

**CALIFORNIA GOVERNOR'S OFFICE OF EMERGENCY SERVICES (Cal OES)
2024 STATE & LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP)
FY22 & FY23 PROGRESS REPORT**

3650 Schriever Avenue • Mather, CA 95655

Please email your completed progress report to your Grants Analyst by December 31, 2025.

SUBRECIPIENT:	FIPS #:
Report Prepared By: Amber Mena	Email Address: Amber.Mena@vc3.com
Authorized Agent: Sheryl Alvernaz	Email Address: salvernaz1@gmail.com
<u>FY2022 FEDERAL SUBAWARD</u>	
Total FY22 Funded:	Balance: \$23,026
M&A Amount Funded:	Balance: \$1816
<u>FY2023 FEDERAL SUBAWARD</u>	
Total FY23 Funded:	Balance: \$48,620
M&A Amount Funded:	Balance: \$1816

This Progress Report should reflect your use of FY22 and FY23 funding for your SLCGP Subaward. Please note that resources and activities supporting the program must be represented in the specified tables respective to the funding year your expenses were drawn from.

1. Since the time of your SLCGP Application being approved, have there been any problems with the implementation of your proposed projects? If so, please describe below.

Yes – Due to funding delays and turnover, Hardware implementations have been delayed.

2. Do you anticipate any issues in completing your proposed projects or fully expending your obligated funding? If so, please describe below. *(Please remember FY22 funds need to be fully expended by August 31, 2026.)*

No, all funding will be required to sustain support.

3. Please describe any technical assistance you need from Cal OES.

None

FY22 CYBERSECURITY PROGRAM METRICS

In the tables provided, please provide information about how your SLCGP projects address the Cybersecurity Metrics listed below. If your projects do not address one or more of the metrics, please enter N/A.

FY22 CYBERSECURITY PROGRAM METRICS			
Program Goal	Program Objective	Associated Metrics	Metric Description (details, source, frequency)
Goal 1: Develop and establish baseline governance structures across California's jurisdictions, including developing, implementing, or revising cybersecurity plans to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.	1.1: Establish cybersecurity governance structures and implement a program to evaluate maturity of the cybersecurity program aligned to Cybersecurity Performance Goals established by CISA and the National Institute of Standards and Technology (NIST).	1.1.1: Jurisdictions have established and documented a uniform cybersecurity governance structure that is accountable to organizational leadership and works together to set the vision for cyber risk management.	Jurisdictional Chief Information Officer, or equivalent position, quarterly reporting to Cal-CSIC (target 90%).
		1.1.2: Jurisdictions have identified senior officials to enable whole-of-organization coordination on cybersecurity policies, processes, and procedures.	Senior officials are identified in the jurisdiction's cyber incident response plan under objective 1.2 (target 90%).
	1.2: Develop, implement, or revise, and test cybersecurity plans, including cyber incident response plans, with clearly defined roles and responsibilities.	1.2.1: Jurisdictions develop, implement, or revise, and exercise their cyber incident response plans every two years.	Jurisdictional biennial reporting to Cal-CSIC and within 30 days of completing the cyber exercise target 90%. Jurisdictional biennial reporting to Cal-CSIC and within 30 days of completing or revising the cyber incident response plan target 90%.
		1.3: Asset (e.g., devices, data, software) protections and recovery actions are prioritized based on the asset's criticality and business value.	1.3.1: Jurisdictions document their prioritization of systems and network functions and set them for reconstitution according to their impact to essential functions.

Subrecipient Projects Supporting FY22 Cybersecurity Program Goal 1			
Project Letter & Title	Program Goal/Objective Supported	Project Description – including anticipated deliverable	Status of Project (not started, in progress, completed)
Project A FY22: Risk Assessment and network evaluation	1.1/ 1.2/1.3	Assess needs of Spalding CSD and develop plan to bring Cyber Security within compliance. This will include planning for new hardware and software for workstations, as well as assessing	In progress

		potential cyber risks and develop a plan to address those risks. (Funding FY22 \$613)	
Project A FY22: Risk Assessment and network evaluation	1.1/ 1.2/1.3	Ongoing process and procedure documentation and developing protocols for day-to-day data interaction and cyber/data hygiene . Regular risk assessment cadence with MSSP for updates on progress. (Funding FY22 \$9,083)	In progress
Project E FY22: Grants & Contract Administration	1.1	Time and expenses for Spalding CSD Grant & MSSP Contract Administration; enhancing organizational administration and capacity for managing the grant. (Funding FY22 \$1,816)	In progress

