
# FISCAL YEAR 2023 STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP)

# APPLICATION GUIDANCE

APPLICATION GUIDANCE

For Local Government Jurisdictions and Departments

North Dakota Department of Emergency Services (NDDES)

Division of Homeland Security

[Left Blank Intentionally]

# Table of Contents

# Program Description

## 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 risk and 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 the Infrastructure Investment and Jobs Act (IIJA), also known as the Bipartisan Infrastructure Law (BIL), the SLCGP enables the United States Department of Homeland Security (DHS) to make targeted cybersecurity investments in SLT government agencies, thus improving the security of critical infrastructure and improving the resilience of the services SLT governments provide their communities.

The FY 2023 SLCGP aligns with the National Cybersecurity Strategy by addressing three of the five pillars:

- Pillar One – Defend Critical Infrastructure,
- Pillar Two – Disrupt and Dismantle Threat Actors, and
- Pillar Four – Invest in a Resilient Future.

The FY 2023 SLCGP also aligns with the Cybersecurity and Infrastructure Security Agency's (CISA) 2023-2025 Strategic Plan Goals of:

- Goal 1: Cyber Defense
- Goal 2: Risk Reduction and Resilience
- Goal 3: Operational Collaboration

### *Assistance Listings Title and Number*

State and Local Cybersecurity Security Grant Program (97.137)

### *Federal Notice of Funding Opportunity Title*

Fiscal Year 2023 State and Local Cybersecurity Grant Program (SLCGP)

### *Federal Funding Availability*

$3,733,118

### *Cost Share or Match*

Eligible entities must meet a 20% cost share requirement for the FY 2023 SLCGP. The State of North

Dakota will provide 4.55% of the required 20% cost share, leaving the eligible entity responsible for 15.45%.

### *Eligible Applicants*

North Dakota local and tribal government entities are eligible to apply. Local government for purposes of being an eligible entity is defined as a county, municipality, city, town, township, school district, special district (example: fire district), or agency or instrumentality of a local government, an Indian tribe or authorized tribal organization.

### *Ineligible Applicants*

Nonprofit organizations, private corporations, and private educational institutions are not eligible.

## Objectives, Priorities, and Project Information

### *Objectives*

The goal of the FY 2023 SLCGP is to assist SLT governments with managing and reducing systemic cyber risk by addressing the following objectives with the focus on objectives 3 and 4.

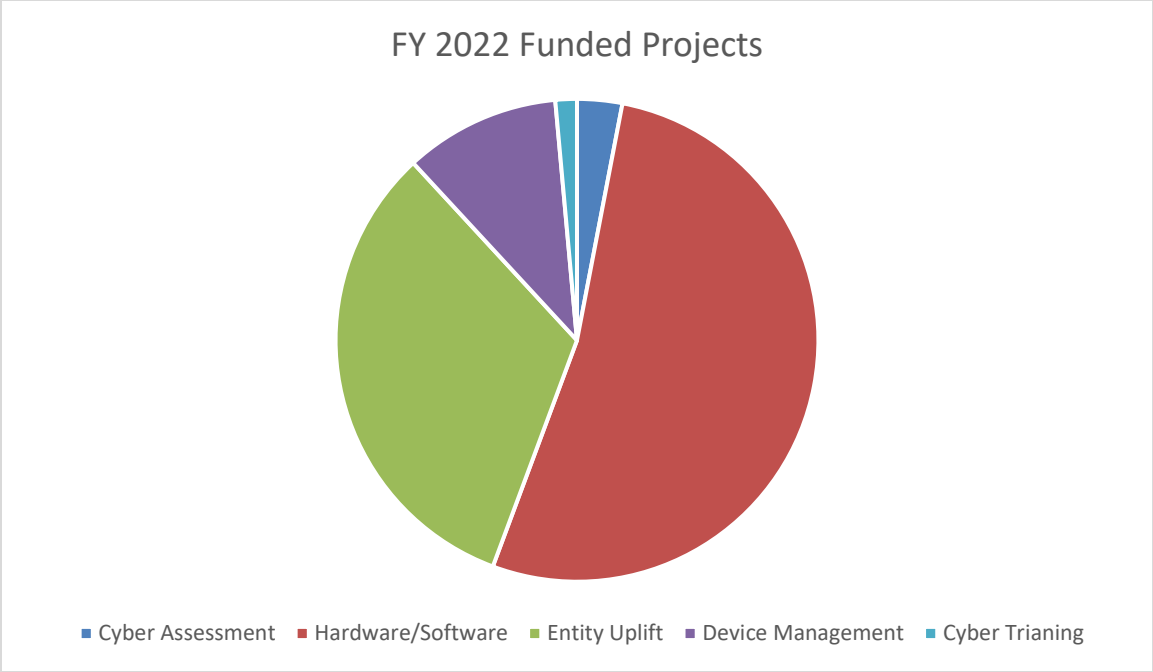
> Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
>
> Objective 2: Understand their current cybersecurity posture 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.

