

State And Local Cybersecurity Grant Program

ESA Application Walk Through

To start an application - [Single Application for Assistance \(pa.gov\)](https://pa.gov)



If the applicant does not have a Keystone Login Account, please register for one before attempting to login

General Facts

- Create a New Keystone Login Account – [Registration](#)
 - Click Register and enter all of the information into the fields with a red asterisk (*) next to them.
 - You will be asked to create your profile, login information and security questions.
 - If you have already created an account with another agency whose application uses the Keystone Login Service, you do not need to register another account with us.
 - If you create a Keystone Login account with us, you will be able to use this account with other agencies that use Keystone Login.
 - Some additional information may be required for those agencies.
- Keystone Login Services
 - There are many account options that can be configured for your Keystone Login account. Please see the help documents provided by the [Keystone Login Service](#)
 - Keystone Login account assistance or password resets, please contact the Keystone Global Help Desk at 877-328-0995
- For technical assistance with an application, please contact the appropriate resource center listed below:
 - **DCED customers:** Please contact the DCED Customer Service Center. Representatives are available Monday through Friday, from 8:30 AM until 5:00 PM, at 800-379-7448. Email inquiries can also be sent to ra-dcedcs@pa.gov.
 - **Customers of all other agencies:** Please contact the appropriate resource center. Representatives are available Monday through Friday, from 8:30 AM until 5:00 PM, at 833-448-0647. Email inquiries can also be sent to ra-dcedcs@pa.gov.

For existing Keystone Login user, please enter Username and Password to get started.

Login

What's New?

For an overview of the changes in the new Single Application, please read [Help](#).

Username

Password

[LOGIN](#)



Powered by

[Register](#)

NOTE: If registering for the first time with Keystone Login, please include an email address with your account. It will be needed to successfully complete grant applications and grant processing.

[Forgot Password](#)

[Forgot Username](#)

[Learn more about Keystone Login](#)

[Having Trouble Registering](#)



Begin a New Application

To begin a new Single Application For Assistance, enter a brief name for the project (up to sixty characters) and answer whether you need help selecting your program. If you already know the name of the program you want to apply for, answer "No".

Project Name

FY2022 SLCGP Entity Name

Enter the Project Name

Do you need help selecting your program?

No

Make sure the drop down is changed to "No"

Click on Create a New Application after entering the project name

CREATE A NEW APPLICATION



Program

Agency: Pennsylvania Department of Community and Economic Development

Applicant:

Program: DCED

Red Diamond (◆) = Required Field.

Blue Diamond (◆) = Conditional Required Field.

Select Program

To search for programs based on your organization and/or project, click the Program Finder button below.

Program Name

SLCGP

Enter **SLCGP** for the program name

Sort By

Program Name

Pick **Program Name** in the drop down

Click on Search

SEARCH

PROGRAM FINDER

Please note there are four applications you will need to apply separately for each project that you would like to participate in

Only apply for the services that you would like to receive

State and Local Cybersecurity Grant Program (SLCGP) – Intrusion Detection Service MS-ISAC Albert Sensors

Pennsylvania Emergency Management Agency

Click on Apply

[Apply](#)

The State and Local Cybersecurity Grant Program is a federal grant that helps support state and local governments to address cybersecurity risks, strengthen cybersecurity of critical infrastructure and ensure resilience against participation in Commonwealth offered services related to this program. The prevention tools/services include:

- Intrusion detection systems placed on government networks and monitored 24/7 to identify intrusion attacks, alert key personnel, and report nationally on coordinated cyberattacks.

State and Local Cybersecurity Grant Program (SLCGP) – Security Awareness Service (Cofense)

Pennsylvania Emergency Management Agency

Click on Apply

[Apply](#)

The State and Local Cybersecurity Grant Program is a federal grant that helps support state and local governments to address cybersecurity risks, strengthen cybersecurity of critical infrastructure and ensure resilience against participation in Commonwealth offered services related to this program. The prevention tools/services include:

- Employee training on how to prevent cyber system breaches and phishing, and penetration testing services.

