12TH ANNUAL LEADERSHIP EVENT

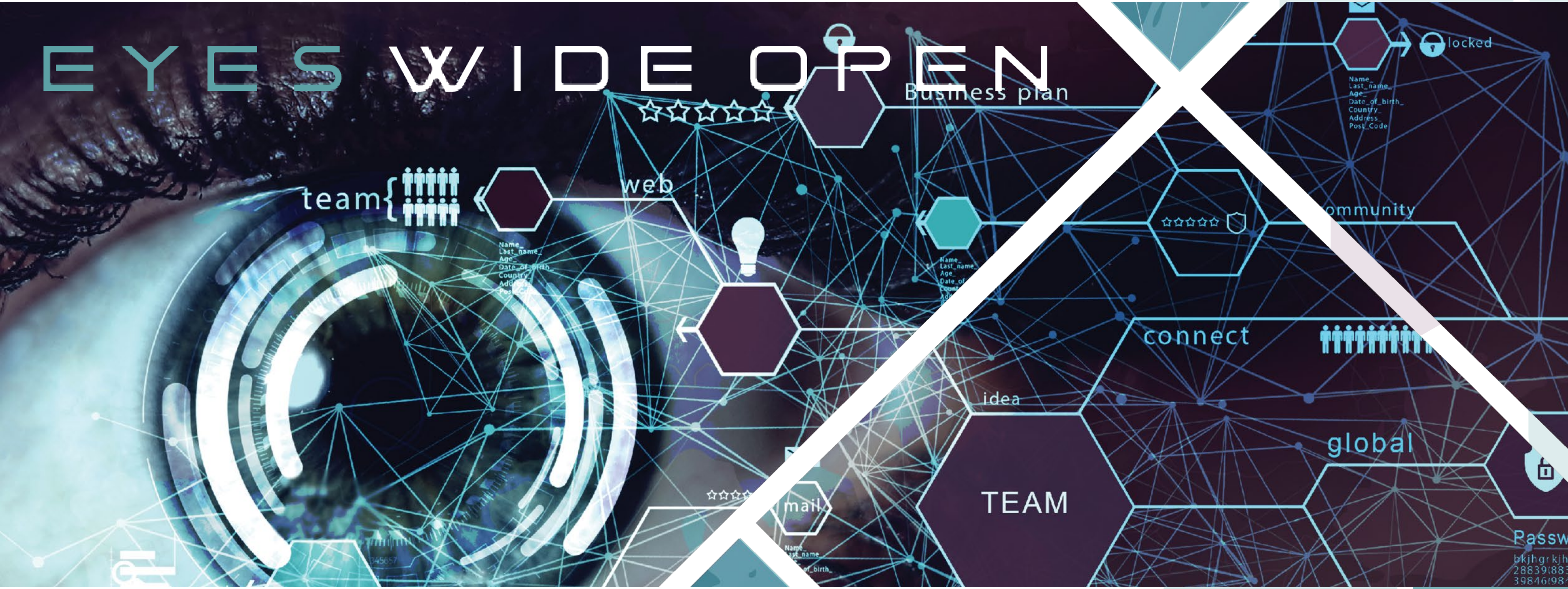
CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island

EYES WIDE OPEN



STATE AND LOCAL CYBERSECURITY GRANT PROGRAM

January 3, 2023

Roles and Responsibilities

- **CISA – Program Management and Subject Matter Expertise**
  - Identify the goals/objectives that define the overarching outcomes for the program;
  - Review and approve cybersecurity plans and projects; and
  - Establish measures of effectiveness that demonstrate achievement of goals/objectives.

- **FEMA – Grants Administration Subject Matter Expertise**
  - Conduct eligibility reviews, issue and programmatically/financially manage grant awards consistent with all applicable laws, regulations, and policies;
  - Place any special award terms and conditions, in coordination with CISA;
  - Monitor and document recipient progress, in coordination with CISA; and
  - Utilize existing grants and financial management systems for State and Local Cybersecurity Grant Program (SLCGP) awards.

