City Council Meeting - Final

October 21, 2024
7:00 PM

D. **ATH2024-161** Approval and acceptance of the 2022 State and Local Cybersecurity Grant Program award to create a 5-year cybersecurity plan, incident response plan, and provide cybersecurity training to staff as awarded by the Georgia Emergency Management and Homeland Security Agency, authorize the City match of 10% of the total award ($6,965.00) to be funded from IT Professional Services line item and authorize the Mayor to sign and execute all related documents.

City of Smyrna

Issue Sheet

A Max Bacon
City Hall
2800 King Street
Smyrna, GA 30080

File Number: ATH2024-161

Agenda Date: 10/21/2024

In Control: City Council

File Type: Authorization

Agenda Section:
Formal Business

Department: Information Systems

Agenda Title:

Approval and acceptance of the 2022 State and Local Cybersecurity Grant Program award to create a 5-year cybersecurity plan, incident response plan, and provide cybersecurity training to staff as awarded by the Georgia Emergency Management and Homeland Security Agency, authorize the City match of 10% of the total award ($6,965.00) to be funded from IT Professional Services line item and authorize the Mayor to sign and execute all related documents.

Citywide

ISSUE AND BACKGROUND:

Two years ago, the Smyrna IT Department applied for the 2022 State and Local Cybersecurity Grant to create a high overview five-year cybersecurity plan for the city. That plan would include a cybersecurity assessment, a roadmap of new cybersecurity improvements, incident response plan, table talk exercises, and cybersecurity training for staff. This grant is funded through the Infrastructure Investment and Jobs Act, also known as the Bipartisan Infrastructure Law, and will be managed by the Georgia Emergency Management and Homeland Security Agency (GEMA/HS). GEMA/HS is awarding the city with $69,650 with a required 10% cost share match in the amount of $6,965.00.

RECOMMENDATION / REQUESTED ACTION:

IT and Purchasing recommend approval and acceptance of the 2022 State and Local Cybersecurity Grant Program award to create a 5-year cybersecurity plan, incident response plan, and provide cybersecurity training to staff as awarded by the Georgia Emergency Management and Homeland Security Agency, authorize the City match of 10% of the total award ($6,965.00) to be funded from IT Professional Services line item and authorize the Mayor to sign and execute all related documents.

OMB Approval No. 0348-0040

ASSURANCES - NON-CONSTRUCTION PROGRAMS

Public reporting burden for this collection of information is estimated to average 15 minutes per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the Office of Management and Budget, Paperwork Reduction Project (0348-0040), Washington, DC 20503.

PLEASE DO NOT RETURN YOUR COMPLETED FORM TO THE OFFICE OF MANAGEMENT AND BUDGET. SEND IT TO THE ADDRESS PROVIDED BY THE SPONSORING AGENCY.

NOTE: Certain of these assurances may not be applicable to your project or program. If you have questions, please contact the awarding agency. Further, certain Federal awarding agencies may require applicants to certify to additional assurances. If such is the case, you will be notified.

As the duly authorized representative of the applicant, I certify that the applicant:

1. Has the legal authority to apply for Federal assistance and the institutional, managerial and financial capability (including funds sufficient to pay the non-Federal share of project cost) to ensure proper planning, management and completion of the project described in this application.

2. Will give the awarding agency, the Comptroller General of the United States and, if appropriate, the State, through any authorized representative, access to and the right to examine all records, books, papers, or documents related to the award; and will establish a proper accounting system in accordance with generally accepted accounting standards or agency directives.

3. Will establish safeguards to prohibit employees from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain.

4. Will initiate and complete the work within the applicable time frame after receipt of approval of the awarding agency.

5. Will comply with the Intergovernmental Personnel Act of 1970 (42 U.S.C. §§4728-4763) relating to prescribed standards for merit systems for programs funded under one of the 19 statutes or regulations specified in Appendix A of OPM's Standards for a Merit System of Personnel Administration (5 C.F.R. 900, Subpart F).

6. Will comply with all Federal statutes relating to nondiscrimination. These include but are not limited to: (a) Title VI of the Civil Rights Act of 1964 (P.L. 88-352) which prohibits discrimination on the basis of race, color or national origin; (b) Title IX of the Education Amendments of 1972, as amended (20 U.S.C. §§1681-1683, and 1685-1686), which prohibits discrimination on the basis of sex; (c) Section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. §794), which prohibits discrimination on the basis of handicaps; (d) the Age Discrimination Act of 1975, as amended (42 U.S.C. §§6101-6107), which prohibits discrimination on the basis of age; (e) the Drug Abuse Office and Treatment Act of 1972 (P.L. 92-255), as amended, relating to nondiscrimination on the basis of drug abuse; (f) the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970 (P.L. 91-616), as amended, relating to nondiscrimination on the basis of alcohol abuse or alcoholism; (g) §§523 and 527 of the Public Health Service Act of 1912 (42 U.S.C. §§290 dd-3 and 290 ee-3), as amended, relating to confidentiality of alcohol and drug abuse patient records; (h) Title VIII of the Civil Rights Act of 1968 (42 U.S.C. §§3601 et seq.), as amended, relating to nondiscrimination in the sale, rental or financing of housing; (i) any other nondiscrimination provisions in the specific statute(s) under which application for Federal assistance is being made; and, (j) the requirements of any other nondiscrimination statute(s) which may apply to the application.

7. Will comply, or has already complied, with the requirements of Titles II and III of the Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970 (P.L. 91-646) which provide for fair and equitable treatment of persons displaced or whose property is acquired as a result of Federal or federally-assisted programs. These requirements apply to all interests in real property acquired for project purposes regardless of Federal participation in purchases.

8. Will comply, as applicable, with provisions of the Hatch Act (5 U.S.C. §§1501-1508 and 7324-7328) which limit the political activities of employees whose principal employment activities are funded in whole or in part with Federal funds.

9. Will comply, as applicable, with the provisions of the Davis-Bacon Act (40 U.S.C. §§276a to 276a-7), the Copeland Act (40 U.S.C. §276c and 18 U.S.C. §874), and the Contract Work Hours and Safety Standards Act (40 U.S.C. §§327-333), regarding labor standards for federally-assisted construction subagreements.

10. Will comply, if applicable, with flood insurance purchase requirements of Section 102(a) of the Flood Disaster Protection Act of 1973 (P.L. 93-234) which requires recipients in a special flood hazard area to participate in the program and to purchase flood insurance if the total cost of insurable construction and acquisition is $10,000 or more.

11. Will comply with environmental standards which may be prescribed pursuant to the following: (a) institution of environmental quality control measures under the National Environmental Policy Act of 1969 (P.L. 91-190) and Executive Order (EO) 11514; (b) notification of violating facilities pursuant to EO 11738; (c) protection of wetlands pursuant to EO 11990; (d) evaluation of flood hazards in floodplains in accordance with EO 11988; (e) assurance of project consistency with the approved State management program developed under the Coastal Zone Management Act of 1972 (16 U.S.C. §§1451 et seq.); (f) conformity of Federal actions to State (Clean Air) Implementation Plans under Section 176(c) of the Clean Air Act of 1955, as amended (42 U.S.C. §§7401 et seq.); (g) protection of underground sources of drinking water under the Safe Drinking Water Act of 1974, as amended (P.L. 93-523); and, (h) protection of endangered species under the Endangered Species Act of 1973, as amended (P.L. 93-205).

12. Will comply with the Wild and Scenic Rivers Act of 1968 (16 U.S.C. §§1271 et seq.) related to protecting components or potential components of the national wild and scenic rivers system.

13. Will assist the awarding agency in assuring compliance with Section 106 of the National Historic Preservation Act of 1966, as amended (16 U.S.C. §470), EO 11593 (identification and protection of historic properties), and the Archaeological and Historic Preservation Act of 1974 (16 U.S.C. §§469a-1 et seq.).

14. Will comply with P.L. 93-348 regarding the protection of human subjects involved in research, development, and related activities supported by this award of assistance.

15. Will comply with the Laboratory Animal Welfare Act of 1966 (P.L. 89-544, as amended, 7 U.S.C. §§2131 et seq.) pertaining to the care, handling, and treatment of warm blooded animals held for research, teaching, or other activities supported by this award of assistance.

16. Will comply with the Lead-Based Paint Poisoning Prevention Act (42 U.S.C. §§4801 et seq.) which prohibits the use of lead-based paint in construction or rehabilitation of residence structures.

17. Will cause to be performed the required financial and compliance audits in accordance with the Single Audit Act Amendments of 1996 and OMB Circular No. A-133, "Audits of States, Local Governments, and Non-Profit Organizations."

18. Will comply with all applicable requirements of all other Federal laws, executive orders, regulations, and policies governing this program.

SIGNATURE OF AUTHORIZED CERTIFYING OFFICIAL	TITLE

APPLICANT ORGANIZATION	DATE SUBMITTED
	February 2, 2011

SUPPLIER CHANGE REQUEST FORM

Agency Supplier Liaisons MUST complete the Agency Liaison Use Only sections AND ensure the supplier has completed sections 1 - 3, the Supplier Use Only sections prior to submitting this form to SAO.

☐ NEW ☐ EXISTING **SUPPLIER ID NUMBER:** Agency Use Only | 0 | 0 | 0 | 0 | | | | | | |

SECTION 1: SUPPLIER IDENTIFICATION

FEI/SSN/TIN

Supplier Name:

Doing Business As (dba): if applicable

SUPPLIER ADDRESS

Address 1:

Address 2:

City:

State: **Postal Code:**

Contact Email:

Primary Phone #: **Ext:** **Secondary Phone #:** **Ext:**

☐ Landline ☐ Cell Used for Identity Verification ☐ Landline ☐ Cell Used for Identity Verification

Driver's License #: For individuals only **DL State:**

SECTION 2: BANK ACCOUNT INFORMATION

Required for New and Reactivating suppliers to add/change bank information to receive payments via ACH.

☑ I do not wish to provide banking information and understand all payments made to me will be via check.

☐ Replace Remittance Address at Loc # With Addr ID #

☐ Replace Invoicing Address at Loc # With Addr ID #

☐ Add New Bank Account ☐ Change Bank Account Enter Loc # Agency Liaisons are required to complete items on this line for bank changes

ROUTING # **NEW ACCOUNT #**

Last Four Digits of Previous Bank Account # For changes only

☐ Check here if General Bank Account can be used by ALL State of Georgia agencies making payments.

☐ Check here if this account can only be used for a SPECIFIC PURPOSE

DESCRIBE SPECIFIC PURPOSE

ACCOUNTS RECEIVABLE NOTIFICATION

PAYMENT REMIT EMAIL ADDRESS 1:

PAYMENT REMIT EMAIL ADDRESS 2:

I authorize the State of Georgia to deposit payment for goods and/or services received into the provided bank account by the Automated Clearing House (ACH). I further acknowledge that this agreement is to remain in full effect until such time as changes to the bank account information are submitted in writing by the vendor or individual named below. It is the sole responsibility of the vendor or individual to notify the State of Georgia of any changes to the bank account information. The State of Georgia independently authenticates bank account ownership.

Printed Name of Company Officer **Signature of Company Officer** **Date**

SECTION 3: DIVERSITY IDENTIFICATION (Check ALL That Apply)

BUSINESS CERTIFICATIONS

- ☐ GA Small Business*
- ☐ GA Resident Business**
- ☐ Not Applicable
- ☐ Women Owned
- ☐ Minority Business Certified
- ☐ Prefer Not to Disclose

MINORITY BUSINESS ENTERPRISE (51% ownership)

- ☐ Hispanic – Latino
- ☐ Native American
- ☐ Pacific Islander
- ☐ Prefer Not to Disclose
- ☐ African American
- ☐ Asian American
- ☐ Not Applicable

*Based on Georgia law (OCGA 50-5-21) (3) **"Small Business** " means any business which is independently owned and operated. Additionally, such business must either have 300 or less employees OR $30 million or less in gross receipts per year.

****Georgia resident business** is defined as any business that regularly maintains a place from which business is physically conducted in Georgia for at least one year prior to any bid or proposal to the state or a new business that is domiciled in Georgia and which regularly maintains a place from which business is physically conducted in Georgia; provided, however, that a place from which business is conducted shall not include a post office box, a leased private mailbox, site trailer, or temporary structure.

VETERAN-OWNED SMALL BUSINESS (Check ALL That Apply)

☐ Nonveteran-owned Small Business ☐ Veteran-owned Small Business ☐ Service Disabled VOSB ☐ Prefer Not to Disclose

SECTION 4: REQUESTED CHANGE(S) – (Check ALL That Apply)

- ☐ **FEI/TIN Change** (Cannot change if supplier is 1099 applicable)
- ☐ **Business Name Change**
- ☐ **1099 Eligible** Cannot change to non-eligible if supplier is already 1099 eligible
  - **1099 Addr ID #** Agency Liaisons are REQUIRED to enter the AddrID # where to mail 1099 ☐
  - ☐ **1099 – M Enter Code (Required for Form 1099 – M)** ☐
  - ☐ **1099 – N** **Code 01** (01 is the only code available for the 1099 – NEC)
- ☐ **Reactivate Supplier Profile**
- ☐ **Deactivate Supplier Profile** (Agency Liaison MUST attach written justification from the supplier with the SCR.)
- ☐ **Add Additional Business Address** (Enter additional address in Section 1)
- ☐ **Change Existing Business Address** **Enter Addr ID # to change:** ☐ (Agency Liaisons are required to enter Addr ID # to change)
  - ☐ **Change/Add Payment Alt Name to an existing address** (if payable to a different name).
    - **Payment Alt Name:** ☐
- ☐ **Classification Change:** (Agency Liaisons are required to check one for Classification Changes.)
  - ☐ **Attorney** ☐ **HCM** ☐ **Student** ☐ **Supplier Non-minority**
  - ☐ **Gov Non-State of GA** ☐ **Non-Supplier** ☐ **Supplier Minority**
- ☐ **Statewide Contract** (DOAS Use Only)
- ☐ **HCM Vendor**
- ☐ **Other** (Provided details in the Comments section below)
- ☐ **Comments**

☐

AGENCY USE ONLY SECTION 5: AGENCY LIAISON CERTIFICATION (REQUIRED)

By my signature below, I certify that all reasonable effort has been made to submit information that is complete, accurate, true, and is associated with the supplier's name and Tax ID listed above.

AGENCY LIAISON NAME	AGENCY LIAISON SIGNATURE	DATE	B/U#

Revised 12/2023

PRINT CLEAR

Form **W-9**
(Rev. March 2024)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

Go to *www.irs.gov/FormW9* for instructions and the latest information.

Give form to the requester. Do not send to the IRS.

Before you begin. For guidance related to the purpose of Form W-9, see *Purpose of Form*, below.

Print or type. See ***Specific Instructions*** on page 3.

1 Name of entity/individual. An entry is required. (For a sole proprietor or disregarded entity, enter the owner's name on line 1, and enter the business/disregarded entity's name on line 2.)

2 Business name/disregarded entity name, if different from above.

3a Check the appropriate box for federal tax classification of the entity/individual whose name is entered on line 1. Check only **one** of the following seven boxes.

☐ Individual/sole proprietor ☐ C corporation ☐ S corporation ☐ Partnership ☐ Trust/estate

☐ LLC. Enter the tax classification (C = C corporation, S = S corporation, P = Partnership) . . . . .

Note: Check the "LLC" box above and, in the entry space, enter the appropriate code (C, S, or P) for the tax classification of the LLC, unless it is a disregarded entity. A disregarded entity should instead check the appropriate box for the tax classification of its owner.

☐ Other (see instructions)

3b If on line 3a you checked "Partnership" or "Trust/estate," or checked "LLC" and entered "P" as its tax classification, and you are providing this form to a partnership, trust, or estate in which you have an ownership interest, check this box if you have any foreign partners, owners, or beneficiaries. See instructions . . . . . ☐

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any)

Exemption from Foreign Account Tax Compliance Act (FATCA) reporting code (if any)

(Applies to accounts maintained outside the United States.)

5 Address (number, street, and apt. or suite no.). See instructions.

Requester's name and address (optional)

6 City, state, and ZIP code

7 List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Note: If the account is in more than one name, see the instructions for line 1. See also *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number

			–		–				

or

Employer identification number

		–							

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
3. I am a U.S. citizen or other U.S. person (defined below); and
4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and, generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here	**Signature of U.S. person**	**Date**

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to *www.irs.gov/FormW9*.

What's New

Line 3a has been modified to clarify how a disregarded entity completes this line. An LLC that is a disregarded entity should check the appropriate box for the tax classification of its owner. Otherwise, it should check the "LLC" box and enter its appropriate tax classification.

New line 3b has been added to this form. A flow-through entity is required to complete this line to indicate that it has direct or indirect foreign partners, owners, or beneficiaries when it provides the Form W-9 to another flow-through entity in which it has an ownership interest. This change is intended to provide a flow-through entity with information regarding the status of its indirect foreign partners, owners, or beneficiaries, so that it can satisfy any applicable reporting requirements. For example, a partnership that has any indirect foreign partners may be required to complete Schedules K-2 and K-3. See the Partnership Instructions for Schedules K-2 and K-3 (Form 1065).

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS is giving you this form because they

must obtain your correct taxpayer identification number (TIN), which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following.

- Form 1099-INT (interest earned or paid).
- Form 1099-DIV (dividends, including those from stocks or mutual funds).
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds).
- Form 1099-NEC (nonemployee compensation).
- Form 1099-B (stock or mutual fund sales and certain other transactions by brokers).
- Form 1099-S (proceeds from real estate transactions).
- Form 1099-K (merchant card and third-party network transactions).
- Form 1098 (home mortgage interest), 1098-E (student loan interest), and 1098-T (tuition).
- Form 1099-C (canceled debt).
- Form 1099-A (acquisition or abandonment of secured property).

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

Caution: If you don't return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See *What is backup withholding*, later.

By signing the filled-out form, you:

1. Certify that the TIN you are giving is correct (or you are waiting for a number to be issued);

2. Certify that you are not subject to backup withholding; or

3. Claim exemption from backup withholding if you are a U.S. exempt payee; and

4. Certify to your non-foreign status for purposes of withholding under chapter 3 or 4 of the Code (if applicable); and

5. Certify that FATCA code(s) entered on this form (if any) indicating that you are exempt from the FATCA reporting is correct. See *What Is FATCA Reporting*, later, for further information.

Note: If you are a U.S. person and a requester gives you a form other than Form W-9 to request your TIN, you must use the requester's form if it is substantially similar to this Form W-9.

Definition of a U.S. person. For federal tax purposes, you are considered a U.S. person if you are:

- An individual who is a U.S. citizen or U.S. resident alien;
- A partnership, corporation, company, or association created or organized in the United States or under the laws of the United States;
- An estate (other than a foreign estate); or
- A domestic trust (as defined in Regulations section 301.7701-7).

Establishing U.S. status for purposes of chapter 3 and chapter 4 withholding. Payments made to foreign persons, including certain distributions, allocations of income, or transfers of sales proceeds, may be subject to withholding under chapter 3 or chapter 4 of the Code (sections 1441–1474). Under those rules, if a Form W-9 or other certification of non-foreign status has not been received, a withholding agent, transferee, or partnership (payor) generally applies presumption rules that may require the payor to withhold applicable tax from the recipient, owner, transferor, or partner (payee). See Pub. 515, Withholding of Tax on Nonresident Aliens and Foreign Entities.

The following persons must provide Form W-9 to the payor for purposes of establishing its non-foreign status.

- In the case of a disregarded entity with a U.S. owner, the U.S. owner of the disregarded entity and not the disregarded entity.
- In the case of a grantor trust with a U.S. grantor or other U.S. owner, generally, the U.S. grantor or other U.S. owner of the grantor trust and not the grantor trust.
- In the case of a U.S. trust (other than a grantor trust), the U.S. trust and not the beneficiaries of the trust.

See Pub. 515 for more information on providing a Form W-9 or a certification of non-foreign status to avoid withholding.

Foreign person. If you are a foreign person or the U.S. branch of a foreign bank that has elected to be treated as a U.S. person (under Regulations section 1.1441-1(b)(2)(iv) or other applicable section for chapter 3 or 4 purposes), do not use Form W-9. Instead, use the appropriate Form W-8 or Form 8233 (see Pub. 515). If you are a qualified foreign pension fund under Regulations section 1.897(l)-1(d), or a partnership that is wholly owned by qualified foreign pension funds, that is treated as a non-foreign person for purposes of section 1445 withholding, do not use Form W-9. Instead, use Form W-8EXP (or other certification of non-foreign status).

Nonresident alien who becomes a resident alien. Generally, only a nonresident alien individual may use the terms of a tax treaty to reduce or eliminate U.S. tax on certain types of income. However, most tax treaties contain a provision known as a saving clause. Exceptions specified in the saving clause may permit an exemption from tax to continue for certain types of income even after the payee has otherwise become a U.S. resident alien for tax purposes.

If you are a U.S. resident alien who is relying on an exception contained in the saving clause of a tax treaty to claim an exemption from U.S. tax on certain types of income, you must attach a statement to Form W-9 that specifies the following five items.

1. The treaty country. Generally, this must be the same treaty under which you claimed exemption from tax as a nonresident alien.

2. The treaty article addressing the income.

3. The article number (or location) in the tax treaty that contains the saving clause and its exceptions.

4. The type and amount of income that qualifies for the exemption from tax.

5. Sufficient facts to justify the exemption from tax under the terms of the treaty article.

Example. Article 20 of the U.S.-China income tax treaty allows an exemption from tax for scholarship income received by a Chinese student temporarily present in the United States. Under U.S. law, this student will become a resident alien for tax purposes if their stay in the United States exceeds 5 calendar years. However, paragraph 2 of the first Protocol to the U.S.-China treaty (dated April 30, 1984) allows the provisions of Article 20 to continue to apply even after the Chinese student becomes a resident alien of the United States. A Chinese student who qualifies for this exception (under paragraph 2 of the first Protocol) and is relying on this exception to claim an exemption from tax on their scholarship or fellowship income would attach to Form W-9 a statement that includes the information described above to support that exemption.

If you are a nonresident alien or a foreign entity, give the requester the appropriate completed Form W-8 or Form 8233.

Backup Withholding

What is backup withholding? Persons making certain payments to you must under certain conditions withhold and pay to the IRS 24% of such payments. This is called "backup withholding." Payments that may be subject to backup withholding include, but are not limited to, interest, tax-exempt interest, dividends, broker and barter exchange transactions, rents, royalties, nonemployee pay, payments made in settlement of payment card and third-party network transactions, and certain payments from fishing boat operators. Real estate transactions are not subject to backup withholding.

You will not be subject to backup withholding on payments you receive if you give the requester your correct TIN, make the proper certifications, and report all your taxable interest and dividends on your tax return.

Payments you receive will be subject to backup withholding if:

1. You do not furnish your TIN to the requester;

2. You do not certify your TIN when required (see the instructions for Part II for details);

3. The IRS tells the requester that you furnished an incorrect TIN;

4. The IRS tells you that you are subject to backup withholding because you did not report all your interest and dividends on your tax return (for reportable interest and dividends only); or

5. You do not certify to the requester that you are not subject to backup withholding, as described in item 4 under "*By signing the filled-out form*" above (for reportable interest and dividend accounts opened after 1983 only).

Certain payees and payments are exempt from backup withholding. See *Exempt payee code*, later, and the separate Instructions for the Requester of Form W-9 for more information.

See also *Establishing U.S. status for purposes of chapter 3 and chapter 4 withholding*, earlier.

What Is FATCA Reporting?

The Foreign Account Tax Compliance Act (FATCA) requires a participating foreign financial institution to report all U.S. account holders that are specified U.S. persons. Certain payees are exempt from FATCA reporting. See *Exemption from FATCA reporting code*, later, and the Instructions for the Requester of Form W-9 for more information.

Updating Your Information

You must provide updated information to any person to whom you claimed to be an exempt payee if you are no longer an exempt payee and anticipate receiving reportable payments in the future from this person. For example, you may need to provide updated information if you are a C corporation that elects to be an S corporation, or if you are no longer tax exempt. In addition, you must furnish a new Form W-9 if the name or TIN changes for the account, for example, if the grantor of a grantor trust dies.

Penalties

Failure to furnish TIN. If you fail to furnish your correct TIN to a requester, you are subject to a penalty of $50 for each such failure unless your failure is due to reasonable cause and not to willful neglect.

Civil penalty for false information with respect to withholding. If you make a false statement with no reasonable basis that results in no backup withholding, you are subject to a $500 penalty.

Criminal penalty for falsifying information. Willfully falsifying certifications or affirmations may subject you to criminal penalties including fines and/or imprisonment.

Misuse of TINs. If the requester discloses or uses TINs in violation of federal law, the requester may be subject to civil and criminal penalties.

Specific Instructions

Line 1

You must enter one of the following on this line; **do not** leave this line blank. The name should match the name on your tax return.

If this Form W-9 is for a joint account (other than an account maintained by a foreign financial institution (FFI)), list first, and then circle, the name of the person or entity whose number you entered in Part I of Form W-9. If you are providing Form W-9 to an FFI to document a joint account, each holder of the account that is a U.S. person must provide a Form W-9.

• **Individual.** Generally, enter the name shown on your tax return. If you have changed your last name without informing the Social Security Administration (SSA) of the name change, enter your first name, the last name as shown on your social security card, and your new last name.

Note for ITIN applicant: Enter your individual name as it was entered on your Form W-7 application, line 1a. This should also be the same as the name you entered on the Form 1040 you filed with your application.

• **Sole proprietor.** Enter your individual name as shown on your Form 1040 on line 1. Enter your business, trade, or "doing business as" (DBA) name on line 2.

• **Partnership, C corporation, S corporation, or LLC, other than a disregarded entity.** Enter the entity's name as shown on the entity's tax return on line 1 and any business, trade, or DBA name on line 2.

• **Other entities.** Enter your name as shown on required U.S. federal tax documents on line 1. This name should match the name shown on the charter or other legal document creating the entity. Enter any business, trade, or DBA name on line 2.

• **Disregarded entity.** In general, a business entity that has a single owner, including an LLC, and is not a corporation, is disregarded as an entity separate from its owner (a disregarded entity). See Regulations section 301.7701-2(c)(2). A disregarded entity should check the appropriate box for the tax classification of its owner. Enter the owner's name on line 1. The name of the owner entered on line 1 should never be a disregarded entity. The name on line 1 should be the name shown on the income tax return on which the income should be reported. For example, if a foreign LLC that is treated as a disregarded entity for U.S. federal tax purposes has a single owner that is a U.S. person, the U.S. owner's name is required to be provided on line 1. If the direct owner of the entity is also a disregarded entity, enter the first owner that is not disregarded for federal tax purposes. Enter the disregarded entity's name on line 2. If the owner of the disregarded entity is a foreign person, the owner must complete an appropriate Form W-8 instead of a Form W-9. This is the case even if the foreign person has a U.S. TIN.

Line 2

If you have a business name, trade name, DBA name, or disregarded entity name, enter it on line 2.

Line 3a

Check the appropriate box on line 3a for the U.S. federal tax classification of the person whose name is entered on line 1. Check only one box on line 3a.

IF the entity/individual on line 1 is a(n) . . .	THEN check the box for . . .
• Corporation	Corporation.
• Individual or • Sole proprietorship	Individual/sole proprietor.
• LLC classified as a partnership for U.S. federal tax purposes or • LLC that has filed Form 8832 or 2553 electing to be taxed as a corporation	Limited liability company and enter the appropriate tax classification: P = Partnership, C = C corporation, or S = S corporation.
• Partnership	Partnership.
• Trust/estate	Trust/estate.

Line 3b

Check this box if you are a partnership (including an LLC classified as a partnership for U.S. federal tax purposes), trust, or estate that has any foreign partners, owners, or beneficiaries, and you are providing this form to a partnership, trust, or estate, in which you have an ownership interest. You must check the box on line 3b if you receive a Form W-8 (or documentary evidence) from any partner, owner, or beneficiary establishing foreign status or if you receive a Form W-9 from any partner, owner, or beneficiary that has checked the box on line 3b.

Note: A partnership that provides a Form W-9 and checks box 3b may be required to complete Schedules K-2 and K-3 (Form 1065). For more information, see the Partnership Instructions for Schedules K-2 and K-3 (Form 1065).

If you are required to complete line 3b but fail to do so, you may not receive the information necessary to file a correct information return with the IRS or furnish a correct payee statement to your partners or beneficiaries. See, for example, sections 6698, 6722, and 6724 for penalties that may apply.

Line 4 Exemptions

If you are exempt from backup withholding and/or FATCA reporting, enter in the appropriate space on line 4 any code(s) that may apply to you.

Exempt payee code.

• Generally, individuals (including sole proprietors) are not exempt from backup withholding.

• Except as provided below, corporations are exempt from backup withholding for certain payments, including interest and dividends.

• Corporations are not exempt from backup withholding for payments made in settlement of payment card or third-party network transactions.

• Corporations are not exempt from backup withholding with respect to attorneys' fees or gross proceeds paid to attorneys, and corporations that provide medical or health care services are not exempt with respect to payments reportable on Form 1099-MISC.

The following codes identify payees that are exempt from backup withholding. Enter the appropriate code in the space on line 4.

1—An organization exempt from tax under section 501(a), any IRA, or a custodial account under section 403(b)(7) if the account satisfies the requirements of section 401(f)(2).

2—The United States or any of its agencies or instrumentalities.

3—A state, the District of Columbia, a U.S. commonwealth or territory, or any of their political subdivisions or instrumentalities.

4—A foreign government or any of its political subdivisions, agencies, or instrumentalities.

5—A corporation.

6—A dealer in securities or commodities required to register in the United States, the District of Columbia, or a U.S. commonwealth or territory.

7—A futures commission merchant registered with the Commodity Futures Trading Commission.

8—A real estate investment trust.

9—An entity registered at all times during the tax year under the Investment Company Act of 1940.

10—A common trust fund operated by a bank under section 584(a).

11—A financial institution as defined under section 581.

12—A middleman known in the investment community as a nominee or custodian.

13—A trust exempt from tax under section 664 or described in section 4947.

The following chart shows types of payments that may be exempt from backup withholding. The chart applies to the exempt payees listed above, 1 through 13.

IF the payment is for . . .	THEN the payment is exempt for . . .
• Interest and dividend payments	All exempt payees except for 7.
• Broker transactions	Exempt payees 1 through 4 and 6 through 11 and all C corporations. S corporations must not enter an exempt payee code because they are exempt only for sales of noncovered securities acquired prior to 2012.
• Barter exchange transactions and patronage dividends	Exempt payees 1 through 4.
• Payments over $600 required to be reported and direct sales over $5,000[1]	Generally, exempt payees 1 through 5.[2]
• Payments made in settlement of payment card or third-party network transactions	Exempt payees 1 through 4.

[1] See Form 1099-MISC, Miscellaneous Information, and its instructions.

[2] However, the following payments made to a corporation and reportable on Form 1099-MISC are not exempt from backup withholding: medical and health care payments, attorneys' fees, gross proceeds paid to an attorney reportable under section 6045(f), and payments for services paid by a federal executive agency.

Exemption from FATCA reporting code. The following codes identify payees that are exempt from reporting under FATCA. These codes apply to persons submitting this form for accounts maintained outside of the United States by certain foreign financial institutions. Therefore, if you are only submitting this form for an account you hold in the United States, you may leave this field blank. Consult with the person requesting this form if you are uncertain if the financial institution is subject to these requirements. A requester may indicate that a code is not required by providing you with a Form W-9 with "Not Applicable" (or any similar indication) entered on the line for a FATCA exemption code.

A—An organization exempt from tax under section 501(a) or any individual retirement plan as defined in section 7701(a)(37).

B—The United States or any of its agencies or instrumentalities.

C—A state, the District of Columbia, a U.S. commonwealth or territory, or any of their political subdivisions or instrumentalities.

D—A corporation the stock of which is regularly traded on one or more established securities markets, as described in Regulations section 1.1472-1(c)(1)(i).

E—A corporation that is a member of the same expanded affiliated group as a corporation described in Regulations section 1.1472-1(c)(1)(i).

F—A dealer in securities, commodities, or derivative financial instruments (including notional principal contracts, futures, forwards, and options) that is registered as such under the laws of the United States or any state.

G—A real estate investment trust.

H—A regulated investment company as defined in section 851 or an entity registered at all times during the tax year under the Investment Company Act of 1940.

I—A common trust fund as defined in section 584(a).

J—A bank as defined in section 581.

K—A broker.

L—A trust exempt from tax under section 664 or described in section 4947(a)(1).

M—A tax-exempt trust under a section 403(b) plan or section 457(g) plan.

Note: You may wish to consult with the financial institution requesting this form to determine whether the FATCA code and/or exempt payee code should be completed.

Line 5

Enter your address (number, street, and apartment or suite number). This is where the requester of this Form W-9 will mail your information returns. If this address differs from the one the requester already has on file, enter "NEW" at the top. If a new address is provided, there is still a chance the old address will be used until the payor changes your address in their records.

Line 6

Enter your city, state, and ZIP code.

Part I. Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. If you are a resident alien and you do not have, and are not eligible to get, an SSN, your TIN is your IRS ITIN. Enter it in the entry space for the Social security number. If you do not have an ITIN, see *How to get a TIN* below.

If you are a sole proprietor and you have an EIN, you may enter either your SSN or EIN.

If you are a single-member LLC that is disregarded as an entity separate from its owner, enter the owner's SSN (or EIN, if the owner has one). If the LLC is classified as a corporation or partnership, enter the entity's EIN.

Note: See *What Name and Number To Give the Requester*, later, for further clarification of name and TIN combinations.

How to get a TIN. If you do not have a TIN, apply for one immediately. To apply for an SSN, get Form SS-5, Application for a Social Security Card, from your local SSA office or get this form online at *www.SSA.gov*. You may also get this form by calling 800-772-1213. Use Form W-7, Application for IRS Individual Taxpayer Identification Number, to apply for an ITIN, or Form SS-4, Application for Employer Identification Number, to apply for an EIN. You can apply for an EIN online by accessing the IRS website at *www.irs.gov/EIN*. Go to *www.irs.gov/Forms* to view, download, or print Form W-7 and/or Form SS-4. Or, you can go to *www.irs.gov/OrderForms* to place an order and have Form W-7 and/or Form SS-4 mailed to you within 15 business days.

If you are asked to complete Form W-9 but do not have a TIN, apply for a TIN and enter "Applied For" in the space for the TIN, sign and date the form, and give it to the requester. For interest and dividend payments, and certain payments made with respect to readily tradable instruments, you will generally have 60 days to get a TIN and give it to the requester before you are subject to backup withholding on payments. The 60-day rule does not apply to other types of payments. You will be subject to backup withholding on all such payments until you provide your TIN to the requester.

Note: Entering "Applied For" means that you have already applied for a TIN or that you intend to apply for one soon. See also *Establishing U.S. status for purposes of chapter 3 and chapter 4 withholding*, earlier, for when you may instead be subject to withholding under chapter 3 or 4 of the Code.

Caution: A disregarded U.S. entity that has a foreign owner must use the appropriate Form W-8.

Part II. Certification

To establish to the withholding agent that you are a U.S. person, or resident alien, sign Form W-9. You may be requested to sign by the withholding agent even if item 1, 4, or 5 below indicates otherwise.

For a joint account, only the person whose TIN is shown in Part I should sign (when required). In the case of a disregarded entity, the person identified on line 1 must sign. Exempt payees, see *Exempt payee code*, earlier.

Signature requirements. Complete the certification as indicated in items 1 through 5 below.

1. Interest, dividend, and barter exchange accounts opened before 1984 and broker accounts considered active during 1983. You must give your correct TIN, but you do not have to sign the certification.

2. Interest, dividend, broker, and barter exchange accounts opened after 1983 and broker accounts considered inactive during 1983. You must sign the certification or backup withholding will apply. If you are subject to backup withholding and you are merely providing your correct TIN to the requester, you must cross out item 2 in the certification before signing the form.

3. Real estate transactions. You must sign the certification. You may cross out item 2 of the certification.

4. Other payments. You must give your correct TIN, but you do not have to sign the certification unless you have been notified that you have previously given an incorrect TIN. "Other payments" include payments made in the course of the requester's trade or business for rents, royalties, goods (other than bills for merchandise), medical and health care services (including payments to corporations), payments to a nonemployee for services, payments made in settlement of payment card and third-party network transactions, payments to certain fishing boat crew members and fishermen, and gross proceeds paid to attorneys (including payments to corporations).

5. Mortgage interest paid by you, acquisition or abandonment of secured property, cancellation of debt, qualified tuition program payments (under section 529), ABLE accounts (under section 529A), IRA, Coverdell ESA, Archer MSA or HSA contributions or distributions, and pension distributions. You must give your correct TIN, but you do not have to sign the certification.