### *Priorities and Eligible Projects*

The North Dakota Cybersecurity Taskforce has set the following priorities to address the above objectives for the FY 2023 SLCGP.

- Cyber Maturity Assessment (CMA)
    - Project Example: Hiring a contractor to complete the CMA and/or CISA's National Cybersecurity Review
    - Project Example: Hire a contractor to develop or revise local cyber incident response plan, with clearly defined roles and responsibilities.
    - Project Example: Test local cyber incident response plan by conducting a tabletop exercise.
    - Project Example: Hire a contractor to develop a plan of prioritized asset (e.g., devices, data, software) protection, recovery, and mitigation actions based on the

asset's criticality and business value (high impact vulnerabilities and those most likely to be exploited).
    - Project Example: Hire a contractor to conduct a physical inventory of local government devices and systems, as well as software platforms and applications.
- Hardware/Software Improvements based on CMA or National Cybersecurity Review (NCSR) assessment
    - Project Example: Replace end of life server
    - Project Example: Replace end of life network devices
    - Project Example: Implement firewalls
    - Project Example: Expansion or implementation of network segments in a secure manner
- Entity Uplift (vulnerability management solutions/extended detection and response platforms)
    - Project Example: Purchase a vulnerability management tool or hire a contractor to scan entity network for weaknesses that are susceptible to exploitation and deploys an automated remediation process.
    - Project Examples: Implement the CISA recommended Cybersecurity Best Practices (see list below under *Key Cybersecurity Best Practices for Individual Projects*)
- Device Management Services for K-12 Schools
    - Project Example: Hire a contractor to install device management solutions such as Intune, Jamf, Manage Engine, etc. on staff and student laptops;
    - Project Example: Contract with North Dakota Information Technology (NDIT) for State to purchase patchmyPC management services on school's behalf.
- Cybersecurity Awareness Training
    - Project Example:  Conduct phishing training
    - Project Example: Conduct cybersecurity awareness campaigns
    - Project Example: Provide role-based cybersecurity awareness training to all employees
    - Project Example: Hire a contractor to develop a cyber workforce development and training plan.




### *Key Cybersecurity Best Practices for Individual Projects*

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. As SLT governments increase their cybersecurity maturity, CISA recommends they move toward implementing more advanced best practices, such as endpoint detection and response capabilities, as well as conducting regular penetration testing. The following Cybersecurity Best Practices are provided for SLT cyber planning consideration:

- 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)
- Actively engage in bidirectional sharing between CISA and SLT entities in cyber relevant time frames to drive down cyber risk
- Migration to the .gov internet domain

### *Smart Computers and Consulting Services*

Smart Computers and Consulting provides many services for to North Dakota local government entities. These services include:

- Endpoint Detection and Resource (EDR) SOC and NOC
- Full managed IT services provider.
- Basic Penetration Testing and Full Penetration Testing Services
- Security Awareness Training

Contact our salesteam@realsmart1.com, we will answer any cybersecurity questions you have.

## Application Submission Deadline

**September 28, 2023, 5:00 p.m. CT**

North Dakota applicants must apply for the funding through the North Dakota Department of Emergency Services (NDDES): Division of Homeland Security.