FY22 CYBERSECURITY PROGRAM METRICS

Program Goal	Program Objective	Associated Metrics	Metric Description (details, source, frequency)
Goal 2: Government jurisdictions across California understand their current cyber security posture and areas for improvement based on continuous testing, evaluation, and structured assessments.	2.1: Physical devices and systems, as well as software platforms and applications, are inventoried.	2.1.1: Jurisdictions establish and regularly update asset inventory.	Assets are inventoried annually by jurisdictions (target 90%).
	2.2: Cybersecurity risk to each jurisdiction's operations and assets are documented and understood.	2.2.1: Jurisdictions conduct an annual cyber risk assessment to identify cyber risk management gaps and areas for improvement once a year.	Jurisdictional annual assessment (target 90%).
	2.3: Vulnerability scans are performed, and a risk-based vulnerability management plan is developed and implemented by each jurisdiction.	2.3.1: Jurisdictions participate in CISA's Vulnerability Scanning service, part of the cyber hygiene program or equivalent service provided by the state or commercial provider.	Number of jurisdictions that participate in vulnerability scanning services (target 100%), measured quarterly.
		2.3.2: Jurisdictions effectively manage vulnerabilities by prioritizing migration of high impact vulnerabilities and those most likely to be exploited.	Methods for tracking and managing vulnerabilities are documented by jurisdictions (target 90%).
	2.4: Capabilities are in place across each jurisdiction to monitor assets to identify cybersecurity events.	2.4.1: Jurisdictions are able to analyze network traffic and activity transiting or traveling to or from information systems, applications, and user accounts to understand baseline activity and identify potential threats.	Personnel or systems are in place to analyze jurisdictions' network traffic and activity (target 90%).
	2.5: Processes are in place across each jurisdiction to action insights derived from deployed capabilities.	2.5.1 Jurisdictions are able to respond to identified events and incidents, document root cause, and share information with partners.	Cyber incident after action reports document root cause of the incident (target 90% of jurisdictions document).

Subrecipient Projects Supporting FY22 Cybersecurity Program Goal 2			
Project Letter & Title	Program Goal/Objective Supported	Project Description – including anticipated deliverable	Status of Project (not started, in progress, completed)
N/A			

FY22 CYBERSECURITY PROGRAM METRICS			
Program Goal	Program Objective	Associated Metrics	Metric Description (details, source, frequency)
Goal 3: Implement highest priority cyber security protections commensurate with risk across California's government jurisdictions.	3.1: Jurisdictions adopt fundamental cybersecurity best practices.	3.1.1: Jurisdictions implement multi-factor authentication (MFA), prioritizing privileged users, Internet-facing systems, and cloud accounts.	Number of jurisdictions that implement MFA (target 90%).
		3.1.2: Jurisdictions end use of unsupported/end of life software and hardware that are accessible from the Internet.	Number of jurisdictions that end use of unsupported/end of life software and hardware that are accessible from the Internet (target 90%).
		3.1.3: jurisdictions prohibit use of known/fixed/default passwords and credentials.	Number of jurisdictions that document the prohibition of using known/fixed/default passwords and credentials (target 100%).
		3.1.4: Jurisdictions ensure the ability to reconstitute systems following an incident with minimal disruption to services.	Number of jurisdictions that can achieve recovery times outlined in cyber incident response and recovery plans (target 90%).
		3.1.5: Jurisdictions migrate to .gov Internet domain.	Number of jurisdictions that migrate to .gov internet domain over the next four years (target 90%).
	3.2: Jurisdictions reduce gaps identified through an assessment and planning process and apply increasingly sophisticated security protections commensurate with risk.	3.2.1: Jurisdictions address items identified through assessments and planning process.	Number of jurisdictions that document, through improvement plans, they are addressing items identified through a assessments (target 90%).

