RESOLUTION AUTHORIZING THE FILING OF THE GRANT APPLICATION TO THE DEPARTMENT OF HOMELAND SECURITY AND STATE AND LOCAL CYBERSECURITY GRANT PROGRAM, ASHTABULA COUNTY COMMISSIONERS

WHEREAS, Casey Kozlowski, Ashtabula County Commissioner, has prepared a grant application to The Department of Homeland Security and State and Local Cybersecurity Grant Program to use for Ashtabula County cyber security; to-wit:

Grantor: Department of Homeland Security, CyberOhio, 4200 Surface Road, Columbus, OH 43228

Purpose: To improve cybersecurity for Ohio local government entities

Amount: Not to Exceed, $20,000.00 with a 20% match of $4,000

Term: 2 years

WHEREAS, the Commissioners feel submitting this grant application is desirable and necessary; now

THEREFORE, BE IT RESOLVED, By the Board of Commissioners of Ashtabula County, Ohio that an application be made in accordance with the terms outlined in the grant, with a copy of such application on file in this office.

ASHTABULA COUNTY COMMISSIONERS

CERTIFICATION PAGE

Resolution No. 2024-443 **September 26, 2024**

RESOLUTION AUTHORIZING THE FILING OF THE GRANT APPLICATION TO THE DEPARTMENT OF HOMELAND SECURITY AND STATE AND LOCAL CYBERSECURITY GRANT PROGRAM, ASHTABULA COUNTY COMMISSIONERS

Upon the motion of Casey R. Kozlowski, seconded by J.P. Ducro IV.

VOTE:

Kathryn L. Whittington	**Aye**
J.P. Ducro IV	**Aye**
Casey R. Kozlowski	**Aye**

CERTIFICATE OF CLERK

IT IS HEREBY CERTIFIED that the foregoing is a true and correct transcript of a resolution acted upon and duly passed by the Board of County Commissioners of Ashtabula County, Ohio, on the date noted above.

Lisa Hawkins

Lisa Hawkins, Clerk of the Board
Board of County Commissioners
Ashtabula County, Ohio

CyberOhio

Mike DeWine, Governor
Kirk Herath, Cybersecurity Strategic Advisor
Sima S. Merick, Executive Director

The Department of Homeland Security (DHS)
and
State and Local Cybersecurity Grant Program (SLCGP)

Application Guidance

for

Round 2 Cybersecurity Software & Services Grant

GRANT APPLICATION
DUE BY SEPTEMBER 16, 2024

CyberOhio
4200 Surface Road, Columbus, Ohio 43228

Ohio Emergency Management Agency
2855 West Dublin-Granville Road, Columbus, Ohio 43235

Contents

All entities wishing to do business with the federal government must have a unique entity identifier (UEI). The UEI number is issued by the system. Instructions for requesting a UEI using Sam.gov can be found at: https://sam.gov/content/entity-registration.

If your organization DOES NOT already have a UEI number, please start this process NOW. This is a prerequisite to receiving federal funds.

Introduction

The State of Ohio's CyberOhio Team, with the support of Ohio Emergency Management Agency (OEMA), HSAC-Cyber Full Planning Subcommittee and the HSAC-Cyber Executive Committee, has applied for and has been awarded funds under the SLCGP grant program.

A portion of these funds will be used to provide cybersecurity grant opportunities for Ohio local government entities (LGEs).

Key Elements

Competitive Application Process

Below are some key points of this grant process.