Summary of State and Local Cybersecurity Grant Program

- Infrastructure Investment and Jobs Act (IIJA) amended Homeland Security Act of 2022 and appropriated $1B over 4 years
  - Funds appropriated to FEMA; CISA identified as subject matter expert
  - Baseline allocation plus population-based allocation formula
  - 80% passthrough to local entities
  - 25% of total state allocation must go to rural communities
  - Increasing SLTT cost share over time
- Eligible entities–States and territories - with subawards made to local entities
- Tribal specific program to be released separately at a later date
- Multi-entity grants can be made to groups of eligible entities
- Defined uses of funds
  - Develop and revise Cybersecurity Plan
  - Implement Cybersecurity Plan (including individual projects)
  - Grant administration (5%)
  - Address imminent cybersecurity threats, as confirmed by the Secretary, acting through the Director of CISA
  - Fund any other appropriate activity determined by the Secretary, acting through the Director of CISA

Appropriated Funding	Federal Cost Share
• FY22: $200M	• FY22: 90%
• FY23: $400M	• FY23: 80%
• FY24: $300M	• FY24: 70%
• FY25: $100M	• FY25: 60%

State and Local Cybersecurity Grant Program Requirements

PLANNING COMMITTEE

All eligible entities must establish a planning committee

Roles

- Develop, implement, and revise Cybersecurity Plans
- Approve Cybersecurity Plans
- Assist with determination of effective funding priorities (i.e., individual projects)

Required membership

- Eligible entity
- State CIO/CISO or equivalent
- Local/counties (if eligible entity is a state)
- Representatives from varying densities
- Public education
- Public health
- 50% of members must have professional experience relating to cybersecurity or information technology