	3.3: Create and operationalize a portfolio of cybersecurity as-a-services offerings at the state level, i.e., security operations center services, to address gaps in a cost-effective manner.	3.3.1: The state develops the required documentation and personnel required to provide cybersecurity as-a-service offerings to all jurisdictions that request it.	All jurisdictions requesting cyber security as a service from the state receive it (target 100%).
--	--	---	---

Subrecipient Projects Supporting FY22 Cybersecurity Program Goal 3

Project Letter & Title	Program Goal/Objective Supported	Project Description – including anticipated deliverable	Status of Project (not started, in progress, completed)
Project C FY22: Network and Workstation Hardware Replacement and Installation Support	3.1/3.2/3.3	Working with MSSP, replace end-of-life network and workstation hardware to facilitate enhanced security posture, replacing firewall, wireless access points, switches, backup power supply for office network environment, and end-of-life computers and software; implementation of workstation backups. (Funding FY22 \$6,833)	In progress

FY22 CYBERSECURITY PROGRAM METRICS

Program Goal	Program Objective	Associated Metrics	Metric Description (details, source, frequency)
Goal 4: Develop and unify California's diverse, innovative cybersecurity workforce to safeguard the data and systems used across jurisdictions to deliver public services.	4.1: Personnel across jurisdictions and job categories are appropriately trained in cybersecurity necessary to recognize and respond to cyber security risk and understand their roles and responsibilities within established cyber security policies, procedures, and practices.	4.1.1: Jurisdictions require ongoing phishing training, awareness campaigns are conducted, an organization provides role-based cyber security awareness training to all employees.	Employee training is documented and reported annually (target 90% of employees).
		4.1.2: The jurisdiction has dedicated resources and funding available for its cybersecurity professionals to attend technical training and conferences.	The number of jurisdictional cybersecurity professionals attending technical training and conferences is documented and reported annually (target 90%).
	4.2: Jurisdictions adopt National Institute for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.	4.2.1: Jurisdictions have established cyber workforce development and training plans, based on the NICE Cybersecurity Workforce Framework.	Each jurisdiction's cyber workforce development and training plan is reported to Cal-CSIC (target 90%).

	4.3: Better align each jurisdiction's workforce with current and future cybersecurity needs by updating cybersecurity talent models and career paths to include cybersecurity job roles, job categories, knowledge, skills, and abilities.	4.3.1: Jurisdictions have or create cybersecurity career path toolkit.	Each jurisdiction documents development of their toolkit (target 90%).
		4.3.2: Jurisdictions create or update their cybersecurity talent model and career paths.	Each jurisdiction documents creation of or the updating of their cybersecurity talent model and career paths (target 90%).
	4.4: Build and expand partnerships with educational institutions and private industry to create a diverse pipeline of cybersecurity professionals seeking careers and public service.	4.4.1: Jurisdictions formalize and document partnerships with educational institutions.	Each jurisdiction has a formal partnership with at least one educational institution (target 90%).

Subrecipient Projects Supporting FY22 Cybersecurity Program Goal 4

Project Letter & Title	Program Goal/Objective Supported	Project Description – including anticipated deliverable	Status of Project (not started, in progress, completed)
Project D FY22: Workforce Development - Cybersecurity Situational Awareness	4.1/4.2/4.3/4.4	Working with MSSP, provide Spalding CSD staff ongoing training & support on new IT systems software/hardware implementation, as well as ongoing training & support on cybersecurity situational awareness and workstation/email security hygiene. (Funding FY22 \$6,497)	In progress

FY22 PERFORMANCE MEASURES:

Please quantify the performance measures below by indicating whether the listed activity has been completed (100%), not yet completed (0%), or is not applicable to your SLCGP Program (N/A).

SLCGP FY22 PROGRAM ACTIVITY	Completion Status
The Subrecipient's SLCGP Program has conducted table-top and full-scope exercises to test Cybersecurity Plans	0%

The Subrecipient's SLCGP Program has conducted a cyber risk assessment to identify cyber risk management gaps and areas for improvement	100%
The Subrecipient's SLCGP Program has: (please check the check boxes below for relevant activities) <input checked="" type="checkbox"/> performed phishing training; <input checked="" type="checkbox"/> conducted awareness campaigns; <input checked="" type="checkbox"/> provided role-based cybersecurity awareness training to employees Identify which of these activities have begun and will be ongoing throughout the performance period on the text line below: _____	100%
The Subrecipient's SLCGP Program has adopted the Workforce Framework for Cybersecurity (NICE Framework) as evidenced by established workforce development and training plans	100%
The Subrecipient Organization has implemented capabilities to analyze network traffic and activities related to potential threats	0%
The Subrecipient's SLCGP Program has implemented multi-factor authentication (MFA) for all remote access and privileged accounts	0%
The Subrecipient Organization has implemented programs to anticipate and discontinue use of end-of-life software and hardware	100%
The Subrecipient Organization prohibits the use of known/fixed/default passwords and credentials	0%
The Subrecipient's SLCGP Program has migrated to the ".gov" internet domain	0%
Number of cybersecurity gaps or issues addressed by the Subrecipient's SLCGP Program Activities	4