What Name and Number To Give the Requester

For this type of account:	Give name and SSN of:
1. Individual	The individual
2. Two or more individuals (joint account) other than an account maintained by an FFI	The actual owner of the account or, if combined funds, the first individual on the account[1]
3. Two or more U.S. persons (joint account maintained by an FFI)	Each holder of the account
4. Custodial account of a minor (Uniform Gift to Minors Act)	The minor[2]
5. a. The usual revocable savings trust (grantor is also trustee)	The grantor-trustee[1]
b. So-called trust account that is not a legal or valid trust under state law	The actual owner[1]
6. Sole proprietorship or disregarded entity owned by an individual	The owner[3]
7. Grantor trust filing under Optional Filing Method 1 (see Regulations section 1.671-4(b)(2)(i)(A))**	The grantor*
8. Disregarded entity not owned by an individual	The owner
9. A valid trust, estate, or pension trust	Legal entity[4]
10. Corporation or LLC electing corporate status on Form 8832 or Form 2553	The corporation
11. Association, club, religious, charitable, educational, or other tax-exempt organization	The organization
12. Partnership or multi-member LLC	The partnership
13. A broker or registered nominee	The broker or nominee
14. Account with the Department of Agriculture in the name of a public entity (such as a state or local government, school district, or prison) that receives agricultural program payments	The public entity
15. Grantor trust filing Form 1041 or under the Optional Filing Method 2, requiring Form 1099 (see Regulations section 1.671-4(b)(2)(i)(B))**	The trust

[1] List first and circle the name of the person whose number you furnish. If only one person on a joint account has an SSN, that person's number must be furnished.

[2] Circle the minor's name and furnish the minor's SSN.

[3] You must show your individual name on line 1, and enter your business or DBA name, if any, on line 2. You may use either your SSN or EIN (if you have one), but the IRS encourages you to use your SSN.

[4] List first and circle the name of the trust, estate, or pension trust. (Do not furnish the TIN of the personal representative or trustee unless the legal entity itself is not designated in the account title.)

* **Note:** The grantor must also provide a Form W-9 to the trustee of the trust.

** For more information on optional filing methods for grantor trusts, see the Instructions for Form 1041.

Note: If no name is circled when more than one name is listed, the number will be considered to be that of the first name listed.

Secure Your Tax Records From Identity Theft

Identity theft occurs when someone uses your personal information, such as your name, SSN, or other identifying information, without your permission to commit fraud or other crimes. An identity thief may use your SSN to get a job or may file a tax return using your SSN to receive a refund.

To reduce your risk:

- Protect your SSN,
- Ensure your employer is protecting your SSN, and
- Be careful when choosing a tax return preparer.

If your tax records are affected by identity theft and you receive a notice from the IRS, respond right away to the name and phone number printed on the IRS notice or letter.

If your tax records are not currently affected by identity theft but you think you are at risk due to a lost or stolen purse or wallet, questionable credit card activity, or a questionable credit report, contact the IRS Identity Theft Hotline at 800-908-4490 or submit Form 14039.

For more information, see Pub. 5027, Identity Theft Information for Taxpayers.

Victims of identity theft who are experiencing economic harm or a systemic problem, or are seeking help in resolving tax problems that have not been resolved through normal channels, may be eligible for Taxpayer Advocate Service (TAS) assistance. You can reach TAS by calling the TAS toll-free case intake line at 877-777-4778 or TTY/TDD 800-829-4059.

Protect yourself from suspicious emails or phishing schemes. Phishing is the creation and use of email and websites designed to mimic legitimate business emails and websites. The most common act is sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

The IRS does not initiate contacts with taxpayers via emails. Also, the IRS does not request personal detailed information through email or ask taxpayers for the PIN numbers, passwords, or similar secret access information for their credit card, bank, or other financial accounts.

If you receive an unsolicited email claiming to be from the IRS, forward this message to *phishing@irs.gov*. You may also report misuse of the IRS name, logo, or other IRS property to the Treasury Inspector General for Tax Administration (TIGTA) at 800-366-4484. You can forward suspicious emails to the Federal Trade Commission at *spam@uce.gov* or report them at *www.ftc.gov/complaint*. You can contact the FTC at *www.ftc.gov/idtheft* or 877-IDTHEFT (877-438-4338). If you have been the victim of identity theft, see *www.IdentityTheft.gov* and Pub. 5027.

Go to *www.irs.gov/IdentityTheft* to learn more about identity theft and how to reduce your risk.

Privacy Act Notice

Section 6109 of the Internal Revenue Code requires you to provide your correct TIN to persons (including federal agencies) who are required to file information returns with the IRS to report interest, dividends, or certain other income paid to you; mortgage interest you paid; the acquisition or abandonment of secured property; the cancellation of debt; or contributions you made to an IRA, Archer MSA, or HSA. The person collecting this form uses the information on the form to file information returns with the IRS, reporting the above information. Routine uses of this information include giving it to the Department of Justice for civil and criminal litigation and to cities, states, the District of Columbia, and U.S. commonwealths and territories for use in administering their laws. The information may also be disclosed to other countries under a treaty, to federal and state agencies to enforce civil and criminal laws, or to federal law enforcement and intelligence agencies to combat terrorism. You must provide your TIN whether or not you are required to file a tax return. Under section 3406, payors must generally withhold a percentage of taxable interest, dividends, and certain other payments to a payee who does not give a TIN to the payor. Certain penalties may also apply for providing false or fraudulent information.

The Department of Homeland Security
Notice of Funding Opportunity
Fiscal Year 2022 State and Local Cybersecurity Grant Program

Effective April 4, 2022, the Federal Government transitioned from using the Data Universal Numbering System or DUNS number, to a new, non-proprietary identifier known as a Unique Entity Identifier or UEI. For entities that had an active registration in the System for Award Management (SAM.gov) prior to this the UEI has automatically been assigned and no action is necessary. For all entities filing a new registration in SAM.gov on or after April 4, 2022, the UEI will be assigned to that entity as part of the SAM.gov registration process.

UEI registration information is available on GSA.gov at: Unique Entity Identifier Update | GSA. Grants.gov registration information can be found at: https://www.grants.gov/web/grants/register.html. Detailed information regarding UEI and SAM is also provided in Section D of this notice.

Table of Contents

A. Program Description

1. Issued By
U.S. Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA)/Resilience/Grant Program Directorate (GPD)

2. Assistance Listings Number
97.137

3. Assistance Listings Title
State and Local Cybersecurity Grant Program (SLCGP)

4. Funding Opportunity Title
Fiscal Year 2022 State and Local Cybersecurity Grant Program (SLCGP)

5. Funding Opportunity Number
DHS-22-137-000-01

6. Authorizing Authority for Program
Section 2220A of the Homeland Security Act of 2002, as amended (Pub. L. No. 107-296) (6 U.S.C. § 665g)

7. Appropriation Authority for Program
Infrastructure Investments and Jobs Appropriations Act (Pub. L. No. 117-58)

8. Announcement Type
Initial

9. Program Category
Preparedness: Community Security

10. Program Overview, Objectives, and Priorities

a. *Overview*

Our nation faces unprecedented cybersecurity risks, including increasingly sophisticated adversaries, widespread vulnerabilities in commonly used hardware and software, and broad dependencies on networked technologies for the day-to-day operation of critical infrastructure. Cyber risk management is further complicated by the ability of malicious actors to operate remotely, linkages between cyber and physical systems, and the difficulty of reducing vulnerabilities.

The potential consequences of cyber incidents threaten national security. 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), also known as the Bipartisan Infrastructure Law (BIL), 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 community.

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.

b. ***Objectives***

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 in their applications:

- 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.
- Objective 2: Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- Objective 3: Implement security protections commensurate with risk.
- Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

For more information on the program goals, objectives, sub-objectives, and desired outcomes, please refer to Appendix A.

c. ***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.

Cybersecurity Planning Committee

The Planning Committee is responsible for developing, implementing, and revising Cybersecurity Plans (including individual projects); formally approving the Cybersecurity Plan (along with the chief information officer, chief information security officer or an

equivalent official); and assisting with determination of effective funding priorities (i.e., work with entities within the eligible entity's jurisdiction to identify and prioritize individual projects). To support these responsibilities, the Planning Committee must include the following entities:

- The eligible entity (i.e., state or territory);
- County, city, and town representation (if the eligible entity is a state);
- Institutions of public education within the eligible entity's jurisdiction;
- Institutions of public health within the eligible entity's jurisdiction; and
- As appropriate, representatives from rural, suburban, and high-population jurisdictions.

For more information on the Cybersecurity Planning Committee responsibilities and composition, please refer to Appendix B.

Cybersecurity Plan

To assist in developing the required Plan, a Cybersecurity Plan Checklist containing information on what must be included in the Plan has been developed for use by SLCGP recipients. Recipients are encouraged to incorporate, where applicable, any existing plans to protect against cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, SLT governments. For more information on the Cybersecurity Plan and Cybersecurity Plan Checklist, please refer to Appendix C.

Key Cybersecurity Best Practices

To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, SLT governments must take decisive steps to modernize their approach to cybersecurity, adopting security best practices and advancing toward Zero Trust Architecture. The following strategic elements, therefore, are required to be included in Cybersecurity Plans and in individual projects:

- 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); and
- Migration to the .gov internet domain.

As individual government entities increase their cybersecurity maturity, implementing more advanced best practices, such as endpoint detection and response capabilities, as well as conducting regular penetration testing, will be recommended.

11. Performance Measures

Each grant recipient is required to collect data to allow DHS to measure performance of the awarded grant in support of the SLCGP metrics, which will be described in each Cybersecurity Plan.

The statute requires that "not later than one year after the date on which an eligible entity receives a grant…for the purpose of implementing [its] Cybersecurity Plan…, including an eligible entity that comprises a multi-entity group that receives a grant for that purpose, and annually thereafter until one year after the date on which funds from the grant are expended or returned, the eligible entity shall submit to the Secretary a report that, using the metrics described in the Cybersecurity Plan of the eligible entity, describes the progress of the eligible entity in:

- Implementing the Cybersecurity Plan;
- Reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a state, local governments within the jurisdiction of the eligible entity."

If an eligible entity does not have a Cybersecurity Plan in place and receives an award, then the statute requires that not later than one year after the date on which the eligible entity receives a grant, and annually thereafter until one year after the date on which funds from the grant are expended or returned, the eligible entity shall submit to the Secretary a report describing how the eligible entity obligated and expended grant funds to:

- Develop or revise a Cybersecurity Plan; or
- Assist with activities that address imminent cybersecurity threats, as confirmed by the Secretary, acting through the CISA Director, to the information systems owned or operated by, or on behalf of, the eligible entity or a local government within the jurisdiction of the eligible entity.

In order to measure performance, DHS may request information throughout the period of performance. In its final performance report submitted at closeout, the recipient must submit sufficient information to demonstrate it has met the performance goals as stated in its award. DHS will measure the recipient's performance of the grant by comparing the number of activities and projects needed and requested in its investment justification with the number of activities and projects acquired and delivered by the end of the period of performance using the following programmatic metrics:

- Percentage of entities with CISA approved state-wide Cybersecurity Plans
- Percentage of entities with statewide cybersecurity planning committees that meet the Homeland Security Act of 2002 and this SLCGP Notice of Funding Opportunity (NOFO) requirements
- Percentage of entities conducting annual table-top and full-scope exercises to test cybersecurity plans; Percent of the entities' SLCGP budget allocated to exercises; or Average dollar amount expended on exercise planning for entities

- Percentage of entities conducting an annual cyber risk assessment to identify cyber risk management gaps and areas for improvement
- Percentage of entities performing phishing training; Percent of entities conducting awareness campaigns; Percent of entities providing role-based cybersecurity awareness training to employees
- Percentage of entities adopting the Workforce Framework for Cybersecurity (NICE Framework) as evidenced by established workforce development and training plans
- Percentage of entities with capabilities to analyze network traffic and activities related to potential threats
- Percentage of entities implementing multi-factor authentication (MFA) for all remote access and privileged accounts
- Percentage of entities with programs to anticipate and discontinue use of end of life software and hardware
- Percentage of entities prohibiting the use of known/fixed/default passwords and credentials
- Percentage of entities operating under the ".gov" internet domain
- Number of cybersecurity gaps or issues addressed annually by entities

B. Federal Award Information

1. Available Funding for the NOFO: **$185 million**

For FY 2022, DHS will award state and territorial funds based on baseline minimums and population as required by the Homeland Security Act of 2002, and described below.

Each state and territory will receive a baseline allocation using thresholds established in the Homeland Security Act of 2002. All 50 States, the District of Columbia, and the Commonwealth of Puerto Rico will receive a minimum of $2,000,000 each, equaling 1% of total funds appropriated to DHS in FY 2022. Each of the four territories (American Samoa, Guam, the Northern Mariana Islands, and the U.S. Virgin Islands) will receive a minimum of $500,000, equaling 0.25% of the total funds appropriated to DHS in FY 2022. $90,500,000, 50% of the remaining amount will be apportioned based on the ratio that the population of each state or territory bears to the population of all states and territories. The remaining $90,500,000, equaling the other 50% of the remaining amount, will be apportioned based on the ratio that the population of each state that resides in rural areas bears to the population of all states that resides in rural areas.

FY 2022 SLCGP Allocations

State/Territory	FY 2022 SLCGP Allocation
Alabama	$3,848,596
Alaska	$2,245,130
Arizona	$3,336,349
Arkansas	$3,162,746
California	$7,981,997

State/Territory	FY 2022 SLCGP Allocation
Colorado	$3,234,143
Connecticut	$2,681,116
Delaware	$2,224,803
District of Columbia	$2,081,394
Florida	$5,889,464
Georgia	$4,877,389
Hawaii	$2,243,739
Idaho	$2,550,109
Illinois	$4,404,622
Indiana	$3,949,173
Iowa	$3,073,518
Kansas	$2,820,015
Kentucky	$3,659,521
Louisiana	$3,327,540
Maine	$2,666,932
Maryland	$3,214,008
Massachusetts	$3,173,589
Michigan	$4,777,219
Minnesota	$3,606,482
Mississippi	$3,274,355
Missouri	$3,841,132
Montana	$2,428,110
Nebraska	$2,555,930
Nevada	$2,488,375
New Hampshire	$2,499,170
New Jersey	$3,380,963
New Mexico	$2,540,767
New York	$5,813,554
North Carolina	$5,362,452
North Dakota	$2,287,118
Ohio	$4,980,243
Oklahoma	$3,294,613
Oregon	$2,988,975
Pennsylvania	$5,207,249
Rhode Island	$2,190,484
South Carolina	$3,661,568
South Dakota	$2,341,978
Tennessee	$4,244,182
Texas	$8,469,945
Utah	$2,619,397
Vermont	$2,310,302
Virginia	$4,292,938
Washington	$3,667,735

State/Territory	FY 2022 SLCGP Allocation
West Virginia	$2,764,988
Wisconsin	$3,795,634
Wyoming	$2,200,558
Puerto Rico	$2,492,381
U.S. Virgin Islands	$500,000
American Samoa	$500,000
Guam	$500,000
Northern Mariana Islands	$500,000
Total	**$185,024,690**

2. Projected Number of Awards: **56**

3. Period of Performance: **48 months**
Extensions to the period of performance are allowed. For additional information on period of performance extensions, please refer to Section H of this NOFO.

FEMA awards under most programs, including this program, only include one budget period, so it will be same as the period of performance. *See* 2 C.F.R. § 200.1 for definitions of "budget period" and "period of performance."

4. Projected Period of Performance Start Date(s): **Sept. 1, 2022**

5. Projected Period of Performance End Date(s): **Aug. 31, 2026**

6. Funding Instrument Type: **Grant**

C. Eligibility Information

1. Eligible Applicants

All 56 states and territories, including any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands, are eligible to apply for SLCGP funds. Accordingly, the Governor designated State Administrative Agency (SAA) is the only entity eligible to submit SLCGP applications to DHS/FEMA.

Although Tribes are not eligible to apply directly for SLCGP funding, they may be eligible subrecipients, and can receive SLCGP funding as a local government. Each individual SAA may determine whether and how much SLCGP funding to pass through to Tribal entities; DHS does not have the authority to mandate that a certain percentage of SLCGP funds are directed to Tribal governments. Additionally, $6 million in funding will be directly available to Tribal entities under the forthcoming Tribal Cybersecurity Grant Program, which DHS expects to publish the NOFO in the fall of 2022.

"State" is defined in 6 U.S.C. § 101(17) to include the 50 states, District of Columbia, Commonwealth of Puerto Rico, U.S. Virgin Islands, Guam, American Samoa, and Commonwealth of the Northern Mariana Islands;

"Local government" is defined in 6 U.S.C. § 101(13) as

A) 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;

B) An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

C) A rural community, unincorporated town or village, or other public entity.

"Tribal government" for purposes of being an eligible entity for the Tribal Cybersecurity Grant Program is defined in 6 U.S.C. § 665g(1)(12) as the recognized governing body of any Indian or Alaska Native Tribe, band, nation, pueblo, village, community, component band, or component reservation, that is individually identified (including parenthetically) in the most recent published list of Federally Recognized Tribes.

In addition to applying as a single entity, an eligible entity under SLCGP (i.e., the SAA) may partner with one or more other eligible entities to form a multi-entity group. Members of multi-entity groups work together to address cybersecurity risks and cybersecurity threats to information systems within their jurisdictions. There is no limit to the number of participating entities in a multi-entity group. Local entities can be included in the project, but their respective eligible entity must also participate at some level (see Appendix D). There is no separate funding for multi-entity awards. Instead, they should be considered as group projects within their existing state or territory allocations. These projects should be included as individual Investment Justifications from each participating eligible entity, each approved by the respective Planning Committee and aligned with each respective eligible entity's Cybersecurity Plan.

2. Applicant Eligibility Criteria

Applicants must be an eligible entity, meaning one of the 56 states and territories that are eligible for the program. One or more eligible entities may form a multi-entity group.

3. Other Eligibility Criteria

Cybersecurity Plan

To be eligible for FY 2022 SLCGP funding, each eligible entity is required to submit a Cybersecurity Plan that aligns with the criteria detailed in Appendix C.

The only exception is if an eligible entity certifies to the Secretary that:

A. The activities that will be supported by a grant are:
   1. Integral to the development of the Cybersecurity Plan of the eligible entity; or
   2. Necessary to assist with activities that address imminent cybersecurity threats, as confirmed by the Secretary, acting through the CISA Director, to the information systems owned or operated by, or on behalf of, the eligible entity or

a local government within the jurisdiction of the eligible entity; and

B. The eligible entity will submit to the Secretary a Cybersecurity Plan for review by September 30, 2023.

Note that for multi-entity groups, in order to be eligible for an award, all eligible entities within the multi-entity group must already have a Cybersecurity Plan in place; multi-entity groups are not eligible for awards to develop a Cybersecurity Plan. *See* 6 U.S.C. § 665g(f), (i)(3).

Cybersecurity Planning Committee

To be eligible for FY 2022 SLCGP funding, each eligible entity is required to establish a Cybersecurity Planning Committee comprised of the members summarized in Appendix B.

4. 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.

DHS/FEMA administers cost-matching requirements in accordance with 2 C.F.R. § 200.306. To meet matching requirements, the recipient contributions must be verifiable, reasonable, allocable and necessary, and otherwise allowable under the grant program, and in compliance with all applicable federal requirements and regulations. Unless otherwise authorized by law, the non-federal cost share requirement cannot be matched with other federal funds.

For example, if the federal award were at a 90% cost share and the total approved budget cost was $100,000, then:

- Federal share is 90% of $100,000 = $90,000
- Recipient share is 10% of $100,000 = $10,000

However, with this example, if the total cost ended up being $120,000, the federal share would remain at $90,000 due to the statutory formula even if it means the federal share ends up being lower than 90%. Any cost overruns will not be matched by this grant program and will be incurred by the recipient. With this example, if the total cost ended up being $80,000, then the 90% federal share would decrease to $72,000, and the recipient cost share would be $8,000.

Additionally, by statute, the cost share applies to each individual activity funded by the grant award rather than just to the cumulative total. Recipients must ensure that each activity's cost share is met. DHS interprets "activity" to mean all items approved as part of a submitted "Project Worksheet."

For a multi-entity group project, a cost share or cost match is not required for the FY 2022 SLCGP. For more information about multi-entity group projects, please refer to Appendix D.

The Secretary of Homeland Security may waive or modify the non-federal share for an individual entity if the entity demonstrates economic hardship. Additional information about the eligibility criteria for a cost share waiver, as well as how to submit a request for a cost share waiver from DHS is included in Appendix H.

D. Application and Submission Information

1. Key Dates and Times

a. ***Application Start Date:*** 09/16/2022

b. ***Application Submission Deadline:*** ***11/15/2022 at 5 p.m. ET***

All applications **must** be received by the established deadline.

The Non-Disaster (ND) Grants System has a date stamp that indicates when an application is submitted. Applicants will receive an electronic message confirming receipt of their submission. For additional information on how an applicant will be notified of application receipt, see the subsection titled "Timely Receipt Requirements and Proof of Timely Submission" in Section D of this NOFO.

DHS will not review applications that are received after the deadline or consider these late applications for funding. DHS may, however, extend the application deadline on request for any applicant who can demonstrate that good cause exists to justify extending the deadline. Good cause for an extension may include technical problems outside of the applicant's control that prevent submission of the application by the deadline, other exigent or emergency circumstances, or statutory requirements for DHS to make an award.

Applicants experiencing technical problems outside of their control must notify DHS as soon as possible and before the application deadline. Failure to timely notify DHS of the issue that prevented the timely filing of the application may preclude consideration of the award. "Timely notification" of DHS means prior to the application deadline and within 48 hours after the applicant became aware of the issue.

A list of FEMA contacts can be found in Section G of this NOFO, "DHS Awarding Agency Contact Information." For additional assistance using the ND Grants System, please contact the ND Grants Service Desk at (800) 865-4076 or NDGrants@fema.dhs.gov. The ND Grants Service Desk is available Monday through Friday, 9 a.m. – 6 p.m. ET. If applicants have programmatic or grants management questions or concerns, please contact the Centralized Scheduling and Information Desk (CSID) by phone at (800) 368-6498 or by e-mail at askcsid@fema.dhs.gov, Monday through Friday, 9 a.m. – 5 p.m. ET.

c. ***Anticipated Funding Selection Date:*** No later than 11/30/2022

d. ***Anticipated Award Date:*** No later than 12/31/2022

e. ***Other Key Dates:***

Event	Suggested Deadline for Completion
Obtaining Unique Entity Identifier (UEI) Number	Four weeks before actual submission deadline
Obtaining a valid Employer Identification Number (EIN)	Four weeks before actual submission deadline
Creating an account with login.gov	Four weeks before actual submission deadline
Registering in SAM or updating SAM registration	Four weeks before actual submission deadline
Registering in Grants.gov	Four weeks before actual submission deadline
Registering in ND Grants	Four weeks before actual submission deadline
Starting application in Grants.gov	One week before actual submission deadline
Submitting the final application in ND Grants	By the submission deadline

2. Agreeing to Terms and Conditions of the Award

By submitting an application, applicants agree to comply with the requirements of this NOFO and the terms and conditions of the award, should they receive an award.

3. Address to Request Application Package

Initial applications are processed through the Grants.gov portal. Final applications are completed and submitted through FEMA's Non-Disaster Grants (ND Grants) System. Application forms and instructions are available at Grants.gov. To access these materials, go to http://www.grants.gov, select "Applicants" then "Apply for Grants". In order to obtain the application package, select "Download a Grant Application Package". Enter the Assistance Listing (formerly CFDA) and/or the funding opportunity number located on the cover of the program's NOFO, select "Download Package," and then follow the prompts to download the application package. In addition, the following Telephone Device for the Deaf (TDD) and/or Federal Information Relay Service (FIRS) number available for this Notice and all relevant NOFO is (800) 462-7585.

4. Steps Required to Obtain a Unique Entity Identifier, Register in the System for Award Management (SAM), and Submit an Application

Applying for an award under this program is a multi-step process and requires time to complete. Applicants are encouraged to register early as the registration process can take four weeks or more to complete. Therefore, registration should be done in sufficient time to ensure it does not impact your ability to meet required submission deadlines.

Please review the table above for estimated deadlines to complete each of the steps listed. Failure of an applicant to comply with any of the required steps before the deadline for submitting an application may disqualify that application from funding.
To apply for an award under this program, all applicants must:

a. Apply for, update, or verify their Unique Entity Identifier (UEI) number from SAM.gov and Employer Identification Number (EIN) from the Internal Revenue Service;
b. In the application, provide an UEI number;
c. Have an account with login.gov;
d. Register for, update, or verify their SAM account and ensure the account is active before submitting the application;
e. Create a Grants.gov account;
f. Add a profile to a Grants.gov account;
g. Establish an Authorized Organizational Representative (AOR) in Grants.gov;
h. Register in ND Grants
i. Submit an initial application in Grants.gov;
j. Submit the final application in ND Grants, including electronically signing applicable forms; and
k. Continue to maintain an active SAM registration with current information at all times during which it has an active federal award or an application or plan under consideration by a federal awarding agency. As part of this, applicants must also provide information on an applicant's immediate and highest-level owner and subsidiaries, as well as on all predecessors that have been awarded federal contracts or federal financial assistance within the last three years, if applicable.

Specific instructions on how to apply for, update, or verify a UEI number or SAM registration or establish an AOR are included below in the steps for applying through Grants.gov.

Applicants are advised that DHS may not make a federal award until the applicant has complied with all applicable SAM requirements. Therefore, an applicant's SAM registration must be active not only at the time of application, but also during the application review period and when DHS is ready to make a federal award. Further, as noted above, an applicant's or recipient's SAM registration must remain active for the duration of an active federal award. If an applicant's SAM registration is expired at the time of application, expires during application review, or expires any other time before award, DHS may determine that the applicant is not qualified to receive a federal award and use that determination as a basis for making a federal award to another applicant.

Per 2 C.F.R. § 25.110(c)(2)(iii), if an applicant is experiencing exigent circumstances that prevents it from receiving a UEI number, if applicable, and completing SAM registration prior to receiving a federal award, the applicant must notify FEMA as soon as possible by contacting askcsid@fema.dhs.gov and providing the details of the circumstances that prevent completion of these requirements. If FEMA determines that there are exigent circumstances and FEMA has decided to make an award, the applicant will be required to obtain a UEI number, if applicable, and complete SAM registration within 30 days of the federal award date.

5. Electronic Delivery

DHS is participating in the Grants.gov initiative to provide the grant community with a single site to find and apply for grant funding opportunities. DHS encourages or requires applicants

to submit their applications online through Grants.gov, depending on the funding opportunity.

For this funding opportunity, FEMA requires applicants to submit initial applications through Grants.gov and a final application through ND Grants.

6. How to Register to Apply through Grants.gov

a. ***General Instructions:***

Registering and applying for an award under this program is a multi-step process and requires time to complete. Read the instructions below about registering to apply for FEMA funds. Applicants should read the registration instructions carefully and prepare the information requested before beginning the registration process. Reviewing and assembling the required information before beginning the registration process will alleviate last-minute searches for required information.

The registration process can take up to four weeks to complete. To ensure an application meets the deadline, applicants are advised to start the required steps well in advance of their submission.

Organizations must have an UEI number, an EIN, an active SAM registration and Grants.gov account to apply for grants.

Organizations must also have a Grants.gov account to apply for an award under this program. Creating a Grants.gov account can be completed online in minutes, but DUNS and SAM registrations may take several weeks. Therefore, an organization's registration should be done in sufficient time to ensure it does not impact the entity's ability to meet required application submission deadlines. Complete organization instructions can be found on Grants.gov here: https://www.grants.gov/web/grants/applicants/organization-registration.html.

If individual applicants are eligible to apply for this grant funding opportunity, refer to:

b. ***Obtain an UEI Number:***

All entities applying for funding, including renewal funding, prior to April 4, 2022, must have a UEI number. Applicants must enter the UEI number in the applicable data entry field on the SF-424 form.

For more detailed instructions for obtaining a UEI number, refer to: Sam.gov.

c. ***Obtain Employer Identification Number***

All entities applying for funding must provide an Employer Identification Number (EIN). The EIN can be obtained from the IRS by visiting: https://www.irs.gov/businesses/small-businesses-self-employed/apply-for-an-employer-identification-number-ein-online.

d. ***Create a login.gov account:***

Applicants must have a login.gov account in order to register with SAM or update their SAM registration. Applicants can create a login.gov account here:

https://secure.login.gov/sign_up/enter_email?request_id=34f19fa8-14a2-438c-8323-a62b99571fd3.

Applicants only have to create a login.gov account once. For applicants that are existing SAM users, use the same email address for the login.gov account as with SAM.gov so that the two accounts can be linked.

For more information on the login.gov requirements for SAM registration, refer to: https://www.sam.gov/SAM/pages/public/loginFAQ.jsf.

e. ***Register with SAM:***
All organizations applying online through Grants.gov must register with SAM. Failure to register with SAM will prevent your organization from applying through Grants.gov. SAM registration must be renewed annually.

For more detailed instructions for registering with SAM, refer to: https://www.grants.gov/web/grants/applicants/organization-registration/step-2-register-with-sam.html.

Note: As a new requirement per 2 C.F.R. § 25.200, applicants must also provide the applicant's immediate and highest-level owner, subsidiaries, and predecessors that have been awarded federal contracts or federal financial assistance within the last three years, if applicable.

I. Additional SAM Reminders

Existing SAM.gov account holders should check their account to make sure it is "ACTIVE." SAM registration should be completed at the very beginning of the application period and should be renewed annually to avoid being "INACTIVE." **Please allow plenty of time before the grant application submission deadline to obtain an UEI number, if applicable, and then to register in SAM. It may be four weeks or more after an applicant submits the SAM registration before the registration is active in SAM, and then it may be an additional 24 hours before FEMA's system recognizes the information.**

It is imperative that the information applicants provide is correct and current. Please ensure that your organization's name, address, and EIN are up to date in SAM and the UEI number used in SAM is the same one used to apply for all other FEMA awards. Payment under any FEMA award is contingent on the recipient's having a current SAM registration.

II. Help with SAM

The SAM quick start guide for new recipient registration and SAM video tutorial for new applicants are tools created by the General Services Administration (GSA) to assist those registering with SAM. If applicants have questions or concerns about a SAM registration, please contact the Federal Support Desk at https://www.fsd.gov/fsd-gov/home.do or call toll free (866) 606-8220.

f. ***Create a Grants.gov Account:***
The next step in the registration process is to create an account with Grants.gov. If applicable, applicants must know their organization's DUNS number to complete this process.

For more information, follow the on-screen instructions or refer to:
https://www.grants.gov/web/grants/applicants/registration.html.

See also Section D.8 in this NOFO, "Submitting the Final Application in ND Grants," for instructions on how to register early in ND Grants.

g. ***Add a Profile to a Grants.gov Account:***
A profile in Grants.gov corresponds to a single applicant organization the user represents (i.e., an applicant) or an individual applicant. If you work for or consult with multiple organizations and have a profile for each, you may log in to one Grants.gov account to access all of your grant applications. To add an organizational profile to your Grants.gov account, if applicable, enter the DUNS number for the organization in the UEI field while adding a profile.

For more detailed instructions about creating a profile on Grants.gov, refer to:
https://www.grants.gov/web/grants/applicants/registration/add-profile.html.

h. EBiz POC Authorized Profile Roles:
After you register with Grants.gov and create an Organization Applicant Profile, the organization applicant's request for Grants.gov roles and access are sent to the EBiz POC. The EBiz POC will then log in to Grants.gov and authorize the appropriate roles, which may include the Authorized Organization Representative (AOR) role, thereby giving you permission to complete and submit applications on behalf of the organization. You will be able to submit your application online any time after you have been assigned the AOR role.

For more detailed instructions about creating a profile on Grants.gov, refer to:
https://www.grants.gov/web/grants/applicants/registration/authorize-roles.html.

i. ***Track Role Status:***
To track your role request, refer to:
https://www.grants.gov/web/grants/applicants/registration/track-role-status.html.

j. ***Electronic Signature:***
When applications are submitted through Grants.gov, the name of the organization applicant with the AOR role that submitted the application is inserted into the signature line of the application, serving as the electronic signature. The EBiz POC **must** authorize individuals who are able to make legally binding commitments on behalf of the organization as an AOR; **this step is often missed, and it is crucial for valid and timely submissions.**

7. How to Submit an Initial Application to DHS via Grants.gov
Standard Form 424 (SF-424) is the initial application for this NOFO.

Grants.gov applicants can apply online using a workspace. A workspace is a shared, online environment where members of a grant team may simultaneously access and edit different web forms within an application. For each Notice of Funding Opportunity, you can create individual instances of a workspace. Applicants are encouraged to submit their initial applications in Grants.gov ***at least*** seven days before the application deadline.

In Grants.gov, applicants need to submit the following forms:

- SF-424, Application for Federal Assistance; and
- Grants.gov Lobbying Form, Certification Regarding Lobbying.

Below is an overview of applying on Grants.gov. For access to complete instructions on how to apply for opportunities using Workspace, refer to: https://www.grants.gov/web/grants/applicants/workspace-overview.html

a. ***Create a Workspace:***
Creating a workspace allows you to complete it online and route it through your organization for review before submitting.

b. ***Complete a Workspace:***
Add participants to the workspace to work on the application together, complete all the required forms online or by downloading PDF versions, and check for errors before submission.

c. ***Adobe Reader:***
If you decide not to apply by filling out webforms you can download individual PDF forms in Workspace so that they will appear similar to other Standard or DHS forms. The individual PDF forms can be downloaded and saved to your local device storage, network drive(s), or external drives, then accessed through Adobe Reader.

NOTE: Visit the Adobe Software Compatibility page on Grants.gov to download the appropriate version of the software at: https://www.grants.gov/web/grants/applicants/adobe-software-compatibility.html

d. ***Mandatory Fields in Forms:***
In the forms, you will note fields marked with an asterisk and a different background color. These fields are mandatory fields that must be completed to successfully submit your application.

e. ***Complete SF-424 Fields First:***
The forms are designed to fill in common required fields across other forms, such as the applicant name, address, and UEI number. To trigger this feature, an applicant must complete the SF-424 information first. Once it is completed, the information will transfer to the other forms.

f. ***Submit a Workspace:***
An application may be submitted through workspace by clicking the "Sign and Submit" button on the Manage Workspace page, under the Forms tab. Grants.gov recommends submitting your application package at least 24-48 hours prior to the close date to provide you with time to correct any potential technical issues that may disrupt the application submission.

g. ***Track a Workspace:***
After successfully submitting a workspace package, a Grants.gov Tracking Number (GRANTXXXXXXXX) is automatically assigned to the application. The number will be listed on the confirmation page that is generated after submission. Using the tracking number, access the Track My Application page under the Applicants tab or the Details tab in the submitted workspace.

h. ***Additional Training and Applicant Support:***
For additional training resources, including video tutorials, refer to: https://www.grants.gov/web/grants/applicants/applicant-training.html
Grants.gov provides applicants 24/7 (except federal holidays) support via the toll-free number (800) 518-4726, email at support@grants.gov and the website at https://www.grants.gov/support.html. For questions related to the specific grant opportunity, contact the number listed in the application package of the grant you are applying for.

If you are experiencing difficulties with your submission, it is best to call the Grants.gov Support Center and get a ticket number. The Support Center ticket number will assist FEMA with tracking your issue and understanding background information on the issue.

8. Submitting the Final Application in ND Grants
After submitting the initial application in Grants.gov, eligible applicants will be notified by FEMA and asked to proceed with submitting their complete application package in ND Grants. Applicants can register early with ND Grants and are encouraged to begin their ND Grants registration at the time of this announcement or, at the latest, seven days before the application deadline. Early registration will allow applicants to have adequate time to start and complete their applications.

Applicants needing assistance registering for the ND Grants system should contact ndgrants@fema.dhs.gov or (800) 865-4076. For step-by-step directions on using the ND Grants system and other guides, please see https://www.fema.gov/grants/guidance-tools/non-disaster-grants-management-system.

In ND Grants, applicants will be prompted to submit the standard application information and any program-specific information required as described in Section D.10 of this NOFO, "Content and Form of Application Submission." The Standard Forms (SF) are auto generated in ND Grants, but applicants may access these forms in advance through the Forms tab under the SF-424 family on Grants.gov. Applicants should review these forms before applying to ensure they have all the information required.

For additional application submission requirements, including program-specific requirements, please refer to the subsection titled "Content and Form of Application Submission" under Section D of this NOFO.

9. Timely Receipt Requirements and Proof of Timely Submission

As application submission is a two-step process, the applicant with the AOR role who submitted the application in Grants.gov will receive an acknowledgement of receipt and a tracking number (GRANTXXXXXXXX) from Grants.gov with the successful transmission of its initial application. **This notification does not serve as proof of timely submission, as the application is not complete until it is submitted in ND Grants.** Applicants can also view the ND Grants Agency Tracking Number by accessing the Details tab in the submitted workspace section in Grants.gov, under the Agency Tracking Number column. Should the Agency Tracking Number not appear, the application has not yet migrated from Grants.gov into the ND Grants System. Please allow 24 hours for your ND Grants application tracking number to migrate.

All applications must be received in ND Grants by **5 p.m. ET** on the application deadline. Proof of timely submission is automatically recorded by ND Grants. An electronic date/time stamp is generated within the system when the application is successfully received by ND Grants. Additionally, the applicant(s) listed as contacts on the application will receive a system-generated email to confirm receipt.

10. Content and Form of Application Submission

a. ***Standard Required Application Forms and Information***

The following forms or information are required to be submitted in either Grants.gov or ND Grants. The Standard Forms (SF) are submitted either through Grants.gov, through forms generated in ND Grants, or as an attachment in ND Grants. Applicants may also access the SFs at https://www.grants.gov/web/grants/forms/sf-424-family.html.

