



State of New Jersey
Federal Fiscal Year 2023
State and Local Cybersecurity Grant Program
Application for Cybersecurity Resources



A. INTRODUCTION

The State and Local Cybersecurity Grant Program (SLCGP) is a federal grant program funded by the U.S. Department of Homeland Security (DHS) that aims to improve cybersecurity in state and local governments. In New Jersey, the SLCGP is administered by the NJ Office of Homeland Security and Preparedness (NJOHSP) through its NJ Cybersecurity and Communications Integration Cell (NJCCIC). The overall goal of the SLCGP is to make state and local government organizations more resilient to cyber threats.

For Federal Fiscal Year (FFY) 2023, SLCGP funds received by NJOHSP to administer the grant will be used to provide hardware, software, and services to state and local government agencies through the NJCCIC. To apply for these grant resources, please complete the application below.

B. ELIGIBILITY

All New Jersey state and local government entities are eligible to apply for NJ FFY 2023 SLCGP resources.

“Local government” entity is defined in 6 U.S.C. § 101(13) as:

- (1) 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;
- (2) An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and
- (3) A rural community, unincorporated town or village, or other public entity.

C. LOCAL CONSENT AGREEMENT

Local government entities (e.g., municipalities, counties, school districts, etc.) must also complete and submit the NJ SLCGP Local Consent Agreement. The Local Consent Agreement can be found at www.cyber.nj.gov/slcgp.

D. APPLICATION DEADLINE

To be eligible to receive FFY23 SLCGP resources, this application, and the local consent agreement, if applicable must be received by the NJCCIC by **December 8, 2023, 11:59:59 PM**.

E. CONFIDENTIALITY

As the information you provide in your application will inherently include administrative or technical information which, if disclosed would jeopardize computer security, this application is deemed confidential and exempt from Open Public Records Act (OPRA) disclosure. Further, as the SLCGP Planning Committee operates under the New Jersey Domestic Security Task Force (DSPTF), in accordance with the NJ Domestic Security Preparedness Act, N.J.S.A. APP. A: 9-74, any record held, maintained, or kept on file shall be treated and deemed as “\records of the Task Force exempt from public disclosure under OPRA.”



**State of New Jersey
Federal Fiscal Year 2023
State and Local Cybersecurity Grant Program
Application for Cybersecurity Resources**



F. ORGANIZATION/APPLICANT INFORMATION

Organization Name: Waterford Township School District Organization Type: Local Government Entity
 Organization Mailing Address: 106 Old Whitehorse Pike
 City: Waterford County: Camden State: NJ NJ Zip Code: 08089
 TaxID: 21-6000115

Executive Sponsor/Authorizing Official

Full Name: Dan Fox Title: Business Administrator
 Email Address: dfox@wtsd.org Work Phone: 856-767-8293 ext 5012

Primary Technical Point of Contact

Full Name: Ed Leypoldt Title: Director of Technology
 Email Address: eleypoldt@wtsd.org Work Phone: 856-768-8465

Primary Organization Point of Contact for this SLCGP Grant Request

Full Name: Ed Leypoldt Title: Director of Technology
 Email Address: eleypoldt@wtsd.org Work Phone: 856-768-8465

G. ABOUT YOUR ORGANIZATION

- (1) Main Website Address: www.wtsd.org
- (2) Organization Domains: wtsd.org
- (3) Organization Public IP Addresses/Ranges: 50.206.210.49-.54
- (4) Total Number of Supported Users (employees and contractors only, **do not include students**): 210
- (5) Total Number of staff members dedicated to IT and/or Cybersecurity (employees and contractors): 2
- (6) Annual Operating Budget for Organization: \$170,000.00
- (7) Annual Cybersecurity Budget: \$18,000
- (8) Total Number of Physical Sites/Locations: 3

H. ABOUT YOUR IT/OT ENVIRONMENT

- (1) Total Number of laptop and desktop computers: 230
- (2) Total Number of servers: 1
- (3) Are your IT/OT environments managed by in-house staff or outsourced to a third party? In-House Staff
- (4) If outsourced, please provide the name of the third-party and contact information for a technical point of contact.

