share/Match

For FY 2023, the SLCGP requires a 20% non-federal cost share; however, the State has appropriated the funding for this fiscal year. When submitting your applications, enter the full project amount and do not separate out the match portion. All documentation of the federal/state split will be handled by the WVEMD Grant Staff.

Funding

The total funding available for subawards is $6,674,893. Of this amount, 80% ($5,339,914.40) must be passed through to local government entities and up to 20% ($1,334,978.60) can be used for state projects. Please note that state agencies and state funded higher education institutions fall in the latter category, which makes that pool of

funding highly competitive. It is suggested that these applicants submit as early as feasible as applications will be reviewed in batches and funding is limited.

Period of Performance

The period of performance for the FY 2023 SLCGP is December 1, 2023, through November 30, 2027. All project work must be completed before the end of the POP.

Sub-recipient requirements

- All sub-recipients are required to participate in certain free services provided by CISA. These are not required for submission and approval but are a post-award requirement.

    1. **Cyber Hygiene Services** – Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static Internet Protocols for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts. To register for this service, email vulnerability@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 SLCGP. For more information, visit CISA's Cyber Hygiene Information Page.

    2. **Nationwide Cybersecurity Review** – 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 NIST Cybersecurity Framework and is sponsored by DHS and MS-ISAC. Eligible entities and their subrecipients are required to 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 (www.cisecurity.org/ms-isac/services/ncsr).

    3. **Membership in MS-ISAC and/or EI-ISAC** – The Multi-State Information Sharing and Analysis Center, 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 (www.cisecurity.org). The EI-ISAC is a collaborative partnership between the Center for Internet Security (CIS), CISA, and the Election Infrastructure Subsector 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.

- Each application will require the submission of a Cybersecurity Mini Risk Assessment which will give a baseline understanding of the status of the cybersecurity measures in use by the organization.

    1. The grant review committee will not share these assessments outside of anyone with a valid need-to-know as part of the grant application review, award, and management.
    2. The committee will review these assessments to determine correlation with grant request.
    3. If the committee deems the submitted assessment to be insufficient, an initial award will be made to fund an assessment through a state-contracted provider. Completion of the assessment will be required prior to funding other projects.

Application Process

FY 2023 grant materials will be available through multiple channels including the WV Cyber Grant website and the grants tab of the WV Emergency Management Division website. The grant materials can also be requested by emailing HSSAA@wv.gov.

The application package consists of four documents:

- FY 2023 SLCGP Grant Guidance for the State of West Virginia (this document)
- FY 2023 SLCGP Application – Fillable PDF
- FY 2023 SLCGP Application Instructions
- Mini Risk Assessment Checklist Form

The deadline to submit applications will be April 30, 2025. To expedite the application review and awards, the grant review committee will pull the applications submitted by December 27, 2024, and February 21, 2025, into batches for review. Groups of recommended awards will be sent to FEMA and CISA for approval incrementally so that approved projects can begin prior to the deadline date, as applicable.

Completed applications, and all attachments, should be submitted via email address wvcybergrant@wv.gov.

Performance Measures

As with any federal grant program, there are certain metrics that FEMA/CISA are monitoring to ensure the program is successfully meeting the original intent set forth by Congress. For perspective, here are the Performance Measures for the SLCGP.

Number of satisfactory annual tabletop and full-scale exercises to test Cybersecurity Plans.
The amount of grant funds budgeted for cybersecurity exercises.
Percentage of grant funds expended on exercise plans for entities.
Number of annual cyber risk assessments conducted to identify cyber risk management gaps and areas for improvement.
Number of employees that successfully completed phishing training.
The number of employees that attended and successfully completed awareness campaign training.
Number of employees that received role-based cybersecurity awareness training.
The number of employees completed continuous learning activities on current cyber threats.
Number of employees that completed education or training on software security concepts.[1]
The number of supporting capabilities implemented to analyze network traffic and activities related to potential threats.
Number of multi-factor authentication (MFA) instances that were implemented for all remote access and privileged accounts.
Number of supporting programs created to anticipate and discontinue end-of-life software and hardware.
Number of known/fixed/default passwords and credentials prohibited for use on networks.
Number of unique sites that transitioned to a .gov internet domain.
Number of CISA-identified cybersecurity vulnerabilities that were addressed.
Number of Endpoint Detection Response Systems that were funded for implementation.
The number of capabilities ratings improved.
Number of funding improvements that were made for Continuity of Operations Plans.
Number of SAA performance metrics that were met.
Percent of increase in the use of CISA Services.
Numbers of instances of increased use of Data Encryption.
Numbers of instances of increased use of Enhanced Logging.
Numbers of systems adopting System Reconstitution.
Percentage of increase in membership in the Multi-State Information Sharing and Analysis Center (MS-ISAC).