

97.137

**STATE & LOCAL CYBERSECURITY GRANT PROGRAM  
(SLCGP)**

**State Project/Program**

**STATE & LOCAL CYBERSECURITY GRANT PROGRAM  
(SLCGP)**

**U.S. Department of Homeland Security (DHS)  
Federal Emergency Management Agency (FEMA)**

**Federal Authorization:** Section 2220A of the Homeland Security Act of 2002, as amended  
(Pub. L. No.107-296) (6 U.S.C. § 665g); Infrastructure  
Investment and Jobs Act (Pub. L. No. 117-58, Division J, Title V).

**State Authorization:** North Carolina Department of Public Safety (NCDPS)  
North Carolina Emergency Management (NCEM)

**Agency Contact Person – Program**

William Ray, Director  
NC Division of Emergency Management 1636  
Gold Star Drive  
Raleigh, NC 27607  
Phone: (919) 825-2307  
[William.Ray@ncdps.gov](mailto:William.Ray@ncdps.gov)

**Address Confirmation Letters To:**

Donnie Tim, CICA  
NCDPS Controller's Office 2000  
Yonkers Road  
Raleigh, NC 27604  
(919) 324-1077  
[Donnie.tim@ncdps.gov](mailto:Donnie.tim@ncdps.gov)

**Agency Contact Person – Financial**

Donnie Tim, CICA  
NCDPS Controller's Office 2000 Yonkers  
Road  
Raleigh, NC 27604  
(919) 324-1077  
[Donnie.tim@ncdps.gov](mailto:Donnie.tim@ncdps.gov)

The auditor should not consider the Supplement to be “safe harbor” for identifying audit procedures to apply in a particular engagement, but the auditor should be prepared to justify departures from the suggested procedures. The auditor can consider the supplement a “safe harbor” for identification of compliance requirements to be tested if the auditor performs reasonable procedures to ensure that the requirements in the Supplement are current.

The grantor agency may elect to review audit working papers to determine that audit tests are adequate.

**Auditors may request documentation of monitoring visits by the State Agencies.**

This State compliance supplement must be used in conjunction with the OMB 2025 Compliance Supplement which is scheduled to be issued in May 2025. The OMB supplement will include “Part 3 - Compliance Requirements,” for the types that apply, and “Part 6 - Internal Control.” If a federal Agency issued guidance for a specific program, this will be included in “Part 4 - Agency Program”. The OMB Compliance Supplement is Section A of the State Compliance Supplement.

## **STATE & LOCAL CYBERSECURITY GRANT PROGRAM**

---

### **I. PROGRAM OBJECTIVES**

State & Local Cybersecurity Grant is issued by: Strengthening cybersecurity practices and resilience of state, local, and territorial (SLT) governments is an important homeland security mission and the primary focus of the State and Local Cybersecurity Grant Program (SLCGP). Through funding from Infrastructure Investment and Jobs Act (IIJA), the SLCGP enables DHS to make targeted cybersecurity investments in SLT government agencies, thus improving the security of critical infrastructure and improving the resilience of the services SLT governments provide their communities.

### **II. PROGRAM PROCEDURES**

Development of the SLCGP project application in North Carolina is a three-phased process. The first phase is subrecipient application development and submission to North Carolina Dept. of Public Safety (NCDPS) / North Carolina Emergency Management (NCEM). The second phase is application review and approval by the State Cybersecurity Planning Committee. The third and final phase is the development of the SLCGP via the FEMA Project Worksheet (PW), Investment Justification (IJ). This includes combining all approved applications for submission to the U.S. Department of Homeland Security (DHS) / Federal Emergency Management Agency (FEMA).

Applications are reviewed to ensure compliance with grant program guidance. Throughout the application phase funding allocations are reviewed and approved by NCEM Staff, the State Cybersecurity Planning Committee, and the Homeland Security Advisor (HSA) or designee. Subject Matter Experts (SMEs) also assist with eligibility by reviewing specific applications that relate to their area of expertise.