Third-Party IT Service Provider Company Name:
 Point of Contact: Title:
 Email Address: Work Phone:



**State of New Jersey
Federal Fiscal Year 2023
State and Local Cybersecurity Grant Program
Application for Cybersecurity Resources**



- (5) Do you use public cloud providers to host critical information technology systems and sensitive information? Yes
- (6) If yes, please provide information on the cloud service providers used (e.g. Amazon, Google, Microsoft). Include information with respect to IaaS, PaaS, and SaaS cloud services.
Google, SAAS
- (7) In addition to information technology assets, does your organization also implement and manage operational technologies? Operational technologies (OT) consist of computing systems used to help manage, monitor, and control physical operations such as building management systems, public transportation systems, public safety systems, water and wastewater treatment systems, public lighting systems, electrical generation and transmission, etc.? Yes
- (8) For your IT and OT environments, please list the operating systems and versions in use.
Windows 10, Windows 11, Windows Server
- (9) What is your biggest motivation(s)/ reason(s) to apply for this grant opportunity?
We need to add additional MFA capabilities on our desktops as well as replace our outdated Firewall. We implement 2FA for Google but we do not have the monetary resources to implement it on our desktops

CYBERSECURITY CAPABILITIES

Please tell us about the following cybersecurity capabilities as it pertains to your IT/OT environments and if you are requesting these capabilities for your organization as part of this grant opportunity. If you have questions about any of these capabilities, please contact: njccic@cyber.nj.gov.

I. CYBERSECURITY GOVERNANCE (GV):

Does your organization have a published set of policies that establish the required behaviors and controls necessary to protect your information technology resources, secure personal information, safeguard privacy, and maintain the physical safety of individuals?

- (1) Are you interested in receiving cybersecurity policy templates to help you develop your cybersecurity policies? Yes
- (2) Do you have a cybersecurity incident response plan? Yes
- (3) If yes, when was the last time the plan was exercised? scheduled
- (4) If no, are you interested in assistance in developing a plan?
- (5) Are you interested in participating in cybersecurity incident table-top exercises? Yes
- (6) .GOV top-level domains (TLDs) provide an added level of trust and security to government websites and services. They are free and only available to validated government organizations. If you currently use a .ORG, .COM, .NET, or .US top-level domain (TLD) for your organization, are you interested in receiving information and assistance in migrating your domains to a .GOV TLD?

No



**State of New Jersey
Federal Fiscal Year 2023
State and Local Cybersecurity Grant Program
Application for Cybersecurity Resources**



J. CYBERSECURITY RISK MANAGEMENT (RM):

What is the date of your most recent cybersecurity risk assessment? 2019

As an applicant for the NJ SLCGP:

- (1) You will be provided with directions on completing the NJCCIC Cybersecurity Program Controls Assessment (CPCA). The CPCA is a secure online no-cost self-assessment available to eligible organizations through the NJCCIC portal. The results of the CPCA will be used to help inform SLCGP investment decisions.
- (2) You will also be provided with access to an NJCCIC-administered cybersecurity ratings and continuous risk monitoring service that provides organizations with an easy-to-understand assessments of their cybersecurity posture.

To receive access to the above cybersecurity risk assessment platforms, please provide a point of contact in your organization.

Full Name: Ed LEypoldt

Title: Director of Technology

Email Address: leypoldt@wtsd.org

Work Phone: 856-768-8465

K. CYBERSECURITY RESILIENCE (RE):

The following products and services are offered to NJ State and Local government organizations as part of the FFY23 SLCGP:

RE-1: Advanced Endpoint Protection

The NJCCIC Advanced Endpoint Protection (AEP) solution provides comprehensive visibility into endpoint activity, advanced threat detection, and automated response. It consists of a lightweight endpoint agent and scalable cloud-native management and administration platform that leverages artificial intelligence (AI) and machine learning (ML) to detect and respond to threats on endpoints in real time. The NJCCIC AEP solution includes several modules that together provide a comprehensive, integrated, and proactive approach to security for an organization's laptops, desktops, and servers. This solution also provides for 24/7 managed detection and response services. More information about the NJCCIC AEP solution can be found at www.cyber.nj.gov/slcgp.

- (1) Do you currently have an Endpoint Detection and Response (EDR) solution implemented? Yes
- (2) If yes, please provide information on your EDR solution and its license expiration. As FFY23 funds are limited, this information will be used to prioritize resource needs and plan for FFY24 investments. Malwarebytes EDR renewed each year
- (3) Are you interested in implementing the AEP solution in your environment? No
- (4) If yes, how many AEP licenses are you requesting?