- The total available funding allocated for this grant is **$6,840,000.**
    - If you are interested in the receiving funding for cybersecurity software and/or services, please apply before the deadline. Even though there are limited funds available with this grant, LGEs who apply but are not selected for this grant may be considered for upcoming grant programs. Demand for this program will help us more accurately determine future funding requirements and allocate future resources accordingly.
- As required by the SLCGP, Ohio will place a high priority on projects that support rural LGEs.
    - Per 49 U.S.C. 5302 "rural" is any area with a population of less than 50,000 individuals. The prioritized eligible recipients must be LGEs within a rural area (a jurisdiction with a population of less than 50,000 individuals).
    - There are 39 counties in Ohio that meet this definition of rural based on the 2020 US Census. Ohio will prioritize LGEs located in these rural counties.
- All eligible project applications will be scored and ranked by HSAC-Cyber and any additional Subject Matter Experts (SMEs) as deemed necessary. Recommendations will be made to the HSAC-Cyber Executive Committee for final review and approval.
- Eligible applicants are limited to Ohio LGEs.
- Project applications must be received via email by 12:00 PM EDT on Monday, September 16, 2024. Applications submitted after the deadline will not be reviewed.
- Cybersecurity software and services projects will have a maximum federal funding limit of $20,000 and require the LGE to provide a 20% cost share. LGEs who demonstrate economic hardship may qualify to have the cost share requirement waived.
- LGEs may only submit one Round 2 cybersecurity software and services application. The application allows up to a maximum of five (5) projects.
- Please enter your priority project in Project #1 and proceed in your preferred order to indicate your local preference for projects.

Note: The maximum federal funding limit for this grant is $20,000. However, applicants are encouraged to submit projects that exceed the funding limit. This will help us to better understand the need and build a business case for future funding. Projects not funded in Round 2 may be considered for future grant cycles.

- HSAC-Cyber reserves the right to re-designate the funding priority of a submitted project.

Federal Funding Priorities

DHS/FEMA requires priority be given to LGEs who are rural. Twenty-five percent (25%) of grant funds are required to be passed through to rural LGEs.

Program Overview

The SLCGP supports the implementation of cybersecurity best practices such as:

- Implementation of multi-factor authentication
- Implementation of enhanced logging
- Data encryption of data at rest and in transit
- End use of unsupported /end of life software and hardware that is 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
  Note: To apply for a .gov domain migration, please see the Round 2 SLCGP Grant Application .gov Migration guidance and application, which can be found on the Assisting Local Government Entities page of the CyberOhio website.

The purpose of this document is to provide the following:

- The application materials needed to apply for the CyberOhio Local Government Grant Program, which is funded by the SLCGP grant program.
- Administrative requirements that must be met by all subrecipients to meet the requirements of federal regulations, mandates, and orders.

To be eligible for funding consideration, Ohio requires that LGE projects meet the following criteria:

- Clearly identify how the project supports their organizations cybersecurity mission, goals and objectives.
- Have measurable and detailed goals to explain what gaps are being filled.
- Align with the Ohio Comprehensive Cybersecurity Plan.

SLCGP grant funds may only be used for the purpose set forth in the grant and must be consistent with the statutory authority for the award. Grant funds may not be used for matching funds or 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.

Funding Priorities

All projects must adhere to the guidelines stated within this guidance and applicable laws and regulations.

Federal Funding Priorities

All SLCGP recipients and **subrecipients are required to participate** in a limited number of free services by CISA. This requirement applies to all subrecipients. For these required services and memberships, note that participation is not required for submission and approval of a grant but is a post-award requirement.

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

  To register for this service, email vulnerability@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLCGP. For more information, visit CISA's Cyber Hygiene Information Page.

- **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 Multi-State Information Sharing and Analysis Center (MS-ISAC).

  Eligible entities and their subrecipients are required to complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually.

  For more information, visit Nationwide Cybersecurity Review (cisecurity.org).

- **Membership in the MS-ISAC and/or Election Infrastructure Information Sharing and Analysis Center (EI-ISAC):**
  Recipients and **subrecipients are strongly encouraged** to become a member of the MS-ISAC and/or EI-ISAC, as applicable. Membership is free. To register for MS-ISAC, please visit https://learn.cisecurity.org/ms-isac-registration. For more information, visit MS-ISAC (cisecurity.org). To register for EI-ISAC, please visit https://learn.cisecurity.org/ei-isac-registration. For more information, visit https://www.cisa.gov/election-security.