Applicant Information

To copy your Registration information into the application, click the "Use Account Information" button below.

Red Diamond (◆) = Required Field.

Blue Diamond (◆) = Conditional Required Field.

USE ACCOUNT INFORMATION

Applicant Entity Type:

- Limited Liability Partnership
- Partnership
- Government
- Non-Profit Corporation
- Sole Proprietorship
- Limited Liability Company
- S Corporation
- C Corporation

Applicant Name: Test Entity

NAICS Code: 9211

FEIN/SSN Number: 999999999

*Please enter FEIN as 9 digits, no dashes

UEI Number: AA00BB00CC00

Top Official/Signing Authority: Jack Test

Title: Chairman

SAP Vendor #: 000000

(xxxxxx or xxxxxx-xxx)

Contact Name: Mark Test

Contact Title: Chief Clerk

Phone: 717-000-0000 Ext.

(xxx-xxx-xxxx)

Fax:

E-mail: test@pa.gov

Mailing Address: 1310 Elmerton Avenue

City: Harrisburg

State: PA

Zip Code: 17110

Pick the Applicant Entity Type that best describes the entity

Please enter 9211 as the NAICS Code

Please enter a valid 9 digit FEIN Number

Please enter a valid 12 digit UEI Number

Enterprise Type

Indicate the types of enterprises that describe the organization listed above. You may select more than one type. ◆

- | | | | | |
|--|--|---|---|---|
| <input type="checkbox"/> Advanced Technology | <input type="checkbox"/> Agri-Processor | <input type="checkbox"/> Agri-Producer | <input type="checkbox"/> Authority | <input type="checkbox"/> Biotechnology / Life Sciences |
| <input type="checkbox"/> Business Financial Services | <input type="checkbox"/> Call Center | <input type="checkbox"/> Child Care Center | <input type="checkbox"/> Commercial | <input type="checkbox"/> Community Dev. Provider |
| <input type="checkbox"/> Computer & Clerical Operators | <input type="checkbox"/> Defense Related | <input type="checkbox"/> Economic Dev. Provider | <input type="checkbox"/> Educational Facility | <input type="checkbox"/> Emergency Responder |
| <input type="checkbox"/> Environment and Conservation | <input type="checkbox"/> Exempt Facility | <input type="checkbox"/> Export Manufacturing | <input type="checkbox"/> Export Service | <input type="checkbox"/> Food Processing |
| <input type="checkbox"/> Government | <input type="checkbox"/> Healthcare | <input type="checkbox"/> Hospitality | <input type="checkbox"/> Industrial | <input type="checkbox"/> Manufacturing |
| <input type="checkbox"/> Mining | <input type="checkbox"/> Other | <input type="checkbox"/> Professional Services | <input type="checkbox"/> Recycling | <input type="checkbox"/> Regional & National Headquarters |
| <input type="checkbox"/> Research & Development | <input type="checkbox"/> Retail | <input type="checkbox"/> Social Services Provider | <input type="checkbox"/> Tourism Promotion | <input type="checkbox"/> Warehouse & Terminal |

Pick the Enterprise Type that best describes your entity

Click Continue to move onto the next screen

[Continue](#)

Project Site Location(s)

Site 1

Address: 1310 Elmerton Avenue

City: Harrisburg

State: PA

Zip Code: 17110

County: Dauphin

Municipality: Susquehanna Township

PA House: Andrew Lewis (105)

PA Senate: John DiSanto (15)

Designated Areas:

<input type="checkbox"/> Act 47 Distressed Community	<input type="checkbox"/> Brownfield
<input type="checkbox"/> Enterprise Zone	<input type="checkbox"/> Greenfield
<input type="checkbox"/> Keystone Innovation Zone	<input type="checkbox"/> Keystone Opportunity Zone
<input type="checkbox"/> Prime Agricultural Area	<input type="checkbox"/> Uses PA Port

Enter the address where the funds will be

Enter the zip code plus 4 if known

PA House & PA Senate will populate based on information entered

Click Continue to move onto the next screen

[Continue](#)

Project Narrative

Adequate answers to the Project Narrative questions below are required. Uploaded attachments or mailed documents are no longer permitted in this section of the application. If a more detailed narrative is required for the Program selected, instructions will either be provided in the Addenda section or the Program Guidelines.