The NJCCIC AEP includes 4-years of EDR and managed detection and response services. As SLCGP funds are intended to act as seed money and are limited, the NJCCIC has developed a resource distribution



State of New Jersey
Federal Fiscal Year 2023
State and Local Cybersecurity Grant Program
Application for Cybersecurity Resources



plan that attempts to fulfill as many NJCCIC AEP requests as possible to assist New Jersey local government entities with managing and reducing systematic cyber risk. Thus, if your request for the NJCCIC AEP is approved, you will be required to contribute to a cost match according to the following schedule.

- Year 1: no AEP cost to awardee.
- Year 2: 20% AEP cost match.
- Year 3: 30% AEP cost match.
- Year 4: 40% AEP cost match.

RE-2: Web Application Security

The NJCCIC-offered cloud-based Web Application Firewall (WAF) is a scalable, easy-to-use, and customizable security solution that helps protect government websites and web applications from a variety of cyber threats. It acts as a protective barrier between an organization's web applications and the internet, analyzing incoming traffic and blocking malicious requests. By providing protection against a wide range of threats and vulnerabilities, the WAF helps ensure the security, compliance, and performance of e-government web applications and processes. More information about the NJCCIC WAF solution can be found at www.cyber.nj.gov/slcgp.

- (1) Are you interested in implementing the WAF to protect your websites and web applications? No
- (2) If yes, how many websites and web applications do you manage?
- (3) Do you currently have a WAF solution implemented? No
- (4) If yes, please provide information on your WAF solution and its license expiration. As FFY23 funds are limited, this information will be used to prioritize resource needs and plan for FFY24 investments.

RE-3: Identification and Authentication Protection

Multi-factor authentication (MFA) is a security process in which a user is only granted access to a system after successfully presenting two or more authentication factors. The three most common kinds of factors are:

- Something you know - Like a password, or a memorized PIN.
- Something you have - Like a smartphone, or a hardware token.
- Something you are - Like a fingerprint, or facial recognition.

To help organizations secure remote and privileged access logins, organizations may request MFA hardware tokens for use cases where other MFA methods (SMS token codes or smartphone authenticator apps) are not a viable solution. More information about the SLCGP FFY23 MFA offering can be found at www.cyber.nj.gov/slcgp.

- (1) Have you implemented MFA for remote access to organizational systems and applications? Yes
- (2) Have you implemented MFA for privileged access to organizational systems and applications? No
- (3) If you have use cases where SMS token codes or smartphone authenticator apps are not a viable method, please provide the number of MFA hardware tokens you are requesting: 210



State of New Jersey
Federal Fiscal Year 2023
State and Local Cybersecurity Grant Program
Application for Cybersecurity Resources



L. WORKFORCE DEVELOPMENT (WD)

In order to ensure SLT personnel are trained in cybersecurity commensurate with roles and responsibilities, SLCGP funds will be utilized to develop, implement, and deliver online and in-person cybersecurity training offerings. More information about the SLCGP FFY23 training offerings and resources can be found at: www.cyber.nj.gov/slcgp.

WD-1: Training Classes

High-quality, hands-on, in-person and remote online training covering a wide range of cybersecurity topics, including but not limited to: network, application, and cloud security; IT and cyber operations; incident response; threat and vulnerability management; and more.

Please provide a count of the number of IT and cybersecurity personnel in your organization that would be interested in receiving training classes according to their IT and cybersecurity skill levels. 2

WD-2: Virtual Cyber Range

The cyber range is an online cybersecurity training and simulation platform administered by the NJCCIC.

- (1) Please provide a count of the number of IT and cybersecurity personnel in your organization that you would like to provide access to the virtual cyber range. 2

WD-3: Security Awareness Training

Security Awareness Training is a cybersecurity educational program designed to help organizations educate their employees about various cyber threats and improve their security posture. It aims to reduce the human risk factor in cybersecurity by cultivating a security-conscious culture.

- (1) Do you currently provide security awareness training to your employees? Yes
- (2) If your answer is no, and you would like to receive tailored online cybersecurity awareness training, please enter the number of employees that would require this training.

APPLICATION SUBMISSION

I understand that the submission of this application does not guarantee that I will receive the resources requested. I understand that each application received will be evaluated in accordance with DHS and FEMA SLCGP requirements and those of the NJ SLCGP Planning Committee.