Applicants must submit application to NDDES (SAA) by Thursday, September 28, 2023, no later than 5:00 p.m. CT. All applications **must** be received by the established deadline. **Applicants are solely responsible for completing their application prior to the established deadline.**

## Unique Entity Identifier

Applicants applying for SLCGP funding through NDDES (SAA) **must** have a Unique Entity Identifier (UEI) number. The applicant must provide a UEI with their application.

If you are going to apply for this funding opportunity and have not obtained a UEI, please obtain a UEI by September 14, 2023. If your organization does not yet have a UEI, visit SAM.gov to get a UEI and select "Get Started", then choose "Get Unique Entity ID."

Obtaining a UEI is free of charge, so if you encounter any organizations or websites soliciting a fee or charge to acquire a UEI it is likely a scam or fraudulent.

## Content and Form of Application Submission

Applying for an award under this program is a multi-step process and requires time to complete. To ensure that an application is submitted on time applicants are advised to start the required steps well in advance of their submission. Failure of the applicant to comply with any of the required steps before the application deadline may disqualify their application from funding.

The steps to apply for an award are:

1. Apply for, updating, or verifying the UEI
2. Completing application package
3. Submitting the complete application package to NDDES by the deadline
    a. Application (within GMS system)
    b. Certification Regarding Lobbying form (uploaded to GMS system)

### *Authorized Organizational Representative (AOR)*

The AOR should be the individual who is able to make legally binding commitments for the applicant organization.

### *Electronic Signature*

Applications submitted through the NDDES Grants Management System constitute a submission as electronically signed applications. When submitting the application through GMS the applicant's AOR will type his/her name into the signature line of the application.

## Funding Restrictions

The following types of projects and project costs are **not** eligible:

- Covered (People's Republic of China) Telecommunications Equipment or Services (2 CFR § 200.216). See also FEMA Policy #405-143-1 – Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services.

### *Other Ineligible Projects*

- Physical Security Enhancements such as security cameras, door security access systems
    - Physical Security projects are potentially eligible under the State Homeland Security Grant Program (SHSP). Application timeframe for SHSP funding generally occurs in the spring of each year.
- Renovation/Remodeling projects such as re-wiring
- Construction projects
- Spyware
- Cybersecurity insurance premiums
- If unsure if your project is eligible, please contact a member of the task force for clarification.

## SLCGP Specific Application Instructions

By applying to NDDES, the applicant agrees to comply with the requirements of the Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) for Fiscal Year (FY) 2023 State and Local Cybersecurity Grant Program (SLCGP) and the terms and conditions of the award, should the applicant receive an award.

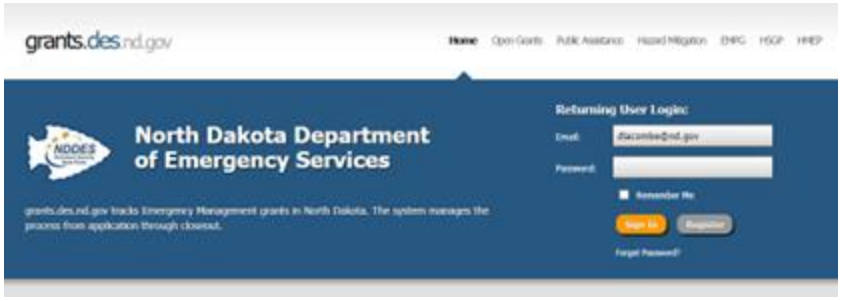
Not all applicants will receive an award.

As part of the FY 2022 SLCGP application, each applicant must address the following in their application:

### How to Apply to NDDES via NDDES Grants Management System

Applications must be submitted to NDDES via the NDDES Grants Management System at grants.des.nd.gov. Below are the steps to apply.