I. GRANTS.GOV

- **SF-424, Application for Federal Assistance**, initial application submitted through Grants.gov; and
- **Grants.gov Lobbying Form, Certification Regarding Lobbying**, submitted through Grants.gov.

II. ND GRANTS

- **SF-424A, Budget Information (Non-Construction)**, submitted via the forms generated by ND Grants;
- **SF-424B, Standard Assurances (Non-Construction)**, submitted via the forms generated by ND Grants;
- **SF-LLL, Disclosure of Lobbying Activities**, submitted via the forms generated by ND Grants; and
- **Indirect Cost Agreement or Proposal**, submitted as an attachment in ND Grants if the budget includes indirect costs and the applicant is required to have an indirect cost rate agreement or proposal. If the applicant does not have or is not required to have an indirect cost rate agreement or proposal, please see Section D.13 of this NOFO, "Funding

Restrictions and Allowable Costs," for further information regarding allowability of indirect costs and whether alternatives to an indirect cost rate agreement or proposal might be available or contact the relevant FEMA staff identified in Section G of this NOFO, "DHS Awarding Agency Contact Information" for further instructions.

b. ***Program-Specific Required Forms and Information***

The following program-specific forms or information are required to be submitted in ND Grants as attachments:

- **SLCGP Investment Justifications**: Each eligible entity is required to submit complete project-level information detailing how the program objectives and goals will be met to develop, implement, or revise its Cybersecurity Plan; establish a Cybersecurity Planning Committee; conduct assessments and evaluations; and adopt key cybersecurity best practices. For more information on the Investment Justification, please refer to Appendix F. The FY 2022 Investment Justification must include the following information:
  - Only one application will be submitted by the eligible entity. It must include a brief description of the capabilities of the SLT agencies across the eligible entity related to the required elements of the Cybersecurity Plan.
  - The application will consist of up to four investments, one for each SLCGP objective (See Appendix F for more information on the goal and objectives).
  - Investments for SLCGP Objectives 1, 2, and 3 must have at least one project. Investments for SLCGP Objective 4 are optional for the FY 2022 SLCGP; however, it is important to note that identifying and mitigating gaps in the cybersecurity workforce, enhancing recruitment and retention efforts, and bolstering the knowledge, skills, and abilities of personnel are still statutory requirements for Cybersecurity Plans to address even if the eligible entity does not use grant funds to carry this out.
  - Requests to use funding to address imminent cybersecurity threats must be addressed in the Investment Justification (IJ) for Objective 3.
  - Each investment must describe how each project aligns to the entity's Cybersecurity Plan if applying for a grant to implement or revise the Cybersecurity Plan, or will align with the entity's Cybersecurity Plan if applying for a grant to develop a Cybersecurity Plan. Applicants must also describe how implementing the plan will be measured (metrics).
  - Each project must include an explanation of how the proposed project(s) will achieve the program objectives as identified in Appendix C. A project schedule with clearly defined milestones must also be included.
- **Cybersecurity Plan**: Each eligible entity is required to submit its Cybersecurity Plan that adheres to the 16 required elements identified in section 2220A of the Homeland Security Act of 2002 as amended by the BIL and included in Appendix C of this NOFO unless the eligible entity is applying for funds to develop a Cybersecurity Plan as described more below. The Cybersecurity Plan must include a description of SLT roles, an assessment of capabilities for each element, address resources and timeline for implementing the Plan, and identify metrics. SLT governments are encouraged to take a holistic approach in the development of their Plan as entities must be able to sustain capabilities once SLCGP funds are no longer available. The role of state entities as coordinator and service provider to local entities should be encouraged and supported.

For more information on the Cybersecurity Plan, please refer to Appendix C.

- **Cybersecurity Planning Committee Membership List**: The Cybersecurity Planning Committee should be seen as a platform to identify and then prioritize state-wide efforts, to include identifying opportunities to consolidate projects to increase efficiencies. Each eligible entity is required to submit confirmation that the committee is comprised of the required representatives. The eligible entity must also confirm that at least one-half of the representatives of the committee have professional experience relating to cybersecurity or information technology. For more information on the composition of the Cybersecurity Planning Committee, including how to leverage existing planning committees, please refer to Appendix B.
- **Cybersecurity Planning Committee Charter**: The Cybersecurity Planning Committee Charter must be submitted with the Cybersecurity Planning Committee Membership List attached as specified in Appendix B.
- **Cybersecurity Plan Submission Exception Request** (if applicable)
    - Applicants may request an exception to submitting their Cybersecurity Plan at the time of application. The exception request must be supported by the Chief Information Officer (CIO), Chief Information Security Office (CISO), or equivalent official.
    - If an exception is requested, SLCGP funds can only initially be used for activities that are integral to the development of the Cybersecurity Plan or are necessary to assist with activities that address imminent cybersecurity threats. Activities integral to the development of a Cybersecurity Plan are limited to investments and projects aligned to Objective 1 and Objective 2. Activities to address imminent cybersecurity threats are limited to investments and projects aligned to Objective 3.
    - **The eligible entity must also include a certification**, either as a separate document or as part of the applicable IJ(s), that all activities funded by the grant are integral to the development of the Cybersecurity Plan or are necessary to assist with activities that address imminent cybersecurity threats, as confirmed by the Secretary, acting through the CISA Director, to the information systems owned or operated by, or on behalf of, the eligible entity or a local government within the jurisdiction of the eligible entity. If grant funding is necessary to assist with activities that address imminent cybersecurity threats, then that should be noted on the applicable IJ.
    - Recipients seeking funding to develop a Cybersecurity Plan must still submit IJs for Objectives 1, 2, and 3, noting that they will need to be updated once the Cybersecurity Plan is completed and approved. It is still optional to submit an IJ for Objective 4.
    - Once the Cybersecurity Plan is completed and approved by the Cybersecurity Planning Committee and CIO, CISO, or equivalent official, the applicant must then submit updated IJs for Objectives 1, 2, and 3, along with an updated IJ for Objective 4 if one was previously submitted, to DHS with the approved Cybersecurity Plan by September 30, 2023.

The following is required to request an exception:

- Statement from the applicant as to why they do not have an approved Cybersecurity

Plan;
- High-level plan, including dates and milestones, for completing and submitting the Plan to DHS; and
- Signatures of support from the eligible entity and CIO, CISO, or equivalent official.

11. Intergovernmental Review

An intergovernmental review may be required. Applicants must contact their state's Single Point of Contact (SPOC) to comply with the state's process under Executive Order 12372 (See https://www.archives.gov/federal-register/codification/executive-order/12372.html; https://www.whitehouse.gov/wp-content/uploads/2020/04/SPOC-4-13-20.pdf).

12. Funding Restrictions and Allowable Costs

All costs charged to awards covered by this NOFO must 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 award. This includes, among other requirements, that costs must be incurred, and products and services must be delivered, within the period of performance of the award. *See* 2 C.F.R. § 200.403(h) (referring to budget periods, which for DHS awards under this program is the same as the period of performance).

In general, the Cost Principles establish standards for the allowability of costs, provide detailed guidance on the cost accounting treatment of costs as direct or administrative costs, and set forth allowability principles for selected items of cost. More specifically, except as otherwise stated in this NOFO, the terms and condition of an award, or other program materials, costs charged to awards covered by this NOFO must be consistent with the Cost Principles for Federal Awards located at 2 C.F.R. Part 200, Subpart E. In order to be allowable, all costs charged to a DHS award or applied to the cost share must be reasonable in nature and amount and allocable to the particular DHS award.

Additionally, all costs charged to awards must comply with the grant program's applicable statutes, policies, requirements in this NOFO as well as with the terms and conditions of the award. If DHS staff identify costs that are inconsistent with any of these requirements, these costs may be disallowed, and DHS may recover funds as appropriate, consistent with applicable laws, regulations, and policies.

As part of these requirements, grant recipients and subrecipients may only use federal funds or funds applied to a cost share for the purposes set forth in this NOFO and the terms and conditions of the award, and those costs must be consistent with the statutory authority for the award.

Grant funds may not be used for matching funds for other federal grants/cooperative agreements, lobbying, or intervention in federal regulatory or adjudicatory proceedings. In addition, federal funds may not be used to sue the federal government or any other government entity.

Specific investments made in support of the funding priorities discussed in this NOFO generally fall into one of the following seven allowable expense categories:

- Planning;
- Equipment;
- Exercises;
- Management & Administration (M&A);
- Organization; and
- Training.

In addition, any entity that receives FY 2022 SLCGP funding may not use 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;
- For any recipient cost-sharing contribution;
- To pay a ransom;
- For recreational or social purposes;
- To pay for cybersecurity insurance premiums;
- To acquire land or to construct, remodel, or perform alternations of buildings or other physical facilities; or
- 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.

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

Recipients and subrecipients of FEMA federal financial assistance are subject to the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY 2019 NDAA), Pub. L. No. 115-232 (2018) and 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200. Beginning August 13, 2020, the statute – as it applies to FEMA recipients, subrecipients, and their contractors and subcontractors – prohibits obligating or expending federal award funds on certain telecommunications and video surveillance products and contracting with certain entities for national security reasons.

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

Additional guidance is available at Contract Provisions Guide: Navigating Appendix II to Part 200 - Contract Provisions for Non-Federal Entity Contracts Under Federal Awards.

Effective August 13, 2020, FEMA recipients and subrecipients **may not** use any FEMA funds under open or new awards to:

(1) 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;

(2) Enter into, 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; or

(3) Enter into, 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.

I. REPLACEMENT EQUIPMENT AND SERVICES

FEMA grant funding may be permitted to procure replacement equipment and services impacted by this prohibition, provided the costs are otherwise consistent with the requirements of the NOFO.

II. DEFINITIONS

Per section 889(f)(2)-(3) of the FY 2019 NDAA and 2 C.F.R. § 200.216, covered telecommunications equipment or services means:

i. Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, (or any subsidiary or affiliate of such entities);
ii. For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
iii. Telecommunications or video surveillance services provided by such entities or using such equipment; or
iv. Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the People's Republic of China.

Examples of the types of products covered by this prohibition include phones, internet, video surveillance, and cloud servers when produced, provided, or used by the entities listed in the definition of "covered telecommunications equipment or services." *See* 2 C.F.R. § 200.471.

b. *Pre-Award Costs*

Pre-award costs are allowable only with the prior written approval of DHS/FEMA and as included in the award agreement. To request pre-award costs, a written request must be included with the application, signed by the AOR of the entity. The letter must outline what the pre-award costs are for, including a detailed budget break-out of pre-award costs from the post-award costs, and a justification for approval.

c. ***Management and Administration (M&A) Costs***

Management and administration (M&A) activities are allowable under this program. M&A activities are those 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.

Subrecipients may also retain a maximum of up to five percent of the funding passed through by the state solely for M&A purposes associated with the SLCGP award.

While the eligible entity may retain up to five percent of this total for M&A, the state must still ensure that all subrecipient award amounts meet the mandatory minimum pass-through requirements that are applicable to SLCGP. To meet this requirement, the percentage of funds passed through to local or tribal jurisdictions must be based on the state's total SLCGP award prior to withholding any M&A.

d. ***Indirect Facilities & Administrative (F&A) Costs***

Indirect costs are allowable under this program as described in 2 C.F.R. Part 200, including 2 C.F.R. § 200.414. Applicants with a current negotiated indirect cost rate agreement that desire to charge indirect costs to an award must provide a copy of their negotiated indirect cost rate agreement at the time of application. Not all applicants are required to have a current negotiated indirect cost rate agreement. Applicants that are not required by 2 C.F.R. Part 200 to have a negotiated indirect cost rate agreement but are required by 2 C.F.R. Part 200 to develop an indirect cost rate proposal must provide a copy of their proposal at the time of application. Applicants who do not have a current negotiated indirect cost rate agreement (including a provisional rate) and wish to charge the de minimis rate must reach out to the FEMA Grants Management Specialist for further instructions. Applicants who wish to use a cost allocation plan in lieu of an indirect cost rate must also reach out to the FEMA Grants Management Specialist for further instructions. Post-award requests to charge indirect costs will be considered on a case-by-case basis and based upon the submission of an agreement or proposal as discussed above or based upon on the de minimis rate or cost allocation plan, as applicable.

e. ***Other Direct Costs***

Funding guidelines established within this section support the development, updating, and implementing a cybersecurity plan. Allowable investments made in support of this goal must fall into the categories of planning, organization, exercises, training, or equipment, aligned to closing capability gaps or sustaining capabilities.

I. PLANNING

Planning costs are allowable under this program. SLCGP funds may be used for a range of planning activities, such as those associated with 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.

II. ORGANIZATION

Organization costs are allowable under this program. States must justify proposed expenditures of SLCGP funds to support organization activities within their IJ submission. Organizational activities 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.

III. EQUIPMENT

Equipment costs are allowable under this program. SLCGP equipment is 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 | FEMA.gov. 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.

IV. TRAINING

Training costs are allowable under this program. Allowable training-related costs under SLCGP include the establishment, support, conduct, and attendance of training and/or in conjunction with training by other federal agencies. Training conducted using SLCGP funds should align to the eligible entity's Cybersecurity Plan and address a performance gap identified through assessments and contribute to building a capability that will be evaluated through a formal exercise. Any training or training gaps, including training related to underserved communities that may be more impacted by disasters, including children, seniors, individuals with disabilities or access and functional needs, individuals with diverse culture and language use, individuals with lower economic capacity and other underserved populations, should be identified in an assessment and addressed in the eligible entity's training cycle. Recipients are encouraged to use existing training rather than developing new courses. When developing new courses, recipients are encouraged to apply the Analyze, Design, Develop, Implement, and Evaluate (ADDIE) model of instructional design.

Recipients are also encouraged to utilize FEMA's National Preparedness Course Catalog. Trainings include programs or courses developed for and delivered by institutions and organizations funded by FEMA. This includes the Center for Domestic Preparedness (CDP), the Emergency Management Institute (EMI), and FEMA's Training Partner Programs, including the Continuing Training Grants (CTG), the National Domestic Preparedness Consortium (NDPC), the Rural Domestic Preparedness Consortium (RDPC), and other partners.

The catalog features a wide range of course topics in multiple delivery modes to meet FEMA's mission scope as well as the increasing training needs of federal, state, local, territorial, and tribal audiences. The catalog can be accessed at http://www.firstrespondertraining.gov.

Some training activities require Environmental and Historic Preservation (EHP) Review, including exercises, drills, or trainings that require any type of land, water, or vegetation disturbance or building of temporary structures or that are not located at facilities designed to conduct training and exercises. Additional information on training requirements and EHP review can be found online at https://www.fema.gov/media-library/assets/documents/90195.

V. EXERCISES

Exercise costs are allowable under this program. Exercises conducted with grant funding should be managed and conducted consistent with Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP guidance for exercise design, development, conduct, evaluation, and improvement planning is located at https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep.

Some exercise activities require EHP review, including exercises, drills, or trainings that require any type of land, water, or vegetation disturbance or building of temporary structures or that are not located at facilities designed to conduct training and exercises. Additional information on training requirements and EHP review can be found online at https://www.fema.gov/media-library/assets/documents/90195.

E. Application Review Information

1. Application Evaluation Criteria

a. *Programmatic Criteria*

DHS/FEMA will evaluate the FY 2022 SLCGP applications for completeness and applicant eligibility. DHS/CISA will evaluate the FY 2022 SLCGP applications for adherence to programmatic guidelines, and anticipated effectiveness of the proposed investments. The review will include verification of the following elements:

- Establishment of and composition of the Planning Committee;
- Cybersecurity Plan(s) or request for exception; and
- Proposed projects that are consistent with the Cybersecurity Plan(s), or will be consistent with the Cybersecurity Plan if requesting a grant to develop a Plan, and SLCGP program objectives and requirements.

In addition to the above, DHS/CISA will evaluate whether proposed projects are: 1) both feasible and effective at reducing the risks for which the project was designed; and 2) able to be fully completed within the four-year period of performance. DHS will use the information provided in the application and after the submission of the first Program Performance Report (PPR) to determine the feasibility and effectiveness of a grant project.

b. *Financial Integrity Criteria*

Prior to making a federal award, FEMA is required by 31 U.S.C. § 3354, as enacted by the Payment Integrity Information Act of 2019, Pub. L. No. 116-117 (2020); 41 U.S.C. § 2313; and 2 C.F.R. § 200.206 to review information available through any Office of Management and Budget (OMB)-designated repositories of governmentwide eligibility qualification or financial integrity information, including whether the applicant is suspended or debarred. FEMA may also pose additional questions to the applicant to aid in conducting the pre-award risk review. Therefore, application evaluation criteria may include the following risk-based considerations of the applicant:

i. Financial stability.
ii. Quality of management systems and ability to meet management standards.
iii. History of performance in managing federal award.
iv. Reports and findings from audits.
v. Ability to effectively implement statutory, regulatory, or other requirements.

c. *Supplemental Financial Integrity Criteria and Review*

Prior to making a federal award where the anticipated total federal share will be greater than the simplified acquisition threshold, currently $250,000:

i. FEMA is required to review and consider any information about the applicant, including information on the applicant's immediate and highest-level owner,

subsidiaries, and predecessors, if applicable, that is in the designated integrity and performance system accessible through the System for Award Management (SAM), which is currently the Federal Awardee Performance and Integrity Information System (FAPIIS).

ii. An applicant, at its option, may review information in FAPIIS and comment on any information about itself that a federal awarding agency previously entered.

iii. FEMA will consider any comments by the applicant, in addition to the other information in FAPIIS, in making a judgment about the applicant's integrity, business ethics, and record of performance under federal awards when completing the review of risk posed by applicants as described in 2 C.F.R. § 200.206.

2. Review and Selection Process

FEMA will follow all applicable statutes, rules, and requirements and will take into consideration materials accompanying BIL and annual appropriations acts, such as the Joint Explanatory Statement, as appropriate, in reviewing and determining recipient eligibility.

All proposed investments will undergo a federal review by FEMA and CISA to verify compliance with all administrative and eligibility criteria identified in the NOFO. The federal review for compliance will be conducted by FEMA. FEMA will use a checklist to verify compliance with all administrative and eligibility criteria identified in the NOFO.

Applicants must demonstrate how investments support closing capability gaps or sustaining capabilities. DHS will review IJs at both the investment and project level. The following criteria will be applied to the review of projects:

- Clarity: Sufficient detail to understand what the project is intending to do with grant dollars. (Yes/No)
- Logical/Project Alignment: Alignment with the stated SLCGP objectives and the applicant's Cybersecurity Plan or with the development of a Cybersecurity Plan. (Yes/No)
- Reasonableness: Costs for the items/services outlined within the project description are reasonable. Execution within the period of performance is feasible. (Yes/No)

Projects rated as effective or promising are approved. If an exception request from the FY 2022 Cybersecurity Plan submission requirement was submitted, SLCGP funds can only initially be used for activities that are integral to the development of the Cybersecurity Plan or to assist with activities that address imminent cybersecurity threats. This is limited to investments and projects aligned to Objective 1 and Objective 2.

In addition, investments with emergency communications activities will be reviewed to verify compliance with SAFECOM Guidance. FEMA and CISA will coordinate directly with the recipient on any compliance concerns and will provide technical assistance as necessary to help ensure full compliance.

F. Federal Award Administration Information

1. Notice of Award

Before accepting the award, the AOR and recipient should carefully read the award package. The award package includes instructions on administering the grant award and the terms and conditions associated with responsibilities under federal awards. **Recipients must accept all conditions in this NOFO 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 ND Grants system through an automatic electronic mail to the recipient's authorized official listed in the initial application. The recipient should follow the directions in the notification to confirm acceptance of the award.

Recipients must accept their awards no later than 60 days from the award date. The recipient shall notify FEMA of its intent to accept and proceed with work under the award or provide a notice of intent to decline through the ND Grants system. For instructions on how to accept or decline an award in the ND Grants system, please see the ND Grants Grant Recipient User Guide, which is available at https://www.fema.gov/grants/guidance-tools/non-disaster-grants-management-system along with other ND Grants materials.

Funds will remain on hold until the recipient accepts the award through the ND Grants system 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 60-day timeframe may result in a loss of funds.

2. Pass-Through Requirements

a. *Generally*

The eligible entity or multi-entity group must pass through at least 80 percent of the federal funds provided under the grant to local governments, including rural areas, within the jurisdiction of the eligible entity or multi-entity group.

Four requirements must be met to pass-through grant funds:

- The eligible entity must make a firm written commitment to passing through grant funds or equivalent services to subrecipients;
- The eligible entity's commitment must be unconditional (i.e., no contingencies for the availability of eligible entity funds);
- There must be documentary evidence (i.e., award document, terms, and conditions) of the commitment; and
- The award terms must be communicated to the subrecipient.

The signatory authority of the eligible entity must certify in writing to DHS/FEMA that pass-through requirements have been met. A letter of intent (or equivalent) to distribute funds is not considered sufficient; after the funds have been distributed, the SAA must self-certify, on behalf of the state, that the pass-through requirements have been met.

b. *Rural Area Pass-Through*

As part of the local government pass through requirement, in obligating funds, items,

services, capabilities, or activities to local governments, each eligible entity or multi-entity group is required to pass through at least 25% of the federal funds provided under the grant to rural areas. 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.

The eligible entity or multi-entity group may either pass through 25% of the federal funds provided under the grant; items, services, capabilities, or activities having a value of at least 25% of the federal funds provided under the grant; or grant funds combined with other items, services, capabilities, or activities that have a total value of at least 25% of the federal funds provided under the grant.

Because the pass-through to rural entities is part of the overall 80% pass-through requirement to local governments, the eligible entity or multi-entity must obtain the consent of local governments if intending to pass through items, services, capabilities, or activities to rural areas in lieu of funding in order to count that value as part of the overall 80% pass-through requirement. *See* 6 U.S.C. §665g(n)(2)(A)-(B).

The same four criteria for pass-through to local governments also applies to the pass-through to rural areas within those local governments.

c. ***Exceptions***

The local government pass-through requirement, including the rural area pass-through requirement, does not apply to:

- Grants awarded solely to support activities integral to the development or revision of the Cybersecurity Plan of the eligible entity; or
- The District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, the United States Virgin Islands, or a Tribal government.

d. ***Timing***

The eligible entity must pass-through at least 80% of the funds awarded under the SLCGP to local governments, including at least 25% to rural areas, within 45 calendar days of receipt of the funds. "Receipt of the funds" occurs either when the eligible entity accepts the award or 15 calendar days after the eligible entity receives notice of the award, whichever is earlier.

Eligible entities are sent notification of SLCGP awards via the ND Grants system. If an eligible entity accepts its award within 15 calendar days of receiving notice of the award in the ND Grants system, the 45-calendar days pass-through period will start on the date the eligible entity accepted the award. Should an eligible entity not accept the SLCGP award within 15 calendar days of receiving notice of the award in the ND Grants system, the 45-calendar days pass-through period will begin 15 calendar days after the award notification is sent to the eligible entity via the ND Grants system.

It is important to note that the period of performance start date does not directly affect the

start of the 45-calendar day pass-through period. For example, an eligible entity may receive notice of the SLCGP award on September 20, 2022, while the period of performance dates for that award are October 1, 2022, through September 30, 2025. In this example, the 45-day pass-through period will begin on the date the eligible entity accepts the SLCGP award or October 5, 2022 (15 calendar days after the eligible entity was notified of the award), whichever date occurs first. The period of performance start date of October 1, 2022 would not affect the timing of meeting the 45-calendar day pass-through requirement.

e. ***Other Guidance and Requirements for Passing Through Items, Services, Capabilities, or Activities in Lieu of Funding***

The signatory authority of the eligible entity must certify in writing to DHS/FEMA that pass-through requirements have been met. A letter of intent (or equivalent) to distribute funds is not considered sufficient.

If a state wishes to pass through items, services, capabilities, or activities on a state-wide basis to all local governments and rural areas in lieu of funding, DHS recommends consulting with applicable municipal, city, county, rural area, or other local government councils or associations within the state to gauge the level of interest in and obtain consent to receive these in lieu of funding. DHS also recommends including these councils or associations in the Cybersecurity Planning Committees. States should also inform local governments, including rural areas, that by signing up for state-wide items, services, capabilities, or activities, that they are providing consent to receive these in lieu of funding.

States must still engage individual local governments as applicable to obtain consent where the state wants to pass through items, services, capabilities, or activities to a particular local government or rural area in lieu of funding. Consent can be given at individual local or tribal units of government, and does not have to be for all local governments within the state. If an individual unit of government does not consent to having the state retain a portion of funding, then the state must still pass-through funding to that local government, provided that entity has an approved project as part of the approved Cybersecurity Plan to utilize the funds.

In order for the SAA to retain more than 20% of SLCGP funds, the following conditions must be met:

- Must be for expenditures made by the state on behalf of the local or tribal government; and
- Must have written consent of the local or tribal government, specifying the amount of funds to be retained and the intended use of funds.

In providing these in lieu of funding, states must still ensure they are passing through an amount equal to at least 80% of the federal funding to local governments, including at least 25% to rural areas, within 45 days. The letter certifying the pass-through requirements have been met must indicate whether the state is passing through items, services, capabilities, or activities in lieu of funding as well as identify the consent it obtained from local governments. These decisions must also be documented in accordance with the Cybersecurity Planning Committee's Charter. For further information on Cybersecurity

Planning Committee requirements, see Appendix B.

3. Administrative and National Policy Requirements
In addition to the requirements of in this section and in this NOFO, FEMA may place specific terms and conditions on individual awards in accordance with 2 C.F.R. Part 200.

a. *DHS Standard Terms and Conditions*
All successful applicants for DHS grant and cooperative agreements are required to comply with DHS Standard Terms and Conditions, which are available online at: DHS Standard Terms and Conditions.

The applicable DHS Standard Terms and Conditions will be those in effect at the time the award was made. What terms and conditions will apply for the award will be clearly stated in the award package at the time of award.

b. *Ensuring the Protection of Civil Rights*
As the Nation works towards achieving the National Preparedness Goal, it is important to continue to protect the civil rights of individuals. Recipients and subrecipients must carry out their programs and activities, including those related to the building, sustainment, and delivery of core capabilities, in a manner that respects and ensures the protection of civil rights for protected populations.

Federal civil rights statutes, such as Section 504 of the Rehabilitation Act of 1973 and Title VI of the Civil Rights Act of 1964, along with DHS and FEMA regulations, prohibit discrimination on the basis of race, color, national origin, sex, religion, age, disability, limited English proficiency, or economic status in connection with programs and activities receiving federal financial assistance from FEMA.

The DHS Standard Terms and Conditions include a fuller list of the civil rights provisions that apply to recipients. These terms and conditions can be found in the DHS Standard Terms and Conditions. Additional information on civil rights provisions is available at https://www.fema.gov/about/offices/equal-rights/civil-rights.

Monitoring and oversight requirements in connection with recipient compliance with federal civil rights laws are also authorized pursuant to 44 C.F.R. Part 7.

In accordance with civil rights laws and regulations, recipients and subrecipients must ensure the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment.

c. *Environmental Planning and Historic Preservation (EHP) Compliance*
As a federal agency, FEMA is required to consider the effects of its actions on the environment and historic properties to ensure that all activities and programs funded by FEMA, including grant-funded projects, comply with federal EHP laws, Executive Orders, regulations, and policies, as applicable.

All non-critical new construction or substantial improvement of structures in a Special Flood Hazard Area must, at a minimum, apply the flood elevations of the Federal Flood Risk Management Standard's Freeboard Value Approach unless doing so would cause the project to be unable to meet applicable program cost-effectiveness requirements. All other types of projects may choose to apply the flood elevations of the Federal Flood Risk Management Standard's Freeboard Value Approach. See Executive Order (EO) 14030, Climate-Related Financial Risk and FEMA Policy #-206-21-0003, Partial Implementation of the Federal Flood Risk Management Standard for Hazard Mitigation Assistance Programs (Interim).

Recipients and subrecipients proposing projects that have the potential to impact the environment, including, but not limited to, the construction of communication towers, modification or renovation of existing buildings, structures, and facilities, or new construction including replacement of facilities, must participate in the FEMA EHP review process. The EHP review process involves the submission of a detailed project description along with any supporting documentation requested by FEMA in order to determine whether the proposed project has the potential to impact environmental resources or historic properties.

In some cases, FEMA is also required to consult with other regulatory agencies and the public in order to complete the review process. Federal law requires EHP review to be completed before federal funds are released to carry out proposed projects. FEMA may not be able to fund projects that are not incompliance with applicable EHP laws, Executive Orders, regulations, and policies.

Executive Order (EO) 13985, Advancing Racial Equity and Support for Underserved Communities through the Federal Government, rearticulates and strengthens the environmental justice framework articulated in 1994 in EO 12898, Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations. Specifically, Section 1 of E.O. 13985 states that: "Affirmatively advancing equity, civil rights, racial justice, and equal opportunity is the responsibility of the whole of our Government. Because advancing equity requires a systemic approach to embedding fairness in decision-making processes, executive departments and agencies…must recognize and work to redress inequalities in their policies and programs that serve as barriers to equal opportunity."

Many projects funded by GPD's grant programs can have significant impacts on environmental justice. In particular, construction of buildings and other structures and construction of new communication towers may have disproportionately high and adverse effects on minority and low-income populations. FEMA acknowledges the important role that FEMA recipients and subrecipients play in advancing and achieving environmental justice by identifying low-income and minority populations within a proposed project's affected area as early as possible and taking steps to accommodate these interests.

For consistency with the Administration's policy, FEMA will review and evaluate potential projects for racial equity and justice concerns. If FEMA determines that a proposed project would have a disproportionately high and adverse effect on minority or low-income

populations, FEMA will consult with recipients and subrecipients to discuss the feasibility of revising the scope of work to avoid these adverse impacts, or otherwise applying mitigation measures to alleviate these effects. In addition, FEMA may work with other recipients and subrecipients to solicit public input on the proposed projects for a more informed decision-making process. To learn more about how FEMA environmental justice responsibilities might affect your project, go to https://www.fema.gov/fact-sheet/executive-order-12898-environmental-justice.

DHS and FEMA EHP policy is found in directives and instructions available on the FEMA.gov EHP page, the FEMA website page that includes documents regarding EHP responsibilities and program requirements, including implementation of the National Environmental Policy Act and other EHP regulations and Executive Orders.

The GPD EHP screening form is located at https://www.fema.gov/media-library/assets/documents/90195. Additionally, all recipients under this funding opportunity are required to comply with the FEMA GPD EHP Policy Guidance, FEMA Policy #108-023-1, available at https://www.fema.gov/media-library/assets/documents/85376.

d. ***SAFECOM Guidance Compliance***

All entities using SLCGP funding to support emergency communications investments are required to comply with the SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance). The SAFECOM Guidance provides current information on emergency communications policies, eligible costs, best practices, and technical standards for SLT recipients investing federal funds in emergency communications projects. It is also designed to promote and align with the National Emergency Communications Plan (NECP). Conformance with the SAFECOM Guidance helps ensure that federally funded investments are compatible, interoperable, resilient, and support national goals and objectives for improving emergency communications. Applicants should use the SAFECOM Guidance during planning, development, and implementation of emergency communications projects and in conjunction with other planning documents. Specifically, Appendix D of the SAFECOM Guidance contains compliance instructions for SLCGP grant recipients.

If an entity uses SLCGP funding to support emergency communications investments, the following requirements shall apply to all such grant-funded communications investments in support of the emergency communications priorities and recognized best practices:
The signatory authority for the eligible entity must certify in writing to DHS/FEMA their compliance with the SAFECOM Guidance. The certification letter should be coordinated with the Statewide Interoperability Coordinator (SWIC) for each state and must be uploaded to ND Grants at the time of the first Program Performance Report (PPR) submission.

e. Requirement for using CISA Services

As a condition of receiving SLCGP funding, the grant recipient is required to adhere to or sign up for the following services, sponsored by CISA and further described in Appendix G, upon award as part of the statutory requirements in developing, implementing, or revising a Cybersecurity Plan. Participation in these services and memberships are not required for submission and approval of a grant:

- Sign up for cyber hygiene services, specifically vulnerability scanning and web application scanning; and
- Complete the Nationwide Cybersecurity Review, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually thereafter.

Recipients and subrecipients are also encouraged to sign up for the other services and memberships identified in Appendix G.

4. Reporting

Recipients are required to submit various financial and programmatic reports as a condition of award acceptance. Future awards and funds drawdown may be withheld if these reports are delinquent.

a. *Financial Reporting Requirements*

I. FEDERAL FINANCIAL REPORT (FFR)

Recipients must report obligations and expenditures through the FFR form (SF-425) to FEMA on a quarterly basis through the FFR form (SF-425). Recipients may review the Federal Financial Reporting Form (FFR) (SF-425) at https://www.grants.gov/web/grants/forms/post-award-reporting-forms.html#sortby=1

Recipients must file the FFR electronically using the Payment and Reporting Systems (PARS).

II. FFR REPORTING PERIODS AND DUE DATES

An FFR must be submitted quarterly throughout the period of performance, including partial calendar quarters, as well as in periods where no grant award activity occurs. The final FFR is due within 120 calendar days after the end of the period of performance. Future awards and fund drawdowns may be withheld if these reports are delinquent, demonstrate lack of progress, or are insufficient in detail.

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

b. *Programmatic Performance Reporting Requirements*

I. PERFORMANCE PROGRESS REPORT (PPR)

Recipients are responsible for providing updated performance reports on an annual basis, consistent with the authorizing statute, as an attachment in ND Grants. The PPR should include a:

- 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.

Program Performance Reporting Periods and Due Dates
The annual PPR submission is due January 30 of each year to account for the previous calendar year.

c. *Closeout Reporting Requirements*

I. 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:

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

In addition, pass-through entities are responsible for closing out their subawards as described in 2 C.F.R. § 200.344; subrecipients are still required to submit closeout materials within 90 calendar days of the period of performance end date. When a subrecipient completes all closeout requirements, pass-through entities must promptly complete all closeout actions for subawards in time for the recipient to submit all necessary documentation and information to FEMA during the closeout of the prime award.

After the prime award closeout reports have been reviewed and approved by FEMA, a closeout notice will be completed to close out the grant. The notice will indicate the period of performance as closed, list any remaining funds that will be deobligated, and address the requirement of maintaining the grant records for at least three years from the date of the final FFR. The record retention period may be longer, such as due to an audit or litigation, for equipment or real property used beyond the period of performance, or due to other circumstances outlined in 2 C.F.R. § 200.334.

The recipient is responsible for refunding to FEMA any balances of unobligated cash that FEMA paid that are not authorized to be retained per 2 C.F.R. § 200.344(d).

II. ADMINISTRATIVE CLOSEOUT

Administrative closeout is a mechanism for FEMA to unilaterally move forward with closeout of an award using available award information in lieu of final reports from the recipient per 2 C.F.R. § 200.344(h)-(i). It is a last resort available to FEMA, and if FEMA needs to administratively close an award, this may negatively impact a recipient's ability to

obtain future funding. This mechanism can also require FEMA to make cash or cost adjustments and ineligible cost determinations based on the information it has, which may result in identifying a debt owed to FEMA by the recipient.

When a recipient is not responsive to FEMA's reasonable efforts to collect required reports needed to complete the standard closeout process, FEMA is required under 2 C.F.R. § 200.344(h) to start the administrative closeout process within the regulatory timeframe. FEMA will make at least three written attempts to collect required reports before initiating administrative closeout. If the recipient does not submit all required reports in accordance with 2 C.F.R. § 200.344, this NOFO, and the terms and conditions of the award, FEMA must proceed to administratively close the award with the information available within one year of the period of performance end date. Additionally, if the recipient does not submit all required reports within one year of the period of performance end date, per 2 C.F.R. § 200.344(i), FEMA must report in FAPIIS the recipient's material failure to comply with the terms and conditions of the award.

If FEMA administratively closes an award where no final FFR has been submitted, FEMA uses that administrative closeout date in lieu of the final FFR submission date as the start of the record retention period under 2 C.F.R. § 200.334.

In addition, if an award is administratively closed, FEMA may decide to impose remedies for noncompliance per 2 C.F.R. § 200.339, consider this information in reviewing future award applications, or apply special conditions to existing or future awards.

d. ***Additional Reporting Requirements***

i. DISCLOSING INFORMATION PER 2 C.F.R. § 180.335

This reporting requirement pertains to disclosing information related to government-wide suspension and debarment requirements. Before a recipient enters into a grant award with FEMA, the recipient must notify FEMA if it knows if it or any of the recipient's principals under the award fall under one or more of the four criteria listed at 2 C.F.R. § 180.335:

i. Are presently excluded or disqualified;
ii. Have been convicted within the preceding three years of any of the offenses listed in 2 C.F.R. § 180.800(a) or had a civil judgment rendered against it or any of the recipient's principals for one of those offenses within that time period;
iii. Are presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state or local) with commission of any of the offenses listed in 2 C.F.R. § 180.800(a); or
iv. Have had one or more public transactions (federal, state, or local) terminated within the preceding three years for cause or default.

At any time after accepting the award, if the recipient learns that it or any of its principals falls under one or more of the criteria listed at 2 C.F.R. § 180.335, the recipient must provide immediate written notice to FEMA in accordance with 2 C.F.R. § 180.350.