Full Name: Ed Leypoldt
Email Address: eleypoldt@wtsd.org
Signature: Ed Leypoldt
(eleypoldt@wtsd.org, 2023-10-10 15:47:23)

Title: Director of technology
Work Phone: 856-768-8465







SLCGP FFY23 Resource Request Application

Final Audit Report

2023-11-27

Created:	2023-11-27 (Eastern Standard Time)
By:	Mike Geraghty (mgeraghty@cyber.nj.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAiUPkYMCRg6ppq0Lkf0F25YKJUpteHs8YU

"SLCGP FFY23 Resource Request Application" History

-  Web Form created by Mike Geraghty (mgeraghty@cyber.nj.gov)
2023-11-12 - 10:12:26 AM EST
-  Web Form filled in by Ed Leypoldt (eleypoldt@wtsd.org)
2023-11-27 - 3:49:54 PM EST
-  Email verification link emailed to Ed Leypoldt (eleypoldt@wtsd.org)
2023-11-27 - 3:49:56 PM EST
-  Email viewed by Ed Leypoldt (eleypoldt@wtsd.org)
2023-11-27 - 3:50:08 PM EST
-  E-signature verified by Ed Leypoldt (eleypoldt@wtsd.org)
2023-11-27 - 3:50:10 PM EST
-  Agreement completed.
2023-11-27 - 3:50:10 PM EST



Powered by
Adobe
Acrobat Sign



State of New Jersey
Federal Fiscal Year 2023
State and Local Cybersecurity Grant Program
Local Consent Agreement



I, Full Name: Ed Leypoldt Work Title: Director of Technology
a duly authorized official of Local Governmental Entity: Waterford Township School District
(e.g., municipality, county, school district, or subdivision thereof), located at,
Address: 1106 Old Whitehorse Pike
City: Waterford Works County: Camden State: NJ Zip Code: 08089
, hereby wish to participate in and consent to the State of New Jersey's State Administrative Agency (SAA), namely the New Jersey Office of Homeland Security & Preparedness (NJOHSP), undertaking the following acts in accordance with the State and Local Cybersecurity Grant Program (SLCGP) for Federal Fiscal Year (FFY) 2023, Funding Opportunity Number DHS-23-137-000-01, as authorized by Section 2220A of the Homeland Security Act of 2002, as amended (Pub. L. No. 107-296) (6 U.S.C. § 665g):

1. Retain and pass through to local government entities at least 80% of the State of New Jersey's FFY 2023 SLCGP grant award of \$6,858,348.00 in the form of cybersecurity products and services; and
2. Utilize the estimated \$6,858,348.00 in SLCGP funds for FFY 2023 as follows:
 - o Approximately \$25,000 for Project 1: Cybersecurity Governance and Planning
 - o Approximately \$150,000 for Project 2: Cybersecurity Resilience Assessments
 - o Approximately \$6,275,348 for Project 3: Cybersecurity Resilience (Endpoint, Application, and Identity and Authentication security)
 - o Approximately \$408,000 for Project 4: Cybersecurity Workforce Development

This consent is given with the understanding that Local Government Entity is receiving cybersecurity hardware, software, and/or services in lieu of funds from the SLCGP. This consent is only effective for the Federal Fiscal Year (FFY) 2023 SLCGP Funds.

Email Address: eleepoldt@wtsd.org

Daytime Phone Number: 856-768-8465

Signature: Ed Leypoldt
Ed Leypoldt (NJOHSP, 2021.5.21 ES)







SLCGP FFY23 Local Consent Form

Final Audit Report

2023-11-27

Created:	2023-11-27 (Eastern Standard Time)
By:	Mike Geraghty (mgeraghty@cyber.nj.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAYmIG6IAAnE6nhMfvIW1Ri4eYY93pD1OaP

"SLCGP FFY23 Local Consent Form" History

-  Web Form created by Mike Geraghty (mgeraghty@cyber.nj.gov)
2023-11-12 - 9:18:03 AM EST
-  Web Form filled in by Ed Leypoldt (eleypoldt@wtsd.org)
2023-11-27 - 3:29:12 PM EST
-  Email verification link emailed to Ed Leypoldt (eleypoldt@wtsd.org)
2023-11-27 - 3:29:14 PM EST
-  Email viewed by Ed Leypoldt (eleypoldt@wtsd.org)
2023-11-27 - 3:29:28 PM EST
-  E-signature verified by Ed Leypoldt (eleypoldt@wtsd.org)
2023-11-27 - 3:29:32 PM EST
-  Agreement completed.
2023-11-27 - 3:29:32 PM EST