With the approval of the State Cybersecurity Committee and the HSA, applications proceed to the PW/ IJ development phase of the SLCGP process. During the PW/IJ phase Grants Management Branch staff divide all applications into investment categories that align with the appropriate objectives and elements as determined by DHS/FEMA. Once approved application information is incorporated into the final PW/IJ and all investment categories are completed, the state's SLCGP application is ready for submission to DHS/FEMA. DHS/FEMA receives the state application and approves the grant awards through a web- based grant award notification system. The HSA has the final approval or denial of all SLCGP project proposals. The HSA will also determine any reallocation of funding among the projects as necessary.

NCPDS/NCEM serves as the pass-through entity awarding the SLCGP funds from DHS/FEMA to the subrecipients to complete approved projects. Subrecipients of SLCGP awards receive an award letter

from NCDPS/NCEM specifying the approved project(s), the total amount of the subaward, and the designated period of performance. Subrecipients accepting awards are required to execute a Memorandum of Agreement (MOA) with NCDPS/NCEM detailing the terms, conditions, requirements, and responsibilities of the subaward, including the approved scope of work to be completed by the subrecipient with the funds. Via the MOA, the 45-day obligation is met. The MOA serves as the grant agreement between NCDPS/NCEM and the subrecipient.

No funds are advanced to subrecipients for SLCGP, as NCEM Preparedness Grants are reimbursement based. Subrecipients are required to submit periodic reports and requests for reimbursement of eligible expenditures with all required supporting documentation to receive funds. As specified in the MOA executed by each subrecipient, indirect costs are not authorized for SLCGP.

## STATE & LOCAL CYBERSECURITY GRANT PROGRAM

Auditors should review the award letter and MOA for each subrecipient. Auditors should refer to the applicable SLCGP Notice of Funding Opportunity (NOFO) for the year of the award ([State and Local Cybersecurity Grant Program | FEMA.gov](#)), the FEMA Preparedness Grants Manual [Preparedness Grants Manual | FEMA.gov](#), and applicable FEMA Grant Programs Directorate Information Bulletins ([Grant Programs Directorate Information Bulletins | FEMA.gov](#)) for more detailed information about SLCGP.

Refer to the NCDPS/NCEM website [State and Local Cybersecurity Grant Program | NC DPS](#) for more detailed information on how SLCGP is implemented in the state of NC, including subrecipient application procedures, compliance forms for use, and grants management training videos.

### III. COMPLIANCE REQUIREMENTS

Noted below in the following matrix are the types of compliance requirements (Types) that are applicable to the federal program. These Types are either determined by the federal agency or the State Agency may have added the Type. This is noted by “Y.” If the State determines that the federal requirement does not apply at the local level or if the State modifies the federal requirements, this is discussed in the supplement under the type of compliance requirement. If the federal and/or State agencies have determined that the type is not applicable, this is indicated by “N.”

If the Type is applicable, the auditor must determine if the Type has a direct and material effect on the federal program for the auditee. The auditor must use the OMB 2025 Compliance Supplement, Part 3 and Part 4 (if an OMB supplement is issued) in addition to this State supplement to perform the audit.

A	B	C	E	F	G	H	I	J	L	M	N
Activities Allowed or Unallowed	Allowable Costs/Cost Principles	Cash Management	Eligibility	Equipment/ Real Property Management	Matching, Level of Effort, Earmarking	Period Of Performance	Procurement Suspension & Debarment	Program Income	Reporting	Subrecipient Monitoring	Special Tests and Provisions
Y	Y	N	N	Y	Y	Y	Y	N	Y	N	N

#### A. Activities Allowed or Unallowed

##### Compliance Requirements

Typically, authorized expenditures are for equipment, exercise, training, and planning (and sometimes organizational activities). The following are examples of these categories. Each grant program provides specific expenditure guidance for each category. Refer to the SLCGP application, award letter and MOA/grant agreement for the approved scope of work/project(s) for each subrecipient.

1. Equipment

## STATE & LOCAL CYBERSECURITY GRANT PROGRAM

---

Funds for equipment are to be used to enhance the cybersecurity capabilities. DHS has a detailed authorized equipment list for each grant. Only allowable equipment listed in the [Authorized Equipment List \(AEL\)](#) for SLCGP are eligible for purchases for this grant.