FY23 CYBERSECURITY PROGRAM METRICS

In the tables provided, please provide information about how your SLCGP projects address the Cybersecurity Metrics listed below. If your projects do not address one or more of the metrics, please enter N/A.

FY23 CYBERSECURITY PROGRAM METRICS			
Program Goal	Program Objective	Associated Metrics	Metric Description (details, source, frequency)

<p>Goal 1: Develop and establish baseline governance structures across California's jurisdictions, including developing, implementing, or revising cybersecurity plans to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.</p>	<p>1.1: Establish cybersecurity governance structures and implement a program to evaluate maturity of the cybersecurity program aligned to Cybersecurity Performance Goals established by CISA and the National Institute of Standards and Technology (NIST).</p>	<p>1.1.1: Jurisdictions have established and documented a uniform cybersecurity governance structure that is accountable to organizational leadership and works together to set the vision for cyber risk management.</p>	<p>Jurisdictional Chief Information Officer, or equivalent position, quarterly reporting to Cal-CSIC (target 90%).</p>
		<p>1.1.2: Jurisdictions have identified senior officials to enable whole-of-organization coordination on cybersecurity policies, processes, and procedures.</p>	<p>Senior officials are identified in the jurisdiction's cyber incident response plan under objective 1.2 (target 90%).</p>
	<p>1.2: Develop, implement, or revise, and test cybersecurity plans, including cyber incident response plans, with clearly defined roles and responsibilities.</p>	<p>1.2.1: Jurisdictions develop, implement, or revise, and exercise their cyber incident response plans every two years.</p>	<p>Jurisdictional biennial reporting to Cal-CSIC and within 30 days of completing the cyber exercise target 90%. Jurisdictional biennial reporting to Cal-CSIC and within 30 days of completing or revising the cyber incident response plan target 90%.</p>
	<p>1.3: Asset (e.g., devices, data, software) protections and recovery actions are prioritized based on the asset's criticality and business value.</p>	<p>1.3.1: Jurisdictions document their prioritization of systems and network functions and set them for reconstitution according to their impact to essential functions.</p>	<p>Prioritized systems are identified in cyber incident response plans or other cyber security plans (target 90%).</p>

Subrecipient Projects Supporting FY23 Cybersecurity Program Goal 1

Project Letter & Title	Program Goal/Objective Supported	Project Description – including anticipated deliverable	Status of Project (not started, in progress, completed)
Project A FY23: Risk Assessment and network evaluation	1.1/ 1.2/1.3	Assess needs of Spalding CSD and develop plan to bring Cyber Security within compliance. This will include planning for new hardware and software for workstations, as well as assessing potential cyber risks and develop a plan to address those risks. (Funding FY23 \$1244)	In progress
Project E FY23: Grants & Contract Administration	1.1	Time and expenses for Spalding CSD Grant & MSSP Contract Administration; enhancing organizational administration and capacity for managing the grant. (Funding FY22 \$1,816)	In progress