Example Projects

Below is a list of eligible project types supported by the SLCGP.

- MS-ISAC/CIS Cybersecurity Services
  - Email Security
  - Multi-factor Authentication (MFA)
  - Penetration Testing
  - Secure Network Access & Control
  - Vulnerability Management
  - CIS CyberMarket (CIS aggregate purchase offerings)

State Funding Priorities

Participation in Ohio Persistent Cyber Improvement (O-PCI) **is encouraged** but is not mandatory. Ideally, LGEs will enroll in O-PCI and complete the initial assessment within one year of receiving grant funds.

- **O-PCI Overview**
  The State of Ohio has created the O-PCI ecosystem for Ohio LGEs to educate, train, exercise, mentor, and improve in an integrated and persistent cycle supported with continual assessment. The O-PCI model is designed to position LGEs within Ohio to build and sustain the capacity to anticipate, adapt, withstand and, when necessary, recover from cyber aggression.

Below is a list of eligible project types supported by the SLCGP.

- Endpoint Detection and Response (EDR)
- Multi-factor authentication (MFA)
- Secure Mail
- Security Operations Center as a Service (SOCaaS)
- Vulnerability Management (VM)
- Cybersecurity aggregate purchase offerings available to Ohio LGEs through Ohio agencies.
- Security Services (i.e., professional services to implement cybersecurity software)
- Other (For LGE needs that do not fit neatly into the menu items listed above. Alignment with the Ohio Comprehensive Cybersecurity Plan is required.)

Some cybersecurity tools/services may be duplicated between services offered via MS-ISAC and Ohio. Should an LGE select one of these projects, they will be required to select the lowest price option.

LGEs with a need for net-new cybersecurity software and services may be eligible to purchase menu items listed at low, pre-negotiated rates and may receive subsidies.

LGEs who already have menu software and/or services included in their operating budgets will not be eligible to take advantage of the grant subsidies for those same services. However, at the end of their contract terms, the LGE may be able to benefit from pre-negotiated aggregate purchasing agreements, effectively lowering their future operating costs.

Funding Guidelines

Allowable Costs

Recipients must comply with all the requirements in 2 C.F.R. Part 200 (Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards).

Grant recipients and subrecipients may only use federal funds or funds applied to a cost share for the purposes set forth in this notice 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.

Unallowable Costs

For Round 2 SLCGP, grant funds may not be used for the following:

- Spyware
- Construction
- Renovation
- To pay a ransom
- For recreational or social purposes
- To pay for cybersecurity insurance premiums
- To acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities
- For any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the eligible entity that receives the grant or a local government within the jurisdiction of the eligible entity
- To supplant state or local funds
- For any recipient or subrecipient cost-sharing contribution

Application Process

To apply for the Round 2 SLCGP grant program, please download the Round 2 SLCGP Project Application Guidance from the CyberOhio Assisting Local Government Entities webpage.

LGEs will be required to submit the following information with their application for cybersecurity software and services:

- A project narrative containing a description of the cybersecurity software and services including the scope of the effort.
- This subgrant will reimburse migration costs up to $20,000 and requires a 20% cost share.
- See the appendices in this document for information regarding how and where to obtain software and services.

Please keep in mind the following key points when developing your application:

Eligible Applicants

For the Round 2 SLCGP Application Process, eligible applicants include Ohio LGEs. "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 (regardless of whether the council of governments is incorporated as a nonprofit corporation under state law), regional or interstate government entity, or agency or instrumentality of a local government;
b. An Indian tribe or authorized tribal organization; and
c. A rural community, unincorporated town or village, or other public entity.

Ineligible subrecipient entities include non-profit organizations and private corporations.

