FY 2022 State and Local Cybersecurity Grant Program (SLCGP)

Notice of Funding Opportunity (NOFO)

Grant Issued By:

U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), Grant Programs Directorate (GPD)

Grant Issued Through:

Missouri Department of Public Safety (DPS), Office of Homeland Security (OHS)

Assistance Listing:

97.137

Funding Opportunity Title:

State and Local Cybersecurity Grant Program (SLCGP)

Overview:

Our nation faces unprecedented cybersecurity risks, including increasingly sophisticated adversaries, widespread vulnerabilities in commonly used hardware and software, and broad dependencies on networked technologies for the day-to-day operation of critical infrastructure. Cyber risk management is further complicated by the ability of malicious actors to operate remotely, linkages between cyber and physical systems, and the difficulty of reducing vulnerabilities.

The potential consequences of cyber incidents threaten national security. Strengthening cybersecurity practices and resilience of state and local governments is an important homeland security mission and the primary focus of the State and Local Cybersecurity Grant Program (SLCGP). Through funding from the Infrastructure Investment and Jobs Act (IIJA), also known as the Bipartisan Infrastructure Law (BIL), the SLCGP enables DHS to make targeted cybersecurity investments in state and local government agencies, thus improving the security of critical infrastructure and improving the resilience of the services state and local governments provide their community.

The FY 2022 SLCGP aligns with the 2020-2024 DHS Strategic Plan by helping DHS achieve Goal 3: Secure Cyberspace and Critical Infrastructure, Objective 3.3 Assess and Counter Evolving Cybersecurity Risks. The FY 2022 SLCGP also supports the 2022-2026 FEMA Strategic Plan which outlines a bold vision and three ambitious goals, including Goal 3: Promote and Sustain a Ready FEMA and Prepared Nation, Objective 3.2: Posture FEMA to meet current and emergent threats.

Funding Sources:

There are three funding sources available for FY 2022 SLCGP applicants:

1) State and Local Cybersecurity Grant Program (SLCGP) – Rural: SLCGP Rural funds are dedicated for entities encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce. The FY 2022 SLCGP requires 25% of the funds be provided to rural areas.

2) State and Local Cybersecurity Grant Program (SLCGP) – Non-Rural: SLCGP Non-Rural funds are dedicated for entities encompassing a population of greater than 50,000 people that has been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce.

3) State and Local Cybersecurity Grant Program (SLCGP) – State: SLCGP State funds are dedicated for state agency applicants.

Objectives:

The goal of SLCGP is to assist state and local governments with managing and reducing systemic cyber risk. For Fiscal Year (FY) 2022, the objectives of the SLCGP are as follows:

- **Objective 1:** Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- **Objective 2:** Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- **Objective 3:** Implement security protections commensurate with risk.
- **Objective 4:** Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

Requested projects must align to at least one of the above listed objectives. For more information on the program goals, objectives, sub-objectives, and desired outcomes, please refer to Appendix A.

Priorities:

For the FY 2022 SLCGP, the state of Missouri has established the following seven priorities:

1) Implement multi-factor authentication
2) Implement enhanced logging
3) Data encryption for data at rest and in transit
4) End use of unsupported/end of life software and hardware that are accessible from the Internet
5) Prohibit use of known/fixed/default passwords and credentials
6) Ensure the ability to reconstitute systems (backups)
7) Migration to the .gov internet domain

Applicants should consider requesting projects to address the established priorities before other cybersecurity initiatives. Projects that align to Missouri priorities will receive additional points during the application scoring process.

Period of Performance: 36 months

Projected Period of Performance Start Date: September 1, 2022

Projected Period of Performance End Date: August 31, 2025

Funding Instrument: Grant

Allowable Amount: $200,000 Federal share per applicant agency

Cost Share of Match: 10% cost share requirement (cash [hard match] or in-kind [soft match])

DHS/FEMA/OHS administers cost-matching requirements in accordance with 2 C.F.R 200.306. To meet matching requirements, the subrecipient 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. Unless otherwise authorized by law, the non-federal cost share requirement cannot be matched with other federal funds.

For example, if the total cost of the project is $100,000, the subrecipient share of 10% would be $10,000 and the federal share of 90% would be $90,000.