FY23 CYBERSECURITY PROGRAM METRICS			
Program Goal	Program Objective	Associated Metrics	Metric Description (details, source, frequency)
Goal 2: Government jurisdictions across California understand their current cyber security posture and areas for improvement based on continuous testing, evaluation, and structured assessments.	2.1: Physical devices and systems, as well as software platforms and applications, are inventoried.	2.1.1: Jurisdictions establish and regularly update asset inventory.	Assets are inventoried annually by jurisdictions (target 90%).
	2.2: Cybersecurity risk to each jurisdiction's operations and assets are documented and understood.	2.2.1: Jurisdictions conduct an annual cyber risk assessment to identify cyber risk management gaps and areas for improvement once a year.	Jurisdictional annual assessment (target 90%).
	2.3: Vulnerability scans are performed, and a risk-based vulnerability management plan is developed and implemented by each jurisdiction.	2.3.1: Jurisdictions participate in CISA's Vulnerability Scanning service, part of the cyber hygiene program or equivalent service provided by the state or commercial provider.	Number of jurisdictions that participate in vulnerability scanning services (target 100%), measured quarterly.
		2.3.2: Jurisdictions effectively manage vulnerabilities by prioritizing migration of high impact vulnerabilities and those most likely to be exploited.	Methods for tracking and managing vulnerabilities are documented by jurisdictions (target 90%).
	2.4: Capabilities are in place across each jurisdiction to monitor assets to identify cybersecurity events.	2.4.1: Jurisdictions are able to analyze network traffic and activity transiting or traveling to or from information systems, applications, and user accounts to understand baseline activity and identify potential threats.	Personnel or systems are in place to analyze jurisdictions' network traffic and activity (target 90%).
	2.5: Processes are in place across each jurisdiction to action insights derived from deployed capabilities.	2.5.1: Jurisdictions are able to respond to identified events and incidents, document root cause, and share information with partners.	Cyber incident after action reports document root cause of the incident (target 90% of jurisdictions document).

Subrecipient Projects Supporting FY23 Cybersecurity Program Goal 2			
Project Letter & Title	Program Goal/Objective Supported	Project Description – including anticipated deliverable	Status of Project (not started, in progress, completed)
Project B FY23: Risk Assessment and network evaluation	2.1/2.2/2.4/2.5	Working with the MSSP, establish secure centrally managed domain, secure cloud storage (SharePoint/OneDrive) and secure cloud email server (Outlook/Azure Encryption) corresponding to Microsoft Office 365 for Government or similar enterprise licensing and	Not Started

		implement end user security support (Multi-factor Authentication). (Funding FY23 \$18,441)	

FY23 CYBERSECURITY PROGRAM METRICS			
Program Goal	Program Objective	Associated Metrics	Metric Description (details, source, frequency)
Goal 3: Implement highest priority cyber security protections commensurate with risk across California's government jurisdictions.	3.1: Jurisdictions adopt fundamental cybersecurity best practices.	3.1.1: Jurisdictions implement multi-factor authentication (MFA), prioritizing privileged users, Internet-facing systems, and cloud accounts.	Number of jurisdictions that implement MFA (target 90%).
		3.1.2: Jurisdictions end use of unsupported/end of life software and hardware that are accessible from the Internet.	Number of jurisdictions that end use of unsupported/end of life software and hardware that are accessible from the Internet (target 90%).
		3.1.3: jurisdictions prohibit use of known/fixed/default passwords and credentials.	Number of jurisdictions that document the prohibition of using known/fixed/default passwords and credentials (target 100%).
		3.1.4: Jurisdictions ensure the ability to reconstitute systems following an incident with minimal disruption to services.	Number of jurisdictions that can achieve recovery times outlined in cyber incident response and recovery plans (target 90%).
		3.1.5: Jurisdictions migrate to .gov Internet domain.	Number of jurisdictions that migrate to .gov internet domain over the next four years (target 90%).
	3.2: Jurisdictions reduce gaps identified through an assessment and planning process and apply increasingly sophisticated security protections commensurate with risk.	3.2.1: Jurisdictions address items identified through assessments and planning process.	Number of jurisdictions that document, through improvement plans, they are addressing items identified through a assessments (target 90%).
	3.3: Create and operationalize a portfolio of cybersecurity as-a-services offerings at the state level, i.e., security operations center services, to address gaps in a cost-effective manner.	3.3.1: The state develops the required documentation and personnel required to provide cybersecurity as-a-service offerings to all jurisdictions that request it.	All jurisdictions requesting cyber security as a service from the state receive it (target 100%).

Subrecipient Projects Supporting FY23 Cybersecurity Program Goal 3			
Project Letter & Title	Program Goal/Objective Supported	Project Description – including anticipated deliverable	Status of Project (not started, in progress, completed)
Project C FY23: Network and Workstation Hardware Replacement and Installation Support	3.1/3.2/3.3	Working with MSSP, replace end-of-life network and workstation hardware to facilitate enhanced security posture, replacing firewall, wireless access points, switches, backup power supply for office network environment, and end-of-life computers and software; implementation of workstation backups. (Funding FY23 \$22,872)	In progress