**Step 1:** Register for Access




- **New Users** Click on the Register button. Fill out the Register for Access Form. Under Request Type, select New User Requesting Access. Under the Grant Number Select FY 2023 – Cybersecurity Grant Program (SLCGP) (Dec 1, 2023). After filling out the form click on the blue Register button at the bottom of the form. You will receive an email to set up a password before they will be able to log into the system and access the application.
- **Existing Users** Click on the Register button. Fill out the Register for Access Form. Under Request Type, select Existing User Selecting Additional Access. Under the Grant Number Select FY 2023 – Cybersecurity Grant Program (SLCGP) (Dec 1, 2023). Once approve you will be able to use their existing password to access the application after they request access to the application.

**Note: If you do not receive an email, check your Junk Email box before calling NDDES**.

**Step 2:** Accessing the Application

- Once a user is active and access to grants.des.nd.gov has been granted, the user will only have access to the jurisdiction or organization they represent. All applicants are separated to ensure privacy and prevent fraud.
- To access the application, click on the Grant Name (FY 2022 Cybersecurity Grant Program SLCGP)) on your Home Page, this will take you to a screen with a red band at the top.

- Next, click on Projects on the left-hand side which will bring up a dropdown list.
- Next, click on Applications from the dropdown list. This will bring up the application on the right. Click on the Application, this will take you to a screen with a red band at the top.
- Finally, click on Form on the left-hand side. This will take you to the application. Then following the instructions in Step 3 below.

**Note:** Be sure to **Save** the application by clicking the Save button on the top left of the page as you complete each section of the application to prevent losing the information you input. If you go out of the application and come back to complete it later the draft can be accessed from you home page in your **Inbox** which can be found on the right-hand side.

**Step 3:** Completing the Application:
Once in the application, click on the left tab entitled "Form". The word "Form" will be in red with a red star next to it. The red color and star indicate that the form has not been completed and needs additional information before it can be submitted. The application cannot be submitted until all required information has been entered into the form. **Parts of the form we'll be pre-populated with the information from your NOI. Please double check this information and make any necessary corrections.**

**Introduction Page**

- Title: Identify the Project Name, include the appropriate priority in the name (ex. Device Management – Microsoft Intune)
- Primary Contact: This must be a legal representative of the jurisdiction that is applying since the jurisdiction will be legally responsible for the project.
- Alternate Contact: Representative of the jurisdiction other than primary contact.
- Authorized Contact: Representative of the jurisdiction other than primary contact.
- Work Activity: Areas that coincide with your work activity and costs. Choose Planning, Training, Exercise, Equipment only. *Hold the **Ctrl** key to select multiple areas.*
- Mark the appropriate statement at the bottom of the page.

**Costs Page:**
This represents your budget request for the SLCGP grant. The costs for a project should be broken down into direct cost categories. For each cost, click the "Add Line" button and enter the specific information for that cost item. *FY 2022 SLCGP may **not** be used to supplant local funds.*

- Cost Line Items
    - Area: Choose Planning, Training, Exercise, or Equipment
    - Type: Choose Contractor, Equipment, Materials and Supplies, Travel, Other
    - AEL Code: Enter the AEL Code. If you are unsure of the Code, you can click on the blue "List" link, and it will show you the available codes. (A list of commonly used codes is listed at the end of this document.)
    - Description: When you enter the AEL Code the Description will auto-populate. DO NOT CHANGE THE AUTO-POPULATED DESCRIPTION. **Add** additional information AFTER the auto-populated information.
    - Quantity: Enter the Quantity of the item.

- Price: Enter the Unit Price of the item.
- Total: The Total column will auto-calculate.

- Funding Sources: This will auto-populate.
  - 80% in the Estimated Federal Share box.
  - 4.55% in the Estimated State Share box.
  - 15.45% in the Estimated Local Share box.

**Agreements Page**

- Check the small box stating the documentation is being electronically signed
- Enter name and date of Agency Authorized Representative

**Work Activity Pages:**

- Start Date: Enter the date the project is estimated to start. Note projects should not have a start date prior to December 1, 2023.

- End Date: Enter the date the project is estimated to be complete. Note projects should be complete by November 30, 2026.