Eligible Applicants:

- Local governments as defined in 6 U.S.C. section 101(13) as
    - 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
    - A rural community, unincorporated town or village, or other public entity
- State units of government

Ineligible Applicants:

- Non-profit organizations
- For-profit organizations

Other Eligibility Criteria:

Cybersecurity Risk Assessment Applicant agencies must have a completed cybersecurity risk assessment such as the Nationwide Cybersecurity Review (NCSR). The requested project must align to closing gaps and/or strengthening capabilities in the agency's cybersecurity risk assessment.

Application and Submission Information:

1. **Key Dates and Times**

   a. Application Start Date: November 16, 2022

   b. Application Submission Deadline: December 16, 2022 5:00 p.m. CST

2. **Agreeing to Terms and Conditions of the Award**

By submitting an application, applicants agree to comply with the requirements of this NOFO and the terms and conditions of the award, should they receive an award.

Applications will only be accepted through the Missouri Department of Public Safety (DPS) online WebGrants System. https://dpsgrants.dps.mo.gov/index.do

An application workshop with instructions on how to apply through the WebGrants System will be available on the DPS website, at the following link under Grant Applications and Forms, FY 2022 State and Local Cybersecurity Grant Program (SLCGP): https://dps.mo.gov/dir/programs/ohs/grantstraining/

As part of the FY 2022 SLCGP application, each eligible applicant must complete all application forms and provide all required documents:

1. **Contact Information Form**

2. **SLCGP Project Package**

3. **Budget**

4. **Named Attachments**
   a. **Audit/Financial Statement (REQUIRED)**
   b. **Federal Fund Schedule (REQUIRED, if not included in Audit**
   c. **Quote or Cost Basis**
   d. **Other Supporting Documentation**
   e. **Other Supporting Documentation**
   f. **Other Supporting Documentation**
   g. **Other Supporting Documentation**

Each application must only include one project, and all requested funding in the application must be directly associated to that specific project.

Funding Restrictions and Allowable Costs:

All costs charged to awards covered by this NOFO must comply with the Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2 C.F.R. Part 200, unless otherwise indicated in the NOFO, the terms and conditions of the award. This includes, among other requirements that costs must be incurred, and products and services must be delivered, within the period of performance of the award. *See* 2 C.F.R. § 200.403(h) (referring to budget periods, which for FEMA awards under this program is the same as the period of performance).

Allowable Costs:

There are five allowable expense categories as listed below.

1. Planning
2. Organization
3. Equipment
4. Training
5. Exercises

Requested projects must strengthen state and local cybersecurity preparedness by focusing on cybersecurity measures to help manage state and local risk and enhance Missouri's cybersecurity posture. The requested project **MUST**:

- Close gaps and strengthen capabilities identified in an agencies' Nationwide Cybersecurity Review (NCSR) or other cybersecurity risk assessment
- Align with the Missouri Comprehensive Cybersecurity Plan (CCP)
- Align with at least one of the FY 2022 SLCGP Objectives (FY 2022 SLCGP Objectives can be found in Appendix A)

Examples of allowable costs include but are not limited to planning, organization, equipment, training, and exercise costs for local end-user cybersecurity training and awareness campaigns, cybersecurity planning, monitoring, scanning, and protection solutions for equipment and networks, cybersecurity protection for critical infrastructure, and upgrading legacy technology.

Planning:

Planning costs are allowable under this program. Funds may be used for planning activities that support the FY 2022 SLCGP objectives, Missouri Comprehensive Cybersecurity Plan (CCP), and closing gaps and strengthening capabilities in the applicant's cybersecurity risk assessment.

Organization:

Organization costs are allowable under this program. Organizational activities include:

- Program management
- Development of whole community partnerships
- Structures and mechanisms for information sharing between the public and private sector
- Operational support

Personnel, hiring, overtime, and backfill expenses are permitted under this grant to perform allowable SLCGP planning, organization, training, exercise, and equipment activities. Personnel expenses may include, but are not limited to, training and exercise coordinators, program managers and planners, cybersecurity navigators.

Equipment:

Equipment costs are allowable under this program. SLCGP equipment is intended to be used to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state and local governments.