### 2. Exercises

Funds for exercises may be used to plan for, design, develop, conduct, and evaluate exercises that strengthen cybersecurity. It is recommended that exercises should be threat and performance-based, in accordance with the Homeland Security Exercise and Evaluation Program ([HSEEP](#)) manual. This manual provides explicit direction on the design, conduct, and evaluation of exercises.

### 3. Training

Funds for cybersecurity related training may be used to enhance capabilities, awareness and operations of personnel.

### 4. Planning

Funds for planning may be used in planning for cybersecurity or cybersecurity support programs. Planning funds can be used to develop prevention activities, planning to enhance security, conducting education campaigns, and evaluating equipment. Risk and vulnerability assessments fall under this category.

### **Suggested Audit Procedures**

- Review subrecipient's SLCGP application, award letter and MOA/grant agreement for approved scope of work/project(s) and applicable terms, conditions, requirements & responsibilities of subrecipient, and then cross-check against awarded projects.
- Test expenditures and related records for adherence to approved budget activity in each budget category: equipment, exercise, training and planning (and sometimes organizational activities).

## **B. Allowable Costs/Cost Principles**

### **Compliance Requirement**

Only relevant and necessary costs as authorized by the applicable SLCGP Notice of Funding Opportunity (NOFO), application, investment justification, award letter and MOA/grant agreement are allowed, subject to applicable cost principles in 2 CFR 200 Subpart E (Uniform Guidance, Cost Principles). Allowable equipment listed in the [Authorized Equipment List \(AEL\)](#) for SLCGP are eligible for purchases for this grant.

### **Suggested Audit Procedures**

1. Review SLCGP application, award letter and MOA/grant agreement for approved scope of work/project(s) and applicable terms, conditions, requirements, and responsibilities of subrecipient.
2. Review requests for reimbursement and/or cost reports submitted by subrecipient.
3. Test expenditures and related records for adherence to approved budget and cost principles of 2 CFR 200 for local government.
4. Verify costs did not consist of improper payments, including (1) payments that should not have been made or that were made in incorrect amounts (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements; (2) payments that do not account for credit for applicable discounts; (3) duplicate payments; (4) payments that were made to an ineligible party or for an ineligible good or service; and (5) payments for goods or services not received

## STATE & LOCAL CYBERSECURITY GRANT PROGRAM

---

(except for such payments where authorized by law).

5. Review and test the expenditures and reports to ascertain total cost of project and verify that they are eligible. Verify costs were adequately documented.
6. Verify costs were not included as a cost of any other federally financed program, in either the current or a prior period.
7. Verify costs were not used to meet the cost-sharing or matching requirements of another federal program, except where authorized by federal statute.

### **C. Cash Management**

Funds are paid to subrecipients on a reimbursement basis. No funds are advanced to subrecipients for SLCGP.

### **D. Reserve**

### **F. Equipment and Real Property Management Compliance Requirement**

While this compliance requirement is not listed for SLCGP in the OMB Compliance Supplement Part 2 federal matrix, NCDPS/NCCEM has added it because equipment can be (and often is) purchased with SLCGP funds. "Equipment" means tangible personal property, including information technology systems, having a useful life of more than one year and a per-unit acquisition cost which equals or exceeds the lesser of the capitalization level established by the non-federal entity for financial statement purposes or \$10,000. The subrecipient has sole responsibility for the maintenance, insurance, upkeep, and replacement of any property and equipment purchased with SLCGP funds as specified in the MOA/grant agreement executed by each subrecipient.

#### **Suggested Audit Procedures**

##### **Inventory Management of Equipment Acquired Under SLCGP Awards**

1. Identify equipment acquired and trace selected purchases to the property records. Verify that the property records contain the required information.
2. Verify that the required physical inventory of equipment was performed. Test whether any differences between the physical inventory and equipment records were resolved.
3. Select a sample from all equipment acquired under federal awards from the property records and physically inspect the equipment and determine whether the equipment is appropriately safeguarded and maintained.

### **G. Matching, Level of Effort, Earmarking**

There is a matching requirement with SLCGP. FY22 DHS/FEMA funded 90% of the eligible costs of each project and the required 10% match was provided by the state on behalf of the local. FY23 DHS/FEMA funded 80% of the eligible costs of each project and the required 20% match was provided by the state on behalf of the local. FY24 SLCGP the state will not be providing the match for the local.