A public educational institution (e.g., elementary school, secondary school, or institution of higher education) is generally eligible to receive assistance under SLCGP if it is an agency or instrumentality of a state or local government under state and/or local law. In contrast, a private educational institution would not be eligible to receive SLCGP assistance because it is not an agency or instrumentality of a state or local government. "Assistance" means either funding, non-funding assistance (i.e., items, services, capabilities, or activities), or a combination of both. The eligibility of charter schools depends on the function of the charter school – it will be eligible if, and only if, it is an agency or an instrumentality of the state or local government. This will be a determination for the State Administrative Agency (SAA) to make (and to justify, if necessary), based on state or local law. The SAA for an SLCGP grant award is responsible for demonstrating the eligibility of each entity receiving assistance and should consult with FEMA if there is uncertainty regarding eligibility for a particular entity.

Project Requirements

Projects for cybersecurity software and services will have a maximum funding cap of $20,000 to purchase any combination of software/services that would provide them with the most benefit. The SLCGP requires LGEs to meet a 20% match requirement. However, LGEs who demonstrate economic hardship may apply for a FEMA waiver of the 20% match if they demonstrate hardship.

The performance period for this grant is December 1, 2024, through June 30, 2026. Approved projects must be completed within this timeframe.

Cost Share or Match

Eligible entities must meet a 20% cost share requirement for the Round 2 SLCGP. The recipient contribution can be cash (hard match) or third-party in-kind (soft match). Eligible applicants must agree to make available non-federal funds to carry out an SLCGP award in an amount not less than 20% of the total project costs (federal award amount plus cost share amount).

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. The non-federal cost share requirement cannot be matched with other federal funds, unless specifically authorized by the legislation governing that other source of federal funding.

Cost Share Waiver

The Secretary of Homeland Security (or designee) may waive or modify the non-federal share for an individual entity if the entity demonstrates economic hardship. The Homeland Security Act of 2002, as amended, requires Round 2 SLCGP recipients to provide a non-federal cost share of 20% if they are applying as a single entity (6 U.S.C. § 665g(m)(1)). 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. Click here for more information on applying for a FEMA economic hardship waiver.

Application Format and Submission

All project applications must be submitted by Monday, September 16, 2024, by 12:00 pm EDT. Please adhere to the following requirements:

- Complete and submit your application via the online form. Submission of the application in any other format will not be reviewed.

- **The form must be completed in one session.** The form will not timeout, but if you leave the form prior to submission (e.g., close the browser window) prior to submission, any data entered will be lost.

  Note: You can download a PDF of the sample form from the CyberOhio website. It is recommended that you use this PDF as a working document to ensure you have all the information required before you start completing the form online.

  Note: In the PDF version of the form, selections have been made throughout the form to display conditional questions (e.g., questions that are triggered by the answer to a previous question). When you fill out the form online, some questions represented in the PDF may not display in the form based on your LGE's answers to previous questions.

  Note: All applications *MUST* be submitted via the online form. Do NOT attempt to submit the application by sending a completed version of the PDF.

  Note: Your application will contain sensitive information about your LGE's computer security environment. Pursuant to §149.433 of the Ohio Revised Code, your application and any supporting documents are exempt from public disclosure.

- Please use the following naming convention when uploading supporting documentation:
  - R2 SLCGP SW-Svcs Narrative-LGE Name
  - R2 SLCGP SW-Svcs Budget-LGE Name
  - R2 SLCGP SW-Svcs Duo Contact Form-LGE Name
  - R2 SLCGP SW-Svcs CrowdStrike Contact Form-LGE Name

Round 2 SLCGP Project Application Instructions

Please use the following information as a basic instructional guide in completing the *Round 2 SLCGP Project Application.*

Note: Once you start filling out the application online, do not close your browser window until you have submitted the application.

Form Page 1 - Organizational Information

Provide the LGE information requested in this section.

Form Page 2 – Contact Information

Provide the contact information requested in this section.

Form Page 3 – LGE Information

Provide the information requested in this section.

Form Page 4 – Participation Requirements and Opportunities

Select Yes or No for the questions posed in this section.

Form Page 5 – Metrics

Select Yes or No for the questions posed in this section.