II. Reporting of Matters Related to Recipient Integrity and Performance

Per 2 C.F.R. Part 200, Appendix I § F.3, the additional post-award reporting requirements in 2 C.F.R. Part 200, Appendix XII may apply to applicants who, if upon becoming recipients, have a total value of currently active grants, cooperative agreements, and procurement contracts from all federal awarding agencies that exceeds $10,000,000 for any period of time during the period of performance of an award under this funding opportunity.

Recipients that meet these criteria must maintain current information reported in FAPIIS about civil, criminal, or administrative proceedings described in paragraph 2 of Appendix XII at the reporting frequency described in paragraph 4 of Appendix XII.

III. Single Audit Report

For audits of fiscal years beginning on or after December 26, 2014, recipients that expend $750,000 or more from all federal funding sources during their fiscal year are required to submit an organization-wide financial and compliance audit report, also known as the single audit report.

The audit must be performed in accordance with the requirements of U.S. Government Accountability Office's (GAO) Government Auditing Standards, located at https://www.gao.gov/yellowbook/overview, and the requirements of Subpart F of 2 C.F.R. Part 200, located at http://www.ecfr.gov/cgi-bin/text-idx?node=sp2.1.200.f.

5. Program Evaluation

Recipients and subrecipients are encouraged to incorporate program evaluation activities from the outset of their program design and implementation to meaningfully document and measure their progress towards the outcomes proposed. Title I of the Foundations for Evidence-Based Policymaking Act of 2018 (Evidence Act), Pub. L. No. 115-435 (2019) defines evaluation as "an assessment using systematic data collection and analysis of one or more programs, policies, and organizations intended to assess their effectiveness and efficiency." Evidence Act § 101 (codified at 5 U.S.C. § 311). Credible program evaluation activities are implemented with relevance and utility, rigor, independence and objectivity, transparency, and ethics (OMB Circular A-11, Part 6 Section 290).

Evaluation costs are allowable costs (either as direct or indirect), unless prohibited by statute or regulation, and such costs may include the personnel and equipment needed for data infrastructure and expertise in data analysis, performance, and evaluation. (2 C.F.R. § 200).

In addition, recipients are required to participate in a DHS-led evaluation if selected, which may be carried out by a third-party on behalf of the Program Office or DHS. By accepting grant funds, recipients agree to participate in the evaluation, which may include analysis of individuals who benefit from the grant, and provide access to program operating personnel and participants, as specified by the evaluator(s) for six months after the period of performance.

6. Monitoring and Oversight

Per 2 C.F.R. § 200.337, DHS, through its authorized representatives, has the right, at all reasonable times, to make site visits or conduct desk reviews to review project accomplishments and management control systems to review award progress and to provide any required technical assistance, in the form of one-on-one guidance from a combination of Regional or Headquarters FEMA and CISA Staff. During site visits or desk reviews, DHS will review recipients' files related to the award. As part of any monitoring and program evaluation activities, recipients must permit DHS, upon reasonable notice, to review grant-related records and to interview the organization's staff and contractors regarding the program. Recipients must respond in a timely and accurate manner to DHS requests for information relating to the award.

Effective monitoring and oversight help DHS ensure that recipients use grant funds for their intended purpose(s); verify that projects undertaken are consistent with approved plans; and ensure that recipients make adequate progress toward stated goals and objectives. Additionally, monitoring serves as the primary mechanism to ensure that recipients comply with applicable laws, rules, regulations, program guidance, and requirements. DHS regularly monitors all grant programs both financially and programmatically in accordance with federal laws, regulations (including 2 C.F.R. Part 200), program guidance, and the terms and conditions of the award. All monitoring efforts ultimately serve to evaluate progress towards grant goals and proactively target and address issues that may threaten grant success during the period of performance. If the monitoring results in a determination that basic, minimum requirements as outlined in this NOFO are not being met, DHS may require corrective actions and/or initiate termination of the award.

DHS staff will periodically monitor recipients to ensure that administrative processes, policies and procedures, budgets, and other related award criteria are meeting Federal Government-wide and DHS regulations. Aside from reviewing quarterly financial and annual programmatic reports, DHS may also conduct enhanced monitoring through either desk-based reviews, onsite monitoring visits, or both. Enhanced monitoring will involve the review and analysis of the financial compliance and administrative processes, policies, activities, and other attributes of each federal assistance award, and it will identify areas where the recipient may need technical assistance, corrective actions, or other support.

Financial and programmatic monitoring are complementary processes within DHS's overarching monitoring strategy that function together to ensure effective grants management, accountability, and transparency; validate progress against grant and program goals; and safeguard federal funds against fraud, waste, and abuse. Financial monitoring primarily focuses on statutory and regulatory compliance with administrative grant requirements, while programmatic monitoring seeks to validate and assist in grant progress, targeting issues that may be hindering achievement of project goals and ensuring compliance with the purpose of the grant and grant program. Both monitoring processes are similar in that they feature initial reviews of all open awards, and additional, in-depth monitoring of grants requiring additional attention.

Recipients and subrecipients who are pass-through entities are responsible for monitoring their subrecipients in a manner consistent with the terms of the federal award at 2 C.F.R. Part 200, including 2 C.F.R. § 200.332. This includes the pass-through entity's responsibility to monitor the activities of the subrecipient as necessary to ensure that the subaward is used for authorized purposes, in compliance with federal statutes, regulations, and the terms and conditions of the subaward; and that subaward performance goals are achieved.
In terms of overall award management, recipient and subrecipient responsibilities include, but are not limited to: accounting of receipts and expenditures, cash management, maintaining adequate financial records, reporting and refunding expenditures disallowed by audits, monitoring if acting as a pass-through entity, or other assessments and reviews, and ensuring overall compliance with the terms and conditions of the award or subaward, as applicable, including the terms of 2 C.F.R. Part 200.

I. FINANCIAL MONITORING OVERVIEW AND APPROACH

FEMA's approach to financial monitoring provides a standard monitoring framework that promotes consistent processes across all monitoring staff. There are four core components of the monitoring process:

1. **Monitoring Assessment:** Monitoring staff measure each grant's monitoring needs using a system of pre-determined evaluation criteria. The criteria help assess the recipient and potential challenges to the success of the grant award.

2. **Monitoring Selection and Scheduling:** Monitoring staff make selection and scheduling decisions in accordance with applicable statutory requirements, such as the Homeland Security Act of 2002, as amended, and consider the results of the monitoring assessment process.

3. **Monitoring Activities:** Monitoring activities include cash analysis, desk reviews, and site visits. Grants Management Specialists are responsible for conducting quarterly or semi-annual reviews of all grants via cash analysis. Desk reviews and site visits are additional monitoring activities conducted on grants where the monitoring assessment process identified the need for additional monitoring and validated the use of FEMA resources for these activities.

4. **Post-Monitoring Actions:** Monitoring staff may follow up with recipients via post-monitoring actions based on the outcomes of monitoring activities. Post-monitoring actions include conducting additional monitoring; reviewing Corrective Action Plans (CAP) and monitoring the progress of CAP deliverables; documenting the resolution of identified corrective actions and issues; providing technical assistance and recipient training; and debt collection.

G. DHS Awarding Agency Contact Information

1. Contact and Resource Information

a. *Centralized Scheduling and Information Desk (CSID)*

CSID is a non-emergency comprehensive management and information resource developed by FEMA for grants stakeholders. CSID provides general information on all FEMA grant

programs and maintains a comprehensive database containing key personnel contact information at the federal, state, and local levels. When necessary, recipients will be directed to a federal point of contact who can answer specific programmatic questions or concerns. CSID can be reached by phone at (800) 368-6498 or by e-mail at askcsid@fema.dhs.gov, Monday through Friday, 9a.m. – 5 p.m. ET.

b. ***Grant Programs Directorate (GPD) Award Administration Division***
GPD's Award Administration Division (AAD) provides support regarding financial matters and budgetary technical assistance. Additional guidance and information can be obtained by contacting the AAD's Help Desk via e-mail at ASK-GMD@fema.dhs.gov.

c. ***Equal Rights***
The FEMA Office of Equal Rights (OER) is responsible for compliance with and enforcement of federal civil rights obligations in connection with programs and services conducted by FEMA and recipients of FEMA financial assistance. All inquiries and communications about federal civil rights compliance for FEMA grants under this NOFO should be sent to FEMA-CivilRightsOffice@fema.dhs.gov.

d. ***Environmental Planning and Historic Preservation***
GPD's EHP Team provides guidance and information about the EHP review process to recipients and subrecipients. All inquiries and communications about GPD projects under this NOFO or the EHP review process, including the submittal of EHP review materials, should be sent to gpdehpinfo@fema.dhs.gov.

2. Systems Information

a. ***Grants.gov***
For technical assistance with Grants.gov, call the customer support hotline 24 hours per day, 7 days per week (except federal holidays) at (800) 518-4726 or e-mail at support@grants.gov.

b. ***Non-Disaster (ND) Grants***
For technical assistance with the ND Grants system, please contact the ND Grants Helpdesk at ndgrants@fema.dhsgov or (800) 865-4076, Monday through Friday, 9 a.m. – 6 p.m. ET. User resources are available at https://www.fema.gov/grants/guidance-tools/non-disaster-grants-management-system

c. ***Payment and Reporting System (PARS)***
FEMA uses the Payment and Reporting System (PARS) for financial reporting, invoicing, and tracking payments. FEMA uses the Direct Deposit/Electronic Funds Transfer (DD/EFT) method of payment to recipients. To enroll in the DD/EFT, recipients must complete a Standard Form 1199A, Direct Deposit Form. If you have questions about the online system, please call the Customer Service Center at (866) 927-5646 or email ask-GMD@fema.dhs.gov.

H. Additional Information

1. Termination Provisions

FEMA may terminate a federal award in whole or in part for one of the following reasons. FEMA and the recipient must still comply with closeout requirements at 2 C.F.R. §§ 200.344-200.345 even if an award is terminated in whole or in part. To the extent that subawards are permitted under this NOFO, pass-through entities should refer to 2 C.F.R. § 200.340 for additional information on termination regarding subawards.

a. ***Noncompliance***

If a recipient fails to comply with the terms and conditions of a federal award, FEMA may terminate the award in whole or in part. If the noncompliance can be corrected, FEMA may first attempt to direct the recipient to correct the noncompliance. This may take the form of a Compliance Notification. If the noncompliance cannot be corrected or the recipient is non-responsive, FEMA may proceed with a Remedy Notification, which could impose a remedy for noncompliance per 2 C.F.R. § 200.339, including termination. Any action to terminate based on noncompliance will follow the requirements of 2 C.F.R. §§ 200.341-200.342 as well as the requirement of 2 C.F.R. § 200.340(c) to report in FAPIIS the recipient's material failure to comply with the award terms and conditions. See also the section on Actions to Address Noncompliance in this NOFO.

b. ***With the Consent of the Recipient***

FEMA may also terminate an award 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.

c. ***Notification by the Recipient***

The recipient may terminate the award, in whole or in part, by sending written notification to FEMA 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, FEMA may determine that a partially terminated award will not accomplish the purpose of the federal award, so FEMA may terminate the award in its entirety. If that occurs, FEMA will follow the requirements of 2 C.F.R. §§ 200.341-200.342 in deciding to fully terminate the award.

2. Period of Performance Extensions

Extensions to the period of performance for this program are allowed. Extensions to the period of performance identified in the award will only be considered through formal, written requests to FEMA and must contain specific and compelling justifications as to why an extension is required. Recipients are advised to coordinate with FEMA and CISA, as needed, when preparing an extension request.

All extension requests must address the following:

a. The grant program, fiscal year, and award number;
b. Reason for the delay –including details of the legal, policy, or operational challenges that prevent the final outlay of awarded funds by the deadline;
c. Current status of the activity(ies);

d. Approved period of performance termination date and new project completion date;
e. Amount of funds drawn down to date;
f. Remaining available funds, both federal and, if applicable, non-federal;
g. Budget outlining how remaining federal and, if applicable, non-federal funds will be expended;
h. Plan for completion, including milestones and timeframes for achieving each milestone and the position or person responsible for implementing the plan for completion; and
i. Certification that the activity(ies) will be completed within the extended period of performance without any modification to the original statement of work, as described in the investment justification and as approved by DHS.

Extension requests will be granted only due to compelling legal, policy, or operational challenges. Extension requests will only be considered for the following reasons:

- Contractual commitments by the recipient or subrecipient with vendors prevent completion of the project, including delivery of equipment or services, within the existing period of performance;
- The project must undergo a complex environmental review that cannot be completed within the existing period of performance;
- Projects are long-term by design, and therefore acceleration would compromise core programmatic goals; or
- Where other special or extenuating circumstances exist.

Recipients should submit all proposed extension requests to DHS for review and approval at least 120 days prior to the end of the period of performance to allow sufficient processing time. Extensions are typically granted for no more than a six-month period.

3. Disability Integration

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.

The following are examples that demonstrate the integration of the needs of people with disabilities in carrying out FEMA awards under this program:

- Include representatives of organizations that work with/for people with disabilities on planning committees, work groups and other bodies engaged in development and implementation of the grant programs and activities.
- Hold all activities related to the grant in locations that are accessible to persons with physical disabilities to the extent practicable.

- Acquire language translation services, including American Sign Language, that provide public information across the community and in shelters.
- Ensure shelter-specific grant funds are in alignment with FEMA's Guidance on Planning for Integration of Functional Needs Support Services in General Population Shelters.
- If making alterations to an existing building to a primary function area utilizing federal funds, complying with the most recent codes and standards and making path of travel to the primary function area accessible to the greatest extent possible.
- Implement specific procedures used by public transportation agencies that include evacuation and passenger communication plans and measures for individuals with disabilities.
- Identify, create, and deliver training to address any training gaps specifically aimed toward whole-community preparedness. Include and interact with individuals with disabilities, aligning with the designated program capability.
- Establish best practices in inclusive planning and preparedness that consider physical access, language access, and information access. Examples of effective communication access include providing auxiliary aids and services such as sign language interpreters, Computer Aided Real-time Translation (CART), and materials in Braille or alternate formats.

FEMA grant recipients can fund projects towards the resilience of the whole community, including people with disabilities, such as training, outreach and safety campaigns, provided that the project aligns with this NOFO and the terms and conditions of the award.

4. Conflicts of Interest in the Administration of Federal Awards or Subawards

For conflicts of interest under grant-funded procurements and contracts, refer to the section on Procurement Integrity in this NOFO and 2 C.F.R. §§ 200.317 – 200.327.

To eliminate and reduce the impact of conflicts of interest in the subaward process, recipients and pass-through entities must follow their own policies and procedures regarding the elimination or reduction of conflicts of interest when making subawards. Recipients and pass-through entities are also required to follow any applicable federal and SLT statutes or regulations governing conflicts of interest in the making of subawards.

The recipient or pass-through entity must disclose to the respective Preparedness Officer or Program Manager, in writing, any real or potential conflict of interest that may arise during the administration of the federal award, as defined by the federal or SLT statutes or regulations or their own existing policies, within five days of learning of the conflict of interest. Similarly, subrecipients, whether acting as subrecipients or as pass-through entities, must disclose any real or potential conflict of interest to the recipient or next-level pass-through entity as required by the recipient or pass-through entity's conflict of interest policies, or any applicable federal or SLT statutes or regulations.

Conflicts of interest may arise during the process of DHS making a federal award in situations where an employee, officer, or agent, any members of his or her immediate family,

his or her partner has a close personal relationship, a business relationship, or a professional relationship, with an applicant, subapplicant, recipient, subrecipient, or DHS employees.

5. Procurement Integrity

Through audits conducted by the DHS Office of Inspector General (OIG) and FEMA grant monitoring, findings have shown that some FEMA recipients have not fully adhered to the proper procurement requirements at 2 C.F.R. §§ 200.317 – 200.327 when spending grant funds. Anything less than full compliance with federal procurement requirements jeopardizes the integrity of the grant as well as the grant program. To assist with determining whether an action is a procurement or instead a subaward, please consult 2 C.F.R. § 200.331. For detailed guidance on the federal procurement standards, recipients and subrecipients should refer to various materials issued by FEMA's Procurement Disaster Assistance Team (PDAT), such as the PDAT Field Manual and Contract Provisions Guide. Additional resources, including an upcoming trainings schedule can be found on the PDAT Website: https://www.fema.gov/grants/procurement.

The below highlights the federal procurement requirements for FEMA recipients when procuring goods and services with federal grant funds. FEMA will include a review of recipients' procurement practices as part of the normal monitoring activities. **All procurement activity must be conducted in accordance with federal procurement standards at 2 C.F.R. §§ 200.317 – 200.327.** Select requirements under these standards are listed below. The recipient and any of its subrecipients must comply with all requirements, even if they are not listed below.

Under 2 C.F.R. § 200.317, when procuring property and services under a federal award, states (including territories) must follow the same policies and procedures they use for procurements from their non-federal funds; additionally, states must now follow 2 C.F.R. § 200.321 regarding socioeconomic steps, 200.322 regarding domestic preferences for procurements, 200.323 regarding procurement of recovered materials, and 2 C.F.R. § 200.327 regarding required contract provisions.

All other non-federal entities, such as tribes (collectively, non-state entities), must have and use their own documented procurement procedures that reflect applicable SLT 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.

a. *Important Changes to Procurement Standards in 2 C.F.R. Part 200*

OMB recently updated various parts of Title 2 of the Code of Federal Regulations, among them, the procurement standards. States are now required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. § 200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States per 2 C.F.R. § 200.322. More

information on OMB's revisions to the federal procurement standards can be found in Purchasing Under a FEMA Award: OMB Revisions Fact Sheet.

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).

See 2 C.F.R. §§ 200.216, 200.471, and Appendix II as well as section D.13.a of the NOFO regarding prohibitions on covered telecommunications equipment or services.

b. ***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; and
- Any arbitrary action in the procurement process.

Per 2 C.F.R. § 200.319(c), non-federal entities other than states must conduct procurements in a manner that prohibits the use of statutorily or administratively imposed SLT geographical preferences in the evaluation of bids or proposals, except in those cases where applicable federal statutes expressly mandate or encourage geographic preference. Nothing in this section preempts state licensing laws. When contracting for architectural and engineering services, geographic location may be a selection criterion provided its application leaves an appropriate number of qualified firms, given the nature and size of the project, to compete for the contract.

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.** Such conflicts of interest would arise when the employee, officer or agent, any member of his or her immediate family, his or her partner, or an organization that employs or is about to employ any of the parties indicated herein, has a financial or other interest in or a tangible personal benefit from a firm considered for a contract. The officers, employees, and agents of the non-federal entity may neither solicit nor accept gratuities, favors, or anything of monetary value from contractors or parties to subcontracts. However, non-federal entities may set standards for situations in which the financial interest is not substantial, or the gift is an unsolicited item of nominal value. The standards of conduct must provide for disciplinary actions to be applied for violations of such standards by officers, employees, or agents of the non-federal entity.

Under 2 C.F.R. 200.318(c)(2), if the recipient or subrecipient (other than states) has a parent, affiliate, or subsidiary organization that is not a state, local, tribal, or territorial government, the non-federal entity must also maintain written standards of conduct covering organizational conflicts of interest. In this context, organizational conflict of interest means that because of a relationship with a parent company, affiliate, or subsidiary organization, the non-federal entity is unable or appears to be unable to be impartial in conducting a procurement action involving a related organization. The non-federal entity must disclose in writing any potential conflicts of interest to FEMA or the pass-through entity in accordance with applicable FEMA policy.

c. ***Supply Schedules and Purchasing Programs***

Generally, a non-federal entity may seek to procure goods or services from a federal supply schedule, state supply schedule, or group purchasing agreement.

I. General Services Administration Schedules

States, tribes, and local governments, and any instrumentality thereof (such as local education agencies or institutions of higher education) may procure goods and services from a General Services Administration (GSA) schedule. GSA offers multiple efficient and effective procurement programs for state, tribal, and local governments, and instrumentalities thereof, to purchase products and services directly from pre-vetted contractors. The GSA Schedules (also referred to as the Multiple Award Schedules and the Federal Supply Schedules) are long-term government-wide contracts with commercial firms that provide access to millions of commercial products and services at volume discount pricing.

Information about GSA programs for states, tribes, and local governments, and instrumentalities thereof, can be found at https://www.gsa.gov/resources-for/programs-for-State-and-local-governments and https://www.gsa.gov/buying-selling/purchasing-programs/gsa-schedules/schedule-buyers/state-and-local-governments.

For tribes, local governments, and their instrumentalities that purchase off of a GSA schedule, this will satisfy the federal requirements for full and open competition provided that the recipient follows the GSA ordering procedures; however, tribes, local governments, and their instrumentalities will still need to follow the other rules under 2 C.F.R. §§ 200.317 – 200.327, such as solicitation of minority businesses, women's business enterprises, small businesses, or labor surplus area firms (§ 200.321), domestic preferences (§ 200.322), contract cost and price (§ 200.324), and required contract provisions (§ 200.327 and Appendix II).

II. Other Supply Schedules and Programs

For non-federal entities other than states, such as tribes, local governments, and nonprofits, that want to procure goods or services from a state supply schedule, cooperative purchasing program, or other similar program, in order for such procurements to be permissible under federal requirements, the following must be true:

- The procurement of the original contract or purchasing schedule and its use by the non-federal entity complies with state and local law, regulations, and written procurement procedures;
- The state or other entity that originally procured the original contract or purchasing schedule entered into the contract or schedule with the express purpose of making it available to the non-federal entity and other similar types of entities;
- The contract or purchasing schedule specifically allows for such use, and the work to be performed for the non-federal entity falls within the scope of work under the contract as to type, amount, and geography;
- The procurement of the original contract or purchasing schedule complied with all the procurement standards applicable to a non-federal entity other than states under at 2 C.F.R. §§ 200.317 – 200.327; and
- With respect to the use of a purchasing schedule, the non-federal entity must follow ordering procedures that adhere to applicable state, tribal, and local laws and regulations and the minimum requirements of full and open competition under 2 C.F.R. Part 200.

If a non-federal entity other than a state seeks to use a state supply schedule, cooperative purchasing program, or other similar type of arrangement, FEMA recommends the recipient discuss the procurement plans with its FEMA Grants Management Specialist.

d. ***Procurement Documentation***

Per 2 C.F.R. § 200.318(i), non-federal entities other than states and territories are required to maintain and retain records sufficient to detail the history of procurement covering at least the rationale for the procurement method, selection of contract type, contractor selection or rejection, and the basis for the contract price. States and territories are encouraged to maintain and retain this information as well and are reminded that in order for any cost to be allowable, it must be adequately documented per 2 C.F.R. § 200.403(g).

Examples of the types of documents that would cover this information include but are not limited to:

- Solicitation documentation, such as requests for quotes, invitations for bids, or requests for proposals;
- Responses to solicitations, such as quotes, bids, or proposals;
- Pre-solicitation independent cost estimates and post-solicitation cost/price analyses on file for review by federal personnel, if applicable;
- Contract documents and amendments, including required contract provisions; and
- Other documents required by federal regulations applicable at the time a grant is awarded to a recipient.

Additional information on required procurement records can be found on pages 24-26 of the PDAT Field Manual.

6. Record Retention

a. ***Record Retention Period***

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).

b. ***Types of Records to Retain***

FEMA requires that non-federal entities 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.

7. Actions to Address Noncompliance

Non-federal entities receiving financial assistance funding from FEMA are required to comply with requirements in the terms and conditions of their awards or subawards, including the terms set forth in applicable federal statutes, regulations, NOFOs, and policies. Throughout the award lifecycle or even after an award has been closed, FEMA or the pass-through entity may discover potential or actual noncompliance on the part of a recipient or subrecipient. This potential or actual noncompliance may be discovered through routine monitoring, audits, closeout, or reporting from various sources.

In the case of any potential or actual noncompliance, FEMA may place special conditions on an award per 2 C.F.R. §§ 200.208 and 200.339, FEMA may place a hold on funds until the matter is corrected, or additional information is provided per 2 C.F.R. § 200.339, or it may do both. Similar remedies for noncompliance with certain federal civil rights laws are authorized pursuant to 44 C.F.R. Parts 7 and 19.

In the event the noncompliance is not able to be corrected by imposing additional conditions or the recipient or subrecipient refuses to correct the matter, FEMA might take other remedies allowed under 2 C.F.R. § 200.339. These remedies include actions to disallow costs, recover funds, wholly or partly suspend or terminate the award, initiate suspension and debarment proceedings, withhold further federal awards, or take other remedies that may be legally available. For further information on termination due to noncompliance, see the section on Termination Provisions in the NOFO.

FEMA may discover and take action on noncompliance even after an award has been closed. The closeout of an award does not affect FEMA's right to disallow costs and recover funds as long the action to disallow costs takes place during the record retention period. *See* 2 C.F.R. §§ 200.334, 200.345(a). Closeout also does not affect the obligation of the non-federal entity to return any funds due as a result of later refunds, corrections, or other transactions. 2 C.F.R. § 200.345(a)(2).

The types of funds FEMA might attempt to recover include, but are not limited to, improper payments, cost share reimbursements, program income, interest earned on advance payments, or equipment disposition amounts.

FEMA may seek to recover disallowed costs through a Notice of Potential Debt Letter, a Remedy Notification, or other letter. The document will describe the potential amount owed, the reason why FEMA is recovering the funds, the recipient's appeal rights, how the amount can be paid, and the consequences for not appealing or paying the amount by the deadline.

If the recipient neither appeals nor pays the amount by the deadline, the amount owed will become final. Potential consequences if the debt is not paid in full or otherwise resolved by the deadline include the assessment of interest, administrative fees, and penalty charges; administratively offsetting the debt against other payable federal funds; and transferring the debt to the U.S. Department of the Treasury for collection.

FEMA notes the following common areas of noncompliance for FEMA's grant programs:

- Insufficient documentation and lack of record retention;
- Failure to follow the procurement under grants requirements;
- Failure to submit closeout documents in a timely manner;
- Failure to follow EHP requirements; and
- Failure to comply with the POP deadline.

8. Audits

FEMA grant recipients are subject to audit oversight from multiple entities including the DHS OIG, the GAO, the pass-through entity, or independent auditing firms for single audits,

and may cover activities and costs incurred under the award. Auditing agencies such as the DHS OIG, the GAO, and the pass-through entity (if applicable), and FEMA in its oversight capacity, must have access to records pertaining to the FEMA award. Recipients and subrecipients must retain award documents for at least three years from the date the final FFR is submitted, and even longer in many cases subject to the requirements of 2 C.F.R. § 200.334. In the case of administrative closeout, documents must be retained for at least three years from the date of closeout, or longer subject to the requirements of 2 C.F.R. § 200.334. If documents are retained longer than the required retention period, the DHS OIG, the GAO, and the pass-through entity, as well as FEMA in its oversight capacity, have the right to access these records as well. *See* 2 C.F.R. §§ 200.334, 200.337.

Additionally, non-federal entities must comply with the single audit requirements at 2 C.F.R. Part 200, Subpart F. Specifically, non-federal entities, other than for-profit subrecipients, that expend $750,000 or more in federal awards during their fiscal year must have a single or program-specific audit conducted for that year in accordance with Subpart F. 2 C.F.R. § 200.501. A single audit covers all federal funds expended during a fiscal year, not just FEMA funds. The cost of audit services may be allowable per 2 C.F.R. § 200.425, but non-federal entities must select auditors in accordance with 2 C.F.R. § 200.509, including following the proper procurement procedures. For additional information on single audit reporting requirements, see section F of this NOFO under the header "Single Audit Report" within the subsection "Additional Reporting Requirements."

The objectives of single audits are to:

- Determine whether financial statements conform to generally accepted accounting principles (GAAP);
- Determine whether the schedule of expenditures of federal awards is presented fairly;
- Understand, assess, and test the adequacy of internal controls for compliance with major programs; and
- Determine whether the entity complied with applicable laws, regulations, and contracts or grants.

For single audits, the auditee is required to prepare financial statements reflecting its financial position, a schedule of federal award expenditures, and a summary of the status of prior audit findings and questioned costs. The auditee also is required to follow up and take appropriate corrective actions on new and previously issued but not yet addressed audit findings. The auditee must prepare a corrective action plan to address the new audit findings. 2 C.F.R. §§ 200.508, 200.510, 200.511.

Non-federal entities must have an audit conducted, either single or program-specific, of their financial statements and federal expenditures annually or biennially pursuant to 2 C.F.R. § 200.504. Non-federal entities must also follow the information submission requirements of 2 C.F.R. § 200.512, including submitting the audit information to the Federal Audit Clearinghouse within the earlier of 30 calendar days after receipt of the auditor's report(s) or nine months after the end of the audit period. The audit information to be submitted include the data collection form described at 2 C.F.R. § 200.512(c) and Appendix X to 2 C.F.R. Part 200 as well as the reporting package described at 2 C.F.R. § 200.512(b).

The non-federal entity must retain one copy of the data collection form and one copy of the reporting package for three years from the date of submission to the Federal Audit Clearinghouse. 2 C.F.R. § 200.512; *see also* 2 C.F.R. § 200.517 (setting requirements for retention of documents by the auditor and access to audit records in the auditor's possession).

FEMA, the DHS OIG, the GAO, and the pass-through entity (if applicable), as part of monitoring or as part of an audit, may review a non-federal entity's compliance with the single audit requirements. In cases of continued inability or unwillingness to have an audit conducted in compliance with 2 C.F.R. Part 200, Subpart F, FEMA and the pass-through entity, if applicable, are required to take appropriate remedial action under 2 C.F.R. § 200.339 for noncompliance, pursuant to 2 C.F.R. § 200.505.

9. Payment Information

FEMA uses the Direct Deposit/Electronic Funds Transfer (DD/EFT) method of payment to recipients. To enroll in the DD/EFT, the recipient must complete SF-1199A, Direct Deposit Form.

FEMA utilizes the Payment and Reporting System (PARS) for financial reporting, invoicing and tracking payments. For additional information, refer to https://isource.fema.gov/sf269/execute/LogIn?sawContentMessage=true.

10. Whole Community Preparedness

Preparedness is a shared responsibility that calls for the involvement of everyone—not just the government—in preparedness efforts. By working together, everyone can help keep the nation safe from harm and help keep it resilient when struck by hazards, such as natural disasters, acts of terrorism, and pandemics.

Whole Community includes:

- Individuals and families, including those with access and functional needs;
- Businesses;
- Faith-based and community organizations;
- Nonprofit groups;
- Schools and academia;
- Media outlets; and
- All levels of government, including state, local, tribal, territorial, and federal partners.

The phrase "Whole Community" or "Whole of Community" often appears in preparedness materials, as it is one of the guiding principles. It means:

1. Involving people in the development of national preparedness documents, and
2. Ensuring their roles and responsibilities are reflected in the content of the materials.

11. Continuity Capability

Continuity should be integrated into each core capability and the coordinating structures that provide them. Protection of critical systems and networks that ensure continuity of operation, business and government are fundamental to ensuring the delivery of all core capabilities. Continuity capabilities increase resilience and the probability that organizations can perform

essential functions in the delivery of core capabilities that support the mission areas. FEMA is responsible for developing, managing, and promulgating national continuity planning, guidance, training, and exercise programs for the whole community.

FEMA develops and promulgates directives, policy, and guidance for continuing SLT government jurisdictions, nongovernmental organizations, and private sector organizations' essential functions across a broad spectrum of emergencies. This direction and guidance assist in developing capabilities for continuing the essential functions of SLT governmental entities, as well as public/private critical infrastructure owners, operators, and regulators enabling them.

Continuity Guidance Circular outline continuity requirements for agencies and organizations and provide guidance, methodology, and checklists. For additional information on continuity programs, guidance, and directives, visit the Continuity Resource Toolkit at https://www.fema.gov/emergency-managers/national-preparedness/continuity/toolkit. For additional information on continuity programs, guidance, and directives, visit https://www.fema.gov/emergency-managers/national-preparedness/continuity.

This aligns with the requirements that Cybersecurity Plans ensure continuity of operations of the state or territory as well as applicable local governments in the event of a cybersecurity incident, as well as continuity of communications and data networks within the state or territory and between the state or territory and applicable local governments. 6 U.S.C. § 665g(e)(2)(B)(vii), (ix).

12. Appendices

Appendix A. Program Goals and Objectives
Appendix B. Cybersecurity Planning Committee
Appendix C. Cybersecurity Plan
Appendix D. Multi-Entity Group Projects
Appendix E. Imminent Cybersecurity Threats Process Overview
Appendix F. Investment Justification Template and Instructions
Appendix G. Required, Encouraged, and Optional Services, Memberships, and Resources
Appendix H. Economic Hardship Cost Share Waiver

Appendix A: Goals and Objectives

Our nation faces unprecedented cybersecurity risk due to increasingly sophisticated adversaries, widespread vulnerabilities in commonly used software and hardware, and broad dependencies on networked technologies for the delivery of National Critical Functions, the disruption of which would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Cyber risk management is particularly complex due to several factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyber and physical systems, and the difficulty of reducing vulnerabilities in cyber infrastructure. In light of the risk and potential consequences of cyber incidents, strengthening the cybersecurity practices and resilience of SLT governments have become an important homeland security mission.

As part of DHS, CISA is at the heart of mobilizing a collective defense to understand and manage risk to our critical infrastructure partners. In its unique role, CISA is proactively working to achieve a cybersecurity ecosystem in which malicious actors face insurmountably high costs to execute damaging intrusions, vulnerabilities are rapidly identified before exploitation, and technology is used to reduce the most harmful and systemic risks. CISA programs and services are driven by a comprehensive understanding of the risk environment and the corresponding needs identified by our partners. The SLCGP is key to achieving this vision and enables the Department to make targeted investments in SLT government agencies, improving the security and resilience of critical infrastructure upon which Americans rely. The goals and objectives outlined below, if achieved, will significantly reduce the risk of a cybersecurity threat against SLT government information technology (IT) networks.

These broad outcomes are listed in logical sequence to aid recipients in focusing on the overall intent of the SLCGP. These outcomes will help establish priorities the use of scarce resources and to develop metrics to gage success at both the project and organizational level. Outcomes of the program will be measured by how well recipients can achieve outlined goals and improve the risk posture of the information systems they either own or those that are operated on their behalf.

The program goals for the SLCGP are as follows: (1) develop and establish appropriate governance structures, as well as develop, implement, or revise cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations; (2) ensure SLT agencies understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments; (3) implement security protections commensurate with risk (outcomes of Objectives 1 & 2); and (4) ensure organization personnel are appropriately trained in cybersecurity, commensurate with their responsibilities.

These program objectives are further divided into sub-objectives and outcomes, as well as sample evidence of implementation are provided to assist the reader.

Goal of the State and Local Cybersecurity Grant Program: Assist SLT governments with managing and reducing systemic cyber risk.

OBJECTIVE 1: Develop and establish appropriate governance structures, as well as develop, implement, or revise cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.

Sub-objective 1.1: 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).

1.1.1. *Outcome*: 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.

1.1.2. *Outcome*: Participants have identified senior officials to enable whole-of-organization coordination on cybersecurity policies, processes, and procedures.
- **Sample Evidence of Implementation:** Organization has a cybersecurity defense concept of operations, with responsibilities assigned to specific organizational roles.

Sub-objective 1.2: Develop, implement, or revise, and test cybersecurity plans, including cyber incident response plans, with clearly defined roles and responsibilities.

1.2.1 *Outcome*: Develop, implement, or revise, and exercise cyber incident response plans.
- **Sample Evidence of Implementation:** Organization conducts annual table-top and full-scope exercises that include practical execution of restoration and recovery processes to test cybersecurity plans. Conducting these exercises allow organizations to test cybersecurity plans to identify, protect, detect, respond to, and recover from cybersecurity incidents, in line with the NIST Cybersecurity Framework, and demonstrates process to incorporate lessons learned from the exercise into their cybersecurity program.

Sub-objective 1.3: Asset (e.g., devices, data, software) protections and recovery actions are prioritized based on the asset's criticality and business value.

1.3.1 *Outcome*: Ensure that systems and network functions are prioritized and reconstituted according to their impact to essential functions.
- **Sample Evidence of Implementation:** Organization conducts a regular business impact assessment to prioritize which systems must be protected and recovered first.

OBJECTIVE 2: SLT agencies understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.

Sub-objective 2.1: Physical devices and systems, as well software platforms and applications, are inventoried.

2.1.1 *Outcome*: Establish and regularly update asset inventory.
- **Sample Evidence of Implementation:** Organization maintains and regularly updates an asset inventory list.

Sub-objective 2.2: Cybersecurity risk to the organization's operations and assets are understood.

2.2.1 *Outcome*: Conduct an annual cyber risk assessment to identify cyber risk management gaps and areas for improvement

- **Sample Evidence of Implementation:** Organization annually completes the Nationwide Cybersecurity Review (NCSR).

Sub-objective 2.3: Vulnerability scans are performed, and a risk-based vulnerability management plan is developed and implemented.

2.3.1 *Outcome*: Participate in CISA's Vulnerability Scanning service, part of the Cyber Hygiene program.

- **Sample Evidence of Implementation:** Organization is an active participant in CISA's Cyber Hygiene program.

2.3.2 *Outcome*: Effectively manage vulnerabilities by prioritizing mitigation of high impact vulnerabilities and those most likely to be exploited.