Unless otherwise stated, all equipment must meet all applicable statutory, regulatory, and DHS/FEMA/OHS standards to be eligible for purchase using these funds. Please refer to FEMA's Authorized Equipment List. In addition, subrecipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment. Investments in emergency communications systems and equipment must meet applicable SAFECOM Guidance recommendations. Such investments must coordinated with the Statewide Interoperability Coordinator (SWIC) and the State Interoperability Governing Body (SIGB) to ensure interoperability and long-term compatibility.

SLCGP funds may be used to purchase maintenance contracts or agreements, warranty coverage, licenses, and user fees in support of a system or equipment. These contracts may exceed the period of performance if they are purchased incidental to the original purchase of the system or equipment as long as the original purchase of the system or equipment is consistent with that which is typically provided for, or available through, these types of agreements, warranties, or contracts. When purchasing a stand-alone warranty or extending an existing maintenance contract on an already-owned piece of equipment system, coverage purchased may not exceed the period of performance of the award used to purchase the maintenance agreement or warranty, and it may only cover equipment purchased with SLCGP funds or for equipment dedicated for SLCGP-related purposes. As with warranties and maintenance agreements, this extends to licenses and user fees as well.

Training:

Training costs are allowable under this program. Allowable training-related costs under SLCGP include the establishment, support, conduct, and attendance of training and/or in conjunction with training by other federal agencies. Training conducted using SLCGP funds should align to the Missouri's Comprehensive Cybersecurity Plan (CCP) and address a performance gap identified through assessments and contribute to building a capability that will be evaluated through a formal exercise.

Some training activities require Environmental and Historic Preservation (EHP) Review, including exercises, drills, or trainings that require any type of land, water, or vegetation disturbance or building of temporary structures or that are not located at facilities designed to conduct training and exercises. Additional information on training requirements and EHP review can be found online at https://www.fema.gov/media-library/assets/documents/90195.

Exercise:

Exercise costs are allowable under this program. Exercises conducted with grant funding should be managed and conducted consistent with Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP guidance for exercise, design, development, conduct, evaluation, and improvement planning is located at https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep.

Some training activities require Environmental and Historic Preservation (EHP) Review, including exercises, drills, or trainings that require any type of land, water, or vegetation disturbance or building of temporary structures or that are not located at facilities designed to conduct training and exercises. Additional information on training requirements and EHP review can be found online at https://www.fema.gov/media-library/assets/documents/90195.

Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services

Recipients and subrecipients of FEMA federal financial assistance are subject to the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY 2019 NDAA), Pub. L. No. 115-232 (2018) and 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200. Beginning August 13, 2020, the statute – as it applies to FEMA recipients, subrecipients, and their contractors and subcontractors – prohibits obligating or expending federal award funds on certain telecommunications and video surveillance products and contracting with certain entities for national security reasons.

Guidance is available at Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services (Interim) FEMA Policy #405-143-1, or superseding document.

Additional guidance is available at Contract Provisions Guide: Navigating Appendix II to Part 200 – Contract Provisions for Non-Federal Entity Contracts Under Federal Awards (fema.gov).

Effective August 13, 2020, FEMA recipients and subrecipients **may not** use any FEMA funds under open or new awards to:

a. Procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system;

b. Enter into, extend, or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system; or

c. Enter into, extend, or renew contracts with entities that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

I. Replacement Equipment and Services

FEMA grant funding may be permitted to procure replacement equipment and services impacted by this prohibition, provided the costs are otherwise consistent with the requirements of the NOFO and the Preparedness Grants Manual.

II. Definitions

Per section 889(f)(2)-(3) of the FY 2019 NDAA and 2 C.F.R. § 200.216, covered telecommunications equipment or services means:

i. Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, (or any subsidiary or affiliate of such entities);

ii. For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology

Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

iii. Telecommunications or video surveillance services provided by such entities or using such equipment; or

iv. Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the People's Republic of China.

Examples of the types of products covered by this prohibition include phones, internet, video surveillance, and cloud servers when produced, provided, or used by the entities listed in the definition of "covered telecommunications equipment or services." See 2 C.F.R. § 200.471.