Form Page 6 – Projects

- Determine how many projects you are submitting and number them 1-5 in priority order. Project 1 should be your highest priority project, and Project 5 your lowest priority project. Every applicant will be required to submit at least one project.
- Projects 1 - 5
    - Complete the information required for your projects.
    - There will be options to upload supporting documentation such as contact forms, project narratives, and project budgets.
    - Funding Request Amount should be 80% of the Total Cost of the Project (unless you are applying for a FEMA economic hardship waiver).

Note: Funding is limited for this particular grant, but applicants are encouraged to submit projects that exceed the funding limit. This will help us to better understand the need and build a business case for future funding. Projects not funded in Round 2 may be considered for future grant cycles.

Form Page 7 - Finish Line

- At the end of the form, each LGE will be asked to provide an email address where the CyberOhio Team can request any additional supporting documentation or information required.
- When requesting additional information, the CyberOhio Team will send requests using a secure email system. Using this system, you will be able to create a username and password, and send any additional information needed in a secure manner.
- **Please DO NOT submit detailed security related documents via regular email, as it is not a secure method for transmitting sensitive information.**

Application Resources

CyberOhio Assisting Local Government Entities page

Online Cybersecurity Software& Services Application Form

CISA's Cyber Hygiene Information Page

FEMA Economic Hardship Waiver Information Bulletin

https://www.cisa.gov/election-security

https://learn.cisecurity.org/ei-isac-registration

https://learn.cisecurity.org/ms-isac-registration

https://sam.gov/content/entity-registration

MS-ISAC (cisecurity.org)

Nationwide Cybersecurity Review (cisecurity.org)

OARnet

Ohio Persistent Cyber Improvement (O-PCI)

Points of Contact

For Grant Application questions and technical assistance, please contact:

CyberOhio Team cyberohio@governor.ohio.gov

Carolyn Jordan, SLCGP Program Manager cjordan@dps.ohio.gov

Appendix A – Cybersecurity Tools and Services Minimum Requirements

With SLCGP funds, Ohio has established a grant process and has set aside over $7.3 million to be used to help support LGE purchases of cybersecurity software and services.

Note: If you are interested in getting support for cybersecurity software and services, please apply before the deadline. Even though there are limited funds available with this program, LGEs who apply but are not selected for this program may be considered for upcoming grant programs. Demand for this program will help us more accurately determine future funding requirements and allocate future resources accordingly.

The HSAC-Cyber Full Planning Subcommittee has developed a menu of security software and services offerings. LGEs should complete a risk assessment to determine the needs and priorities of their particular organization.

Below is a list of eligible project types supported by the SLCGP.

- Endpoint Detection and Response (EDR)
- Multi-factor authentication (MFA)
- Secure Mail
- Security Operations Center as a Service (SOCaaS)
- Vulnerability Management
- Security Services (i.e., professional services to implement cybersecurity controls)
- Other (For LGE needs that do not fit neatly into the menu items listed above. Alignment with the Ohio Comprehensive Cybersecurity Plan is required.)

Note: The State of Ohio does not endorse any of the vendors listed in this document. The vendors are provided as examples of industry leaders in their fields. LGEs can select to work with any vendor who best suits their particular needs and provides a product or service that meets the minimum requirements outlined below.

Endpoint Detection and Response (EDR)

Sample of Potential Vendors with Comparable Eligible Services

- Carbon Black
- CrowdStrike
- SentinelOne

Minimum Requirements for EDR

- Real-time malware detection and prevention to detect and block known malware in real-time.
- Behavioral Analysis to detect and block suspicious activities and malware based on their behavior in addition to signature-based detection.
- Built-in firewall to monitor and control incoming and outgoing network traffic to prevent unauthorized access and data exfiltration.

- Centralized management to manage and monitor endpoints from a single console and simplify configuration, deployment, monitoring and updating endpoints.
- Automated updates and patch management to update definitions, signatures and software patches.
- Device Control for defining and enforcing policies governing the use of removable storage devices to prevent data leakage and malware.
- Reporting and Logging to facilitate tracking and investigating security events.