- **Sample Evidence of Implementation:** Organization has a plan to manage vulnerabilities based on those with the highest criticality, internet-facing vulnerabilities, as well as known exploited vulnerabilities identified in CISA's Known Exploited Vulnerabilities Catalog.

Sub-objective 2.4: Capabilities are in place to monitor assets to identify cybersecurity events.

2.4.1 *Outcome*: SLT agencies are able to analyze network traffic and activity transiting or traveling to or from information systems, applications, and user accounts to understand baseline activity and identify potential threats.

Sub-objective 2.5: Processes are in place to action insights derived from deployed capabilities.

2.5.1 *Outcome*: SLT agencies are able to respond to identified events and incidents, document root cause, and share information with partners.

OBJECTIVE 3: Implement security protections commensurate with risk (outcomes of Objectives 1 & 2)

Sub-objective 3.1: SLT agencies adopt fundamental cybersecurity best practices.

3.1.1 *Outcome*: Implement multi-factor authentication (MFA), prioritizing privileged users, Internet-facing systems, and cloud accounts.

- **Sample Evidence of Implementation:** The organization implements MFA for all remote access and privileged accounts.

3.1.2. *Outcome*: End use of unsupported/end of life software and hardware that are accessible from the Internet.

- **Sample Evidence of Implementation:** The organization has a program to anticipate and discontinue use of end of life software and hardware.

3.1.3 *Outcome*: Prohibit use of known/fixed/default passwords and credentials.

- **Sample Evidence of Implementation:** The organization has a policy that prohibits fixed passwords, requires known/default passwords be immediately changed, and that passwords and credentials be periodically changed.
- **Sample Evidence of Implementation:** The organization has reviewed all of its current passwords and credentials to ensure they are updated appropriately.

3.1.4 *Outcome*: Ensure the ability to reconstitute systems following an incident with minimal disruption to services.

- **Sample Evidence of Implementation:** Organization policies require that backups for all critical systems and data be maintained, updated, and regularly tested according to organizational policy (e.g., quarterly), stored offline, and encrypted.

3.1.5 *Outcome*: Migrate to .gov internet domain.

- **Sample Evidence of Implementation:** Organization operates only the .gov internet domain, and does not use .com, .org, or any other domain.

Sub-Objective 3.2: Reduce gaps identified through assessment and planning process and apply increasingly sophisticated security protections commensurate with risk.

3.2.1 *Outcome*: Individual participants address items identified through assessments and planning process.

3.2.2 *Outcome*: SLT entities improve cybersecurity ecosystem by collaborating to address items identified through assessments and planning process (e.g., regional and intra-state efforts)

Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

Sub-Objective 4.1: 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.

4.1.1 *Outcome*: Organization requires regular ongoing phishing training, awareness campaigns are conducted, and organization provides role-based cybersecurity awareness training to all employees.

4.1.2 *Outcome*: Organization has dedicated resources and funding available for its cybersecurity professionals to attend technical trainings and conferences.

Sub-Objective 4.2: Organization has adopted the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.

4.2.1 *Outcome*: Organization has established cyber workforce development & training plans, based on the NICE Cybersecurity Workforce Framework.

Appendix B: Planning Committee

Governance

In keeping with the guiding principles of governance for all Federal Emergency Management Agency (FEMA) preparedness programs and statutory requirements, recipients must coordinate activities across preparedness disciplines and levels of government, including SLT governments. A cohesive planning framework should incorporate FEMA resources, as well as those from other federal and SLT entities, the private sector, and faith-based community organizations. Specific attention should be paid to how available preparedness funding sources can effectively support a Whole Community approach to emergency preparedness and management and the enhancement of Core Capabilities. To ensure this, the State Administrative Agency (SAA) must establish or reestablish a unified Cybersecurity Planning Committee. A Cybersecurity Planning Committee is also required pursuant to the statute authorizing the SLCGP (see section 2220A(g) of the Homeland Security Act of 2002, as amended (6 U.S.C. § 665g(g)).

Cybersecurity Planning Committee

The Cybersecurity Planning Committee builds upon previously established advisory bodies under other preparedness grant programs. The membership of the Cybersecurity Planning Committee must reflect an eligible entity's unique cybersecurity risk profile.

An existing multijurisdictional planning committee must meet the membership requirements as outlined in the next section, or the existing committee's membership can be expanded or leveraged to meet the membership requirements as well as the unique requirements of each eligible entity. It is recommended that eligible entities consider using Senior Advisory Committees or create a subcommittee within an existing multijurisdictional committee for this purpose, modified to meet the membership and purpose requirements. Any reference to a Cybersecurity Planning Committee elsewhere in this NOFO, and the accompanying requirements, also apply to these alternative planning committee options.

Cybersecurity Planning Committee Composition and Scope Requirements

Cybersecurity Planning Committee membership shall include at least one representative from relevant stakeholders including:

- The eligible entity;
- The Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or equivalent official of the eligible entity;
- If the eligible entity is a state (including territories), then representatives from counties, cities, and towns within the jurisdiction of the eligible entity;
- Institutions of public education and health within the jurisdiction of the eligible entity; and
- As appropriate, representatives of rural, suburban, and high-population jurisdictions.

At least one half of the representatives of the Cybersecurity Planning Committee must have professional experience relating to cybersecurity or information technology. Qualifications are determined by the states.

Eligible entities are given the flexibility to identify the specific public health and public education agencies and communities these members represent.
DHS strongly encourages eligible entities to consider naming additional members to the Cybersecurity Planning Committee, including but not limited to representatives from:

- State and county judicial entities;
- The Chief Information Officer (CIO), the Chief Information Security Officer (CISO, or equivalent official of the eligible entity;
- State legislature;
- Election Infrastructure officials, including Secretaries of State and Election Directors;
- Representatives from state, territorial, and local public safety, homeland security, emergency management, and law enforcement agencies;
- Emergency Communications Officials, such as Interoperability Coordinators;
- City and county CIOs and CISOs;
- Publicly owned or operated critical infrastructure;
- State National Guard if such entities have a cybersecurity mission;
- Municipal, city, county, rural area, or other local government councils or associations; and
- Other entities with expertise and skillsets that best represent the cybersecurity interests across the eligible entity.

The composition, structure, and charter of the Cybersecurity Planning Committee should focus on building cybersecurity capabilities across the eligible entity instead of simply combining previously existing advisory bodies under other grant programs. The Cybersecurity Planning Committee POC's contact information must be provided to FEMA as part of the grant application. Eligible entities must ensure that information for current points of contact is on file with FEMA.

Eligible entities must submit the list of Cybersecurity Planning Committee members at the time of application as an attachment in ND Grants. Eligible entities must verify compliance with Cybersecurity Planning Committee charter requirements. The below table provides a suggested format for submitting the list of required Cybersecurity Planning Committee members.

Planning Committee Membership				
Representation	**Name**	**Title**	**Organization**	**Cybersecurity/IT Experience (Yes/No)**
Eligible entity				
If eligible entity is a state, counties, cities, and towns within the jurisdiction of the entity				

Institution of Public Education within the eligible entity				
Institution of Public Health within the eligible entity				
(Additional)				
As appropriate, representatives of rural, suburban, and high-population jurisdictions				
(here the entity may add others at their discretion)				

Cybersecurity Planning Committee Responsibilities
The responsibilities of the Cybersecurity Planning Committee include:

- Assisting with the development, implementation, and revision of the Cybersecurity Plan;
- Approving the Cybersecurity Plan;
- Assisting with the determination of effective funding priorities;
- 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.

Limitations
Cybersecurity Planning Committees that meet the requirements of this NOFO and the statute are not permitted to make decisions relating to information systems owned or operated by, or on behalf of, the state.

Local Consent
Eligible entities or multi-entity groups are statutorily required to provide at least 80% of the federal funding to local governments, including at least 25% rural areas. With the consent of the local governments, part or all of this pass-through can be in the form of items, services, capabilities, or activities. This flexibility in the type of funds that are passed through may assist eligible entities or multi-entity groups in promoting projects that have state-wide (or broader)

impacts, and they may be able to more effectively reduce cybersecurity risk if managed at the state or multi-state level. Examples of these types of projects include the purchase of software licenses or development of capabilities. Any decision to pass through some or all of the funds via items, services, capabilities, or activities must be explicitly consented to by the local governments and must be documented in accordance with the Cybersecurity Planning Committee's Charter and comply with Section F.2 of this NOFO for further information.

Cybersecurity Planning Committee Charter
The governance of the SLCGP through the Cybersecurity Planning Committee should be directed by a charter. All members of the Cybersecurity Planning Committee should sign and date the charter showing their agreement with its content and their representation on the committee. Eligible entities must submit the Cybersecurity Planning Committee charter at the time of application as an attachment in ND Grants. Revisions to the governing charter must also be sent to the recipient's assigned FEMA HQ Preparedness Officer. The Cybersecurity Planning Committee charter must, at a minimum, provide:

- A detailed description of the Cybersecurity Planning Committee's composition and an explanation of key governance processes;
- A description of the frequency at which the Cybersecurity Planning Committee will meet;
- An explanation as to how the committee will leverage existing governance bodies;
- A detailed description of how decisions on programmatic priorities funded by SLCGP will be made and how those decisions will be documented and shared with its members and other stakeholders, as appropriate; and
- A description of defined roles and responsibilities for financial decision making and meeting administrative requirements.

To ensure ongoing coordination efforts, eligible entities are encouraged to share community preparedness information from other preparedness grant programs as submitted in a state's Biannual Strategy Implementation Report with members of the Cybersecurity Planning Committee. Eligible entities are also encouraged to share their Threat and Hazard Identification and Risk Assessment/Stakeholder Preparedness Review data with members of the Cybersecurity Planning Committee who are applying for other FEMA preparedness grants to enhance their understanding of statewide capability gaps.

To manage this effort and to further reinforce collaboration and coordination across the stakeholder community, a portion of the 20% funding holdback of a state (including territories) award may be utilized by the eligible entity to support the Cybersecurity Planning Committee and to ensure representation and active participation of Cybersecurity Planning Committee members. Funding may be used for hiring and training planners, establishing and maintaining a program management structure, identifying and managing projects, conducting research necessary to inform the planning process, and developing plans that bridge mechanisms, documents, protocols, and procedures.

Appendix C: Cybersecurity Plan

Submission of a Cybersecurity Plan is required for any eligible entity participating in the State and Local Cybersecurity Grant Program (SLCGP). The Cybersecurity Plan is a key component of a strategic approach to building cyber resilience. The Cybersecurity Planning Committee, with a holistic membership representing the various stakeholder groups across the entity, is responsible for developing, approving, revising, and implementing the Cybersecurity Plan.

Accordingly, the Cybersecurity Plan should establish high level goals and finite objectives to reduce specific cybersecurity risks at SLT governments across the eligible entity. The Cybersecurity Plan should also serve as the overarching framework for the achievement of the SLCGP goal, with grant-funded projects working to achieve outcomes. Regional approaches, as part of an entity-wide approach, should also be considered.

Cybersecurity Plan Basics

- Comprehensive strategic plan to reduce cybersecurity risk and increase capability across the entity
- Entity-wide plan, not a single entity
- Should cover 2 to 3 years
- Must include required elements, with discretion to add other elements as necessary
- Existing plans can be utilized
- There is no required template, but required elements must be identifiable for review purpose
- Individual projects must align to Cybersecurity Plan
- Must be approved by the Cybersecurity Committee **and** CIO/CISO/Equivalent
- CISA approves for DHS
- Plans are initially approved for 2 years; annually thereafter

In developing the Cybersecurity Plan, the Cybersecurity Planning Committee should consider the following:

- Existing governance and planning documents and identification of any planning gaps that should be addressed by the Cybersecurity Plan;
- Existing assessments and evaluations (e.g., reports, after action reports) conducted by SLT governments within the entity and any planning gaps that require additional assessments and/or evaluations; and
- Identification of potential SLCGP projects to address planning gaps and prioritize mitigation efforts.

Cybersecurity Plan Overview

The following identifies the overall plan requirements and additional considerations that eligible entities should consider when constructing the Cybersecurity Plan. Although there is no required format for the Cybersecurity Plan, Cybersecurity Planning Committees are encouraged to review the Cybersecurity Plan Template, which includes additional details, samples, and templates.

Plan Components

- Roles and responsibilities
- Required elements
- Discretionary elements
- Capabilities assessment
- Implementation plan
- A summary of projects
- Metrics

Cybersecurity Plans must include and address the following items:

- **Incorporate, to the extent practicable, any existing plans to protect against cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, SLTs.** Building upon and incorporating existing structures and capabilities allows entities to provide governance and a framework to meet the critical cybersecurity needs across the entity while making the best use of available resources. For example, consider referencing an existing emergency management plan to address potential downstream impacts affecting health and safety when responding to or recovering from a cybersecurity incident.
- **Describe how input and feedback from local governments and associations of local governments was incorporated.** For states, the SLCGP is intended to reduce cybersecurity risk across the eligible entity. Incorporating input from local entities is critical to building a holistic Cybersecurity Plan.
- **Include the specific required elements** (see Required Elements section of this Appendix below). There are 16 required elements that are central to the Cybersecurity Plan and represent a broad range of cybersecurity capabilities and activities. They also include specific cybersecurity best practices that, when implemented over time, will substantially reduce cybersecurity risk and cybersecurity threats. While each of the 16 required elements must be addressed in the plan, this may include a brief explanation as to why certain elements are not currently being prioritized. Not all 16 elements are required to be aligned to projects and have associated funding. These determinations should be addressed in accordance with capability gaps and vulnerabilities identified through an objective assessment process.
- **Describe, as appropriate and to the extent practicable, the individual responsibilities of the state and local governments within the state in implementing the Cybersecurity Plan.** Defining the roles and responsibilities of SLT governments is critical from both governance and implementation perspectives.
- **Assess the required elements from an entity-wide perspective.** The candid assessment of the current capabilities of SLT entities is the first step in reducing cybersecurity risk across the entity. This assessment also serves as the justification for individual projects. Additional information on the assessment is provided below and in the Cybersecurity Plan Template.
- **Outline, to the extent practicable, the necessary resources and a timeline for implementing the plan.** The Cybersecurity Plan is a strategic planning tool that looks two to three years into the future. Accordingly, it should map how the Cybersecurity Planning Committee seeks to achieve plan goals and objectives. Cybersecurity Plans should address how SLCGP funds will help develop and/or implement the plan. It should also map how other activities and funding sources contribute to the achieving the outcomes described in the plans.
- **Summary of associated projects.** Individual projects are the way elements of the plan are implemented over time. The plan must include a summary of projects associated with each required and discretionary element, designating which will use SLCGP funds. Details for each project using SLCGP funds must be included in the Investment Justification.
- **Describe the metrics that the eligible entity will use to measure progress.** The metrics that will be used must measure implementation of the Cybersecurity Plan and, more broadly, cybersecurity risks reduction across the state. These are different than the

metrics that will be used to measure outcomes of the SLCGP, as described in Section A.10-A.11 and Appendix A of this NOFO. Additional information is provided in the Cybersecurity Plan Metric Section below and also in the Cybersecurity Plan Template.
- **Approvals - the Cybersecurity Plan must be approved by the Cybersecurity Planning Committee and the CIO/CISO/Equivalent.** The eligible entity, upon submitting the Cybersecurity Plan, must certify that the Cybersecurity Plan has been formally approved by the Cybersecurity Planning Committee and the CIO/CISO/Equivalent of the eligible entity.

Cybersecurity Planning Committees should also consider the following when constructing the Cybersecurity Plan:

- **Holistic approach to the Cybersecurity Plan**. The Cybersecurity Plan should be strategic in nature, guiding development of capabilities to address cybersecurity risks and threats across the state or territory. Individual projects should demonstrably support the state, territorial, and local entities in achieving those capabilities over time.
- **Focused investments that are sustainable over time**. The SLCGP currently is authorized for four years and limited funds are available. Cybersecurity Plans must address how SLT entities will sustain capabilities once the program ends or funds are no longer available.
- **State role as leader and service provider.** Many states have significant cyber defenses and elect to provide services to local entities to improve capabilities. Where appropriate, states should consider approaches to support state-wide efforts, that may include using funds to provide services to local entities. Multi-entity projects are another way that eligible entities can group together to address cybersecurity risk and build capabilities (See Appendix D for additional information on multi-entity activities).
- **Building from existing efforts.** Cybersecurity Committees should consider describing how cooperative programs developed by groups of local governments are integrated into the entity-wide approach.
- Additional cybersecurity elements prioritized by the Cybersecurity Planning Committee.

Required Elements

If there are any existing plans that meet the required elements, references to them may be used in lieu of incorporating them in their entirety. The Cybersecurity Plan must describe, to the extent practicable, how the state plans to address the below elements. The Cybersecurity Plan is a strategic document, looking broadly across the entire jurisdiction. The description should support the vision, mission and other strategic guidance set by the Cybersecurity Planning Committee.

1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.

2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.

4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed further below.
   The following cybersecurity best practices under required element 5 must be included in each eligible entity's Cybersecurity Plan:
   - 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); and
   - Migration to the .gov internet domain.

   Additional best practices that the Cybersecurity Plan can address include:
   - The National Institute of Standards and Technology (NIST) Cybersecurity Framework;
   - NIST's cyber chain supply chain risk management best practices; and
   - Knowledge bases of adversary tools and tactics.

Required Cybersecurity Best Practices: Although these cybersecurity best practices must be addressed in the Cybersecurity Plan, immediate adoption by every SLT entity is not required. Cybersecurity Plans must clearly articulate efforts to implement these cybersecurity best practices across the eligible entity within reasonable timelines. Individual projects that assist SLT entities adopt these best practices should also be prioritized by the Cybersecurity Planning Committee. As there are multiple ways to implement the best practices, this approach provides committees the flexibility to work with SLT entities to design a plan that takes resource constraints, existing programs, and other factors into account.

6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.

7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.

8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.

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 may impact the performance of information systems within the jurisdiction of the state.

11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.

12. Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).

13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.

14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.

15. Ensure adequate access to, and participation in, the services and programs described in this subparagraph by rural areas within the state.

16. Distribute funds, items, services, capabilities, or activities to local governments.

Cybersecurity Planning Committees are strongly encouraged to expand their Cybersecurity Plans beyond the required elements. This may include a focus on specific critical infrastructure or emphasis on different types of SLT entities.

Required Capabilities Assessment

Given the Cybersecurity Plan is a strategic document, it should not identify specific vulnerabilities but instead capture the broad level of capability across the jurisdiction. The assessment will become the road map for individual projects and activities using SLCGP funds. **All Investment Justifications must reference the capability gaps identified in the assessment.** The Cybersecurity Plan Capabilities Assessment Worksheet (see Cybersecurity Plan

Template) provides an easy way for Cybersecurity Planning Committees to capture this information and can be customized as appropriate.

Summary of Projects

Although the Cybersecurity Plan is a strategic document, it must show how individual projects and activities will implement the plan over time. A summary of projects using FY 2022 SLCGP funds associated with each required and discretionary element provides a helpful snapshot of state- and territory-wide capability and capacity that will be achieved as a result of this funding. Details for each project using SLCGP funds must be included in Investment Justification (see Appendix F) and is to include a description of the purpose of the project and what it will accomplish, and, more specifically, how the project will address an identified gap or need and how it supports one or more of the required elements.

The Cybersecurity Plan Template includes a fillable Project Plan Worksheet, a sample of which is below.

- **Column 1**. Project number assigned by the entity
- **Column 2.** Name the project
- **Column 3.** Brief (e.g., 1-line) Description of the purpose of the project
- **Column 4.** The number of the Required Elements the project addresses
- **Column 5.** Estimated project cost
- **Column 6.** Status of project (future, ongoing, complete)
- **Column 7.** Project priority listing (high, medium, low)
- **Column 8.** Project Type (Plan, Organize, Equip, Train, Exercise)]

Sample Table - Project Plan Worksheet							
1. #	**2. Project Name**	**3. Project Description**	**4. Related Required Element #**	**5. Cost**	**6. Status**	**7. Priority**	**8. Project Type**

Cybersecurity Plan Metrics

Cybersecurity Plans must include language detailing how the state will measure both: 1) how the state will implement the plan; and 2) how the state will reduce cybersecurity risks to, and identify, respond to, and recover from cybersecurity threats to, information systems owned or operated by, or on behalf of, the state or local governments within the state. These measures should be at the macro level, related to the goals, objectives, and priorities as part of the overarching strategic plan and not associated with individual projects. See page 6 of this NOFO for additional information on required metrics and reporting.

States, and their Cybersecurity Planning Committees in helping with Cybersecurity Plans, should consider the following when developing metrics:

- Aligning metrics to the Cybersecurity Plan and the established program goals and objectives included at Appendix A.
- Reviewing existing metrics that are in use across the state; and
- The data for each metric must be available and reportable and should not create unnecessary burdens to collect.

The Cybersecurity Plan Template provides a fillable table for reporting metrics.

Sample Table - Cybersecurity Plan Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
1.	1.1		
	1.2		
	1.3		
2.	2.1		
3.	3.1		
	3.2		
4.	4.1		
	4.2		
	4.3		

Appendix D: Multi-Entity Grants

Multiple eligible entities can group together to address cybersecurity risks and cybersecurity threats to information systems within the jurisdictions that comprise the group. There is no separate funding for multi-entity awards. Instead, these investments would be considered as group projects and be funded out of the participating entities' published allocations. These projects should be included as individual Investment Justifications from each participating eligible entity, each approved by the respective Cybersecurity Planning Committee, and each aligned with the eligible entity's Cybersecurity Plan.

Eligibility

In addition to applying as a single entity, an eligible entity (e.g., the SAA) may partner with one or more other eligible entities to form a multi-entity group. Members of multi-entity groups work together to address cybersecurity risks and cybersecurity threats to information systems within their jurisdictions. There is no limit to the number of participating entities in a multi-entity group. Local entities can be included in the project, but their respective eligible entity (i.e., State) must also participate at some level. There is no separate funding for multi-entity awards. Instead, they should be considered as group projects within their existing state or territory allocations. Projects should be included as individual Investment Justifications from each participating eligible entity, each approved by the respective Planning Committee and aligned with each respective eligible entity's Cybersecurity Plan.

Additionally, note that for multi-entity groups, all individual eligible entities must have already developed a Cybersecurity Plan.

Benefits

Cost Savings:

A multi-entity grant will be counted against the total apportionment of each entity. However, multi-entity grants may permit smaller entities to combine resources with larger entities to reap the benefits associated with larger acquisitions. At the same time, all parties to a multi-entity grant may realize cost savings due to volume purchases. The multi-entity group will also benefit from a total of 10% reduction in cost share requirements for that specific project. For FY 2022, this means that multi-entity projects would not require any recipient cost share.

Shared Resources:

Since the multi-entity group may be comprised of state (including territorial) governments, each shall benefit from information sharing and awareness opportunities.

Requirements and Process Overview

- Eligible entities work collaboratively to define the group project and the roles and responsibilities for each eligible entity.
- Each eligible entity must have a Cybersecurity Plan that has been approved by CISA – there is no exception to allow multi-entity groups to use a grant to develop any entity's Cybersecurity Plan.
- The project must improve or sustain capabilities identified in the respective Cybersecurity Plans for each eligible entity.

- The Cybersecurity Planning Committee of each participating eligible entity must approve the individual project.
- Each eligible entity will be required to submit an Investment Justification describing the following:
    - A description of the overarching multi-entity project;
    - The other eligible entities and all participating state, local, tribal, and territorial entities and identify the division of responsibilities amongst the multi-entity group;
    - The distribution of funding from the grant among the eligible entities that comprise the multi-entity group, to include any subawards made to local entities; and
    - How the eligible entities that comprise the multi-entity group will work together to implement the Cybersecurity Plan of each of those eligible entities.

Additional details can be found in Appendix F – Investment Justification.
Note: It is expected that Investment Justifications for multi-entity projects will be almost identical. Any differences should be as a result of alignment with the entities' respective Cybersecurity Plans.

Appendix E: Imminent Cybersecurity Threat

The SLCGP is primarily a security preparedness program focused on reducing cyber risks by helping SLT entities address cybersecurity vulnerabilities and build cybersecurity capabilities. Over time, the program activities and investments will reduce the potential impact of cybersecurity threats and incidents. The State and Local Cybersecurity Improvement Act enumerates, as one eligible use of funds, activities that address imminent cybersecurity threats, as follows: "An eligible entity that receives a grant under this section and a local government that receives funds from a grant under this section, as appropriate shall use the grant to…(4) assist with activities that address imminent cybersecurity threats as confirmed by the Secretary, acting through the [CISA] Director, to the information systems owned or operated by, or on behalf of, the eligible entity or a local government within the jurisdiction of the eligible entity." 6 U.S.C. § 665g(d)(4).

The following provides an overview of the processes for the FY 2022 grant cycle from a grant management perspective. Specific details on CISA's criteria and process for confirming an imminent cybersecurity threat are not included here. The following also does not supersede or replace existing threat notification procedures or existing methods to collaborate on operational cybersecurity matters.

Process Overview

- Any eligible entity seeking to use SLCGP funds to address an imminent cybersecurity threat, as confirmed by the Secretary, acting through the CISA Director, must have a Cybersecurity Plan approved by CISA unless DHS has granted the eligible entity an exception for the FY 2022 grant cycle to use the grant to develop a Cybersecurity Plan.
- Only DHS, through CISA, confirms an imminent cybersecurity threat.
- SLT entities cannot request a threat to be confirmed an imminent cybersecurity threat.
- Upon confirmation, DHS will notify the State Administrative Agency (SAA) at the eligible entity. DHS will notify impacted SLT entities as appropriate.
- FEMA will issue an Information Bulletin detailing the impacted entities and procedures for reprograming SLCGP funds in support of the specific imminent cybersecurity threat. The scope of the Information Bulletin will be dependent on the nature of the imminent cybersecurity threat.
- The eligible entity must notify the Cybersecurity Planning Committee and chief information officer (CIO)/chief information security officer (CISO)/equivalent of the eligible entities, which are responsible for reviewing, prioritizing, and approving projects under SLCGP.
    - Impacted SLT entities should be notified consistent with established governance structures and notification processes within the eligible entity.
- It will be left at the discretion of eligible entity, in consultation with the Cybersecurity Planning Committee and CIO/CISO/equivalent, and in collaboration with other entities as necessary, to review the imminent cybersecurity threat information and determine if SLCGP funds are to be used to assist with activities that address the imminent cybersecurity threats.
- If the eligible entity wants to use any of its grant funds to address imminent cybersecurity threats that may arise during the period of performance, the eligible entity must include

this in and submit an Investment Justification aligned to Objective 3. There is no minimum amount that the eligible entity must request or reserve through this Investment Justification, and if the eligible entity needs to reallocate funding across its approved Investment Justifications to address imminent cybersecurity threats, the eligible entity should collaborate with any subrecipient potentially impacted by the reallocation of funds.

Appendix F: Investment Justification Form and Instructions

Overview

Only one application will be submitted by the eligible entity. The application will consist of up to four (4) Investments, one for each SLCGP objective (see Appendix A for more information on the goal and objectives).

Investments for SLCGP Objectives 1, 2, and 3 must have at least one project. Investments for SLCGP Objective 4 are optional for the FY 2022 SLCGP. If an IJ is submitted for Objective 4, then it also must have at least one project.

For each objective, whether required or optional, Applicants must submit up to one IJ form per SLCGP objective, and at least one Project Worksheet for each submitted Investment Justification. Each IJ should have the same application-level information. Project level information should vary based on the associated SLCGP Objective.

Use the following naming convention for the IJs and Project Worksheets: [Insert name of state or territory] Objective [insert number of corresponding objective – 1, 2, 3 or 4]. For example: Alaska Objective 2.

Multi-entity efforts must be included as individual projects in the Project Worksheet, aligned to the appropriate investment (i.e., SLCGP objective). Additional information is provided below

General Process

- Download IJ Template
- Download IJ Project Worksheet
- Save a separate IJ Template and Project worksheet for each SLCGP Objective.
- Add the same portfolio information to each IJ file.
- Complete the investment level information for each objective.
- Identify individual projects for each objective using the Project Worksheet.
- Submit the following files via ND Grants:
    - Cybersecurity Plan (unless requesting an exemption)
    - One (1) IJ form for each SLCGP objective.
    - One (1) Project worksheet for each SLCGP objective.

The IJ Template and special completion instructions are provided below as a reference, but applicants should download the IJ Template at the link provided above to complete for each SLCGP objective. The IJ Template used for this program is from the approved collection for the Homeland Security Grant Program, but many of the elements still apply to SLCGP. The instructions in the last column explain how a field in the IJ Template applies or does not apply to SLCGP. Please contact the applicable FEMA Preparedness Officer if unsure whether any elements of the IJ Template are required to be filled out.

Paperwork Burden Disclosure Notice:

Public reporting burden for this data collection is estimated to average 72 hours per response. The burden estimate includes the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and submitting this form. This collection of information is required to obtain or retain benefits. You are not required to respond to this collection of information unless a valid OMB control number is displayed on this form. Send comments regarding the accuracy of the burden estimate and any suggestions for reducing the burden to: Information Collections Management, Department of Homeland Security, Federal Emergency Management Agency, 500 C Street, SW., Washington, DC 20472-3100, Paperwork Reduction Project (1660-0125) NOTE: Do not send your completed form to this address.

HSGP IJ PLANNING TEMPLATE	SLCGP SPECIAL INSTRUCTIONS
The IJ Template is useful for the Portfolio and Investment section questions. For the project section, applicants should use the Project Worksheet to record all proposed projects. The Project Worksheet is available at grants.gov. The template allows applicants to use spelling and grammar as well as character count functions available in MS Word during the IJ development process. To ensure adherence with formatting requirements, applicants are strongly encouraged to utilize these functions prior to copying text from MS Word to the Grant Reporting Tool (GRT). Please note that character count limits include spacing and all forms of punctuation. To simplify the transfer of the narrative information section into the GRT, it is also recommended that applicants save a working copy of this Template, deleting Part III and the Appendix.	The GRT will NOT be used for the SLCGP. Instead, applicants must use the MS Excel version of the Project Worksheet and submit one file for each SLCGP Objective.
PART I. PORTFOLIO INFORMATION	
The portfolio provides the overall context for the investments and projects included in the application. The applicant must answer the two portfolio questions only once.	*The portfolio provides the overall context for the investments and projects included in the application. The applicant must answer the two portfolio questions only once. The responses should be copied into each of the IJs.*
I. A. Describe how this portfolio of investments and projects addresses gaps and/or sustainment in the Threat and Hazard Identification Risk Assessment (THIRA)/Stakeholder Preparedness Review (SPR).	
Guidance for Completing this Section (2500 character limit): For purposes of the State Homeland Security Program (SHSP) and the Urban Area Security Initiative (UASI), DHS/FEMA requires states, territories, and Urban Areas to prioritize grant funding to support closing capability gaps or sustaining capabilities identified in the THIRA and SPR process (formerly known as the State Preparedness Report). Each IJ must describe how proposed investments will help build or sustain capabilities (SPR step 1) and/or address capability gaps and sustainment needs (SPR step 2) to help them achieve capability targets (THIRA step 3). IJs may also describe how proposed investments will help address functional area gaps identified in the SPR that may not be directly tied to capability targets. At a high level, applicants should identify the relevant portions of their THIRA/SPR that most of the activities in the investment will address. Then applicants must identify how the proposed investment will address one or more of the capability gaps identified in the most recent SPR. The specific capability gap as found in the SPR must be noted in the investment. The applicant should then	A 2500 character limit is allowed for this response. Guidance for Completing this Section: **THIS SECTION IS NOT REQUIRED IF ELIGIBLE ENTITIES IS REQUESTING AN EXEMPTION FROM SUBMITTING A CYBERSECURITY PLAN (SEE NOTICE OF FUNDING OPPORTUNITY PAGE 22 FOR MORE DETAILS ON THE EXEMPTION PROCESS).** If an exemption is being requested, please state "Exemption requested. Section will be updated when Cybersecurity Plan is submitted for review and approval." Applicants will be required to update this section once the Cybersecurity Plan is submitted for review, along with updated individual projects. **THE FOLLOWING ASSESSMENT IS REQUIRED IF AN eligible entity IS SUBMITTING A CYBERSECURITY PLAN FOR REVIEW BY CISA.**

HSGP IJ PLANNING TEMPLATE	SLCGP SPECIAL INSTRUCTIONS
specifically describe why those proposed activities outlined within the investment are a priority for the applicant.	Applicants should briefly describe the capabilities of the SLT agencies across the eligible entity related to the required elements of the Cybersecurity Plan. Note the inclusion of the priority Cybersecurity Best Practices. The description should provide the framework for all investment requests provided within the IJ. It is important to provide the best possible assessment of capabilities of SLT entities within the eligible entity, not only the eligible entity itself. In the case of states, this means including local entities, providing a state-wide assessment of capabilities specifically related to the required elements of the Cybersecurity Plan. Wherever possible, applicants should cite the source (e.g., assessment, survey, exercise) used to evaluate each capability. **Use the list of elements below as headers for each section or subsection, to the extent practicable and as applicable.** 1. Manage, monitor, and track information systems, applications, and user accounts 2. Monitor, audit, and track network traffic and activity 3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts 4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by risk 5. Adopt and use best practices and methodologies to enhance cybersecurity • Implementation of multi-factor authentication. • End the use of unsupported/end of life software and hardware that are accessible from the Internet. • Prohibition against use of known/fixed/default passwords and credentials. • Ensure the ability to reconstitute systems (backups); and • Migration to the .gov internet domain. • Implement enhanced logging. • Data encryption for data at rest and in transit. 6. Promote the delivery of safe, recognizable, and trustworthy online services, including through the use of the .gov internet domain 7. Ensure continuity of operations including by conducting exercises 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)

<table>
<tr><th>HSGP IJ PLANNING TEMPLATE</th><th>SLCGP SPECIAL INSTRUCTIONS</th></tr>
<tr><td></td><td>9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks
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 may impact the performance of information systems
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department
12. Leverage cybersecurity services offered by the Department
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats
15. Ensure rural communities have adequate access to, and participation in plan activities
16. Distribute funds, items, services, capabilities, or activities to local</td></tr>
<tr><td>I. B. Identify the amount and percentage of funding that will be allocated for Management and Administration expenditures.</td><td></td></tr>
<tr><td>Note: The total Management and Administration (M&A) amount and total M&A percentage <u>will not</u> be automatically calculated in the table below. The GRT will automatically calculate the total when applicants transfer their answers. The total M&A percentage may not exceed 5% of the allocated funding. Please note that M&A should be calculated at the portfolio level per funding source (e.g., [State Homeland Security Program (SHSP) or Urban Area Security Initiative (UASI)] and not at the individual Investment level. Any M&A funds retained for the administration of the Operation Stonegarden Program will be reported in the Bi-annual Strategy Implementation Report (BSIR).</td><td>Note: The total Management and Administration (M&A) amount and total M&A percentage <u>will not</u> be automatically calculated in the table below. As the GRT is not being used, applicants will have to calculate the total M&A manually. Please note that M&A should be calculated at the portfolio level – all of SLCGP – and not at the individual Investment level.</td></tr>
</table>

Program	**Requested Amount**	**M&A Amount**	**M&A Percentage**	**Subtotal** (Requested Amount + M&A)
SHSP	$	$	%	$
UASI	$	$	%	$
Total:	**$**	**$**	**%**	**$**

Do not enter any figures here.
Do not enter any figures here.
Enter figures only in the Total row.