1. What do you want to accomplish with this project? ♦

Character Count: 85 characters.

Please click continue at the bottom right. Nothing additional is needed in this field

This area is prepopulated.
There is no need to enter any
information.

Click Continue to move
onto the next screen

[Continue](#)

This screen applies to the Security Awareness Training - Cofense application

Addenda

Below are additional application requirements specific to the program you selected. If you are having problems completing the Addenda because your organization or pr

Security Awareness training- Cofense

(Security awareness services ensure that all end users receive and complete security awareness training. This service provides for social engineering (phishing) , the training and the overall risk level for this type of attack. Additional testing can be conducted as needed to further reinforce the concepts from this training. Rec

Are existing services (Cofense) in place? ◆

(This could be because of the grant or budgeted expenses)

Answer "Yes" or "No"

If Yes, what is the end date of the current contract?

If you answered "Yes" to the above question, you will need to input a date in the field. If answered "No", you can leave the field blank.

Eligible service dates: Must start before 11/30/2027. Supplanting is NOT allowable. Refer to this documentation for more guidance on supplanting [Download SLCGP additional guidance -ESA.pdf](#)

Requested service dates:

Start date: ◆

(Today's date if you do not currently have Cofense or the first day following the end of any current Tenable agreement/contract)

Remember to put your start date in the field.

End date: ◆

11/30/2027

Input the number of licenses you will need.

Total Number of licenses requested (each individual will need their own license, e.g. 200 employees you would need 200 licenses): ◆

This screen applies to **Intrusion Detection Services – Albert Sensors** application

Intrusion Detection Services – Albert Sensors

(Intrusion detection services increase information security capabilities through the deployment of a turnkey network security monitoring and management service. An Albert Sensor provides network security enhanced monitoring and notification of malicious activity. It is critical that such a service be managed centrally, to provide collaborative insight and to offer an enhanced, correlated perspective into events th

Are existing services (Albert Sensors) in place? ◆

Pick "Yes" or "No"

If NO, Please upload the following forms

[Download Albert_PIQ_CIS_FEB_2024.pdf](#)

Upload Files

Use the control below to select your file. Each file can be no larger than 30MB.

File 1 No file chosen

If "No" was selected, download the attached files and fill them out. The completed forms will then need uploaded into the application. The application cannot be submitted without them

Upload 2

[Download Blank_Escalation_Procedures_Dec_2021.pdf](#)

Upload Files

Use the control below to select your file. Each file can be no larger than 30MB.

File 1 No file chosen

Eligible service dates: Must start before 11/30/2027. Supplanting is NOT allowable. Refer to this documentation for more guidance on supplanting

[Download SLCGP_additional_guidance_-ESA.pdf](#)

Requested service dates:

Start date: ◆

Remember to put your start date in the field.

End date: ◆

11/30/2027

This screen applies to **Intrusion Detection Services – Albert Sensors** application
continued

Specific Service-Related Requirements. Refer to this document for more guidance.

[Download Technical requirements - Intrusion Detection.pdf](#)

Check the box if the requirements are met.

Eligible Entities must meet the definition of "Local government": ♦

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.

By checking this box, I certify that the entity meets the definition of "local government"

This screen applies to **Vulnerability Management Solution - Tenable** application

Addenda

Below are additional application requirements specific to the program you selected. If you are having problems completing the Addenda because your organization or project do not meet the requirements listed below, please try [changing your program](#).