- Objective: Explain the goal your project is intended to accomplish. Use the S.M.A.R.T philosophy when developing your objective/goal.
  - **S**pecific
  - **M**easurable
  - **A**chievable
  - **R**elevant
  - **T**ime-bound

  *Objective Examples:*
  Reduce phishing attacks by 15% with employee training and improved security protocols in 12 months.
  Enhance security awareness by conducting monthly 5-minute virtual training sessions for all staff members for the next 3 years.
  Create incident response plans by identifying roles, responsibilities, and procedures for different scenarios by November 30, 2025.

Note: If you have more than one project, complete a separate Objective for each project. To do so, click **Add an Objective** button at the bottom of the form.

- Justification: Describe your project in detail.

  *Justification Narrative Example:*
  The City of Simplia Police Department will use FY23 funding for Cybersecurity training and equipment to increase security of the department's network to include $5,000 to conduct 2 cybersecurity training workshops for 50 law enforcement officers on phishing to reduce

susceptibility to cyber-attacks, $25,000 to purchase 2 unsupported/end of life network servers.

Note: Describe, should this project not be funded through this program, if you have an alternate source of funding to complete this project (example: E-rate)

**Note:** *The Justification section has a maximum of 1000 characters. If your justification narrative exceeds 1000 characters attach a separate word document to your application*.

- Action Steps: Explain the steps required for successful completion of the project. (A project schedule with clearly defined milestones).
    - Example:
        - Q1 obtain quotes and procure equipment hardware from vendor.
        - Q2 arrange installation with technical resources.
        - Q3 finalize install and complete testing.
        - Q4 Finalize project, collect metrics, and submit for final reimbursement.

**Finishing the Application**
Once you have completed the application be sure to hit the **"Save"** button at the top of the page. From there, the user will need to upload their backup documentation, including any additional forms required in the Notice of Funding Opportunity.

- Uploading documents:
    - Click on the Summary tab above the Form tab in the application.
    - Click the "Add Document" button at the bottom of the page. This will bring up a window to add files.
    - Select the "Choose Files" button, locate, and select the files needing to be uploaded and click Open.
    - Once they are added to the list, assign a document type from the drop-down list.
    - Click the Upload button

After everything is uploaded and completed, hit the "**Advance**" button. This will notify NDDES that the application is ready for review. NDDES will review the application for eligibility and completeness. If the application is missing documentation or needs revisions, the application will be returned to the applicant with a Request for Information (RFI) that outlines what revisions are required. Once the RFI has been completed, the applicant will need to re-submit the application to the State again for further review.

## Review and Selection Process

### Cybersecurity Task Force Review

The North Dakota Cybersecurity Task Force will review applications and recommend to NDDES which applications should be selected for funding. The Task Force's review will include verification that each project aligns with at least one FY 2023 SLCGP Objective; aligns with at least one Priority area;

demonstrates how investments support closing capability gaps identified through the National Cybersecurity Review (NCSR) or the State's Cyber Maturity Assessment (CMA), or another Cybersecurity Assessment.

Successful applicants will be notified via the Grants Management System (GMS) no later than January 15, 2024.

Task Force's review will include verification that the project:

- Alignment to one of the Priority Areas
- How project supports closing gaps identified in a Cyber Assessment
- Is feasible and effective
- Budget that maximizes $ requested/is reasonable

Note: Projects cannot be started before a) award is issued to and accepted by sub-recipient, and b) 2023 NCSR is completed, and c) EHP (if required) is approved. Any projects started before these three steps occur will be result in sub-recipient not receiving the funding.

# Award Administration Information

## Notice of Grant Award

Notification of award approval is made through the NDDES Grants Management System (GMS) to the sub-recipient's authorized official listed in the initial application. The sub-recipient should follow the directions in the notification to confirm acceptance of the award.

Sub-recipients must accept their awards no later than 10 days from the award date. The sub-recipient shall notify NDDES of its intent to accept and proceed with work under the award by signing the Notice of Grant Award and uploading it to the Project page in the GMS.

Funds will remain on hold until the sub-recipient accepts the award and all other conditions of award have been satisfied, or the award is otherwise rescinded. Failure to accept the grant award within the 10-day timeframe may result in a loss of funds. Sub-recipients who wish to decline the award must provide a written notice of intent to decline through the GMS.