HSGP IJ PLANNING TEMPLATE	SLCGP SPECIAL INSTRUCTIONS
PART II. SPECIFIC INVESTMENT INFORMATION	
II. A. Provide the Investment name: (100 character limit)	Insert the related objective (i.e., "Objective 1", "Objective 2", "Objective 3" or "Objective 4"). No additional text is needed.
II. B. Investment Type: Choose one of the following from the GRT dropdown menu: Consolidated Fusion Center Investment, Consolidated Cybersecurity Investment, or Standard Investment	Select "Consolidated Cybersecurity Investment" from the dropdown menu.
Please note that all fusion center-related funding requests **must be consolidated into a single investment per funding source** (e.g., SHSP or UASI) in which recognized fusion centers reside. The consolidated fusion center Investment per funding source must address direct funding support for the recognized fusion center. For a list of recognized fusion centers, please see (http://www.dhs.gov/fusion-center-locations-and-contact-information). Also note that there must be at least one investment in support of the state, urban area or territory's cybersecurity efforts.	N/A
II. C. What is the funding source for this investment: Each investment must identify a programmatic funding source (SHSP or UASI). If a project will use multiple sources of funding, separate the amounts of funding from each source under different investments. If UASI funds are used by the eligible entity in support of the Urban Area, the eligible entity must, as part of the up to 10 UASI investments, propose an investment describing how UASI funds will be used by the eligible entity to directly support the Urban Area.	**N/A**

Funding Source		**Funding Amount**	
Proposed Funding Source (*Select One*)		$	N/A
Proposed Amount		**$**	**Enter total proposed funding for the entire investment (i.e., all projects associated with SLCGP Objective)**

II. D. How much of this Investment will be obligated towards Law Enforcement Terrorism Prevention Activities (LETPA)? $	**How much of this investment will be obligated towards local and rural governments?** **Enter the local total followed by the rural total, using "/" between the two numbers. For example: $100/$50**
Per section 2006 of the *Homeland Security Act of 2002*, as amended, (6 U.S.C. § 607), FEMA is required to ensure that at least 25 percent (25%) of grant funding appropriated for the Homeland Security Grant Program are used for LETPA. FEMA meets this requirement, in part, by requiring all SHSP and UASI recipients to ensure that at least 25% of grant funding appropriated for grants awarded under HSGP's authorizing statute is used for LETPA. The LETPA allocation can be from SHSP, UASI or both. This requirement does not include award funds from OPSG.	LETPA does not apply to SLCGP but all eligible entities that receive an SLCGP grant are required to ensure that at least 80% of grant funding appropriated for the SLCGP are obligated or otherwise made available to local governments. Additionally, at least 25% of grant funding appropriated for the SLCGP must be obligated or otherwise made available to rural governments within the jurisdiction of the eligible entity, consistent with their Cybersecurity Plan.
II. E. Describe the investment, specifically how it addresses gaps and/or sustainment in the Threat and Hazard Identification Risk Assessment (THIRA)/Stakeholder Preparedness Review (SPR).	The purpose of this section is to describe how projects for each investment (e.g., Objective 1) align to the entity's Cybersecurity Plan. It

HSGP IJ PLANNING TEMPLATE	SLCGP SPECIAL INSTRUCTIONS
	also allows the applicant to describe how implementing the plan will be measured (metrics).
Guidance for Completing this Section (2500, character limit): At a high level, applicants should identify the relevant portions of their THIRA/SPR that most of the activities in the investment will address. Then applicants must identify how the proposed investment will address one or more of the capability gaps identified in the most recent SPR. The specific capability gap as found in the SPR must be noted in the investment. The applicant should then specifically describe why those proposed projects outlined within the investment are a priority for the applicant.	Guidance for Completing this Section: The purpose of this section is to describe how projects for each investment (e.g., Objective 1) align to the entity's Cybersecurity Plan. It also allows the applicant to describe how implementing the plan will be measured (metrics). **IF AN EXEMPTION FROM THE CYBERSECURITY PLAN IS REQUESTED IN SECTION I.A. (SEE THE NOTICE OF FUNDING OPPORTUNITY PAGE 22 FOR MORE DETAILS ON THE EXEMPTION PROCESS)** If an exemption is being requested, please state "Exemption requested. Section will be updated when Cybersecurity Plan is submitted for review and approval." Applicants will be required to update this section once the Cybersecurity Plan is submitted for review, along with updated individual projects. **IF AN EXEMPTION FROM THE CYBERSECURITY PLAN IS NOT REQUESTED** **A. Cybersecurity Plan Alignment** • Applicants should list each project and reference the specific sections of their Cybersecurity Plan that each of the projects within this investment are aligned. The applicant should use page numbers and identify specific sections of their Cybersecurity Plan to aid the reviewer in the analysis of the response provided. • Then applicants must identify how the proposed project will address one of the capability gaps referenced in section I.A. The applicant should then specifically describe why those proposed activities outlined within the IJ are a priority for the applicant. **B. Performance Metrics** • Applicants must provide the metrics described in their Cybersecurity Plan. • For each metric, applicants must define key terms, identify the source of the data, how the data is collected, the frequency of data collection, and association to any specific projects, if applicable.
PART III. PROJECT INFORMATION	
All requested funding must be associated with specific projects. For each project, several pieces of information, or attributes, must be provided to submit the project for consideration in the application. The tables below list each attribute, followed by a description and a set of instructions for the applicant to follow to provide the appropriate information.	All requested funding must be associated with specific projects. For each project, several pieces of information, or attributes, must be provided to submit the project for consideration in the application. The tables below

<table>
<tr><th colspan="3">HSGP IJ PLANNING TEMPLATE</th><th>SLCGP SPECIAL INSTRUCTIONS</th></tr>
<tr><td colspan="3">To prepare for completing the IJ in the GRT, applicants should utilize the Project Worksheet (http://www.fema.gov/grants) to plan their applications and to record the necessary information for each project. The Project Worksheet is divided into two tabs: Baseline Project Information and Project Implementation. Once applicants provide a name for a project on the Baseline Project Information tab, the name will auto-populate on the Project Implementation tab.

The Project Worksheet provides drop-down selections for several of the project attributes. The applicant may then use the information collected in the worksheet for rapid transfer to the GRT interface. Each project will be given a unique identifier as it is submitted via the GRT. Applicants should keep a record of the project identifiers as they will be required to report on each project using that identifier.</td><td>list each attribute, followed by a description and a set of instructions for the applicant to follow to provide the appropriate information.

As previously stated, the GRT will not be used, and applicants must submit one Project Worksheet for each SLCGP objective.

The Project Worksheet is divided into two tabs: Baseline Project Information and Project Implementation. Once applicants provide a name for a project on the Baseline Project Information tab, the name will auto-populate on the Project Implementation tab.</td></tr>
<tr><td colspan="3">III. A. Project Alignment to Core Capability Gaps</td><td></td></tr>
<tr><td colspan="3">The first section of project attributes contains basic information about how the projects support or build core capabilities. These attributes are required for every project. If an attribute is left blank in the GRT an error message will appear and the applicant will not be able to submit the application.

The GRT will provide a list of sub-recipients from previous awards. Alternatively, the applicant will have the opportunity to add a new subrecipient to the list. The attribute of `Sub-recipient type' will be auto-populated based on the sub-recipient selection. The applicant must ensure that 80% of the award funds are passed through to local entities.

For additional information on the National Preparedness Goal (NPG) and core capabilities, please visit https://www.fema.gov/national-preparedness-goal.</td><td></td></tr>
<tr><td>Attribute Name</td><td>Description</td><td>Application Instructions</td><td></td></tr>
<tr><td>Project Name</td><td>Descriptive identifier of the project</td><td>Provide a title for specified project (100 character maximum). The title must reflect the nature of work to be completed under the project.</td><td>Provide a title for specified project (100 character max). Title must reflect nature of work to be completed under the project.

Multi-entity projects: Include “multi-entity” at the beginning of the project name.</td></tr>
<tr><td>Project Description</td><td>Descriptive narrative of the project</td><td>Provide a brief narrative describing the project at a high level (1500 character maximum). Identify the National Incident Management System (NIMS) typed resource if any, that is supported by this project. Refer to the Resource Typing Library Tool at http://www.fema.gov/resource-management-mutual-aid.</td><td>Provide a brief narrative describing the project at a high level. (15001500, chars.) NIMS typed resource does not apply.
The first line must identify the required element(s) of the cybersecurity plan the project addresses (see Appendix C of the NOFO). Simply include the number of the required element(s) in brackets separated by a comma. For example: [1,5]. If the project supports the plan development specifically, include [Plan Development].</td></tr>
</table>

HSGP IJ PLANNING TEMPLATE			SLCGP SPECIAL INSTRUCTIONS
			Multi-entity projects: Group project must explicitly include the following in their description: • A description of the overarching multi-entity project; • The other eligible entities and all participating SLT entities and identify the division of responsibilities amongst the multi-entity group; • The distribution of funding from the grant among the eligible entities that comprise the multi-entity group, to include any sub-awards made to local entities; and • How the eligible entities that comprise the multi-entity group will work together to implement the Cybersecurity Plan of each of those eligible entities.
Attribute Name	**Description**	**Application Instructions**	
Recipient Type	State or local recipient for purposes of meeting the 80% pass through requirement	This attribute will auto populate in the GRT based on what state agency or subrecipient is selected.	Input either "State" or "Local".
Project Location	Zip code of the primary location of the project	Provide the 5-digit zip code where the project will be executed. The project location could be distinct from the sub-recipient address.	Provide the 5-digit zip code where the project will be executed. The project location could be distinct from the sub-recipient address.
Primary Core Capability	Primary core capability that the project will impact	Every project must support a core capability. Select the primary core capability associated with this project.	Every project must support a SLCGP Objective. The dropdown box in the Project Worksheet is limited to the Core Capabilities. Use the following options to identify the primary SLCGP objective associated with the project: Objective 1 = Planning Objective 2 = Threats and Hazards Identification Objective 3 = Cybersecurity Objective 4 = Operational Collaboration
Sustain or Build	Indicates whether the project will sustain or build a core capability	Select "build" if this project focuses on starting a new capability or the intent of the project is to close a capability gap (i.e., taking the core capability as a whole from an SPR score 1 to a 2), or "sustain" if the purpose of the project strictly maintains a core capability at its existing current level (i.e., the project does not move the core	Select "build" if this project focuses on starting a new capability or the intent of the project is to close a capability gap or "sustain" if the purpose of the project strictly maintains an existing capability at its existing current level.

HSGP IJ PLANNING TEMPLATE			SLCGP SPECIAL INSTRUCTIONS
		capability as a whole neither up nor down from its existing SPR score).	
Deployable	Indicates if the assets or activities of the project are deployable to other states.	Is the core capability supported by this project deployable to other jurisdictions? (Yes/No)	Select "Yes" the project supports multiple jurisdictions (e.g., multiple cities), entities across the entire eligible entity (e.g., state providing service to local entities), or is a multi-entity project. Select "No" if the project primarily supports a single entity.
Shareable	Indicates if the assets or activities of the project are shareable within the state or with other states because the activities assets are not physically deployable.	Is the core capability supported by this project shareable with other jurisdictions? (Yes/No)	N/A
III. B. Project Alignment to Solution Areas			
The grant funded activities of every project must align to the HSGP solution areas: Planning, Organization, Exercises, Training and/or Equipment (POETE). A project may have activities in more than one solution area. For the POETE funding amounts the GRT will automatically calculate the total amount as you enter funding amounts. For additional information on the allowable cost categories, please refer to the HSGP NOFO.			Complete the following section as originally designed. The grant funded activities of every project must align to the SLCGP solution areas: Planning, Organization, Exercises, Training and/or Equipment (POETE). A project may have activities in more than one solution area. For the POETE funding amounts the Project Worksheet will automatically calculate the total amount as you enter funding amounts.
Attribute Name	**Description**	**Application Instructions**	
Planning	Dollar amount of the project supporting planning	Identify the amount of funds in the project that will be for planning activities.	

HSGP IJ PLANNING TEMPLATE			SLCGP SPECIAL INSTRUCTIONS
Organization	Dollar amount of the project supporting organization	Identify the amount of funds in the project that will be for organization activities.	
Equipment	Dollar amount of the project supporting equipment	Identify the amount of funds in the project that will be for the purchase of equipment.	
Training	Dollar amount of the project supporting training	Identify the amount of funds in the project that will be for training activities.	
Exercises	Dollar amount of the project supporting exercises	Identify the amount of funds in the project that will be for exercise activities.	
Total	Total dollar amount for the project.	Automatically generated by the GRT from the sum of the POETE cost categories.	
II. C. Project Implementation and Management			
For every project, identify the baseline for project implementation according to whether it builds on a previous investment. Not all projects will be linked to previous investments. Next, determine the appropriate project management phase. For new projects, this will likely be the `initiate' or `planning' phase. However, if the project builds on a previous investment, the project may be in a more advanced execution"”" or `control"“" phase. As the project is implemented the recipient will be expected to report on the progress of the project through the management phases. Please reference Appendix A for a detailed description of the Project Management Life-cycle. The applicant will then be required to provide start and end dates for the project, within the36 month period of performance. Finally, indicate whether the activities of the project will require new construction or renovation, retrofitting, or modification of existing structures. This project attribute is required as some project activities may require extensive environmental review which can affect when implementation can begin.			This section does not apply to the SLCGP.
Attribute Name	**Description**	**Application Instructions**	
Does the Project Support a Previously	Indicates whether the project is related to an investment	Select yes if the current project is a continuation of an existing investment that has used grant funds for implementation from previous DHS/FEMA awards.	

HSGP IJ PLANNING TEMPLATE			SLCGP SPECIAL INSTRUCTIONS
Awarded Investment?	awarded in a previous year.		
If yes, from which year?	Fiscal year of the previous award.	If the project is a continuation of a previous investment, select the specific investment from the list.	
If Yes, which investment?	The previously awarded investment that the project supports.	If the project is a continuation of a previous investment, select the specific investment from the list.	
What is the Last Completed milestone of the previous investment?	A description of the last completed milestone from the previously awarded investment.	Please refer to the investment identified above and then identify the last completed milestone from that investment. (250 character maximum)	
Project Management Step	The current Project Life-cycle phase of the previously awarded investment, or the new project.	Select the most applicable step.	
Start Date	Start date of the project/ previously Awarded Investment	Provide the approximate start date of the project, based on the expected notification of an award. If the project is a continuation of a previous investment, provide the approximate start date of that investment.	
End Date	End date of the project/ previously awarded investment	Provide the approximate end date of the project. If the end date is the end of the expected period of performance, provide that.	

HSGP IJ PLANNING TEMPLATE			SLCGP SPECIAL INSTRUCTIONS
Construction Activity	Indicates whether activities of the project will involve construction, renovation, retrofitting or modifications to an existing structure.	Select yes if the project may involve construction related activity.	
APPENDIX A. PROJECT MANAGEMENT LIFE-CYCLE			
The standard definition of a project is a temporary endeavor with a defined beginning and end (usually time-constrained, and often constrained by funding or a deliverable), undertaken to meet unique goals and objectives, typically to bring about beneficial change or added value. Applying this standard to projects using preparedness grant funds, a project is a related set of activities and purchases supporting the building or sustaining of core capabilities; and is associated with a single entity responsible for execution. This approach will allow DHS/FEMA and applicants to categorize the grant funded project as a discrete unit for post-award management, reporting, and monitoring purposes. The main steps and processes of the Project Management Life-cycle are summarized in this table:			
Steps	**Description**	**Process**	
Initiate	The authorization to begin work or resume work on any particular activity.	Involves preparing for, assembling resources and getting work started. May apply to any level, e.g., program, project, phase, activity, task.	
Steps	**Description**	**Process**	
Execute	The period within the project life-cycle during which the actual work of creating the project's deliverables is carried out.	Involves directing, accomplishing, managing, and completing all phases and aspects of work for a given project.	

HSGP IJ PLANNING TEMPLATE			SLCGP SPECIAL INSTRUCTIONS
Control	A mechanism which reacts to the current project status to ensure accomplishment of project objectives. This involves planning, measuring, monitoring, and taking corrective action based on the results of the monitoring.	Involves exercising corrective action as necessary to yield a required outcome consequent upon monitoring performance. Or the process of comparing actual performance with planned performance, analyzing variances, evaluating possible alternatives, and taking appropriate correct action as needed.	
Close Out	The completion of all work on a project. Can also refer to completion of a phase of the project.	Involves formally terminating and concluding all tasks, activities, and component parts of a particular project, or phase of a project.	
For additional information on the Project Management Life-cycle, please visit Project Management Institute's (PMI) *A Guide to the Project Management Body of Knowledge* (PMBOK Guide) at http://www.pmi.org/PMBOK-Guide-and-Standards.aspx. Specifically, applicants are encouraged to reference Chapter three of the PMBOK Guide, *The Standard for Project Management of a Project.*			

Appendix G: Required, Encouraged, and Optional Services, Memberships, and Resources

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

- **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.
- **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 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.

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:

- CYBER RESOURCE HUB
- Ransomware Guide (Sept. 2020)
- Malicious Domain Blocking and Reporting
- 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 H: Economic Hardship Cost Share Waiver

The Homeland Security Act of 2002, as amended, requires SLCGP recipients in FY 2022 to provide a non-federal cost share of 10% if they are applying as a single entity (6 U.S.C. § 665g(m)(1)). For entities unable to meet the requirement, an economic hardship waiver may be granted by the DHS Secretary (or designee). However, DHS is not able to provide additional funds even if it does grant a cost share waiver. The federal funding will remain at the same amount as indicated by the statutory formula.

Note that there is no cost share requirement for multi-entity groups for FY 2022. In addition, in accordance with 48 U.S.C. § 1469a, the Secretary has issued a blanket waiver of cost share requirements 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.

Economic Hardship Factors

Requests for cost share waivers may be granted by the Secretary (or designee) to an eligible entity that demonstrates economic hardship.

The statute, at 6 U.S.C. § 665g(m)(2)(C) requires the Secretary (or designee) to consider the following factors when determining economic hardship:

- Changes in rates of unemployment in the jurisdiction from previous years; and
- Changes in the percentage of individuals who are eligible to receive benefits under the supplemental nutrition assistance program established under the Food and Nutrition Act of 2008 (7 U.S.C. § 2011 et seq.) from previous years.

In addition, for FY 2022, the Secretary (or designee) will also consider the following factors in determining economic hardship:

- Demonstration of fiscal distress that could be caused by changes to statewide budgets already approved prior to knowledge of the SLCGP cost share requirement;
- Demonstration that the rate of unemployment has exceeded the annual national average rate of unemployment for three of the past five years;
- Demonstration that the entity has filed for bankruptcy or been placed under third-party financial oversight or receivership within the past three years; and
- For local units of government only, demonstration that those localities have areas within them that are designated as either “high” or “very high” on the Centers for Disease Control and Prevention’s Social Vulnerability Index.

To be considered for a cost share waiver, eligible entities must meet at least one of the six criteria described above, but do not necessarily need to meet all of them; requests for waivers will be considered on a case-by-case basis and evaluated holistically.

Waiver Request Requirements

Eligible entities that would like to request an economic hardship waiver should submit a waiver request with its FY 2022 SLCGP application submission in ND Grants with the following information in a written narrative:

- The entity’s background/history of economic hardship.

- Any austerity measure(s) the entity has taken to address economic hardship.
- A description of how the lack of a waiver will impact the entity's ability to develop, implement, or revise a Cybersecurity Plan or address imminent cybersecurity threats.
- A detailed justification explaining why the state (or specific local government(s) or specific project(s) if requesting only a partial waiver) is unable to fulfill the cost share requirement. The applicant must identify specific economic hardship(s) and address the factors listed above.

Approval Process

Once a decision on a waiver request is made, the state will be notified in writing. If approved, the award package will indicate that the cost share has been waived in full or in part and might indicate a requirement for the state to submit a revised budget and/or scope (as applicable) for the identified project(s). If the waiver request is approved after the award has been issued, FEMA will amend the award package to indicate the cost share has been waived in full or in part and whether the recipient must submit a revised budget and/or scope (as applicable) for the identified project(s).

Questions regarding the cost share waiver process may be directed to your FEMA Preparedness Officer or the Centralized Scheduling and Information Desk at askcsid@fema.dhs.gov or 1-800-368-6498.

Certifications Regarding Lobbying; Debarment, Suspension And Other Responsibility Matters; And Drug-Free Workplace Requirements

Applicants should refer to the regulations cited below to determine the certification to which they are required to attest. Applicants should also review the instructions for certification included in the regulations before completing this form. Signature of this form provides for compliance with certification requirements under 34 CFR Part 82, "New Restrictions on Lobbying," and 34 CFR Part 85, "Government-wide Debarment and Suspension (Nonprocurement) and Government-wide Requirements for Drug-Free Workplace (Grants)." The certifications shall be treated as a material representation of fact upon which reliance will be placed when the Department of Education determines to award the covered transaction, grant, or cooperative agreement.

1. **LOBBYING**

As required by Section 1352, Title 31 of the U.S. Code, and implemented at 34 CFR Part 82, for persons entering into a grant or cooperative agreement over $100,000, as defined at 34 CFR Part 82, Sections 82.105 and 82.110, the applicant certifies that:

(a) No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the making of any Federal grant, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal grant or cooperative agreement;

(b) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal grant or cooperative agreement, the undersigned shall complete and submit Standard Form - LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions;

(c) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subgrants, contracts under grants and cooperative agreements, and subcontracts) and that all subrecipients shall certify and disclose accordingly.

---

2. **DEBARMENT, SUSPENSION, AND OTHER RESPONSIBILITY MATTERS**

As required by Executive Order 12549, Debarment and Suspension, and implemented at 34 CFR Part 85, for prospective participants in primary covered transactions, as defined at 34 CFR Part 85, Sections 85.105 and 85.110--

A. The applicant certifies that it and its principals:

(a) Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal department or agency;

(b) Have not within a three-year period preceding this application been convicted of or had a civil judgement rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State, or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

(c) Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State, or local) with commission of any of the offenses enumerated in paragraph (2)(b) of this certification; and

(d) Have not within a three-year period preceding this application had one or more public transaction (Federal, State, or local) terminated for cause or default; and

B. Where the applicant is unable to certify to any of the statements in this certification, he or she shall attach an explanation to this application.

---

3. **DRUG-FREE WORKPLACE (GRANTEES OTHER THAN INDIVIDUALS)**

As required by the Drug-Free Workplace Act of 1988, and implemented at 34 CFR Part 85, Subpart F, for grantees, as defined at 34 CFR Part 85, Sections 85.605 and 85.610 -

A. The applicant certifies that it will or will continue to provide a drug-free workplace by:

(a) Publishing a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance is prohibited in the grantee's workplace and specifying the actions that will be taken against employees for violation of such prohibition;

(b) Establishing an on-going drug-free awareness program to inform employees about:

(1) The dangers of drug abuse in the workplace;

(2) The grantee's policy of maintaining a drug-free workplace;

(3) Any available drug counseling, rehabilitation, and employee assistance programs; and

(4) The penalties that may be imposed upon employees for drug abuse violations occurring in the workplace;

(c) Making it a requirement that each employee to be engaged in the performance of the grant be given a copy of the statement required by paragraph (a);

(d) Notifying the employee in the statement required by paragraph (a) that, as a condition of employment under the grant, the employee will:

(1) Abide by the terms of the statement; and

(2) Notify the employer in writing of his or her conviction for a violation of a criminal drug statute occurring in the workplace no later than five calendar days after such conviction;

(e) Notifying the agency, in writing, within 10 calendar days after receiving notice under subparagraph (d)(2) from an employee or otherwise receiving actual notice of such conviction. Employers of convicted employees must provide notice, including position title, to: Director, Grants Policy and Oversight Staff, U.S. Department of Education, 400 Maryland Avenue, S.W. (Room 3652, GSA Regional Office Building No. 3), Washington, DC 20202-4248. Notice shall include the identification number(s) of each affected grant;

(f) Taking one of the following actions, within 30 calendar days of receiving notice under subparagraph (d)(2), with respect to any employee who is so convicted:

(1) Taking appropriate personnel action against such an employee, up to and including termination, consistent with the requirements of the Rehabilitation Act of 1973, as amended; or

(2) Requiring such employee to participate satisfactorily in a drug abuse assistance or rehabilitation program approved for such purposes by a Federal, State, or local health, law enforcement, or other appropriate agency;

(g) Making a good faith effort to continue to maintain a drug-free workplace through implementation of paragraphs (a), (b), (c), (d), (e), and (f).

B. The grantee may insert in the space provided below the site(s) for the performance of work done in connection with the specific grant:

Place of Performance (Street address. city, county, state, zip code)

_____

_____

_____

DRUG-FREE WORKPLACE
(GRANTEES WHO ARE INDIVIDUALS)

As required by the Drug-Free Workplace Act of 1988, and implemented at 34 CFR Part 85, Subpart F, for grantees, as defined at 34 CFR Part 85, Sections 85.605 and 85.610-

A. As a condition of the grant, I certify that I will not engage in the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance in conducting any activity with the grant; and

B. If convicted of a criminal drug offense resulting from a violation occurring during the conduct of any grant activity, I will report the conviction, in writing, within 10 calendar days of the conviction, to: Director, Grants Policy and Oversight Staff, Department of Education, 400 Maryland Avenue, S.W. (Room 3652, GSA Regional Office Building No. 3), Washington, DC 20202-4248. Notice shall include the identification number(s) of each affected grant.

Check **[ ]** if there are workplaces on file that are not identified here.

As the duly authorized representative of the applicant, I hereby certify that the applicant will comply with the above certifications.

NAME OF APPLICANT	PR/AWARD NUMBER AND / OR PROJECT NAME
PRINTED NAME AND TITLE OF AUTHORIZED REPRESENTATIVE	
SIGNATURE	DATE

View Burden Statement

ASSURANCES - CONSTRUCTION PROGRAMS

OMB Number: 4040-0009
Expiration Date: 02/28/2025

Public reporting burden for this collection of information is estimated to average 15 minutes per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the Office of Management and Budget, Paperwork Reduction Project (0348-0042), Washington, DC 20503.

PLEASE DO NOT RETURN YOUR COMPLETED FORM TO THE OFFICE OF MANAGEMENT AND BUDGET. SEND IT TO THE ADDRESS PROVIDED BY THE SPONSORING AGENCY.

NOTE: Certain of these assurances may not be applicable to your project or program. If you have questions, please contact the Awarding Agency. Further, certain Federal assistance awarding agencies may require applicants to certify to additional assurances. If such is the case, you will be notified.

As the duly authorized representative of the applicant:, I certify that the applicant:

1. Has the legal authority to apply for Federal assistance, and the institutional, managerial and financial capability (including funds sufficient to pay the non-Federal share of project costs) to ensure proper planning, management and completion of project described in this application.
2. Will give the awarding agency, the Comptroller General of the United States and, if appropriate, the State, the right to examine all records, books, papers, or documents related to the assistance; and will establish a proper accounting system in accordance with generally accepted accounting standards or agency directives.
3. Will not dispose of, modify the use of, or change the terms of the real property title or other interest in the site and facilities without permission and instructions from the awarding agency. Will record the Federal awarding agency directives and will include a covenant in the title of real property acquired in whole or in part with Federal assistance funds to assure non-discrimination during the useful life of the project.
4. Will comply with the requirements of the assistance awarding agency with regard to the drafting, review and approval of construction plans and specifications.
5. Will provide and maintain competent and adequate engineering supervision at the construction site to ensure that the complete work conforms with the approved plans and specifications and will furnish progressive reports and such other information as may be required by the assistance awarding agency or State.
6. Will initiate and complete the work within the applicable time frame after receipt of approval of the awarding agency.
7. Will establish safeguards to prohibit employees from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain.
8. Will comply with the Intergovernmental Personnel Act of 1970 (42 U.S.C. §§4728-4763) relating to prescribed standards of merit systems for programs funded under one of the 19 statutes or regulations specified in Appendix A of OPM's Standards for a Merit System of Personnel Administration (5 C.F.R. 900, Subpart F).
9. Will comply with the Lead-Based Paint Poisoning Prevention Act (42 U.S.C. §§4801 et seq.) which prohibits the use of lead-based paint in construction or rehabilitation of residence structures.
10. Will comply with all Federal statutes relating to non-discrimination. These include but are not limited to: (a) Title VI of the Civil Rights Act of 1964 (P.L. 88-352) which prohibits discrimination on the basis of race, color or national origin; (b) Title IX of the Education Amendments of 1972, as amended (20 U.S.C. §§1681 1683, and 1685-1686), which prohibits discrimination on the basis of sex; (c) Section 504 of the Rehabilitation Act of 1973, as amended (29) U.S.C. §794), which prohibits discrimination on the basis of handicaps; (d) the Age Discrimination Act of 1975, as amended (42 U.S.C. §§6101-6107), which prohibits discrimination on the basis of age; (e) the Drug Abuse Office and Treatment Act of 1972 (P.L. 92-255), as amended relating to nondiscrimination on the basis of drug abuse; (f) the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970 (P.L. 91-616), as amended, relating to nondiscrimination on the basis of alcohol abuse or alcoholism; (g) §§523 and 527 of the Public Health Service Act of 1912 (42 U.S.C. §§290 dd-3 and 290 ee 3), as amended, relating to confidentiality of alcohol and drug abuse patient records; (h) Title VIII of the Civil Rights Act of 1968 (42 U.S.C. §§3601 et seq.), as amended, relating to nondiscrimination in the sale, rental or financing of housing; (i) any other nondiscrimination provisions in the specific statue(s) under which application for Federal assistance is being made; and (j) the requirements of any other nondiscrimination statue(s) which may apply to the application.

11. Will comply, or has already complied, with the requirements of Titles II and III of the Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970 (P.L. 91-646) which provide for fair and equitable treatment of persons displaced or whose property is acquired as a result of Federal and federally-assisted programs. These requirements apply to all interests in real property acquired for project purposes regardless of Federal participation in purchases.

12. Will comply with the provisions of the Hatch Act (5 U.S.C. §§1501-1508 and 7324-7328) which limit the political activities of employees whose principal employment activities are funded in whole or in part with Federal funds.

13. Will comply, as applicable, with the provisions of the Davis-Bacon Act (40 U.S.C. §§276a to 276a-7), the Copeland Act (40 U.S.C. §276c and 18 U.S.C. §874), and the Contract Work Hours and Safety Standards Act (40 U.S.C. §§327-333) regarding labor standards for federally-assisted construction subagreements.

14. Will comply with flood insurance purchase requirements of Section 102(a) of the Flood Disaster Protection Act of 1973 (P.L. 93-234) which requires recipients in a special flood hazard area to participate in the program and to purchase flood insurance if the total cost of insurable construction and acquisition is $10,000 or more.

15. Will comply with environmental standards which may be prescribed pursuant to the following: (a) institution of environmental quality control measures under the National Environmental Policy Act of 1969 (P.L. 91-190) and Executive Order (EO) 11514; (b) notification of violating facilities pursuant to EO 11738; (c) protection of wetlands pursuant to EO 11990; (d) evaluation of flood hazards in floodplains in accordance with EO 11988; (e) assurance of project consistency with the approved State management program developed under the Coastal Zone Management Act of 1972 (16 U.S.C. §§1451 et seq.); (f) conformity of Federal actions to State (Clean Air) implementation Plans under Section 176(c) of the Clean Air Act of 1955, as amended (42 U.S.C. §§7401 et seq.); (g) protection of underground sources of drinking water under the Safe Drinking Water Act of 1974, as amended (P.L. 93-523); and, (h) protection of endangered species under the Endangered Species Act of 1973, as amended (P.L. 93-205).

16. Will comply with the Wild and Scenic Rivers Act of 1968 (16 U.S.C. §§1271 et seq.) related to protecting components or potential components of the national wild and scenic rivers system.

17. Will assist the awarding agency in assuring compliance with Section 106 of the National Historic Preservation Act of 1966, as amended (16 U.S.C. §470), EO 11593 (identification and protection of historic properties), and the Archaeological and Historic Preservation Act of 1974 (16 U.S.C. §§469a-1 et seq).

18. Will cause to be performed the required financial and compliance audits in accordance with the Single Audit Act Amendments of 1996 and OMB Circular No. A-133, "Audits of States, Local Governments, and Non-Profit Organizations."

19. Will comply with all applicable requirements of all other Federal laws, executive orders, regulations, and policies governing this program.

20. Will comply with the requirements of Section 106(g) of the Trafficking Victims Protection Act (TVPA) of 2000, as amended (22 U.S.C. 7104) which prohibits grant award recipients or a sub-recipient from (1) Engaging in severe forms of trafficking in persons during the period of time that the award is in effect (2) Procuring a commercial sex act during the period of time that the award is in effect or (3) Using forced labor in the performance of the award or subawards under the award.

SIGNATURE OF AUTHORIZED CERTIFYING OFFICIAL	TITLE
APPLICANT ORGANIZATION	DATE SUBMITTED

GRANT AGREEMENT
FOR
FISCAL YEAR 2022
STATE AND LOCAL CYBERSECURITY GRANT PROGRAM

BETWEEN

THE GEORGIA EMERGENCY MANAGEMENT AND HOMELAND SECURITY AGENCY

AND

Smyrna

GRANT NO: 14

GRANT TERMS AND CONDITIONS

The United States Department of Homeland Security's ("DHS") Federal Fiscal Year ("FY") 2022 State and Local Cybersecurity Grant Program ("SLCGP") assists state, local, and territorial ("SLT") governments with managing and reducing systemic cyber risk. Through funding from the Infrastructure Investment and Jobs Act, also known as the Bipartisan Infrastructure Law, 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 to their communities.

This Grant Agreement ("Agreement") is made and entered into by and between the Georgia Emergency Management and Homeland Security Agency ("GEMA/HS"), an agency of the State of Georgia ("State"), and Smyrna ("Subrecipient"). GEMA/HS and the Subrecipient are sometimes referred to herein individually as a "Party" or collectively, the "Parties".

For the purposes of this Agreement, GEMA/HS serves as the pass-through entity for a Federal award, and the Subrecipient serves as the recipient of a subaward.

THIS AGREEMENT IS ENTERED INTO BASED ON THE FOLLOWING REPRESENTATIONS:

2 C.F.R. §200.92 states that a "subaward may be provided through any form of legal agreement, including an agreement that the pass-through entity considers a contract."

As defined by 2 C.F.R. §200.74, "pass-through entity" means "a non-Federal entity that provides a subaward to a Subrecipient to carry out part of a Federal program."

As defined by 2 C.F.R. §200.93, "Subrecipient" means "a non-Federal entity that receives a subaward from a pass-through entity to carry out part of a Federal program."

As defined by 2 C.F.R. §200.38, "Federal award" means "Federal financial assistance that a non-Federal entity receives directly from a Federal awarding agency or indirectly from a pass-through entity."

As defined by 2 C.F.R. §200.92, "subaward" means "an award provided by a pass-through entity to a Subrecipient for the Subrecipient to carry out part of a Federal award received by the passthrough entity."

THEREFORE, DIVISION AND SUBRECIPIENT AGREE TO THE FOLLOWING:

I. PERIOD OF PERFORMANCE.

The Parties hereby agree as follows: This Agreement shall become effective on the Projected

Start Date and shall continue through the Projected End Date listed below.

Projected Period of Performance Start Date(s): October 1, 2024

Projected Period of Performance End Date(s): September 30, 2025

No modifications to the Budget Cost Lines can be made after the termination date, September 30, 2025, or when all funds have been used.

GEMA/HS will maintain overall responsibility and accountability to the federal government for the duration of the program. GEMA/HS, as the Recipient, has awarded the amount of $69,650.00 to Smyrna as the Subrecipient**,** in accordance with the Fiscal Year 2022 State and Local Cybersecurity Grant Program. Subrecipient shall meet a 10% cost share requirement in the amount of $6,965.00.

SLCGP Grant funding may not commence until this Agreement is effective. The Subrecipient agrees that all purchases and expenditures authorized under this program must be completed by the effective end date. Extensions are at the discretion of GEMA/HS and will only be granted for cause when requested in EM Grants Manager before the end date of this Agreement. Extensions should be requested 30 days before the end of this agreement, but no longer than 30 days after the end date.

DHS/FEMA HAS RESERVED THE RIGHT TO CHANGE THE FY22 SLCGP GRANT; INCLUDING SHORTENING THE PERFORMANCE PERIOD AND/OR GRANT END DATE. ANY CHANGE IN THE GRANT AND/OR PERFORMANCE PERIOD OF THE FY22 SLCGP AWARD WILL BE PASSED THROUGH TO THE SUBRECIPIENT BY GEMA/HS.

II. STANDARD OF PERFORMANCE.

The Subrecipient agrees to use allocated funds only as approved; to comply with the terms, conditions, and guidelines, as stated within this agreement; and to request reimbursement only for expenditures made in accordance with the SLCGP Investment Justification Worksheet and the approved Budget Detail Worksheet(s). Any modifications to the approved Budget Detail Worksheet(s) must be requested in writing by the Subrecipient and must be approved by the Program Manager prior to the execution of that modification.

Subrecipient shall perform all activities as approved by GEMA/HS. Any change to a project shall receive prior written approval by GEMA/HS and, if required, by FEMA or other awarding agency. Subrecipient shall perform all activities in accordance with all terms, provisions and requirements set forth in this Agreement, including but not limited to the following Exhibits and Attachments:

A. Exhbitis:

1. SLCGP Goals and Objectives

B. Attachments:

1. Attachment A: Standard Assurances:

(Attachment A1) Standard Form 424B (Non-Construction) or
(Attachment A2) Standard Form 424D (Construction), as applicable

(COMPLETE, SIGN, AND RETURN WITH AGREEMENT)

2. Attachment B: FY 2022 State and Local Cybersecurity Grant Program Agreement Articles;

3. Attachment C: FY 2022 State and Local Cybersecurity Grant Program Amendment Letter;

4. Attachment D: Federal Terms and Conditions;

5. Attachment E: Certifications Regarding Lobbying; Debarment, Suspension And Other Responsibility Matters; And Drug-Free Workplace Requirements;

(COMPLETE, SIGN, AND RETURN WITH AGREEMENT)

6. Attachment F: DHS Fiscal Year 2022 State and Local Cybersecurity Grant Program Notice of Funding Opportunity, (available online at https://www.fema.gov/print/pdf/node/641059);

7. Attachment G: SLCGP Investment Justification Worksheet; and

8. Attachment H: Approved Budget Detail Worksheet(s).

III. FUNDING OBLIGATIONS.

GEMA/HS shall not be liable to Subrecipient for any costs incurred by Subrecipient that are not allowable costs.

A. Notwithstanding any other provision of this Agreement, the total of all payments and other obligations incurred by GEMA/HS under this Agreement shall not exceed the total cumulative award amounts listed on the Subawards (projects and subsequent versions).

B. Subrecipient shall meet a 10% cost share requirement for the FY 2022 SLCGP as listed in the FY 2022 SLCGP DHS/FEMA NOFO.