FY23 CYBERSECURITY PROGRAM METRICS

Program Goal	Program Objective	Associated Metrics	Metric Description (details, source, frequency)
Goal 4: Develop and unify California's diverse, innovative cybersecurity workforce to safeguard the data and systems used across jurisdictions to deliver public services.	4.1: Personnel across jurisdictions and job categories are appropriately trained in cybersecurity necessary to recognize and respond to cyber security risk and understand their roles and responsibilities within established cyber security policies, procedures, and practices.	4.1.1: Jurisdictions require ongoing phishing training, awareness campaigns are conducted, an organization provides role-based cyber security awareness training to all employees.	Employee training is documented and reported annually (target 90% of employees).
		4.1.2: The jurisdiction has dedicated resources and funding available for its cybersecurity professionals to attend technical training and conferences.	The number of jurisdictional cybersecurity professionals attending technical training and conferences is documented and reported annually (target 90%).
	4.2: Jurisdictions adopt National Institute for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.	4.2.1: Jurisdictions have established cyber workforce development and training plans, based on the NICE Cybersecurity Workforce Framework.	Each jurisdiction's cyber workforce development and training plan is reported to Cal-CSIC (target 90%).
	4.3: Better align each jurisdiction's workforce with current and future cybersecurity needs by updating cybersecurity talent models and career paths to include cybersecurity job roles, job categories, knowledge, skills, and abilities.	4.3.1: Jurisdictions have or create cybersecurity career path toolkit.	Each jurisdiction documents development of their toolkit (target 90%).
		4.3.2: Jurisdictions create or update their cybersecurity talent model and career paths.	Each jurisdiction documents creation of or the updating of their cybersecurity talent model and career paths (target 90%).
4.4: Build and expand partnerships with educational institutions and private industry to create a diverse pipeline of	4.4.1: Jurisdictions formalize and document partnerships with educational institutions.	Each jurisdiction has a formal partnership with at least one educational institution (target 90%).	

	cybersecurity professionals seeking careers and public service.		
--	---	--	--

Subrecipient Projects Supporting FY23 Cybersecurity Program Goal 4

Project Letter & Title	Program Goal/Objective Supported	Project Description – including anticipated deliverable	Status of Project <small>(not started, in progress, completed)</small>
Project D FY23: Workforce Development - Cybersecurity Situational Awareness	4.1/4.2/4.3/4.4	Working with MSSP, provide Spalding CSD staff ongoing training & support on new IT systems software/hardware implementation, as well as ongoing training & support on cybersecurity situational awareness and workstation/email security hygiene. (Funding FY22 \$6,063)	In progress

FY23 PERFORMANCE MEASURES:

Please quantify the performance measures below by indicating whether the listed activity has been completed (100%), not yet completed (0%), or is not applicable to your SLCGP Program (N/A).

SLCGP FY23 PROGRAM ACTIVITY	Completion Status
The Subrecipient's SLCGP Program has conducted table-top and full-scope exercises to test Cybersecurity Plans	0%
Percent of Subrecipient's SLCGP FY23 funding expended on exercises thus far	N/A
The Subrecipient's SLCGP Program has conducted a cyber risk assessment to identify cyber risk management gaps and areas for improvement	100%
The Subrecipient's SLCGP Program has performed phishing training <i><input checked="" type="checkbox"/> Check box if this activity has begun and will be ongoing throughout the performance period.</i>	100%

The Subrecipient's SLCGP Program has conducted awareness campaigns <input checked="" type="checkbox"/> Check box if this activity has begun and will be ongoing throughout the performance period.	100%
The Subrecipient's SLCGP Program has provided role-based cybersecurity awareness training to employees <input checked="" type="checkbox"/> Check box if this activity has begun and will be ongoing throughout the performance period.	100%
The Subrecipient's SLCGP Program has adopted the Workforce Framework for Cybersecurity (NICE Framework) as evidenced by established workforce development and training plans	100%
The Subrecipient Organization has implemented capabilities to analyze network traffic and activities related to potential threats	0%
The Subrecipient's SLCGP Program has implemented multi-factor authentication (MFA) for all remote access and privileged accounts	0%
The Subrecipient Organization has implemented programs to anticipate and discontinue use of end-of-life software and hardware	0%
The Subrecipient Organization prohibits the use of known/fixed/default passwords and credentials	0%
The Subrecipient's SLCGP Program has migrated to the ".gov" internet domain	0%
Number of cybersecurity gaps or issues addressed annually by the Subrecipient's SLCGP Program Activities	5