Unallowable Costs:

Any entity that receives FY 2022 SLCGP funding may not use the grant:

- To supplant state or local funds; however this shall not be construed to prohibit the use of funds from a grant under this NOFO for otherwise permissible uses on the basis that the state and local government has previously used state and local government funds to support the same or similar uses;
- For any recipient cost-sharing contribution;
- 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; or
- For any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, on or behalf of, the eligible entity that receives the grant or a local government within the jurisdiction of the eligible entity.

Required Cybersecurity Posture

If the applicant's cybersecurity posture does not contain the below listed benchmarks, the applicant **MUST** achieve these benchmarks during the grant period of performance, if selected for an award under SLCGP:

- Cybersecurity and/or data security policies
- Cybersecurity training awareness program
- Cybersecurity incident response plan
- Receive cybersecurity threat intelligence

The OHS Cybersecurity Team has resources available to assist with these benchmarks. If assistance is needed, please contact the OHS Cybersecurity Team by phone at 573-526-0153 or by email at securityintel@mshp.dps.mo.gov.

Required Services and Memberships

If awarded funding, all SLCGP subrecipients are required to participate in a limited number of free services by CISA/OHS. For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement.

OHS Cybersecurity Program

If awarded funding, subrecipients must subscribe to the Missouri Office of Homeland Security (OHS) Cybersecurity Program and participate in information sharing with federal, state, and local agencies (i.e., Missouri Office of Homeland Security (OHS), Missouri Information Analysis Center (MIAC), St. Louis Fusion Center, Kansas City Regional Fusion Center). Entities can subscribe to the OHS Cybersecurity Program by emailing securityintel@mshp.dps.mo.gov with your name, agency/entity, title, desk phone, work phone, and email address.

Cyber Hygiene Services

Web Application Scanning is an "internet scanning-as-a-service." This service assess the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security 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 (NCSR)

The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a state and local government's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC.

Subrecipients must complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually, throughout the grant period of performance.

Administrative and National Policy Requirements:

In addition to the requirements in this section and elsewhere in this NOFO, FEMA/OHS may place specific terms and conditions on individual awards in accordance with 2 C.F.R. Part 200.

DHS Standard Terms and Conditions:

All successful applicants for DHS grant and cooperative agreements are required to comply with DHS Standards Terms and Conditions, which are available online at: DHS Standard Terms and Conditions.

Ensuring the Protection of Civil Rights:

As the Nation works towards achieving the National Preparedness Goal, it is important to continue to protect the civil rights of individuals. Subrecipients must carry out their programs and activities, including those related to the building, sustainment, and delivery of core capabilities, in a manner that respects and ensures the protection of civil rights for protected populations.

Federal civil rights statutes, such as Section 504 of the Rehabilitation Act of 1973 and Title VI of the Civil Rights Act of 1964, along with DHS and FEMA regulations, prohibit discrimination on the basis of race, color, national origin, sex, religion, age, disability, limited English proficiency, or economic status in connection with programs and activities receiving federal financial assistance from FEMA.

The DHS Standard Terms and Conditions include a fuller list of the civil rights provisions that apply to subrecipients. These terms and conditions can be found in the DHS Standard Terms and Conditions. Additional information on civil rights provisions is available at https://www.fema.gov/about/offices/equal-rights/civil-rights.

Monitoring and oversight requirements in connection with subrecipient compliance with federal civil rights laws are also authorized pursuant to 44 C.F.R. Part 7.

In accordance with civil rights laws and regulations, subrecipients must ensure the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment.

Environmental Planning and Historic Preservation (EHP) Compliance:

As a federal agency, FEMA is required to consider the effects of its actions on the environment and historic properties to ensure that all activities and programs funded by FEMA, including grant-funded projects, comply with federal EHP laws, Executive Orders, regulations, and policies, as applicable.

Subrecipients proposing projects that have the potential to impact the environment, including, but not limited to, the construction of communication towers, modification or renovation of existing buildings, structures, and facilities, or new construction including replacement of facilities, must participate in the FEMA EHP review process. The EHP review process involves the submission of a detailed project description along with any supporting documentation requested by FEMA in order to determine whether the proposed project has the potential to impact environmental resources or historic properties.

In some cases, FEMA is also required to consult with other regulatory agencies and the public in order to complete the review process. Federal law required EHP review to be completed before federal funds are released to carry out proposed projects. FEMA may not be able to fund projects that are not incompliance with applicable EHP laws, Executive Orders, regulations, and policies.