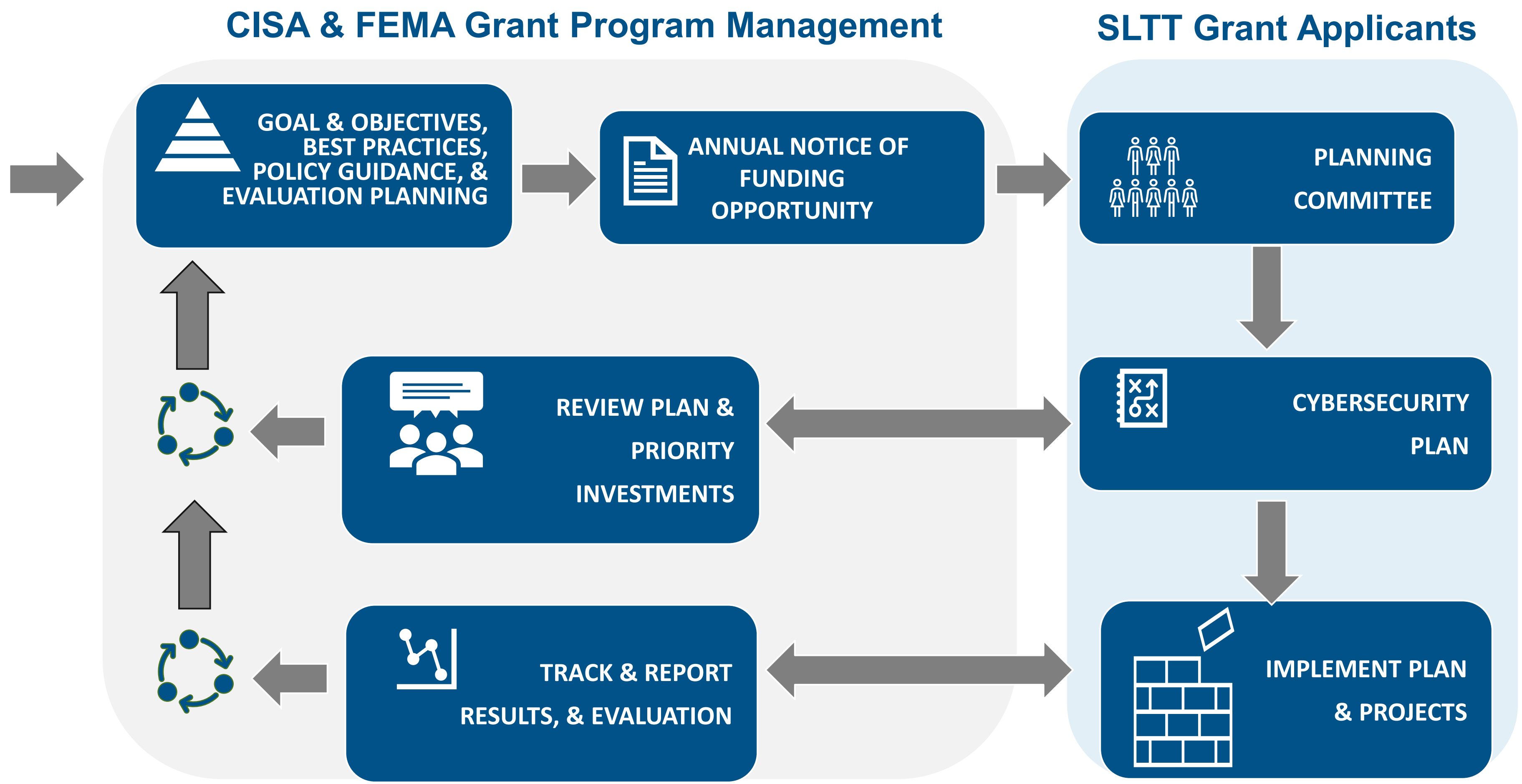
CYBERSECURITY PLAN

Mandates Cybersecurity Plan submission, approved by planning committee and state Chief Information Officer (CIO)

- 16 cyber-specific elements, including list of projects for SLCGP funding
- Description of SLTT roles in overarching plan
- Assessment of capabilities (16 elements)
- Resources and timeline for implementing plan
- Metrics

FEMA

Strategic Approach Leverages Feedback Loops



Inputs

Statutory Requirements

E.O. 14028

SLTT Engagements

CISA & FEMA Grant Program Management

GOAL & OBJECTIVES, BEST PRACTICES, POLICY GUIDANCE, & EVALUATION PLANNING

ANNUAL NOTICE OF FUNDING OPPORTUNITY

REVIEW PLAN & PRIORITY INVESTMENTS

TRACK & REPORT RESULTS, & EVALUATION

SLTT Grant Applicants

PLANNING COMMITTEE

CYBERSECURITY PLAN

IMPLEMENT PLAN & PROJECTS

Grant Program Goal & Objectives

GOAL: Assist SLTT governments with managing and reducing systemic cyber risk.

Objective 1-Governance & Planning

- Develop and establish appropriate governance structures, as well as plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- Establish cybersecurity governance structures and implement a program to evaluate maturity of the cybersecurity program aligned to Cybersecurity Performance Goals established by CISA and National Institute of Standards and Technology (NIST).
- Implement and test cybersecurity response plans with clearly defined roles and responsibilities.
- Asset (e.g., devices, data, software) protections and recovery actions are prioritized based on the asset's criticality and business value.

Objective 2-Assessment & Evaluation

- SLTT governments understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- Physical devices and systems, as well software platforms and applications, are inventoried.
- Cybersecurity risk to the organization's operations and assets are understood.
- Vulnerability scans are performed, and a risk-based vulnerability management plan is developed and implemented.
- Capabilities are in place to monitor assets to identify cybersecurity events.
- Processes are in place to action insights derived from deployed capabilities.

Objective 3-Mitigation

- Implement security protections commensurate with risk (outcomes of Objectives 1 & 2)
- SLTT agencies adopt fundamental cybersecurity best practices.
- Reduce gaps identified through assessment and planning process and apply increasingly sophisticated security protections commensurate with risk.

Objective 4-Workforce Development

- Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

Notice of Funding Opportunity (NOFO)

- The State and Local Cybersecurity Grant Program (SLCGP) NOFO was released Friday, September 16, 2022
  - Included detailed allocations for all 56 State and Territories
  - Eligible entities have 60 days to submit applications, **due November 15, 2022**
  - NOFO outlines administrative and programmatic requirements
  - Applications will be reviewed by CISA and FEMA with awards being made NLT December 31
  - Tribal consultation is ongoing, Tribal Cybersecurity NOFO will be released at a later date

Requirements

- Notice of Funding Opportunity (NOFO) Requirements
  - Existing State Administrative Agency will serve as state-level applicant
  - CIO, Chief Information Security Officer (CISO), or an equivalent official must be on planning committee
  - Specific best practices that must be in Cybersecurity Plan and projects

Eligibility

- The State Administrative Agency (SAA) is the only entity eligible to submit SLCGP applications to DHS/FEMA.