### **H. Period of Performance**

The period of performance for each SLCGP award is generally 3 years. That means an SLCGP grant awarded by the federal government to NCDPS/NCCEM on behalf of the state in 2024 closes three years later in 2027, effectively providing three years to spend the money awarded in 2024. If/when another federal SLCGP grant is awarded to NCDPS/NCCEM in 2025, that grant will close in 2028. This creates a loop of overlapping federal SLCGP grants that must be carefully managed by NCDPS/NCCEM.

When NCDPS/NCEM subawards these funds, the specific period of performance for each subrecipient is specified in the award letter and MOA/grant agreement. It is not uncommon for subrecipients to receive SLCGP awards in different or even consecutive years. For example, a subrecipient may receive an SLCGP award in 2023 with a period of performance ending in 2026, and the same subrecipient may receive another SLCGP award in 2024 with a period of performance ending in 2027. The award letter and MOA/grant agreement for each year's SLCGP award should be separately reviewed to determine the specific period of performance for each award.

### **Suggested Audit Procedures**

Verify that the funds were encumbered within the period of performance for each subrecipient. Verify existence of sufficient documentation from NCDPS/NCEM authorizing any period of performance extensions claimed by subrecipient. If a subrecipient has received multiple SLCGP awards across different or consecutive years, the award letter and MOA/grant agreement for each year's SLCGP award should be separately reviewed to determine the specific period of performance for each award.

### **I. Procurement and Suspension and Debarment**

Procurement and suspension/debarment requirements are detailed in the MOA/grant agreement executed by each subrecipient.

#### **Procurement**

For procurement with SLCGP funds, [state agencies are generally required to follow state of NC procurement policies and procedures](#), plus a few additional federal requirements when purchasing goods and services with federal grant funds. [Local governments and non-profit organizations that receive grant funding through NCDPS/NCEM are generally required to follow the most restrictive of all federal, state of NC, and their own local procurement policies and procedures](#) that allows for compliance with all applicable layers (federal, state & their own).

Subrecipients are also prohibited from procurement, contracting and/or sub-granting with any entity listed on the [Suspension of Funding List](#) (SOFL) maintained by the State Office of State Budget Management (OSBM).

#### **Suggested Audit Procedures**

1. Review subrecipient's procurement policies and verify that the policies comply with applicable federal and state requirements if subrecipient has purchased goods or services with SLCGP funds
2. Verify that subrecipient has written standards of conduct that cover conflicts of interest and govern the performance of its employees engaged in the selection, award, and administration of contracts (2 CFR 200.318(c) and 48 CFR 52.203-13 and 52.303-16).
3. Ascertain if subrecipient has a policy to use statutorily or administratively imposed in-state or local geographical preferences in the evaluation of bids or proposals. If yes, verify that these limitations were not applied to federally funded procurements except where applicable federal statutes expressly mandate or encourage geographic preference (2 CFR 200.319(c)).
4. Select a sample of procurements and perform the following procedures:
  - a. Examine contract files and verify that they document the history of the procurement, including the rationale for the method of procurement, selection of contract type, basis for contractor selection, and the basis for the contract price (2

## STATE & LOCAL CYBERSECURITY GRANT PROGRAM

---

CFR 200.318(i) and 48 CFR Part 44 and section 52.244-2).

- b. Verify that the procurement method used was appropriate based on the dollar amount and conditions specified in 2 CFR section 200.320. Current micro-purchase and simplified acquisition thresholds can be found in the FAR (48 CFR Subpart 2.1, "Definitions").
- c. Verify that procurements provide full and open competition (2 CFR 200.319 and 48 CFR 52.244-5).
- d. Examine documentation in support of the rationale to limit competition in those cases where competition was limited and ascertain if the limitation was justified (2 CFR sections 200.319 and 200.320(f) and 48 CFR 52.244-5).
- e. Ascertain if cost or price analysis was performed in connection with all procurement actions exceeding the simplified acquisition threshold, including contract modifications, and that this analysis supported the procurement action (2 CFR 200.323 and 48 CFR 15.404-3).