DHS and FEMA EHP policy is found in directives and instructions available on the FEMA.gov EHP page, the FEMA website page that includes documents regarding EHP responsibilities and program requirements, including implementation of the National Environmental Policy Act and other EHP regulations and Executive Orders.

The GPD EHP screening is located at https://www.fema.gov/media-library/assets/documents/90195. Additionally, all subrecipients under this funding opportunity are required to comply with the FEMA

GPD EHP Policy Guidance, FEMA Policy #108-023-1, available at https://www.fema.gov/media/library/assets/documents/85376.

SAFECOM Guidance Compliance:

All entities using SLCGP funding to support emergency communications investments are required to comply with the SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance). The SAFECOM Guidance provides current information on emergency communications policies, eligible costs, best practices, and technical standards for state and local recipients investing federal funds in emergency communications projects. It is also designed to promote and align with the National Emergency Communications Plan (NECP). Conformance with the SAFECOM Guidance helps ensure that federally funded investments are compatible, interoperable, resilient, and support national goals and objectives for improving emergency communications. Applicants should use the SAFECOM Guidance during planning, development, and implementation of emergency communications projects and in conjunction with other planning documents.

Contact Information:

Additional information and resources can be located on the Missouri Department of Public Safety, Office of Homeland Security website: https://dps.mo.gov/dir/programs/ohs/grantstraining/

WebGrants System, application submission site: https://dpsgrants.dps.mo.gov/index.do

For project specific questions, please contact the Office of Homeland Security Cybersecurity. Contact information for the cybersecurity team is listed below.

Office of Homeland Security Cybersecurity:

573-526-0153
securityintel@mshp.dps.mo.gov

For grant or WebGrants specific questions, please contact the Office of Homeland Security Grants. Contact information the grants team is listed below.

Office of Homeland Security Grants:

Chelse Dowell
Grants Specialist
(573) 751-3879
chelse.dowell@dps.mo.gov

Chelsey Call
Grants Supervisor
(573) 526-9203
Chelsey.call@dps.mo.gov

Joni McCarter
Program Manager
(573) 526-9020
Joni.mccarter@dps.mo.gov

Kelsey Saunders
Administrative Assistant
(573) 522-6125
kelsey.saunders@dps.mo.gov

Appendix A Goals and Objectives

The program goals for the SLCGP are as follows: (1) develop and establish appropriate governance structures, as well as develop, implement, or revise cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations; (2) ensure state and local agencies understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments; (3) implement security protections commensurate with risk (outcomes of Objectives 1 & 2); and (4) ensure organization personnel are appropriately trained in cybersecurity, commensurate with their responsibilities.

These program objectives are further divided into sub-objectives and outcomes, as well as sample evidence of implementation are provided to assist the reader.

Goal of the State and Local Cybersecurity Grant Program: Assist state and local governments with managing and reducing systemic cyber risk.

Objective 1: Develop and establish appropriate governance structures, as well as develop, implement, or revise cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.

Sub-objective 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. Outcome: Participants 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.

1.1.2. Outcome: Participants have identified senior officials to enable whole-of-organization coordination on cybersecurity policies, processes, and procedures.

- Sample Evidence of Implementation: Organization has a cybersecurity defense concept of operations, with responsibilities assigned to specific organizational roles.

Sub-objective 1.2: Develop, implement, or revise, and test cybersecurity plans, including cyber incident response plans, with clearly defined roles and responsibilities.

1.2.1 Outcome: Develop, implement, or revise, and exercise cyber incident response plans.

- Sample Evidence of Implementation: Organization conducts annual table-top and full-scope exercises that include practical execution of restoration and recovery processes to test cybersecurity plans. Conducting these exercises allow organizations to test cybersecurity plans to identify, protect, detect, respond to, and recover from cybersecurity incidents, in line with the NIST Cybersecurity Framework, and demonstrates process to incorporate lessons learned from the exercise into their cybersecurity program.

Sub-objective 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 Outcome: Ensure that systems and network functions are prioritized and reconstituted according to their impact to essential functions.