- Local government" is defined in 6 U.S.C. § 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;

- As part of the local government pass through requirement, in obligating funds, items, services, capabilities, or activities to local governments, each eligible entity or multi-entity group is required to pass through at least 25% of the federal funds provided under the grant to rural areas. Per the Homeland Security Act of 2002, **a rural area is defined in 49 U.S.C. § 5302 as an area 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.**

Eligibility (continued)

- Local governments are eligible as sub-applicants to their SAA and must work with their state or territory’s Cybersecurity Planning Committee to receive subawards.
- Local governments are defined in the law as 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; an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and a rural community, unincorporated town or village, or other public entity.

FUNDING

- Eligible entities or multi-entity groups are statutorily required to provide at least 80% of the federal funding to local governments, including at least 25% rural areas. With the consent of the local governments, part or all of this pass-through can be in the form of items, services, capabilities, or activities. This flexibility in the type of funds that are passed through may assist eligible entities or multi-entity groups in promoting projects that have state-wide (or broader) impacts, and they may be able to more effectively reduce cybersecurity risk if managed at the state or multi-state level. Examples of these types of projects include the purchase of software licenses or development of capabilities. Any decision to pass through some or all of the funds via items, services, capabilities, or activities must be explicitly consented to by the local governments and must be documented in accordance with the Cybersecurity Planning Committee's Charter and comply with Section F.2 of the NOFO for further information.

FUNDING FY 2022 – Minnesota : $3,605,449

- State Government (20%) $ 721,089.80
- Locals (80%) $2,884,359.20
- **Minnesota 2022 Total Funding $3,605,449**
- Rural (25%) $ 901,362.25
- Remaining Locals: $1,982,996.95
- State Government 5%
  Maintenance & Administration $36,054.49
- Period of Performance is 48 months, extensions permitted on a case-case basis.

Locals	**$2,884,359.20**
87 Counties	**$33,153.55**
Counties plus 94 cities with pop range between 10,000 and 100,000	**$15,935.69**
Counties plus 803 total cities	**$3,240.85**

FUNDING NOT PERMITTED

- 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 SLT has previously used SLT 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 alternations 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, or on behalf of, the eligible entity that receives the grant or a local government within the jurisdiction of the eligible entity.

Policy Areas of Emphasis

- **Holistic approach** to the Cybersecurity Plan. The Cybersecurity Plan should be strategic in nature, guiding development of capabilities to address cybersecurity risks and threats across the state or territory. Individual projects should demonstrably support the state, territorial, and local entities in achieving those capabilities over time.
- **Focused investments** that are sustainable over time. The SLCGP currently is authorized for 4 years, and limited funds are available. Cybersecurity Plans must address how SLT entities will sustain capabilities once the program ends or funds are no longer available.
- **State role as leader and service provider**. Many states have significant cyber defenses and elect to provide services to local entities to improve capabilities. Where appropriate, states should consider approaches to support state-wide efforts, that may include using funds to provide services to local entities. Multi-entity projects are another way that eligible entities can group together to address cybersecurity risk and build capabilities (See Appendix D for additional information on multi-entity activities).
- **Building from existing efforts.** Cybersecurity Committees should consider describing how cooperative programs developed by groups of local governments are integrated into the entity-wide approach.
- Additional cybersecurity elements prioritized by the Cybersecurity Planning Committee.

Cybersecurity Best Practices

- Recipients may be required to include adoption of specific cybersecurity best practices in their Cybersecurity Plans
- Individual projects support implementation over time, as appropriate:
  - Implement multi-factor authentication.
  - Implement enhanced logging.
  - Data encryption for data at rest and in transit.
  - End use of unsupported/end of life software and hardware that are accessible from the Internet.
  - Prohibit use of known/fixed/default passwords and credentials.
  - Ensure the ability to reconstitute systems (backups).
  - Migration to the .gov internet domain.

Required Services

- All SLCGP grant recipients and sub-recipients will be required to participate in a limited number of free services and memberships sponsored by CISA. Participation in these services and memberships are not required for submission and approval of a grant.
- Memberships in the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) are highly recommended but not required.
- NOFO will include descriptions and instructions.
- CISA will prioritize service delivery for awardee/sub-awardee applications.

Required Services (continued)

Cyber Hygiene Services

- **Web Application Scanning** is an “internet scanning-as-a-service.” This service assesses the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, 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.

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 National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC.
- Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually.