Vulnerability Management Solution (Tenable)

Vulnerability Management Solution provides the ability of an organization to improve their cybersecurity posture by identifying, prioritizing and remediating vulnerabilities in their IT infrastructure. Tenable helps organizations identify, understand and manage the vulnerabilities and risks across their IT infrastructure.

Eligible service dates: Must start before **11/30/2027**. Supplanting is **NOT** allowable. Refer to this documentation for more guidance on supplanting [Download SLCGP additional guidance -ESA.pdf](#)

Are existing services (Tenable) in place? (this could be because of the grant or budgeted expenses) ◆

Answer "Yes" or "No"

If Yes, what is the end date of the current contract?

If you answered "Yes" to the above question, you will need to input a date in the field. If answered "No", you can leave the field blank.

Requested service dates:

Start date: (today's date if you do not currently have Tenable or the first day following the end of any current Tenable agreement/contract) ◆

Remember to put your start date in the field.

End date: ◆

11/30/2027

Specific Service-Related Requirements. Refer to this document for more guidance.

Type of Services Requested: ◆

Select the type of service that you will need. There are 3 different options.

Asset types to consider: Desktops, Laptops, Workstations, Networking Gear, Servers, Traditional IT Endpoints

What is licensed: Each asset is 1 license. If a device is multi-homed, has multiple IPs, etc., this still only counts as 1 licensed asset.

Total Number of licenses requested based on information above: ◆

Input the number of licenses you will need.

This screen applies to **Cyber Exposure Management and Asset Intelligence Platform - ARMIS** application

Addenda

Below are additional application requirements specific to the program you selected. If you are having problems completing the Addenda because your organization or project do not meet the requirements listed below, please try [changing your program](#).

Cyber Exposure Management and Asset Intelligence Platform (ARMIS)

ARMIS is a cyber exposure management and asset intelligence platform that provides unified protection for all connected devices within an organization through holistic asset visibility and data-driven risk prioritization.

Are existing services (ARMIS) in place? (this could be because of the grant or budgeted expenses) ◆

Answer "Yes" or "No"

If Yes, what is the end date of the current contract?

If you answered "Yes" to the above question, you will need to input a date in the field. If answered "No", you can leave the field blank.

Eligible service dates: Must start before 11/30/2027. Supplanting is NOT allowable. Refer to this documentation for more guidance on supplanting [Download SLCGP additional guidance -ESA.pdf](#)

Requested service dates:

Start date: ◆

Remember to put your start date in the field.

End date: ◆

11/30/2027

Specific Service-Related Requirements. Refer to this document for more guidance.

Number of Employees (Full-time/Contractors): ◆

Input the number of employees.

Estimated Number of covered assets: (Asset types to consider: Desktops, laptops, servers, networking gear, traditional endpoints, IoT, OT, cloud assets. Any managed or unmanaged device or asset that connects to an organization's network or infrastructure.) ◆

Input the number of assets you have.

The following screens apply to all applications

Other requirements that must be completed within a year (12 month period) after receiving the 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, Cybersecurity and Infrastructure 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 SLCGP. For more information, visit [CISA's Cyber Hygiene Information Page](#).

Nationwide Cybersecurity Review

The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and administered by the MS-ISAC, within a year (12-month period) after receiving the services. Annual NCSR submission is generally open from October through February. For more information, visit [Nationwide Cybersecurity Review \(NCSR\) \(cisecurity.org\)](https://www.cisecurity.org/nationwide-cybersecurity-review)

By checking this box, you confirm that you have read and understand the content of the following PDF document prior to submitting the application. ♦

[Download SLCGP Grant Process FFY2023.pdf](#)

Download the Instructions and then click on the check box.

IT contact information:

Name: ♦

Email: ♦

Phone Number: ♦

Enter the IT contact information for the entity.