C. The Subrecipient agrees that all allocations and use of funds under this grant will be in accordancewith the FY 2022 SLCGP DHS/FEMA NOFO (Attachment H),

and to comply with all DHS/FEMA requirements and cooperate with GEMA/HS to comply with federal and state requirements relatedto the grant funding.

D. The Subrecipient understands and agrees that any allocations and use of grant funding must support and may only be used to fund the investments identified in the Fiscal Year 2022 SLCGP grant application submitted by GEMA/HS to DHS/FEMA and to use grant funding only for projects pre- approved by GEMA/HS.

E. Federal funds under this grant program are provided through reimbursement of all eligible expenditures. The Subrecipient shall follow procurement standards as stated in federal and state laws and regulations.

F. The Subrecipient understands and agrees that it cannot use any federal funds, either directly or indirectly, in support of the enactment, repeal, modification, or adoption of any law, regulation, or policy, at any level of government, without the express prior written approval of GEMA/HS and DHS.

G. No elected or appointed official or employee of the Subrecipient shall be admitted to any share or part of any benefit, directly or indirectly, from this agreement or grant award. This provision shallnot be construed to extend to any contract made with a corporation for its general benefit.

H. **Non-Supplanting Requirement**. The Subrecipient agrees that federal grant funds received under this award will not replace (supplant) funds that have been budgeted for the same purpose through non-federal sources. Applicants or Recipients may be required to demonstrate if a reduction in non- federal resources occurred for reasons other than the receipt or expected receipt of federal funds. The Subrecipient will be expected to demonstrate how these funds will be used to supplement, but not supplant, state or local funds for the same purposes.

I. **Prior Approval for Modification of Approved Budget**. Before making any change to the FEMA approved budget for this award, you must request prior written approval from FEMA where required by 2 C.F.R. section 200.308.

1. For purposes of non-construction projects, FEMA is utilizing its discretion to impose an additional restriction under 2 C.F.R. section 200.308(f) regarding the transfer of funds among direct cost categories, programs, functions, or activities. Therefore, for awards with an approved budget where the federal share is greater than the simplified acquisition threshold (currently $250,000), you may not transfer funds among direct cost categories, programs, functions, or activities without prior written approval from FEMA where the cumulative amount of such transfers exceeds or is expected to exceed ten percent (10%) of the total budget FEMA last approved.

2. For purposes of awards that support both construction and non-construction work, FEMA is utilizing its discretion under 2 C.F.R. section 200.308(h)(5) to require the recipient to obtain prior written approval from FEMA before making any fund or budget transfers between the two types of work.

3. Subrecipient must report any deviations from FEMA-approved budget in the first Federal Financial Report (SF-425) you submit following any budget deviation, regardless of whether the budget deviation requires prior written approval.

J. After all approved items on the approved Budget Detail Worksheet(s)have been reimbursed to the Subrecipient; this Subrecipient Agreement shall be terminated. Any remaining funds shall be forfeited by the Subrecipient.

K. The terms of the approved Investment Justification(s) and Budget Detail Worksheet(s) submitted by the recipient are incorporated into the terms of this Federal award, subject to the additional description and limitations stated in this Agreement Article and the limitations stated in subsequent reviews by FEMA and the Cybersecurity and Infrastructure Security Agency ("CISA") of the award budget. Post-award documents uploaded into Non-Disaster Grants Management System ("ND Grants") for this award are also incorporated into the terms and conditions of this award, subject to any limitations stated in subsequent approvals by FEMA and CISA of changes to the award. Investments not listed in this Agreement Article are not approved for funding under this award.

IV. UNIFORM ADMINISTRATIVE REQUIREMENTS.

A. Except as specifically modified by law or this Grant, Subrecipient shall administer this Agreement through compliance with the most recent version of all applicable federal and state laws and regulations, including but not limited to DHS program legislation, Federal awarding agency regulations, and the terms and conditions of this Grant. A non-exclusive list is provided below [not all may apply in every project]:

1. Public Law 93-288, as amended (Stafford Act);

2. 44 C.F.R., Emergency Management and Assistance;

3. Disaster Mitigation Act of 2000;

4. OMB Regulations 2 C.F.R., Grant and Agreements;

5. Executive Order 11988, Floodplain Management

6. Executive Order 11990, Protection of Wetlands

7. Executive Order 12372, Intergovernmental Review of Programs and Activities

8. Executive Order 12549, Debarment and Suspension

9. Executive Order 12612, Federalism

10. Executive Order 12699, Seismic Design

11. Executive Order 12898, Environmental Justice

12. Coastal Barrier Resources Act, Public Law 97-348

13. Single Audit Act, Public Law 98-502

14. Sandy Recovery Improvement Act publications

15. Disaster Recovery Reform Act of 201816 U.S.C. § 470, National Historic Preservation Act

16. 16 U.S.C. § 1531, Endangered Species Act References

17. FEMA program publications, guidance, and policies

18. 2 CFR Part 200, Subpart E, Cost Principles for Non-Profit Organizations

19. 2 CFR Part 200, Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations

B. **Unique Entity Identifier ("UEI").** Effective April 4, 2022, the Federal Government transitioned from using the Data Universal Numbering System or DUNS number, to a new, non-proprietary identifier known as a Unique Entity Identifier or UEI. For entities that had an active registration in the System for Award Management (SAM) prior to this date, the UEI has automatically been assigned and no action is necessary. For all entities filing a new registration in SAM.gov on or after April 4, 2022, the UEI will be assigned to that entity as part of the SAM.gov registration process. UEI registration information is available on GSA.gov at https://www.gsa.gov/about-us/organization/federal-acquisitionservice/office-of-systems-management/integrated-award-environment-iae/iae-systems-information-kit/unique-entityidentifier-update.

C. **Accounting System**. The Subrecipient agrees to maintain an accounting system integrated with adequate internal fiscal and management controls to capture and

report grant data with accuracy, providing full accountability for revenues, expenditures, assets, and liabilities. This system shall provide reasonable assurance that the Subrecipient is managing federal and state financial assistance programs in compliance with all applicable laws and regulations.

D. The Subrecipient Agency shall utilize the U.S. Department of Homeland Security's E-Verify System to verify the employment eligibility of all persons hired during the Agreement term.

V. PURCHASING.

A. **Purchasing.** Subrecipient must follow federal, state, and local procurement guidance and regulations as standards for purchasing or acquiring equipment and services. All spending or purchases must be made in accordance with the agreed spending plan as outlined in the Budget Cost Lines (Attachment G) and all equipment purchases must be in accordance with the Department of Homeland Security Authorized Equipment List (DHS/AEL) located on the internet at: https://www.fema.gov/grants/guidance-tools/authorized-equipment-list.

B. **Payment Request Forms.** Payments to the Subrecipients will be made only upon presentation of the approved Payment Request. Reimbursements from invoices and applicable proof of payment (or other justifying documentation) will only be made for eligible equipment, materials, expenses, and costs upon approval of the Program Manager. Omission of pertinent documentation will constitute justification for non-payment of any amounts submitted on the Payment Request.

C. **Allowable Costs**. Funds must be spent in compliance with applicable rules and regulations noted in the FY 2022 SLCGP DHS/FEMA NOFO. All costs charged to awards covered by this FY 2022 SLCGP DHS/FEMA NOFO must comply with the Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2 C.F.R. Part 200, unless otherwise indicated in the FY 2022 SLCGP DHS/FEMA NOFO or the terms and conditions of the award. This includes, among other requirements, that costs must be incurred, and products and services must be delivered, within the period of performance of the award. See 2 C.F.R. § 200.403(h) (referring to budget periods, which for DHS awards under this program is the same as the period of performance).

1. **General Allowable Costs**. Subrecipients can use SLCGP grant funds for:

i. Developing the Cybersecurity Plan;

ii. Implementing or revising the Cybersecurity Plan;

iii. Paying expenses directly relating to the administration of the grant, which cannot exceed 5% of the amount of the grant award;

iv. Assisting with allowed activities that address imminent cybersecurity threats confirmed by DHS; and

v. Other appropriate activities as noted in the FY 2022 SLCGP DHS/FEMA NOFO.

2. **Planning**. SLCGP funds may be used for a range of planning activities, such as those associated with 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.

3. **Organization**. Organization costs are allowable under this program. States must justify proposed expenditures of SLCGP funds to support organization activities within their IJ submission. Organizational activities include:

i. Organizational activities include:

a) Program management;

b) Development of whole community partnerships that support the Cybersecurity Planning Committee;

c) Structures and mechanisms for information sharing between the public and private sector; and

d) Operational support.

ii. 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.

4. **Equipment**. Funding may be used to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state and local governments. Subrecipients may spend their portion of the funds on ransomware protections, data backups, basic cybersecurity protections, risk management frameworks. Subrecipient should limit purchases to the equipment referenced in the FY 2022 SLCGP DHS/FEMA NOFO and the Authorized Equipment List ("AEL").

i. Software and software licenses are authorized expenditures under SLCGP. Software can be included in the "equipment" cost category of the project budget under the appropriate AEL number. Software licenses would generally be covered under the same AEL as the software.

ii. There are currently 21 different sections of the AEL, including information technology (section 4) and cybersecurity equipment (section 5). Each AEL section includes numerous categories and subcategories. SLCGP applicants should search all AEL sections, categories, and subcategories on the FEMA AEL website to find the appropriate AEL. For example, the AEL for SAAS (software as a service) is 04AP-11-SAAS - Applications, Software as a Service.

iii. Personnel must be properly trained to use the equipment purchased under this grant program in accordance with all applicable federal, state, and local laws including, but not limited to regulations established by the Environmental Protection Agency ("EPA"), the Occupational Safety and Health Administration ("OSHA"), and the National Fire Protection Association ("NFPA"). By signing and submitting grant acceptance documents, the authorized official certifies employees have received or will receive required training prior to utilizing equipment purchased with FEMA funding.

iv. Subrecipient is responsible for replacing or repairing equipment that is lost, stolen, damaged, or destroyed as a result of Subrecipient's willful or negligent action. Property losses should be reported to GEMA/HS immediately.

5. Additionally, recipients that are using SLCGP funds to support emergency communications equipment activities must comply with the SAFECOM Guidance on Emergency Communications Grants, including provisions on technical standards that ensure and enhance interoperable communications. You can access the Fiscal Year 2023 SAFECOM Guidance on Emergency Communications Grants at the following link: https://www.cisa.gov/sites/default/files/2023-04/fy23_safecom_guidance.pdf

6. **Maintenance and Sustainment.** Funding may be used for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees as described in DHS/FEMA Policy FP 205-402-125-1, available at http://www.fema.gov/media-library/assets/documents/32474.

7. **Training.** Subrecipients may use SLCGP funds to attend training courses, exercises, and programs in the United States.

i. Allowable training-related costs under SLCGP include the establishment, support, conduct, and attendance of training and/or in conjunction with training by other federal agencies. Training conducted using SLCGP funds should align with the eligible entity's Cybersecurity Plan, address a performance gap identified through assessments, and contribute to building a capability that will be evaluated through a formal exercise.

ii. Any training or training gaps, including training related to underserved communities that may be more impacted by disasters, including children, seniors, individuals with disabilities or access and functional needs, individuals with diverse culture and language use, individuals with lower economic capacity, and other underserved populations, should be identified in an assessment and addressed in the eligible entity's training cycle.

iii. Subrecipients are encouraged to utilize FEMA's National Preparedness Course Catalog. Training includes programs or courses developed for and delivered by institutions and organizations funded by FEMA. This consists of the Center for Domestic Preparedness (CDP), the Emergency Management Institute (EMI), and FEMA's Training Partner Programs, including the Continuing Training Grants (CTG), the National Domestic Preparedness Consortium (NDPC), the Rural Domestic Preparedness Consortium (RDPC), and other partners. The catalog features a wide range of course topics in multiple delivery modes to meet FEMA's mission scope and the increasing training needs of federal, state, local, territorial, and tribal audiences. The catalog can be accessed at http://www.firstrespondertraining.gov.

iv. Proposed attendance at training courses and all associated costs leveraging the FY 2022 SLCGP must be included in the Subrecipient's Investment Justification. Proposed attendance at training and all associated costs using SLCGP must be included in the Subrecipient's Investment Justification.

v. Some training activities require Environmental and Historic Preservation Review, including exercises, drills, or trainings that require any type of land, water, or vegetation disturbance or building of temporary structures or that are not located at facilities designed to conduct training and exercises. Additional information on training requirements and EHP review can be found online at https://www.fema.gov/media-library/assets/documents/90195.

8. Exercises.

i. Exercise costs are allowable under this program. Exercises conducted with grant funding should be managed and run consistent with the Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP guidance for exercise design, development, conduct, evaluation, and improvement planning is at https://www.fema.gov/emergency-managers/nationalpreparedness/exercises/hseep.

ii. Any exercise conducted with SLCGP grant funds must comply with the Nation Incident Management System ("NIMS") requirements. These requirements can be found at https://www.fema.gov/sites/default/files/2020-04/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf. Exercise documentation, including but not limited to objectives, after-action reports, and participants, must be coordinated with and submitted to the GEMA/HS.

9. **Management and Administration ("M&A")**.

i. Subrecipients that receive an award under this program may use and expend up to five percent (5%) of their FY 2022 SLCGP funds for M&A purposes.

ii. M&A costs are for activities directly related to the management and administration of the award, such as financial management and monitoring, submitting required programmatic and financial reports, establishing, and maintaining equipment inventory.

10. **Indirect (Facilities & Administrative (F&A)) Costs.** Indirect costs are allowable under this program as described in 2 C.F.R. § 200.414. With the exception of subrecipients who have never received a negotiated indirect cost rate as described in 2 C.F.R. § 200.414(f). Subrecipients must have an approved indirect cost rate agreement with their cognizant federal agency to charge indirect costs to this award.

11. **Construction and Renovation.** Any Subrecipient project that involves construction and renovation cost must contact GEMA/HS prior to submission. All Subrecipients must request and receive approval from DHS/FEMA before any funds are used for construction or renovation.

12. The Subrecipient understands and agrees that compensation for individual consultant services is to be reasonable and consistent and should represent fair market value for services. Time and effort reports for consultant

services are required, and competitive bidding is encouraged, as explained in 2 C.F.R. § 200.317-326.

D. **Unallowable Costs.** The following projects and costs are considered **ineligible** for award consideration:

1. Initiatives that duplicate capabilities being provided by the Federal Government;

2. Reimbursement of pre-award security expenses;

3. To supplant state or local funds; however, this shall not be construed to prohibit the use of funds from a grant under this FY 2022 SLCGP DHS/FEMA NOFO for otherwise permissible uses on the basis that the Subrecipient has previously used SLT funds to support the same or similar uses;

4. For any recipient cost-sharing contribution;

5. Payment of a ransom from cyberattacks;

6. For recreational or social purposes, or for any purpose that does not address cybersecurity risks or cybersecurity threats on SLT information systems;

7. Lobbying or intervention in federal regulatory or adjudicatory proceedings;

8. Suing the federal government or any other government entity;

9. Paying for cybersecurity insurance;

10. Acquiring land or to construct, remodel, or perform alternations of buildings or other physical facilities; or

11. 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.

VI. GENERAL PROHIBITIONS

A. **Use of Funds**. DHS/FEMA Grant funds may only be used for the purposes set forth in this Grant and shall be consistent with the statutory authority for this Grant. Grant funds may not be used for matching funds for other Federal grants/cooperative agreements, lobbying, or intervention in Federal regulatory or adjudicatory proceedings. In addition, Federal funds may not be used to sue the Federal government or any other government entity.

B. **Federal Employee Prohibition**. Federal employees are prohibited directly benefiting from any funds under this Agreement.

C. The employment of unauthorized aliens by the Subrecipient is considered a violation of Section 274A(e) of the Immigration and Nationality Act. If the Subrecipient knowingly employs unauthorized aliens, such violation shall cause the unilateral cancellation of the Agreement. Any services performed by any such unauthorized aliens shall not be paid.

VII. MODIFICATIONS

The Subrecipient understands and agrees that, in addition to the provisions in the "Termination" section below, GEMA/HS shall have the right to make unilateral changes, cancel, or terminate this agreement in the event that FEMA and/or DHS makes changes to the FY22 SLCGP grant awarded to GEMA/HS. With the exception of termination or changes included in this agreement, there shall be no other changes to this Agreement unless mutually agreed upon by all parties to the Agreement.

VIII. SUSPENSION

In the event Subrecipient fails to comply with any term of this Grant, GEMA/HS may, upon written notification to Subrecipient, suspend this Agreement, in whole or in part, withhold payments to Subrecipient and prohibit Subrecipient from incurring additional obligations of this Grant's funds.

IX. TERMINATION

A. Cause/Default: This agreement may be terminated for cause, in whole or in part, at any time by the State of Georgia for the failure of the Subrecipient to perform any of the provisions or to comply with any of the terms and conditions herein. If the State exercises its right to terminate this agreement under the provisions of this paragraph, the termination shall be accomplished in writing and specify the reason and termination date. The Subrecipient will be required to submit the final invoice no later than 30 days after the effective date of written notice of termination. Upon termination of this agreement, the State shall not incur any new obligations after the effective date of the termination and shall cancel outstanding obligations, as possible. The above remedies are in addition to any other remedies provided by law or the terms of this agreement.

B. Notwithstanding and without waiving any other remedies available for the Subrecipient's failure to comply with the terms and conditions of this agreement, if the Subrecipient fails to meet its obligations, voluntarily or otherwise, as part of a GEMA/HS program, GEMA/HS will have the right, privilege, and option to immediately terminate this Agreement. Failure to exercise the right of termination for previous occurrences or omissions will not act as a waiver for future noncompliance by the Subrecipient. Should GEMA/HS exercise the right,

privilege, and option to terminate this Agreement, the Subrecipient shall immediately transfer ownership of any SLCGP grant-funded equipment purchased under this agreement to GEMA/HS or whomever GEMA/HS shall designate, without cost, as directed by GEMA/HS.

C. GEMA/HS may terminate this Agreement for cause after thirty (30) days written notice. Cause can include misuse of funds, fraud, lack of compliance with applicable rules, laws, and regulations, failure to perform on time, and refusal by the Subrecipient to permit public access to any document, paper, letter, or other material subject to disclosure under O.C.G.A. Section 50-18-70 et seq.

D. GEMA/HS may terminate this Agreement for convenience or when it determines, in its sole discretion, that continuing the Agreement would not produce beneficial results in line with the further expenditure of funds, by providing the Subrecipient with thirty (30) calendar days prior written notice.

E. Non-Availability of Funding: Notwithstanding any other provision of this agreement, in the event that either of the sources of funding for reimbursement under this agreement (appropriations from the General Assembly of the State of Georgia or the Congress of the United States of America) no longer exist, in the event, the sum of all obligations of GEMA/HS incurred under this and all other agreements entered into for this program exceeds the balance of such funding, then this agreement shall immediately terminate without further obligation of GEMA/HS. The certification by the Director of GEMA/HS of the occurrence of either of the events stated above shall be conclusive.

F. In the event this Agreement is terminated, the Subrecipient will not incur new obligations for the terminated portion of the Agreement after the Subrecipient has received the notification of termination.

G. The Subrecipient will cancel as many outstanding obligations as possible. Costs incurred after receipt of the termination notice will be disallowed. The Subrecipient shall not be relieved of liability to GEMA/HS because of any breach of Agreement by the Subrecipient. GEMA/HS may, to the extent authorized by law, withhold payments to the Subrecipient for the purpose of set-off until the exact amount of damages due GEMA/HS from the Subrecipient is determined.

H. **Subrecipient's Responsibilities Upon Termination**. If GEMA/HS provides a notice of termination to the Subrecipient, except as otherwise specified by GEMA/HS in that notice, the Subrecipient shall:

1. Stop work under this Agreement on the date and to the extent specified in the notice.

2. Complete performance of such part of the work that has not been terminated by GEMA/HS, if any.

3. Take such action as may be necessary, or as GEMA/HS may specify, to protect and preserve any property which is in the possession and custody of the Subrecipient, and in which GEMA/HS has or may acquire an interest.

4. Transfer, assign, and make available to GEMA/HS all property and materials belonging to GEMA/HS upon the effective date of termination of this Agreement. No extra compensation will be paid to the Subrecipient for its services in connection with such transfer or assignment.

I. **Withholding and Repayment of Funds**. In addition to any other remedies provided by law or the terms of this Agreement, if the Subrecipient fails to comply with any of the terms or conditions of this Agreement, including all attachments hereto, or with any applicable federal or state law or regulation, GEMA/HS may withhold or require repayment of grant funds in connection with which the violation occurred. In addition, GEMA/HS may withhold or require repayment of all or any portion of the financial award which has been or is to be made available to the Subrecipient. Specifically, without limitation, GEMA/HS will be entitled to payment from the Subrecipient for any funds paid by the State or that the State is responsible to pay on behalf of the Subrecipient for which GEMA/HS is unable to receive payment or required to repay due to the Subrecipient's failure to cooperate in providing the required documentation showing receipt of the goods or services, completing and returning the Acknowledgment Form to GEMA/HS in the time required, purchasing of equipment in the time required, submitting a request for reimbursement with complete supporting documents, or any other activity that GEMA/HS deems a failure by the Subrecipient under this Agreement.

X. CLOSING OF THIS GRANT.

A. GEMA/HS will close each subaward after receiving all required final documentation from the Subrecipient. If the close out review and reconciliation indicates that Subrecipient is owed additional funds, GEMA/HS will send the final payment automatically to Subrecipient. If Subrecipient did not use all the funds received, GEMA/HS will recover the unused funds.

B. At the completion and closure of all Subrecipient's projects (subawards), GEMA/HS will request the Subrecipient to Certify the completion of all projects (subawards) in accordance with the grant terms and conditions to state there are no further claims under this subgrant.

C. The closeout of this Grant does not affect:

1. DHS/FEMA or GEMA/HS' right to disallow costs and recover funds on the basis of a later audit or other review;

2. Subrecipient's obligation to return any funds due as a result of later refunds, corrections, or other transactions;

3. Records retention requirements, property management requirements, and audit requirements, as set forth herein; and

4. Any other provisions of this Agreement that impose continuing obligations on Subrecipient or that govern the rights and limitations of the parties to this Agreement after the expiration or termination of this Agreement.

XI. INDEMNIFICATION.

A. The Subrecipient shall be fully liable for the actions of its agents, employees, partners, subrecipients, or contractors and shall fully indemnify, defend, and hold harmless the State and GEMA/HS, and their officers, agents, and employees, from suits, actions, damages, and costs of every name and description, arising from or relating to personal injury and damage to real or personal tangible property alleged to be caused in whole or in part by the Subrecipient, its agents, employees, partners, subrecipients, or contractors provided, however, that the Subrecipient shall not indemnify for that portion of any loss or damages proximately caused by the negligent act or omission of the State or GEMA/HS.

B. The Subrecipient shall fully indemnify, defend, and hold harmless the State and GEMA/HS from any suits, actions, damages, and costs of every name and description, including attorneys' fees, arising from or relating to violation or infringement of a trademark, copyright, patent, trade secret, or intellectual property right provided, however, that the foregoing obligation shall not apply to GEMA/HS' misuse or modification of the Subrecipient's products or GEMA/HS' operation or use of the Subrecipient's products in a manner not contemplated by the Agreement. GEMA/HS will not be liable for any royalties.

XII. DISPUTE RESOLUTION.

A. Disputes concerning performance under the Agreement will be decided by GEMA/HS, who shall reduce the decision to writing and serve a copy to the Subrecipient. In the event a Party is dissatisfied with the dispute resolution decision, jurisdiction for any dispute arising under the terms of the Agreement will be in Superior Court of Fulton County, Georgia. Subrecipient hereby waive any defenses or objections thereto, including defenses based on the doctrine of forum non conveniens.

B. Except as otherwise provided by law, the Parties agree to be responsible for their own attorney fees incurred in connection with disputes arising under the terms of this Agreement.

XIII. COMPLIANCE WITH LAW

A. **Compliance With Applicable Laws And Regulations**. It is understood and agreed that nothing contained in this Agreement, or any related agreement shall require any of the Parties herein to violate any policies of GEMA/HS, DHS, or any laws or regulations of the United States or the State of Georgia.

B. **State Laws**. The validity, construction, and effect of this Agreement shall be governed by the laws of the State of Georgia.

C. **Jurisdiction And Venue**. In the event that any dispute, litigation, or other legal proceedings shall arise under or in connection with this Agreement, such litigation or other legal proceeding shall be conducted in the courts located within Fulton County, Georgia. Furthermore, the Parties consent to jurisdiction and venue in the Superior Court of Fulton County, Georgia, and hereby waive any defenses or objections thereto, including defenses based on the doctrine of forum non conveniens.

D. **Effect of Changes in Federal and State Laws**. Any alterations, additions, or deletions to this Agreement that are required by changes in federal and state laws, regulations or policy are automatically incorporated into this Agreement without written amendment to this Agreement and shall become effective upon the date designated by such law or regulation. In the event DHS/FEMA or GEMA/HS determines that changes are necessary to this Agreement after an award has been made, including changes to the period of performance or terms and conditions, Subrecipient shall be notified of the changes in writing. Once notification has been made, any subsequent request for funds will indicate Subrecipient's acceptance of the changes to this Agreement.

E. **Conflict of Interest**. This Agreement is subject to the State of Georgia Code of Ethics found in O.C.G.A. § 45-10-1. The Subrecipient shall disclose the name of any officer, director, employee, or other agent who is also an employee of the State. The Subrecipient shall also disclose the name of any state employee who owns, directly or indirectly, more than a five percent (5%) interest in the Subrecipient or its affiliates.

1. Subrecipients should take every precaution to avoid the appearance of a conflict of interest. Violations of the conflict-of-interest standards may result in criminal, civil, or administrative penalties. In the use of agency project funds, officials, or employees of State or local units of government shall avoid any action that might result in, or create the appearance of:

a) Using his or her official position for private gain;

b) Giving preferential treatment to any person;

c) Losing complete independence or impartiality;

d) Making an official decision outside official channels; or

e) Affecting adversely the confidence of the public in the integrity of the government or the program. For example, where a Subrecipient of federal funds makes sub-awards under any competitive process and an actual conflict or an appearance of a conflict of interest exists, the person for whom the actual or apparent conflict of interest exists should recuse himself or herself not only from reviewing the application for which the conflict exists, but also from the evaluation of all competing applications.

F. **Boycott Of The Nation Of Israel Prohibited.** Each Party certifies that it is not currently engaged in a boycott of the nation of Israel, and that it will not engage in such a boycott for the duration of this Agreement.

G. **Drug-Free Workplace**. The Parties hereby certify as follows:

1. The Parties will not engage in the unlawful manufacture, sale, distribution, dispensation, possession, or use of a controlled substance or marijuana during the performance of this Agreement; and

2. If the Parties have more than one employee, that Party shall provide for such employee(s) a drug-free workplace, in accordance with the Georgia Drug-free Workplace Act as provided in O.C.G.A. § 50-24-1 et seq., throughout the duration of this Agreement; and

3. Parties will secure from any sub-contractor hired to work on any job assigned under this Agreement the following written certification: "As part of the subcontracting contract with (the Party's name). (Sub-Contractor's Name) certifies to (the Party's name) that a drug-free workplace will be provided for the sub-Contractor's employees during the performance of this MOU pursuant to paragraph 7 of subsection (b) of O.C.G.A. § 50-24-3."

4. A Party may be suspended, terminated, or debarred if it is determined that:

a) A Party has made false certification here in above; or

b) A Party has violated such certification by failure to carry out the requirements of O.C.G.A. § 50-24-3(b).

H. Sexual Harassment Prevention.

The State of Georgia promotes respect and dignity and does not tolerate sexual harassment in the workplace. The State is committed to providing a workplace and environment free from sexual harassment for its employees and for all persons who interact with state government. All State of Georgia employees are expected and required to interact with all persons including other employees, contractors, and customers in a professional manner that contributes to a respectful work environment free from sexual harassment. Furthermore, the State of Georgia maintains an expectation that its contractors and their employees and subcontractors will interact with entities of the State of Georgia, their customers, and other contractors of the State in a professional manner that contributes to a respectful work environment free from sexual harassment.

Pursuant to the State of Georgia's Statewide Sexual Harassment Prevention Policy (the "Policy"), all contractors who are regularly on State premises or who regularly interact with State personnel must complete sexual harassment prevention training on an annual basis.

If any of the Parties, including its employees and subcontractors, violates the Policy, including but not limited to engaging in sexual harassment and/or retaliation, that Party may be subject to appropriate corrective action. Such action may include, but is not limited to, notification to the employer, removal from State premises, restricted access to State premises and/or personnel, termination of contract, and/or other corrective action(s) deemed necessary by the State.

1. If the Party is an individual who is regularly on State premises or who will regularly interact with State personnel, that Party certifies that:

a) the Party has received, reviewed, and agreed to comply with the State of Georgia's Statewide Sexual Harassment Prevention Policy located at http://doas.ga.gov/human-resources-administration/board-rules-policy-and-compliance/jointly-issued-statewide-policies/sexual-harassment-prevention-policy;

b) the Party has completed sexual harassment prevention training in the last year and will continue to do so on an annual basis; or will complete the Georgia Department of Administrative Services' sexual harassment prevention training located at this direct link https://www.youtube.com/embed/NjVt0DDnc2s?rel=0 prior to accessing State premises and prior to interacting with State employees; and on an annual basis thereafter; and

c) Upon request by the State, the Party will provide documentation substantiating the completion of sexual harassment training.

2. If the Party has employees and subcontractors that are regularly on State premises or who will regularly interact with State personnel, that Party certifies that:

a) the Party will ensure that such employees and subcontractors have received, reviewed, and agreed to comply with the State of Georgia's Statewide Sexual Harassment Prevention Policy located at http://doas.ga.gov/human-resources-administration/board-rules-policy-and-compliance/jointly-issued-statewide-policies/sexual-harassment-prevention-policy;

b) the Party has provided sexual harassment prevention training in the last year to such employees and subcontractors and will continue to do so on an annual basis; or Contractor will ensure that such employees and subcontractors complete the Georgia Department of Administrative Services' sexual harassment prevention training located at this direct link https://www.youtube.com/embed/NjVt0DDnc2s?rel=0 prior to accessing State premises and prior to interacting with State employees; and on an annual basis thereafter; and

c) Upon request of the State, the Party will provide documentation substantiating such employees and subcontractors' acknowledgment of the State of Georgia's Statewide Sexual Harassment Prevention Policy and annual completion of sexual harassment prevention training.

I. **Debarred, Suspended, and Ineligible Status**. The Parties certify that each Party and/or any of its subcontractors have not been debarred, suspended, or declared ineligible by any agency of the State of Georgia or as defined in the Federal Acquisition Regulation (FAR) 48 C.F.R. Ch. 1 Subpart 9.4. Each Party will immediately notify the other Party if the Subrecipient and/or any subcontractors are debarred by the State or placed on the Consolidated List of Debarred, Suspended, and Ineligible Contractors by a federal entity.

XIV. NOTICE

A. All notices provided by Subrecipient under or pursuant to this Agreement shall be in writing GEMA/HS' Grant Manager and delivered by standard or electronic mail using the correct information provided below.

If to Georgia Emergency Management and Homeland Security Agency:

Sheneka Turner
Preparedness Grants & Programs Manager
935 United Avenue Southeast
Atlanta, Georgia 30316
Sheneka.Turner@gema.ga.gov
Office: 404-635-7068
Cell: 470-332-6784

B. In the event that different representatives or addresses are designated by either Party after execution of this Agreement, notice of the name, title and address of the new representative will be provided to the other Party.

XV. PROCUREMENT AND CONTRACTING.

A. The Subrecipient shall ensure that any procurement involving funds authorized by the Agreement complies with all applicable federal and state laws and regulations, to include 2 C.F.R. §§200.318 through 200.327 as well as Appendix II to 2 C.F.R. Part 200 (entitled "Contract Provisions for Non-Federal Entity Contracts Under Federal Awards").

B. As required by 2 C.F.R. §200.318(i), the Subrecipient shall "maintain records sufficient to detail the history of procurement. These records will include but are not necessarily limited to the following: rationale for the method of procurement, selection of contract type, contractor selection or rejection, and the basis for the contract price."

C. As required by 2 C.F.R. §200.318(b), the Subrecipient shall "maintain oversight to ensure that contractors perform in accordance with the terms, conditions, and specifications of their contracts or purchase orders." In order to demonstrate compliance with this requirement, the Subrecipient shall document, in its quarterly report to GEMA/HS, the progress of any and all subcontractors performing work under this Agreement.

D. Except for procurements by micro-purchases pursuant to 2 C.F.R. §200.320(a)(1) or procurements by small purchase procedures pursuant to 2 C.F.R. §200.320(a)(2), if the Subrecipient chooses to subcontract any of the work required under this Agreement, then the Subrecipient shall forward to GEMA/HS a copy of any solicitation (whether competitive or non-competitive) at least fifteen (15) days prior to the publication or communication of the solicitation. GEMA/HS shall review the solicitation and provide comments, if any, to the Subrecipient within seven (7) business days. Consistent with 2 C.F.R. §200.325, GEMA/HS will review the solicitation for compliance with the procurement standards outlined in 2 C.F.R. §§200.318 through 200.327 as well as Appendix II to 2 C.F.R. Part 200. Consistent

with 2 C.F.R. §200.318(k), GEMA/HS will not substitute its judgment for that of the Subrecipient. While the Subrecipient does not need the approval of GEMA/HS in order to publish a competitive solicitation, this review may allow GEMA/HS to identify deficiencies in the vendor requirements or in the commodity or service specifications. GEMA/HS' review and comments shall not constitute an approval of the solicitation. Regardless of GEMA/HS' review, the Subrecipient remains bound by all applicable laws, regulations, and agreement terms. If during its review GEMA/HS identifies any deficiencies, then GEMA/HS shall communicate those deficiencies to the Subrecipient as quickly as possible within the seven (7) business day window outlined above. If the Subrecipient publishes a competitive solicitation after receiving comments from GEMA/HS that the solicitation is deficient, then GEMA/HS may:

1. Terminate this Agreement in accordance with the provisions outlined in Section IX, *Termination* above; and,

2. Refuse to reimburse the Subrecipient for any costs associated with that solicitation.

E. Except for procurements by micro-purchases pursuant to 2 C.F.R. §200.320(a)(1) or procurements by small purchase procedures pursuant to 2 C.F.R. §200.320(a)(2), if the Subrecipient chooses to subcontract any of the work required under this Agreement, then the Subrecipient shall forward to GEMA/HS a copy of any contemplated contract prior to contract execution. GEMA/HS shall review the unexecuted contract and provide comments, if any, to the Subrecipient within seven (7) business days. Consistent with 2 C.F.R. §200.325, GEMA/HS will review the unexecuted contract for compliance with the procurement standards outlined in 2 C.F.R. §§200.318 through 200.327 as well as Appendix II to 2 C.F.R. Part 200. Consistent with 2 C.F.R. §200.318(k), GEMA/HS will not substitute its judgment for that of the Subrecipient. While the Subrecipient does not need the approval of GEMA/HS in order to execute a subcontract, this review may allow GEMA/HS to identify deficiencies in the terms and conditions of the subcontract as well as deficiencies in the procurement process that led to the subcontract. GEMA/HS's review and comments shall not constitute an approval of the subcontract. Regardless of GEMA/HS' review, the Subrecipient remains bound by all applicable laws, regulations, and agreement terms. If during its review GEMA/HS identifies any deficiencies, then GEMA/HS shall communicate those deficiencies to the Subrecipient as quickly as possible within the seven (7) business day window outlined above. If the Subrecipient executes a subcontract after receiving a communication from GEMA/HS that the subcontract is non-compliant, then GEMA/HS may:

1. Terminate this Agreement in accordance with the provisions outlined in Section IX, *Termination* above; and,

2. Refuse to reimburse the Subrecipient for any costs associated with that subcontract.

F. The Subrecipient agrees to include in the subcontract that (i) the subcontractor is bound by the terms of this Agreement, (ii) the subcontractor is bound by all applicable state and federal laws and regulations, and (iii) the subcontractor shall hold GEMA/HS and Subrecipient harmless against all claims of whatever nature arising out of the subcontractor's performance of work under this Agreement, to the extent allowed and required by law.

G. As required by 2 C.F.R. §200.318(c)(1), the Subrecipient shall "maintain written standards of conduct covering conflicts of interest and governing the actions of its employees engaged in the selection, award and administration of contracts."

H. As required by 2 C.F.R. §200.319, the Subrecipient shall conduct any procurement under this agreement "in a manner providing full and open competition." Accordingly, the Subrecipient shall not:

1. Place unreasonable requirements on firms in order for them to qualify to do business;

2. Require unnecessary experience or excessive bonding;

3. Use noncompetitive pricing practices between firms or between affiliated companies;

4. Execute noncompetitive contracts to consultants that are on retainer contracts;

5. Authorize, condone, or ignore organizational conflicts of interest;

6. Specify only a brand name product without allowing vendors to offer an equivalent;

7. Specify a brand name product instead of describing the performance, specifications, or other relevant requirements that pertain to the commodity or service solicited by the procurement;

8. Engage in any arbitrary action during the procurement process; or,

9. Allow a vendor to bid on a contract if that bidder was involved with developing or

10. drafting the specifications, requirements, statement of work, invitation to bid, or request for proposals.