Multi-Factor Authentication (MFA)

Sample of Potential Vendors with Comparable Eligible Options

- Akamai
- Cisco Duo
- ManageEngine ADSelfService Plus

Minimum Requirements for MFA

- Support for at least two different types of authentication factors:
    - Something a user knows (a PIN or password).
    - Something users has (a smartphone, token, etc.).
    - Something user is (biometric data like a fingerprint).
- Centralized management capabilities that enable administrators to configure authentication polices, monitor authentication events, and enforce security controls across the organization from a single console.
- Strong encryption algorithms and applications that employ industry standard security protocols to protect authentication data during transmission and storage.
- Integration with identity management systems, directory services (e.g., LDAP, Active Directory), and single sign-on solutions.
- Comprehensive auditing and reporting features to help track authentication activities, detect suspicious behavior, and investigate security incidents.

Secure Mail

Sample of Potential Vendors with Comparable Eligible Options

- Abnormal Security
- Microsoft
- Trend Micro

Minimum Requirements for Secure Mail

- Ability to encrypt all email communications, including message content and encryption, using strong encryption algorithms to protect against unauthorized access.
- Support TLS encryption during the transmission of emails between mail servers to ensure messages are encrypted with in transit over the internet.

- Support of end-to-end encryption (E2EE) where the message content is encryption on the sender's device and decrypted only on the recipient's device, protecting message content from the email service provider.
- Support strong authentication mechanisms such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting, and Conformance (DMARC).
- Strong authentication mechanisms including MFA and password policies or integration with identity management systems, directory services (e.g., LDAP, Active Directory).
- Include built in malware and anti-phishing features to detect and block malicious attachments, links and content.
- Comprehensive logging and auditing capabilities to monitor email activities, track changes, and investigate security incidents.

Security Operations Center as a Service (SOCaaS)

Sample of Potential Vendors with Comparable Eligible Options

- Agile Blue
- Artic Wolf
- Secure Works

Minimum Requirements for SOCaaS

- Provide 24/7 monitoring and incident response capabilities to detect and respond to security incidents as they occur.
- A team of skilled and experienced security analysts trained in threat detection, incident response, and forensic analysis.
- Employ advanced threat detection technologies, e.g., behavior analytics, anomaly detection and threat intelligence integration to identify and mitigate sophisticated cyber threats in real-time.
- Monitor a wide range of security events and logs from various sources, including network devices, servers, endpoints, applications, and cloud environments.
- Integration with existing security technologies and infrastructure (e.g., Security Information and Event Management (SIEM) systems, endpoint detection and response (EDR) solutions, and threat intelligence feeds.
- Incident reporting communication including alerts, notifications, and incident response coordination that are timely and accurate.

Vulnerability Management

Sample of Potential Vendors with Comparable Eligible Options

- Forta
- Rapid 7
- Tenable

Minimum Requirements for Vulnerability Management

- Automatically discover and inventory devices, systems, applications and network assets within the organizations infrastructure.
- Ability to regularly scan for vulnerabilities across the organization's assets.
- Risk assessment reports and dashboards that summarize the organization's vulnerability posture, trends, and recommendations for risk mitigation.
- Prioritize vulnerabilities based on their severity, potential impact, and exploitability.
- Integration with patch management systems.
- Customizable scanning and scheduling to accommodate different types of assets, network segments and compliance requirements.
- Integration with IT infrastructure such as asset management systems, ticketing systems, and SIEM solutions.
- Continuous monitoring of the organization's infrastructure to detect new vulnerabilities, configuration changes, and emerging threats in real-time.
- Maintain an up-to-date comprehensive database of known vulnerabilities, including severity, affected systems, available patches and remediation techniques.
- Automated vulnerability scanning, ticket generation, and workflow orchestration.

Security Services

Note: Security Services can be a separate project, or a line item in any of the projects that you submit.