Click Continue to move onto the next screen

[Continue](#)

If an entity requires more than one signature to execute a contract, multiple Signatory Authorities can be added on this screen.

Signing Authority

Authorized Signatory contact information:

Signing Authority	Title	First Name	Last Name	Email		
	Chairman	Jack	Test	test@pa.gov	Add	Cancel
No data has been entered.						

Enter the information of the Signatory Authority for the entity and then click Add.

Click Continue to move onto the next screen

[Continue](#)

Application Certification

All of the required sections of the web application have been completed. If you have reviewed the application, you may submit it for processing. **After submitting, you will no longer be able to mail**

Electronic Signature Agreement:

By checking this box and typing your name in the below textbox, I hereby certify that all information contained in the single application and supporting materials submitted via the Internet and its att applicant, I have verified with an authorized representative of the Applicant that such information is true and correct and accurately represents the status and economic condition of the Applicant. I also be subject to criminal prosecution in accordance with 18 Pa. C.S. § 4904 (relating to unsworn falsification to authorities) and 31 U.S.C. §§ 3729 and 3802 (relating to false claims and statements).

- I am the applicant.
- I am an authorized representative of the company, organization or local government.
- I am a "Certified" Partner representative.

Type Name Here:

Electronic Attachment Agreement:

Along with the web application, if you have been requested or need to send any documentation to PEMA please print and send a copy of your E-Signature and mail it to PEMA along with any pap

Please ensure that both Electronic Signature Agreement and the Electronic Attachment Agreement check boxes are checked.

Select the appropriate button for the signer designation.

Enter name of person filling out the application.

Click on button to submit application

SUBMIT APPLICATION

Application Certification

Single Application ID #: 202308175087

The web application has been successfully submitted for processing.

I hereby certify that all information contained in the single application and supporting materials submitted via the Internet, Single Application # 202308175087 and its attachments are true and correct and accurately represents the status and economic condition of the Applicant. I also understand the consequences of the prosecution in accordance with 18 Pa.C.S. § 4904 (relating to unsworn falsification to authorities) and 31 U.S.C. §§ 3729 and 3802 (relating to false claims and statements).

The signature page may also be printed now. You may also print submitted applications from the Home page. Click the link labeled "Submitted Applications" in the top toolbar.

[Print Signature Page only](#)

[Print Entire Application with Signature Page](#)

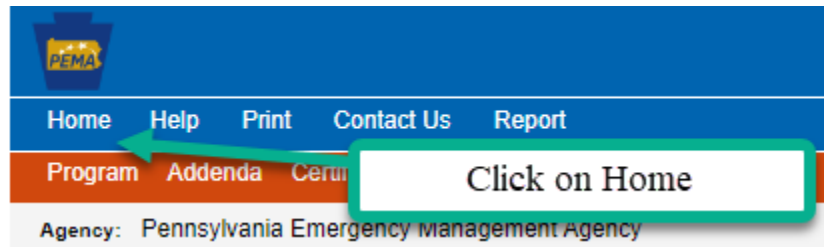
There is an option to print the application signature page or the entire application for the entity's records.

The signature page along with any paper supporting documents can be mailed to the following address:

Pennsylvania Emergency Management Agency

At this time, Pennsylvania Emergency Management is not requesting any U. S. Postal mailings

Here is where you can find your application after it has been submitted.



Id	Single Application Id	Applicant/Company	Project Name	Program	Status	Uid	
8188479	202308175086	Test County	SLCGP	PEMA State and Local Cybersecurity Grant Program (SLCGP) – Intrusion Detection Service MS-ISAC Albert Sensors	UNDER REVIEW	8188479	VIEW
8188481	202308175085	Test County	FY2022 SLCGP Cofense Training	PEMA State and Local Cybersecurity Grant Program (SLCGP) – Security Awareness Service (Cofense)	UNDER REVIEW	8188481	VIEW