Sub-award of sub-recipients whose project(s) require an Environmental Historic Preservation (EHP) review and who's EHP is not approved by DHS/FEMA within 30 days of the State receiving the federal award, will include the condition that the project cannot be started, or any funds expended until the EHP is approved. Projects started prior to EHP approval will result in the award being rescinded. NDDES will notify the sub-recipient when the EHP has been approved.

**All successful applicants will be required to complete and submit the 2023 National Cybersecurity Review (NCSR). The 2023 NCSR is estimated to be open from October 2023 – February 2024.**

See the Preparedness Grants Manual for information on federal administrative and national policy requirements, including the DHS Standard Terms and Conditions.

**Before accepting the award, the AOR should carefully read the award package for instructions on administering the grant award and the terms and conditions associated with responsibilities under Federal Awards. Sub-recipients must accept all conditions in the NOFO as well as any Special Terms and Conditions in the Notice of Award to receive an award under this program.**

## Required Services and Memberships

All SLCGP recipients and subrecipients are required to participate in a limited number of free services by CISA. This requirement applies to all subrecipients.

### *Cyber Hygiene Services*

Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static Internet Protocols for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.

To register for this 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.

### *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 NIST Cybersecurity Framework and is sponsored by DHS and the MS-ISAC.

Subrecipients are required to complete the NCSR, administered by the MS-ISAC, during the first year of the subaward period of performance and annually.

For more information, visit Nationwide Cybersecurity Review.

## Reporting

Sub-recipients are required to submit various financial and programmatic reports as a condition of their award acceptance. Future awards and funds reimbursement may be withheld if these reports are delinquent. **Reporting will be done electronically through the NDDES Grants Management System (GMS) located at https://grants.des.nd.gov/.**

In addition, sub-recipients may have additional reporting requirements to the federal awarding agency. See the Preparedness Grants Manual for information on federal reporting requirements, including financial, programmatic, and closeout reporting and disclosing information per 2 C.F.R. § 180.335.

### *Financial Reporting Requirements*

Sub-recipients must submit at least one reimbursement request through the NDDES Grants Management System (GMS) upon completion of the project; however, quarterly reimbursement requests as the project progresses are preferred. See the Reimbursement Processing Checklist for a list of documentation that must be included with the reimbursement request.

NDDES uses the Direct Deposit/Electronic Funds Transfer (DD/EFT) method of payment to sub-recipients. To enroll in the DD/EFT, the sub-recipient must complete and submit to NDDES a Substitute IRS Form W-9 (SFN 53656) http://www.nd.gov/eforms/Doc/sfn53656.pdf and a voided check.

### *Program Performance Reporting Requirements*

Sub-recipients are responsible for providing updated performance reports on a quarterly basis through the NDDES Grants Management System (GMS).

The following reporting periods and due dates apply for the performance progress reports:

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

## Closeout Reporting Requirements

Within 15 days after the end of the Period of Performance, sub-recipients must submit a final reimbursement request and final project status report detailing all accomplishments and a qualitative summary of the impact of those accomplishments throughout the Period of Performance, as well as other documents required by program guidance or terms and conditions of the award, to include the tangible personal property report (inventory of all equipment and software acquired using funds from the award).

The sub-recipient must liquidate all obligations incurred under the SLCGP award by the end of the period of performance. Unliquidated obligations at the end of the period of performance will result in the costs being disallowed.

After these reports have been reviewed and approved by NDDES, a close-out notice will be completed to close out the grant. The notice will indicate the Period of Performance is closed, list any remaining funds that will be de-obligated, address the requirement of maintaining the grant records for three years from the date of the final Federal Financial Report submitted by NDDES to DHS/FEMA, and disposition and reporting requirements for any equipment purchased using SLCGP funding.

Federal rules require that all equipment purchased with federal funds must be inventoried and tagged. Sub-recipients are to record equipment purchased with a value of $5,000 or more on the Inventory List form and submit it to NDDES. NDDES will then issue the sub-recipient inventory tags based on the submitted form. All inventory tags must be placed on identified equipment within 30 days of receiving the tags.