Sample of Potential Vendors with Comparable Eligible Options

- Cyber Pop-up
- Parallel Technologies
- Tabernacle Technology Solutions

Examples of Security Service Offerings

- Provide qualified and experienced cybersecurity professionals who are knowledgeable of applicable compliance frameworks, and who can:
    - Assist in building and/or maintaining a cybersecurity program.
    - Assist in planning and implementing security controls.
    - Conduct risk and vulnerability assessments.

Cyber Pop-up

Cyber Pop-up is a Google-backed cybersecurity services company dedicated to securing communities, businesses, and nonprofits with enterprise-grade security on a small business budget. With a mission to make cybersecurity accessible to all, Cyber Pop-up offers a platform to connect you to gold-standard vetted cybersecurity experts with 30+ domains of expertise.

Contact:

https://www.cyberpopup.com/get-quote

Parallel Technologies

The Parallel Technologies approach is to meet with the client to thoroughly assess their security needs. Based on this assessment, they then bring multiple partners to the table who can fulfill the specific needs uncovered during the evaluation. This collaborative approach ensures that Parallel Technologies clients receive the most comprehensive and tailored cybersecurity solutions available.

Contact:

Ashleigh Walsh awalsh@ParallelTech.Com 614-718-5110

www.paralleltech.com

Tabernacle Technology Solutions

TTS Technologies, headquartered in Columbus, Ohio, is a leading cybersecurity company dedicated to providing comprehensive cybersecurity services tailored for organizations with fewer than 500 employees. Our mission is to protect small and mid-sized enterprises, agencies, and non-profits from evolving cyber threats by offering a robust suite of security solutions: This includes but is not limited to threat detection, risk assessments, vulnerability management, incident response, and compliance management. At TTS Technologies, we leverage cutting-edge technology and expert knowledge to create customized security strategies that safeguard our clients' digital assets, ensuring business continuity and peace of mind. Serving all 50 states, we are committed to delivering top-tier cybersecurity solutions nationwide."

Contact:

Logan Edmonds sales@tabernacle.tech 614-468-8649

https://tabernacle.tech

Security Product Matrix

Cyber Security Software & Services/Sources	CIS CyberMarket	DAS Cooperative Purchasing Agreement	Management Council via the ITCs	OARnet	Buy Direct
Endpoint Protection	CrowdStrike	CrowdStrike* Form		Carbon Black	SentinelOne, or Other
Multi-Factor Authentication	Akamai	Cisco Duo* Form	Cisco Duo *(K-12 only)*		ManageEngine ADSelfService Plus, or Other
Secure Mail	Duo Circle				Abnormal Security, Microsoft, Trend Micro, or Other
Security Operations Center as a Service (SOC)					Agile Blue, Artic Wolf, Secure Works, or Other
Vulnerability Management	Tenable			Tenable	Forta, Rapid 7, or Other
Cybersecurity Services CISO Advice, Implementation & Planning Services)					Cyber Pop-up, Parallel Technologies, Tabernacle, 3C Technology Solutions, or Other

* If you would like to use DAS cooperative purchasing agreements, please complete the appropriate form(s) and submit them with your application. These forms can be downloaded from CyberOhio.gov.

Appendix B –Purchasing Options

Purchasing Services through CIS

Note: All of the software and services listed on the CIS CyberMarket are elligible projects for consideration under this grant.

https://www.cisecurity.org/services/cis-cybermarket

Purchasing Services through OARnet

OARnet Contact:

Letha Butcher lbutcher@oar.net 614-292-9545

Purchasing Services via DAS Cooperative Purchasing Agreements

Purchasing Cisco Duo under the DAS Cooperative Purchasing Agreement

Complete the **Duo Services Contact Form** and upload it with your application. This form is located on the CyberOhio website.

Purchasing CrowdStrike under the DAS Cooperative Purchasing Agreement

Complete the **CrowdStrike Services Contact Form** and upload it with your application. This form is located on the CyberOhio website.