I. Except in those cases where applicable Federal statutes expressly mandate or encourage otherwise, the Subrecipient, as required by 2 C.F.R. §200.319(c), shall not use a geographic preference when procuring commodities or services under this Agreement.

J. The Subrecipient shall conduct any procurement involving invitations to bid (i.e. sealed bids) in accordance with 2 C.F.R. §200.320(b)(1) as well as O.C.G.A. §50-5-50 et seq.

K. The Subrecipient shall conduct any procurement involving requests for proposals (i.e. proposals) in accordance with 2 C.F.R. §200.320(b)(2) as well as O.C.G.A. §50-5-50 et seq.

L. FEMA has developed helpful resources for Subrecipients when procuring with federal grant funds because Subrecipients must comply with the Federal procurement standards outlined in 2 C.F.R. §§200.318 through 200.327 as well as Appendix II to 2 C.F.R. Part 200. These resources are generally *available at* https://www.fema.gov/procurement-disaster-assistance-team. FEMA periodically updates this resource page so please check back for the latest information. While not all the provisions discussed in the resources are applicable to this subgrant agreement, the Subrecipient may find these resources helpful when drafting its solicitation and contract for compliance with the Federal procurement standards outlined in 2 C.F.R. §§200.318 through 200.327 as well as Appendix II to 2 C.F.R. Part 200. FEMA provides the following hands-on resources for Recipients of federal funding:

1. 2023 Procurement Disaster Assistance Team (PDAT) Roadmap to Procurement Compliance available at https://www.fema.gov/sites/default/files/documents/fema_roadmap_procurement_compliance_checklist.pdf.

M. Contract Provisions. All contracts executed using funds awarded under this Agreement shall contain the contract provisions listed under 2 C.F.R. 200.326 and Appendix II (A), Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments.

N. Procurement activities must follow the most restrictive of Federal, State and Local procurement regulations:

1. Procurement by micro purchase
2. Procurement by small purchase
3. Procurement by sealed bid
4. Procurement by competitive proposal

5. Procurement by non-competitive proposal, solely when the award of a contract is unfeasible under the other methods

O. **Sole Source Procurement.** The Subrecipient's procurement procedures and regulations must conform to federal procurement laws and standards. All procurement transactions without regard to dollar value, whether negotiated or through a competitive bid process shall be conducted in sucha manner as to provide maximum open and free competition.

P. Should the Subrecipient elect to award a non-competitive proposal, justification must be providedand include a description of the program and why it is necessary to enter into a non-competitive agreement. All sole-source procurements as defined in 2 C.F.R. § 200.320(f) must receive prior written approval from GEMA/HS.

Q. Comply with rules related to underutilized businesses (small and minority businesses, women's enterprises and labor surplus firms) at 2 C.F.R. §200.321.

XVI. SUBCONTRACTING.

A. In the event that the Subrecipient uses subcontractors or contractors, the Subrecipient shall use small, minority, women-owned or disadvantaged business concerns and contractors or subcontractors to the extent practicable as prescribed by applicable Federal and State laws.

B. The Subrecipient understands that any public contracts and subcontracts funded by the SLCGP must comply with the requirements of O.C.G.A. § 13-10-90, et seq., and Georgia Department of Labor Rules 300-10-1, et seq., to verify the contractor's or subcontractor's new employees' work eligibility through a federal work authorization program. The Subrecipient shall utilize the U.S. DHS E-Verify System to verify the employment eligibility of all persons hired during the Agreement term.

XVII. MONITORING

A. Subrecipient will be monitored periodically by federal, state or local entities, both programmatically and financially, to ensure that project goals, objectives, performance requirements, timelines, milestone completion, budget, and other program-related criteria are met.

B. GEMA/HS or its authorized representative, reserves the right to perform periodic desk/office-based and/or on-site monitoring of Subrecipient's compliance with this Agreement and of the adequacy and timeliness of Subrecipient's performance pursuant to this Agreement. After each monitoring visit, if the monitoring visit reveals deficiencies in Subrecipient's performance under this Agreement, a monitoring report will be provided to the Subrecipient and shall include requirements for the timely correction of such deficiencies by Subrecipient. Failure

by Subrecipient to take action specified in the monitoring report may be cause for termination of this Agreement pursuant to the Termination Section herein.

C. Subrecipient is responsible for and shall monitor its performance under this Agreement. Subrecipient shall monitor the performance of its contractors, consultants, agents, and who are paid from funds provided under this Agreement or acting in furtherance of this Agreement.

D. In addition to reviews of audits conducted in accordance with federal auditing requirements, monitoring procedures may include, but not limited to, desk reviews and on-site visits by GEMA/HS staff, limited scope audits, and other procedures.

XVIII. REPORTS

A. Consistent with 2 C.F.R. §200.328, the Subrecipient shall provide GEMA/HS with quarterly reports and a close-out report. These reports shall include the current status and progress by the Subrecipient and all subcontractors in completing the work described in the Scope of Work and the expenditure of funds under this Agreement, in addition to any other information requested by GEMA/HS.

B. **Equipment Inventory Report.** The Subrecipient will maintain an inventory of all grant-funded equipment and provide a copy to GEMA/HS at the end of the grant performance period. The Subrecipient will submit an updated inventory every year thereafter or as the equipment is disposed of. Equipment must be used for the intended purpose for the life of the equipment. There must be a decal on all equipment funded by GEMA/HS which states ""Purchased with funding from the Georgia Emergency Management and Homeland Security Agency with funds provided by the U.S. Department of Homeland Security". The decal will be provided GEMA/HS must be given a written disposition plan for any equipment that has a value of $5,000 or more at least 30 days prior to disposal or at the end of its useful life, whichever date is sooner. Also, the GEMA/HS Program Manager will review the disposition plan within 30 days of receipt and provide approval or other instructions for disposal to the Subrecipient.

1. Inventory records must be maintained which include:

i. Award number; • Description of the property;
ii. Serial number or other identification number; • Source of the property (brand/manufacturer);
iii. Vendor of the property;
iv. Identification of title holder;
v. Acquisition date;
vi. Cost of the property;
vii. Percentage of Federal participation in the cost of the property;
viii. Location of the property;

ix. Use and condition of the property; and
x. Disposition data, including the date of disposal and sale price.

C. **Quarterly Progress Report (Progress Report).** The disposition of grant funds, including all obligations and expenditures, must be reported to GEMA/HS quarterly through the Progress Report module in the EM Grants Manager System, which is due within 30 days of the end of each calendar quarter.

The following reporting periods and due dates apply:

Quarter	Date Range	Due Date
First Quarter	October 1 – December 31	January 31
Second Quarter	January 1- March 31	April 30
Third Quarter	April 1 – June 30	July 31
Fourth Quarter	July 1 – September 30	October 31

FAILURE TO HAVE A CURRENT PROGRESS REPORT ON FILE AT GEMA/HS WILL RESULT IN WITHHOLDING OF REIMBURSEMENT UNTIL THE PROGRESS REPORTIS RECEIVED.

D. **Biannual Strategy Implementation Reports ("BSIR")**. The Subrecipient shall complete and submit any other reports as requested by GEMA/HS and cooperate and assist GEMA/HS in complying with the DHS tracking and reporting requirements. Specifically, without limitation, Subrecipient shall submit information at the request of GEMA/HS to assist in the submission of the BSIR, and any other reports, as required.

E. **Grant Closeout Report.** The Subrecipient shall submit a final program report detailing all accomplishments throughout the project with the final Progress Report. After both of these reports have been reviewed and approved by GEMA/HS, a Closeout Report will be generated indicating the project has closed and listing any remaining funds to be de-obligated.

F. If all required reports and copies are not sent to GEMA/HS or are not completed in a manner acceptable to GEMA/HS, then GEMA/HS may withhold further payments until they are completed or may take other action.

G. The Subrecipient shall provide additional program updates or information that may be required by GEMA/HS.

XIX. AUDITS

A. **Audit of Federal Funds**.

1. The Subrecipient agrees to comply with the organizational audit requirements of 2 CFR Part 200, Subpart F, Audits of States, Local Governments, and Non- Profit Organizations.

2. Subrecipient's performance under the Agreement is subject to the applicable requirements published in the *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*, Title 2 of the United States Code of Federal Regulations (C.F.R.) Part 200 hereinafter referred to as the "Uniform Guidance."

3. Subrecipients that expend $750,000.00 or more of federal funds during their fiscal year are required to submit an organization-wide financial and compliance audit report. The audit must be performedin accordance with the Government Accountability Office's ("GAO") Government Auditing Standards, which may be accessed online at http://www.gao.gov/govaud/ybk01.htm, and in accordance with 2 C.F.R. § 200.514 Scope of Audit. Audit reports are currently due to the Federal Audit Clearinghouse no later than nine months after the end of the recipient's fiscal year.

4. If required to submit an audit report under the requirements of 2 CFR Part 200, Subpart F, the Subrecipient shall provide GEMA/HS with written documentation showing that it has complied with the single audit requirements. Such documentation shall be returned to GEMA/HS with this signed Agreement. The Subrecipient shall immediately notify GEMA/HS in writing at any time that it is required to conduct a single audit and provide documentation within a reasonable time period showing compliance with the single audit requirement.

B. **Right to Audit**. Subrecipient shall give DHS, FEMA, CISA, the Comptroller General of the United States, the Georgia Department of Audits and Accounts, GEMA/HS, or any of their duly authorized representatives, access to and the right to conduct a financial or compliance audit of Grant funds received, and performances rendered under this Agreement. Subrecipient shall permit GEMA/HS or its authorized representative to audit Subrecipient's records. Subrecipient shall provide any documents, materials or information necessary to facilitate such audit.

C. **Subrecipient's Liability for Disallowed Costs**. Subrecipient understands and agrees that it shall be liable to GEMA/HS for any costs disallowed pursuant to any financial or compliance audit(s) of these funds. Subrecipient further understands and agrees that reimbursement to GEMA/HS of such disallowed costs shall be paid

by Subrecipient from funds that were not provided or otherwise made available to Subrecipient pursuant to this Grant or any other federal contract.

D. **Subrecipient's Facilitation of Audit**. Subrecipient shall take such action to facilitate the performance of such audit(s) conducted pursuant to this Section as GEMA/HS may require of Subrecipient. Subrecipient shall ensure that this clause concerning the authority to audit funds received indirectly by subcontractors through Subrecipient and the requirement to cooperate is included in any subcontract it awards.

E. **State Auditor's Clause**. Subrecipient understands that acceptance of funds under this Grant acts as acceptance of the authority of the State Auditor's Office to conduct an audit or investigation in connection with those funds. Subrecipient further agrees to cooperate fully with the State Auditor's Office in the conduct of the audit or investigation, including providing all records requested. Subrecipient shall ensure that this clause concerning the State Auditor's Office's authority to audit funds and the requirement to cooperate fully with the State Auditor's Office is included in any subgrants or subcontracts it awards. Additionally, the State Auditor's Office shall at any time have access to and the rights to examine, audit, excerpt, and transcribe any pertinent books, documents, working papers, and records of Subrecipient relating to this Grant.

F. Subrecipient shall retain all records pertaining to this Agreement, regardless of the form of the record (e.g. paper, film, recording, electronic), including but not limited to financial records, supporting documents, statistical records, and any other documents (hereinafter referred to as "Records") for a period of five (5) State fiscal years after all reporting requirements are satisfied and final payments have been received, or if an audit has been initiated and audit findings through ligation or otherwise.

G. Subrecipient's must submit audit reports to the State of Georgia, by sending a copy to the Georgia Department of Audits and Accounts, Nonprofit and Local Governments Audits, 270 Washington Street, SW, Room I-156, Atlanta, Georgia 30334-8400.

XX. RECORDS

A. **Retention and Maintenance of Records**. The Subrecipient shall maintain books, records, and documents (including electronic storage media) in accordance with generally accepted accounting procedures and practices that sufficiently and properly reflect all revenues and expenditures of grant funds. All such records must be retained by the Subrecipient for a minimum of three (3) years from the date that the DHS closes the State of Georgia's 2022 SLCGP grant. GEMA/HS will notify the Subrecipient in writing when the retention period begins.

1. The following are the only exceptions to the 3-year requirement:

i. If any litigation, claim, or audit is started before the expiration of the 3-year period, then the records must be retained until all litigation, claims, or audit findings involving the records have been resolved and final action taken.

ii. When GEMA/HS or the Subrecipient is notified in writing by the Federal awarding agency, cognizant agency for audit, oversight agency for audit, cognizant agency for indirect costs, or pass-through entity to extend the retention period.

iii. Records for real property and equipment acquired with Federal funds must be retained for 5 years after final disposition.

iv. When records are transferred to or maintained by the Federal awarding agency or pass-through entity, the 3-year retention requirement is not applicable to the Subrecipient.

v. Records for program income transactions after the period of performance. In some cases, recipients must report program income after the period of performance. Where there is such a requirement, the retention period for the records pertaining to the earning of the program income starts from the end of the non-Federal entity's fiscal year in which the program income is earned.

vi. Indirect cost rate proposals and cost allocations plans. This paragraph applies to the following types of documents and their supporting records: indirect cost rate computations or proposals, cost allocation plans, and 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).

B. **Access to Records**. As required by 2 C.F.R. §200.337, the Federal awarding agency, Inspectors General, the Comptroller General of the United States, and GEMA/HS, or any of their authorized representatives, shall enjoy the right of access to any documents, papers, or other records of the Subrecipient which are pertinent to the Federal award, in order to make audits, examinations, excerpts, and transcripts. The right of access also includes timely and reasonable access to the Subrecipient's personnel for the purpose of interview and discussion related to such documents. Finally, the right of access is not limited to the required retention period but lasts as long as the records are retained.

C. **Public Records.** The laws of the State of Georgia, including the Georgia Open Records Act, as provided in O.C.G.A. Section 50-18-70 et seq., require

procurement records, including pricing information, and other records to be made public unless otherwise provided by law. The Parties agree that this Agreement, any related purchase orders, related invoices, and related pricing lists will be public documents, and may be available for distribution. The Parties give each other express permission to make copies of this Agreement, any related purchase orders, related invoices, and related pricing lists. The permission to make copies as noted will take precedence over any statements of confidentiality, proprietary information, copyright information, or similar notation.

D. **SLCGP Specific Requirements.**

1. The Subrecipient must use SLCGP funds only to perform tasks as described in the Subrecipient's approved application for funding incorporated into this Agreement.

2. Subrecipients are required to complete the Nationwide Cybersecurity Review, https://www.cisecurity.org/ms-isac/services/ncsr, a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs, to benchmark and measure progress of improvement in their cybersecurity posture. Completion should continue annually. For more information, visit the Nationwide Cybersecurity Review's website at https://www.cisecurity.org.

3. Subrecipients are required to participate in free cyber hygiene services, specifically vulnerability scanning and web application scanning. To register for these services, 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.

4. Subrecipients may retain a maximum of up to five (5) percent of the SLCGP grant agreement amount for management and administration activities, directly relating to the management and administration of SLCGP funds, such as financial management and monitoring.

E. **Program-Specific Required Forms and Information**. The following program-specific forms or information are required to be submitted in ND Grants as attachments:

1. SLCGP Investment Justifications. Each eligible entity is required to submit complete project-level information detailing how the program objectives and goals will be met to develop, implement, or revise its Cybersecurity Plan; establish a Cybersecurity Planning Committee; conduct assessments

and evaluations; and adopt key cybersecurity best practices. The FY 2022 Investment Justification must include the following information:

i. Only one application will be submitted by the eligible entity. It must include a brief description of the capabilities of the SLT agencies across the eligible entity related to the required elements of the Cybersecurity Plan.

ii. The application will consist of up to four investments, one for each SLCGP objective (See Exhibit 1 for more information on the goal and objectives).

iii. Investments for SLCGP Objectives 1, 2, and 3 must have at least one project. Investments for SLCGP Objective 4 are optional for the FY 2022 SLCGP; however, it is important to note that identifying and mitigating gaps in the cybersecurity workforce, enhancing recruitment and retention efforts, and bolstering the knowledge, skills, and abilities of personnel are still statutory requirements for Cybersecurity Plans to address even if the eligible entity does not use grant funds to carry this out.

iv. Requests to use funding to address imminent cybersecurity threats must be addressed in the Investment Justification ("IJ") for Objective 3.

v. Each investment must describe how each project aligns to the Subrecipient's Cybersecurity Plan if applying for a grant to implement or revise the Cybersecurity Plan, or will align with the entity's Cybersecurity Plan if applying for a grant to develop a Cybersecurity Plan. Subrecipients must also describe how implementing the plan will be measured (metrics).

vi. Each project must include an explanation of how the proposed project(s) will achieve the program objectives as identified in Exhibit 1. A project schedule with clearly defined milestones must also be included.

2. Cybersecurity Plan. Each eligible entity is required to submit its Cybersecurity Plan that adheres to the 16 required elements identified in section 2220A of the Homeland Security Act of 2002 as amended by the BIL and included in Appendix C of the FY 2022 SLCGP DHS/FEMA NOFO unless the eligible entity is applying for funds to develop a Cybersecurity Plan as described more below. The Cybersecurity Plan must include a description of Subrecipient's roles, an assessment of capabilities for each element, address resources and timeline for implementing the Plan,

and identify metrics. Subrecipient governments are encouraged to take a holistic approach in the development of their Plan as entities must be able to sustain capabilities once SLCGP funds are no longer available. The role of state entities as coordinator and service provider to local entities should be encouraged and supported. For more information on the Cybersecurity Plan, please refer to Appendix C of the FY 2022 SLCGP DHS/FEMA NOFO.

3. Cybersecurity Planning Committee Membership List. The Cybersecurity Planning Committee should be seen as a platform to identify and then prioritize state-wide efforts, to include identifying opportunities to consolidate projects to increase efficiencies. Each eligible entity is required to submit confirmation that the committee is comprised of the required representatives. The Subrecipient must also confirm that at least one-half of the representatives of the committee have professional experience relating to cybersecurity or information technology. For more information on the composition of the Cybersecurity Planning Committee, including how to leverage existing planning committees, please refer to Appendix B of the FY 2022 SLCGP DHS/FEMA NOFO.

4. Cybersecurity Planning Committee Charter. The Cybersecurity Planning Committee Charter must be submitted with the Cybersecurity Planning Committee Membership List attached as specified in Appendix B of the FY 2022 SLCGP DHS/FEMA NOFO.

5. Cybersecurity Plan Submission Exception Request (if applicable).

i. Subrecipients may request an exception to submitting their Cybersecurity Plan at the time of application. The exception request must be supported by the Chief Information Officer ("CIO"), Chief Information Security Office ("CISO"), or equivalent official.

ii. If an exception is requested, SLCGP funds can only initially be used for activities that are integral to the development of the Cybersecurity Plan or are necessary to assist with activities that address imminent cybersecurity threats. Activities integral to the development of a Cybersecurity Plan are limited to investments and projects aligned to Objective 1 and Objective 2 as listed in Exhibit 1. Activities to address imminent cybersecurity threats are limited to investments and projects aligned to Objective 3 as listed in Exhibit 1.

iii. The Subrecipient must also include a certification, either as a separate document or as part of the applicable IJ(s), that all activities funded by the grant are integral to the development of the Cybersecurity Plan or are necessary to assist with activities that address imminent

cybersecurity threats, as confirmed by the Secretary, acting through the CISA Director, to the information systems owned or operated by, or on behalf of, the eligible entity or a local government within the jurisdiction of the eligible entity. If grant funding is necessary to assist with activities that address imminent cybersecurity threats, then that should be noted on the applicable IJ.

iv. Subrecipient seeking funding to develop a Cybersecurity Plan must still submit IJs for Objectives 1, 2, and 3, noting that they will need to be updated once the Cybersecurity Plan is completed and approved. It is still optional to submit an IJ for Objective 4 as listed in Exhibit 1.

v. Once the Cybersecurity Plan is completed and approved by the Cybersecurity Planning Committee and CIO, CISO, or equivalent official, the applicant must then submit updated IJs for Objectives 1, 2, and 3, along with an updated IJ for Objective 4 if one was previously submitted, to DHS with the approved Cybersecurity Plan.

vi. The following is required to request an exception:

a) Statement from the Subrecipient as to why they do not have an approved Cybersecurity Plan;

b) High-level plan, including dates and milestones, for completing and submitting the Plan to DHS; and

c) Signatures of support from the eligible entity and CIO, CISO, or equivalent official.

F. <u>Other Federal Records Requirements</u>.

1. In accordance with 2 C.F.R. §200.335, the Federal awarding agency must request transfer of certain records to its custody from GEMA/HS or the Subrecipient when it determines that the records possess long-term retention value.

2. In accordance with 2 C.F.R. §200.336, GEMA/HS must always provide or accept paper versions of Agreement information to and from the Subrecipient upon request. If paper copies are submitted, then GEMA/HS must not require more than an original and two copies. When original records are electronic and cannot be altered, there is no need to create and retain paper copies. When original records are paper, electronic versions may be substituted through the use of duplication or other forms of electronic media provided that they are subject to periodic quality control

reviews, provide reasonable safeguards against alteration, and remain readable.

3. As required by 2 C.F.R. §200.303, the Subrecipient shall take reasonable measures to safeguard protected personally identifiable information and other information the Federal awarding agency or GEMA/HS designates as sensitive or the Subrecipient considers sensitive consistent with applicable Federal, state, local, and tribal laws regarding privacy and obligations of confidentiality.

G. **Fusion Centers**. The Subrecipient agrees that any funds utilized to establish or enhance state and local fusion centers must support the development of a statewide fusion process that corresponds with the Global Justice/Homeland Security Advisory Council Fusion Center Guidelines and achievement of a baseline level of capability as defined by the Fusion Capability Planning Tool.

1. The Subrecipient agrees that Homeland Security Information Network must serve as the primary vehicle by which information /intelligence is shared with DHS/FEMA as part of the fusion process across the federal, state, local, regional, tribal and private sectors. All statewide information sharing and analysis centers utilizing SLCGP funds must establish connectivity with the DHS/FEMA Homeland Security Operations Center via the HSIN to comply with FEMA policy legislation as outlined in the Program Guidance.

H. The Subrecipient shall maintain all records for the Subrecipient and for all subcontractors or consultants to be paid from funds provided under this Agreement, including documentation of all program costs, in a form sufficient to determine compliance with the requirements and objectives of the approved Budget Cost Lines and all other applicable laws and regulations.

XXI. Special Conditions.

A. The Subrecipient agrees to comply with the FY 2022 State and Local Cybersecurity Grant Program Agreement Articles and FY 2022 State and Local Cybersecurity Grant Program Amendment Letter, included with this Agreement as Attachment B and C, respectively. References in the attachment to "recipient" apply to the Subrecipient's requirements as subrecipient.

B. The Subrecipient agrees to cooperate with any assessments, national evaluation efforts, requests for information or data collection, including, but not limited to,

the provision of any information regarding any activities within this agreement that may be required for the assessment or evaluation.

C. **Protected Critical Infrastructure Information.** Protected Critical Infrastructure Information ("PCII") will be treated in a manner consistent with the Critical Infrastructure Information Act of 2002 ("CIIA"), 6 U.S.C. §§131 - 134, which created a new framework, that enables state and local jurisdictions and members of the private sector to voluntarily submit sensitive information regarding critical infrastructure to DHS/FEMA. The CIIA also provides statutory protection for voluntarily shared CII from public disclosure and civil litigation. If validated as PCII, these documents can only be shared with authorized users who agree to safeguard the information. PCII accreditation is a formal recognition that the covered government entity has the capacity and capability to receive and store PCII. DHS requires all State Administering Agencies ("SAA") to complete the PCII accreditation process. Accreditation activities include signing a memorandum of agreement with DHS, appointing a PCII Officer, and implementing a self-inspection program.

D. **Selected Items of Cost**: The Subrecipient agrees to comply with the requirements of OMB 2 C.F.R. Part 225, Selected Items of Cost. Physical inventories must be taken at least once every two (2) years to ensure that assets received through this Agreement exist and are in use. Governmental units will manage and maintain equipment in accordance with State laws and procedures.

E. **Environmental Historical Preservation ("EHP")**.

1. The Subrecipient shall comply with all applicable federal, state, and local environmental and historic preservation ("EHP") requirements and shall provide any information requested by FEMA or GEMA/HS to ensure compliance with applicable laws and regulations, including: Federal EHP regulations, laws, and Executive Orders; National Environmental Policy Act; National Historic Preservation Act; Endangered Species Act; and Executive Orders on Floodplains (11988), Wetlands (11990), and Environmental Justice (12898). Failure of the Subrecipient to meet federal, state, and local EHP requirements and obtain applicable permits may jeopardize federal funding. The Subrecipient shall not undertake any project having the potential to impact EHP resources without prior approval from FEMA, through GEMA/HS, including but not limited to communications towers, physical security enhancements, new construction, modifications to buildings, and replacement of facilities. The Subrecipient shall coordinate with GEMA/HS regarding any activities using grant funding that requires specific documentation of compliance with federal laws and/or regulations.

2. The Subrecipient shall provide any information requested by GEMA/HS or FEMA to ensure compliance with applicable federal EHP requirements.

Any change to the approved project or scope of work will require re-evaluation for EHP compliance. If ground-disturbing activities may occur during project implementation, the Subrecipient must ensure monitoring of ground disturbance, and, if any potential archeological resources are discovered, the recipient will immediately cease construction in that area and notify GEMA/HS, and the Georgia Department of Natural Resources, Georgia State Historic Preservation Division.

3. The Subrecipient shall not undertake any project using SLCGP funding to which the National Environmental Policy Act (NEPA) requirements are applicable without first obtaining written approval from FEMA, through GEMA/HS. The Subrecipient shall coordinate with GEMA/HS regarding any activities using grant funding that requires specific documentation of NEPA compliance.

4. Any construction activities initiated prior to the full environmental and historic preservation review and evaluation will result in a non-compliance finding and will not be eligible for SLCGP funding.

5. For more information regarding FEMA's EHP requirements, the Subrecipient should refer to the FY 2022 SLCGP DHS/FEMA NOFO (Attachment H) and FEMA's Information Bulletins 329, 345, 356, 371, 404, and 404 available at https://www.fema.gov/grants/tools/environmental-historic/preparation-resources.

F. <u>Federal Funding Accountability and Transparency Act ("FFATA").</u>

1. All new subawards under this grant of $30,000 or more are subject to FFATA reporting requirements. The Subrecipient is responsible for providing any information requested by GEMA/HS to complete the required report.

2. Unless exempt, the Subrecipient shall report the names and total compensation of its five most highly compensated executives for its preceding completed fiscal year. This report is only required if:

i. In the Subrecipient's preceding fiscal year, the Subrecipient received 80 percent or more of itsannual gross revenues from federal procurement contracts and subcontracts and federal financial assistance subject to the Transparency Act, as defined at 2 CFR 170.320 (and subawards); and

ii. The public does not have access to information about the compensation of the executives through periodic reports filed under section 13(a) or

15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m(a), 78o(d)) or section 61104 of the Internal Revenue Code of 1986.

iii. Additional information regarding the FFATA requirements can be found at the following links:

a) http://www.fema.gov/pdf/government/grant/bulletins/info350.pdf

b) www.fsrs.gov.

G. National Incident Management System (NIMS)

1. National Initiatives: Prior to allocation of any Federal preparedness awards in FY 2022, Subrecipients must ensure and maintain adoption and implementation of the NIMS. Although not required by DHS/FEMA, GEMA/HS requires SLCGP Subrecipients to maintain the adoption and implementation of NIMS. DHS/FEMA describes the specific training and activities involved in NIMS implementation in the NIMS Training Program https://www.fema.gov/training-0 and the NIMS Implementation Objectives https://www.fema.gov/implementation-guidance-and-reporting.

2. Incident management activities require carefully managed resources (personnel, teams, facilities, equipment, and/or supplies). Utilization of the standardized resource management concepts such as typing, credentialing, and inventorying promote a strong national mutual aid capability needed to support the delivery of core capabilities. Recipients should manage resources purchased or supported with DHS/FEMA grant funding according to NIMS resource management guidance. Additional information on resource management and NIMS resource typing definitions and job titles/position qualifications are available on DHS/FEMA's website at https://www.fema.gov/resource-management-mutual-aid.

H. Disposition of Equipment Acquired Under the Federal Award (Article XLVIII). For purposes of original or replacement equipment acquired under this award by a non-state recipient or non-state subrecipients, when that equipment is no longer needed for the original project or program or for other activities currently or previously supported by a federal awarding agency, you must request instructions from FEMA to make proper disposition of the equipment pursuant to 2 C.F.R. section 200.313. State recipients and state subrecipients must follow the disposition requirements in accordance with state laws and procedures.

I. The Subrecipient understands and agrees that for any copyrightable work based on or containing data first produced under this Agreement, the Subrecipient shall grant the government a royalty- free, nonexclusive, and irrevocable license to reproduce,

display, distribute, perform, disseminate, or prepare derivative works, and to authorize others to do so, for government purposes on all such copyrighted works. The Subrecipient shall affix the applicable copyright notices of 17 U.S.C. §401 or 402 and an acknowledgment of government sponsorship, including the grant award number, to any work first produced under this grant award.

J. If the Subrecipient is found to be in violation of any of the conditions of this agreement, including any attachments hereto, or of applicable federal and state laws or regulations, in addition to any other recourse available, GEMA/HS shall notify the Subrecipient that additional funds in connection with which the violation occurred will be withheld until such violation has been corrected to the satisfaction of GEMA/HS. In addition, GEMA/HS may withhold or require repayment of any portion of the financial award which has been or is to be made available to the Subrecipient, or retained and obligated or expended on behalf of the Subrecipient, for other projects under this program until adequate corrective action is taken.

XXII. MISCELLANEOUS TERMS

A. **Headings.** The headings in this Agreement are inserted for reference and convenience only and shall not enter into the interpretation hereof.

B. **Severability.** If any of the provisions of this Agreement shall be held by a court or other tribunal of competent jurisdiction to be illegal, invalid, or unenforceable, such provisions shall be limited or eliminated to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect.

C. **Survivability.** This Agreement shall remain in full force and effect to the end of the specified term or until terminated pursuant to this Agreement. All obligations of the Parties incurred or existing under this Agreement as of the date of expiration or termination will survive the termination or expiration of this Agreement.

D. **Assignment.** A Party may, nor will it have the power to, assign or novate this Agreement with the consent of the other Parties.

E. **Dispute Resolution.** In the event of any conflict involving activities conducted pursuant to this Agreement, the Parties will make reasonable efforts to informally resolve the issue. An attempt will first be made by the respective Parties organizations to resolve the issue at the staff level. If the matter cannot be resolved, the issue will be discussed by the respective decision-makers. Nothing in this section shall be construed to restrain the Parties from issuing correspondence, or other formal written communications to document or clarify an issue that is in conflict or dispute.

F. **Sanctions**. If a Subrecipient materially fails to comply with the terms and conditions of an award, GEMA/HS or DHS/FEMA may take one or more of the following actions, as appropriate in the circumstances:

1. Temporarily withhold cash payments pending correction of the deficiency by the Subrecipient.

2. Disallow (that is, deny both use of funds and any applicable matching credit for) all or part of the cost of the activity or action not in compliance.

3. Wholly or partly suspend or terminate the current award.

4. Withhold future awards for the project or program.

5. Pursue any other legal remedy that may be available.

6. Require reassignment of any tangible or intangible items purchased with SLCGP grant funding to another local jurisdiction.

G. **Reservation of Rights**. This Agreement will in no way diminish or otherwise affect the Parties' authority to fully carry out their rights and responsibilities under applicable laws and regulations nor will it affect the Parties' abilities or rights to raise any defenses available under law in the event that one Party initiates an administrative or judicial enforcement action against another Party. Subject to applicable security, classification, and other confidentiality laws and regulations, nothing in this Agreement shall be construed to prohibit the Parties from using information developed under this Agreement in furtherance of their statutory duties, rights, and obligations.

H. **Parties' Signature and Authority.** The Parties' representatives, in signing this Agreement, sign only as properly authorized representatives of their respective Parties and do not assume any personal liability thereby. The Parties' representatives executing this Agreement warrant that they have full and current legal authority to act and contract on behalf of their Parties.

1. Under this Agreement, GEMA/HS will execute the interests and responsibilities of the Recipient. The individual designated to represent the State of Georgia is James C. Stallings, Authorized Recipient Official. The State has designated Linda Criblez as the Program Manager of this program. The Subrecipient's Authorized Official has the authority to legally bind the Subrecipient and will execute the interests and responsibilities of the Subrecipient. The Subrecipient's Authorized Official is the person whose name and signature appear on page ten (10) of this agreement.

XXIII. Entire Agreement; Waiver; Signature and Delivery.

This Agreement, including the incorporated Attachments and Exhibits, supersedes all prior agreements, both verbal and written, and any discussions and writings and constitutes the entire agreement between the Parties with respect to the specific subject matter hereof. No waiver or modification of this Agreement will be binding upon any Party unless made in writing and signed by a duly authorized representative of such Party and no failure or delay in enforcing any right shall be deemed a waiver of such right. Execution and delivery of this Agreement electronically is hereby deemed valid and effective, and a signed facsimile or electronic copy is hereby deemed an original for all purposes.

(SIGNATURES ON FOLLOWING PAGE)

[THIS SPACE HAS BEEN INTENTIONALLY LEFT BLANK]

SIGNATURE PAGE

IN WITNESS WHEREOF, the Parties state and affirm that they are duly authorized to bind their respective entities designated below as of the day, month, and year indicated.

GEORGIA EMERGENCY MANAGEMENT AND HOMELAND SECURITY AGENCY

Signature

Printed Name of Signatory

Title of Signatory

10 / 01 / 2024

Date of Signature

Smyrna

(NAME OF SUBRECIPIENT)

Signature

Printed Name of Signatory

Title of Signatory

10 / 01 / 2024

Date of Signature

58-6000664

Agency FEID (XX-XXXXXXX)

YLAKSJHK7WB4

Agency UEI Number (XXXXXXXXX)

EXHIBIT B

NIMS Compliance Form

This NIMS Compliance Form is OPTIONAL for Non-Governmental Agencies

Non-Governmental Subrecipients are not required to meet National Incident Management System (NIMS) compliance requirements. For additional guidance on NIMS training, please refer to http://www.training.fema.gov/nims. All emergency preparedness, response, and/or security personnel in the state agencies, tribes, and local governments participating in the development, implementation, and/or operation of resources and/or activities awarded through this grant are compelled to complete training programs consistent with the NIMS National Standard Curriculum Development Guide. Minimum training includes ICS-100 and IS-700. The Subrecipient agrees to comply with the NIMS compliance requirements and to evidence compliance by completing and returning to the Georgia Emergency Management and Homeland Security Agency this NIMS Compliance Form, Exhibit "B" to this agreement.

Please check the box next to each action that the Subgrantee has completed.
Additional NIMS guidance can be found at http://www.fema.gov/national-incident-management-system.

RECOMMENDED:

- ☑ **IS-700 (NIMS) An Introduction**
- ☑ **ICS-100: Introduction to the Incident Command System**

RECOMMENDED:

- ☐ Community Adoption: Adopt NIMS at the community level for all government departments and/or agencies; as well as promote and encourage NIMS adoption by associations, utilities, non-governmental organizations (NGOs), and private sector incident management and response organizations.
- ☐ Incident Command System (ICS): Manage all emergency incidents and preplanned (recurring/special) events in accordance with ICS organizational structures, doctrine, and procedures, as defined in NIMS. ICS implementation must include the consistent application of Incident Action Planning and Common Communications Plans.
- ☐ Public Information System: Implement processes, procedures, and/or plans to communicate timely, accurate information to the public during an incident through a Joint Information System and Joint Information Center.
- ☐ Preparedness/Planning: Establish the community's NIMS baseline against the FY2008 and FY2009 implementation requirements.
- ☐ Develop and implement a system to coordinate all federal preparedness funding to implement the NIMS across the community.
- ☐ Revise and update plans and SOPs to incorporate NIMS components, principles and policies, to include planning, training, response, exercises, equipment, evaluation, and corrective actions.

RECOMMENDED continued:

- ☑ Implementation plans exists at agency level that identifies the appropriate personnel to complete the below listed NIMS training requirements.
  - ☑ **IS-800** National Response Framework, An Introduction
  - ☑ **ICS-200** ICS for Single Resources and Intial Action Incidents
  - ☐ **ICS-300** Intermediate ICS for Expanding Incidents
  - ☐ **ICS-400** Advanced ICS for Command and General Staff
  - ☐ **IS-701** NIMS Mutliagency Coordination Systems (MACS)
  - ☐ **IS-702** NIMS Public Information Systems
  - ☐ **IS-703** NIMS Resource Management
- ☐ Incorporate NIMS/ICS into all tribal, local, and regional training and exercises.
- ☐ Participate in an all-hazard exercise program based on NIMS that involves responders from
- ☐ Incorporate corrective actions into preparedness
- ☐ Inventory community response assets to conform
- ☐ To the extent permissible by law, ensure that relevant national standards and guidance to achieve equipment, communication, and data interoperability are incorporated into tribal and
- ☐ Apply standardized and consistent terminology, including the establishment of plain English communications standards

City of Smyrna, Georgia

Agency

Authorized Signature

Date