- Sample Evidence of Implementation: Organization conducts a regular business impact assessment to prioritize which systems must be protected and recovered first.

Objective 2: State and local agencies understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.

Sub-objective 2.1: Physical devices and systems, as well software platforms and applications, are inventoried.

2.1.1 Outcome: Establish and regularly update asset inventory.

- Sample Evidence of Implementation: Organization maintains and regularly updates an asset inventory list.

Sub-objective 2.2: Cybersecurity risk to the organization's operations and assets are understood.

2.2.1 Outcome: Conduct an annual cyber risk assessment to identify cyber risk management gaps and areas for improvement

- Sample Evidence of Implementation: Organization annually completes the Nationwide Cybersecurity Review (NCSR).

Sub-objective 2.3: Vulnerability scans are performed, and a risk-based vulnerability management plan is developed and implemented.

2.3.1 Outcome: Participate in CISA's Vulnerability Scanning service, part of the Cyber Hygiene program.

- Sample Evidence of Implementation: Organization is an active participant in CISA's Cyber Hygiene program.

2.3.2 Outcome: Effectively manage vulnerabilities by prioritizing mitigation of high impact vulnerabilities and those most likely to be exploited.

- Sample Evidence of Implementation: Organization has a plan to manage vulnerabilities based on those with the highest criticality, internet-facing vulnerabilities, as well as known exploited vulnerabilities identified in CISA's Known Exploited Vulnerabilities Catalog.

Sub-objective 2.4: Capabilities are in place to monitor assets to identify cybersecurity events.

2.4.1 Outcome: state and local agencies 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.

Sub-objective 2.5: Processes are in place to action insights derived from deployed capabilities.

2.5.1 Outcome: state and local agencies are able to respond to identified events and incidents, document root cause, and share information with partners.

Objective 3: Implement security protections commensurate with risk (outcomes of Objectives 1 & 2)

Sub-objective 3.1: state and local agencies adopt fundamental cybersecurity best practices.

3.1.1 Outcome: Implement multi-factor authentication (MFA), prioritizing privileged users, Internet-facing systems, and cloud accounts.

- Sample Evidence of Implementation: The organization implements MFA for all remote access and privileged accounts.

3.1.2. Outcome: End use of unsupported/end of life software and hardware that are accessible from the Internet.

- Sample Evidence of Implementation: The organization has a program to anticipate and discontinue use of end of life software and hardware.

3.1.3 Outcome: Prohibit use of known/fixed/default passwords and credentials.

- Sample Evidence of Implementation: The organization has a policy that prohibits fixed passwords, requires known/default passwords be immediately changed, and that passwords and credentials be periodically changed.

- Sample Evidence of Implementation: The organization has reviewed all of its current passwords and credentials to ensure they are updated appropriately.

3.1.4 Outcome: Ensure the ability to reconstitute systems following an incident with minimal disruption to services.

- Sample Evidence of Implementation: Organization policies require that backups for all critical systems and data be maintained, updated, and regularly tested according to organizational policy (e.g., quarterly), stored offline, and encrypted.

3.1.5 Outcome: Migrate to .gov internet domain.

- Sample Evidence of Implementation: Organization operates only the .gov internet domain, and does not use .com, .org, or any other domain.

Sub-Objective 3.2: Reduce gaps identified through assessment and planning process and apply increasingly sophisticated security protections commensurate with risk.

3.2.1 Outcome: Individual participants address items identified through assessments and planning process.

3.2.2 Outcome: state and local entities improve cybersecurity ecosystem by collaborating to address items identified through assessments and planning process (e.g., regional and intra-state efforts)

Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

Sub-Objective 4.1: Train personnel to have the fundamental knowledge and skills necessary to recognize cybersecurity risks and understand their roles and responsibilities within established cybersecurity policies, procedures, and practices.

4.1.1 Outcome: Organization requires regular ongoing phishing training, awareness campaigns are conducted, and organization provides role-based cybersecurity awareness training to all employees.

4.1.2 Outcome: Organization has dedicated resources and funding available for its cybersecurity professionals to attend technical trainings and conferences.

Sub-Objective 4.2: Organization has adopted the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.

4.2.1 Outcome: Organization has established cyber workforce development & training plans, based on the NICE Cybersecurity Workforce Framework.