Note: A cost or price analysis is required for each procurement action, including each contract modification, when the total amount of the contract and related modifications is greater than the simplified acquisition threshold.

- f. Verify consent to subcontract was obtained when required by the terms and conditions of a cost reimbursement contract under the FAR (48 CFR 52.244-2).

Note: If the non-federal entity has an approved purchasing system, consent to subcontract may not be required unless specifically identified by contract terms or conditions. The auditor should verify that the approval of the purchasing system is effective for the audit period being reviewed.

5. Review the non-federal entity's procedures for verifying that an entity with which it plans to enter into a covered transaction is not debarred, suspended, or otherwise excluded (2 CFR sections 200.212 and 200.318(h); 2 CFR 180.300; 48 CFR 52.2096).
6. Select a sample of procurements and subawards and test whether the non-federal entity followed its procedures before entering into a covered transaction.

### L. Reporting

#### Compliance Requirement

Subrecipients are required to submit various financial and programmatic reports as a condition of their award acceptance. Reporting requirements are detailed in the MOA/grant agreement executed by each subrecipient.

SLCGP subrecipients were required to provide annual progress reports to NCDPS/NCEM by the due by 7/31 each year for the state FY. For example, the annual report for the period 7/1/24 – 6/30/25 (state FY24/25) is due 7/31/25. This has been waived for the 7/31/25 due annual report due to Hurricane Helene. The Nationwide Cybersecurity Review (NCSR) has also been waived by FEMA.

Subrecipients must generally submit requests for reimbursement to NCDPS/NCEM with all required documentation attached within 60 days of payment of invoice. Required documentation includes evidence that funds have been invoiced, goods or services received (e.g., invoices, contracts, itemized expenses, etc.) and proof of payment that the subrecipient in fact paid for the goods or services.

### Closeout Reporting Requirements

In accordance with [2 CFR 200.344](#), subrecipients must submit to NCDPS/NCEM, no later than 30 calendar days after the end date of the period of performance, all financial, performance, and other reports as required by the terms and conditions of the federal award and the MOA/grant agreement. This includes all final cost reports/requests for reimbursement submitted by subrecipient to NCDPS/NCEM, as requests submitted beyond 30 days after the end date of the period of performance may not be processed for payment by NCDPS/ NCEM.

The federal regulations provide up to 90 days after the end date of the period of performance for subrecipients to submit all final reports to the pass-through entity, unless the pass-through entity specifies a shorter period. NCDPS/NCEM only provides 30 days from the end of the period of performance for subrecipients to submit all final reports to NCDPS/NCEM.

1. Review application, award letter and MOA/grant agreement for reporting requirements and approved scope of work/project(s).
2. Verify that reports submitted by subrecipient (including cost reports and requests for reimbursement) have adequate supporting documentation, that funds were expended as represented by subrecipient, and that all required authorizations/approvals were obtained by subrecipient.
3. Verify that goods and services for which subrecipient was reimbursed by NCDPS/NCEM were in fact obtained/completed in accordance with the approved scope of work/project(s) specified in the SLCGP application, award letter and MOA/grant agreement.

### **M. Subrecipient Monitoring Compliance Requirement**

While this compliance requirement is listed for SLCGP in the OMB Compliance Supplement Part 2 federal matrix, it is only applicable to NCDPS/NCEM itself as the recipient of the SLCGP award from DHS/FEMA on behalf of the state of North Carolina. It is not applicable to any subrecipients that NCDPS/NCEM subawards SLCGP funds to in execution of the award.

NCDPS/NCEM serves as the pass-through entity awarding the SLCGP funds from DHS/FEMA to the subrecipients to complete approved projects. The subrecipients generally do not further subgrant the funds to other entities. If they do, they are required to transfer all funds awarded to them to the designated third-party entity, and the third-party entity is required to assume entire responsibility for all terms, conditions, requirements, and responsibilities of the award. The subrecipient has no responsibility to monitor the third-party entity in that case.

NCDPS/NCEM monitors subrecipients in accordance with the provisions of 2 CFR 200.332. These provisions are detailed in the MOA/grant agreement that NCDPS/NCEM executes with each subrecipient. Audits of subrecipients required under federal and state law are an important component of the NCDPS/NCEM subrecipient monitoring program.