## Environmental Planning and Historic Preservation (EHP) Compliance

As a Federal agency, DHS/FEMA is required to consider the effects of its actions on the environment and/or historic properties to ensure that all activities and programs funded by the agency, including grants-funded projects, comply with federal EHP regulations, laws, and Executive Orders as applicable. Sub-recipients proposing projects that have the potential to impact the environment, including but not limited to construction of communication towers, modification or renovation of existing buildings, structures and facilities, or new construction including replacement of facilities, must participate in the DHS/FEMA EHP review process. The EHP review process involves the submission of a detailed project description EHP Screening Form along with supporting documentation so that DHS/FEMA may determine whether the proposed project has the potential to impact environmental resources and/or historic properties. In some cases, DHS/FEMA is also required to consult with other

regulatory agencies and the public to complete the review process.

**The EHP review process must be completed before funds are released to carry out the proposed project, otherwise, NDDES will not be able to fund the project due to non- compliance with EHP laws, executive orders, regulations, and policies.**

Additionally, all sub-recipients are required to comply with GPD EHP Policy Guidance. This EHP Policy Guidance can be found in FP 108-023-1 at https://www.fema.gov/media-library/assets/documents/85376 and GPD EHP Compliance and Reference Documentation at: https://www.fema.gov/environmental-planning-and-historic-preservation-compliance.

Costs incurred to comply with the EHP requirements are the responsibility of the sub- recipient. This includes costs associated with the preparation, collection, or assembly of the necessary documentation, the submission of the EHP clearance form, and the consultation fees for the development of an Environmental Assessment (EA) or an Environmental Impact Statement (EIS).

## NDDES Awarding Agency Contact Information

NDDES staff will provide programmatic support and technical assistance. A list of contacts is provided below:

Programmatic or Administrative Questions (grant guidance, reimbursement requests, change requests, etc.)

- Dave Rice drice@nd.gov
- Debbie LaCombe dlacombe@nd.gov
- Karen Hilfer khilfer@nd.gov
    - EHP Review Process (EHP guidance, screening form, etc.)

## Commonly Used AEL Codes

| AELCode | Title | Description |
|---|---|---|
| 05AU-00-BIOM | Device, Biometric User Authentication | Devices that utilize biometric characteristics (fingerprints, palm prints, iris or retinal scanning, tissue matrix, etc.) to authorize access to facilities and/or systems. |
| 05AU-00-TOKN | System, Remote Authentication | System used to provide enhanced remote authentication, usually consisting of a server, some synchronization scheme, and a device, token, or smartphone application. |
| 05EN-00-ECRP | Software, Encryption | Encryption software for protecting stored data files or email messages. |
| 05EN-00-ETRN | Encryption, Data Transmission | A class of network access solutions, usually for remote access, that provide encrypted user access. May be used for remote access, point to point, or link encryption. Includes virtual private networks, and encrypted transmission modes such as SSH and SSL. |
| 05HS-00-FRNS | Software, Forensic | Application suites that allow in-depth analysis of hosts based on operating system and file systems. Software of this type may be used by law enforcement officers, government/corporate investigators and consultants to investigate the aftermath of computer-related crimes. Forensics software generally includes disk analysis tools, tools for the recovery of deleted files, and integrated database support to mark files and data of interest to investigators. This functionality may also be obtainable via subscription as a cloud-based service using a web browser interface, as opposed to purchasing software. See 04AP-11-SAAS for further information. |
| 05HS-00-MALW | Software, Malware/Anti-Virus Protection | Software for protection against viruses, spyware, and malicious code. May be obtained for individual hosts or for entire network segments. |
| 05HS-00-PFWL | System, Personal Firewall | Personal firewall for operation on individual workstations. Usually a software solution, but appliances are also available. See also: 05NP-00-FWAL. |
| 05NP-00-FWAL | Firewall, Network | Firewall (software or standalone appliance) for use in protecting networks. See also 05HS-00-PFWL. |
| 05NP-00-IDPS | System, Intrusion Detection/Prevention | Intrusion Detection and/or Prevention System (IDS, IPS) deployed at either host or network level to detect and/or prevent unauthorized or aberrant behavior on the network. Software and hardware (appliance) solutions exist. This replaces item 05NP-00-IDS and incorporates more recent prevention technology. |
| 05NP-00-SCAN | Tools, Vulnerability Scanning | Tools designed to identify security vulnerabilities on networks, databases, web applications or individual hosts on target networks. |
| 05NP-00-SIEM | System, Security Information and Event Management | Software or appliance that gathers data from multiple security sources such as firewalls, intrusion detection |