Powered by
Adobe
Acrobat Sign

FISCAL YEAR 2024 NOTIFICATION OF GRANT AWARD
 NJ High Impact Tutoring Competitive COMPETITIVE Grant

Date: 12/15/2023

To: Chief School Administrator

Agency Name/Code: Waterford Township (075560)
 County Name/Code: Camden
 DUNS Number:

Attention
 Board
 Secretary:
 Board Action
 Received

From: New Jersey Department of Education
 PO Box 500
 Trenton, NJ 08625
 Office of Grants Management

Purpose:

Your Grant application for the programs indicated below, which was received by the New Jersey Department of Education (NJDOE) in substantially approvable form on 11/3/2023, has been reviewed by the offices listed above and recommended for funding for fiscal year 2024 pending the availability of funds.

PROGRAM DURATION: START: October 11, 2023 END: August 31, 2024

PROGRAM NAME	PROGRAM DESCRIPTION	GRANT NUMBER	FY 2024 AWARD AMOUNT	FAIN	CFDA
NJ High Impact Tutoring Competitive	Pursuant to Title IV, Part B of the Every Student Succeeds Act (ESSA), the Nita M. Lowey 21st Century Community Learning Centers (21st CCLC) program, a federally funded program, supports out-of-school time (OST) programs in New Jersey, which includes befo	E2400284	97000		
Total Amount Obligated to LEA			\$97,000		

Total Amount Committed to LEA			\$97,000		
-------------------------------	--	--	----------	--	--

Pursuant to EDGAR, 34 CFR Part 76.708, a local education agency (LEA) may begin to obligate these funds the later of the following dates:

1. The program duration start date indicated above or
2. The date the application was received by the State in substantially approvable form.

We wish you success in the implementation of this educational program. If you have questions regarding this grant award, please contact the Office of Grants Management at (609) 663-6974

[Return To Application Select](#)



Sample

This Letter Agreement outlines the terms under which Delta-T Group North Jersey Inc. ("Delta-T") will refer interim professionals to **Sample School District** ("Client"). This Agreement shall commence on the date first stated above and continue for an initial term of one (1) year or such shorter period in the event that the parties execute a more comprehensive agreement. This Agreement shall automatically renew for successive 1-year terms. This Agreement may be terminated without cause by either party upon thirty (30) days written notice to the other party.

The professionals referred to Client through Delta-T are Independent Contractors ("Contractor(s)"). Delta-T requires, as part of our arrangement with the Contractors, that each Contractor sign an operating agreement with Delta-T before they are contracted out to a facility such as yours. You must immediately notify Delta-T of any and all job offers made to Contractors that were referred to you by Delta-T. Delta-T's Temp to Perm Policy is that from the time Client notifies Delta-T of its intention to hire or contract directly with a Contractor, the Contractor must work seven hundred and fifty (750) hours through Delta-T at a Client facility before the Contractor may accept a position with Client. Client may hire or contract with Contractor without meeting this 750-hour requirement by making payment to Delta-T the sum of \$7,500.00 or a sum equal to 1/3 of the total compensation package (including bonuses and fringe benefits) offered to Contractor, whichever sum is greater. This 750-hour requirement remains in effect for a period of six (6) months after the last date of a Contractor's assignment with Client.

All invoices for services are due net thirty (30) days and will be forwarded to your attention. Client shall notify Delta-T of any disputed amounts within fifteen (15) business days of Client's receipt of invoice. Invoices or amounts not disputed within this time period shall be deemed accepted by Client. Client shall not withhold payment of any undisputed amounts. All outstanding balances are subject to statutory interest and a late charge. If payment is not made in accordance with these terms, Delta-T will cease referring Contractors to Client and Contractors will not be released for referral until payment is received in full. Delta-T shall be entitled to recover reasonable attorneys fees in the event legal action is necessary to enforce the terms of this Letter Agreement.

Thank you for choosing Delta-T. We look forward to continuing our business relationship. If these terms are acceptable, please sign and return this to our office as soon as possible.

Respectfully,
Scott R. McAndrews, EVP

Scott R. McAndrews

By: _____
Signature of Client Representative

Date

Print Name and Title