| | | |
|---|---|---|
| | (SIEM) | systems, malware protection systems, etc. to provide log file consolidation and event correlation capability in support of network security operations.<br>While some client-side software may be required, this functionality may also be obtainable via subscription as a cloud-based service using a web browser interface, as opposed to purchasing software. However, special security considerations apply for data stored remotely. See 04AP-11-SAAS for further information. |
| 05PM-00-PTCH | System, Patch/Configuration Management | System to manage the update and installation of patches, applications, and/or operating systems utilized by an organization in order to maintain current "version control." This functionality may also be obtainable via subscription as a cloud-based service using a web browser interface, as opposed to purchasing software. However, special security considerations apply for data stored remotely. See 04AP-11-SAAS for further information. |
| 04AP-07-INVN | Software, Equipment Tracking and Inventory | Application software for tracking of tangible equipment, including location and person(s)/organization(s) responsible. This functionality may also be obtainable via subscription as a cloud-based service, as opposed to purchasing software. However, special security considerations apply for data stored remotely. See 04AP-11-SAAS for further information. |
| 04AP-11-SAAS | Applications, Software as a Service | Sometimes referred to as "on-demand software", SAAS applications run on the provider's servers, delivering functionality via the internet to any device having connectivity and the required browser or interface. Access to the application is obtained via a service subscription rather than outright purchase, with all updates and configuration requirements handled by the service provider. Some example SAAS applications include equipment tracking and maintenance, intra-application communication among client devices, and specialized software such as plume modeling. Note that purchasers of SAAS should consider the security aspects of the planned usage, particularly availability and the protection of sensitive information stored remotely. Internet connectivity is required to utilize SAAS applications unless specific failover measures such as a "hybrid cloud" are available. In addition, data is stored remotely on vendor equipment. Use of SAAS for mission critical applications should be thoroughly vetted before implementation. |
| 04HW-01-INHW | Hardware, Computer, Integrated | Computer hardware and operating system software designated for use in an integrated system allowable under the indicated grant programs. Such systems include detection, communication, cybersecurity, logistical support and Geospatial Information Systems. This item may include |

| | | |
|---|---|---|
| | | networking hardware (routers, wireless access points, etc. servers, workstations, etc., procured with an allowable system and necessary for its implementation. Only hardware procured as part of a system allowable under the indicated grant programs is allowable under this item. |
| 04SW-04-NETW | Software, Network | Software for networking, monitoring network performance and/or maintaining configuration.<br>This functionality may also be obtainable via subscription as a cloud-based service using a web browser interface, as opposed to purchasing software. However, special security considerations apply for data stored remotely. See 04AP-11-SAAS for further information. |
| 04SW-05-SCAD | System, SCADA (Supervisory Control and Data Acquisition) | A software/hardware system designed primarily to monitor and control remote sensors and actuators. Uses vary from large-scale examples such as refinery or power grid control to building HVAC systems.<br>While some sensors and other hardware may be required, this functionality may also be obtainable via subscription as a cloud-based service using a web browser interface, as opposed to purchasing software. However, special security considerations apply for data stored remotely. See 04AP-11-SAAS for further information. |
| 21GN-00-INST | Installation | Installation costs for authorized equipment purchased through FEMA grants. |
| 21GN-00-MAIN | Maintenance Warranty | Equipment maintenance packages. Maintenance contracts are allowable only for authorized equipment purchased through FEMA grants. |
| 21GN-00-SHIP | Shipping | Shipping costs for equipment purchased with grant funding. |