Planning Committee Membership

- Can be an existing committee but must follow the defined guidance.
- The responsibilities of the Cybersecurity Planning Committee include:
  - The Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or equivalent official of the eligible entity;
  - If the eligible entity is a state, then representatives from counties, cities and towns within the jurisdiction of the eligible entity;
  - Public education institutions within the jurisdiction of the eligible entity;
  - Public health institutions within the jurisdiction of the eligible entity; and
  - As appropriate, representatives of rural, suburban, and high population jurisdictions.

Planning Committee Membership (continued)

At least half of the representatives of the Cybersecurity Planning Committee must have professional experience in cybersecurity or information technology.

Consideration should be given to include other members, including but not limited to representatives from:

- State and county judicial entities;
- State legislature;
- Election infrastructure officials, including secretaries of state and election directors;
- Representatives from state, territorial, and local public safety, homeland security, emergency management and law enforcement agencies;
- Emergency communications officials;
- City and county CIOs and CISOs;
- Publicly owned or operated critical infrastructure;
- State National Guard if such entities have a cybersecurity mission;
- Municipal, city, county, rural area or other local government councils or associations; and
- Other entities with expertise and skillsets that best represent the cybersecurity interests across the eligible entity.

Planning Committee Membership (continued)

- CISA may designate one or more employees to serve as a liaison to the Committee, as allowed by DHS Management Directive 2300, Committee Management, pg. 11 ("In lieu of official participation as a member, the approving official should consider permitting DHS personnel to participate as an observer or liaison, particularly for non-Government committees.") A CISA employee acting in a liaison capacity may provide technical assistance to the Committee on cybersecurity matters and may attend Committee meetings if invited, but should not participate in the Committee's decision-making, such as by voting on or approving the Cybersecurity Plan or other proposed activities or projects.

Planning Committee Responsibilities

The responsibilities of the Cybersecurity Planning Committee include:

- Assisting with the development, implementation, and revision of the Cybersecurity Plan;
- Approving the Cybersecurity Plan;
- Assisting with the determination of effective funding priorities;
- Coordinating with other committees and like entities with the goal of maximizing coordination and reducing duplication of effort;
- Ensuring investments support closing capability gaps or sustaining capabilities; and
- Assisting the state in ensuring local government members, including representatives from counties, cities, and towns within the eligible entity provide consent on behalf of all local entities across the eligible entity for services, capabilities or activities provided by the eligible entity through this program.

Cybersecurity Plan Components

- Roles and responsibilities
  - Statewide Plan
  - Plan not required of local governments
- Required elements
- Discretionary elements
- Capabilities assessment
- Implementation plan
- A summary of projects
- Metrics

Cybersecurity Plan Basics

- Statewide comprehensive strategic plan to reduce cybersecurity risk and increase capability;
- Entity-wide plan, not a single entity;
- Should cover 2 to 3 years;
- Must describe how input and feedback from local governments and associations of local governments was incorporated;
- Must describe the individual responsibilities of the state and local governments within;
- Must include required elements, with discretion to add other elements as necessary;
- Current documents:
  - Existing governance and planning documents and identification of any planning gaps that should be addressed by the Cybersecurity Plan;
  - Existing assessments and evaluations (e.g., reports, after action reports) conducted by SLT governments within the entity and any planning gaps that require additional assessments and/or evaluations;
- Template available but not required to use. Required elements must be identifiable for review purpose;
- Individual projects & identified gaps must align to Cybersecurity Plan;
- Must be approved by the Cybersecurity Committee **and** CIO/CISO/Equivalent;
- CISA approves for DHS;
- Plans are initially approved for 2 years; annually thereafter;

Evaluation Criteria

- DHS/FEMA will evaluate applications for completeness and applicant eligibility. DHS/CISA will evaluate applications for adherence to programmatic guidelines and anticipated effectiveness of the proposed investments. The review will include verification of the following elements:
- Cybersecurity Plan(s) or request for exception;
- Proposed projects that are consistent with the Cybersecurity Plan(s), or will be consistent with the Cybersecurity Plan if requesting a grant to develop a Plan, and SLCGP program objectives and requirements;
- Proposed projects are feasible and effective as reducing the risks the project was designed to address; and
- Proposed projects will be completed within the period of performance.

For more information:
www.cisa.gov

Chris Gabbard
Cybersecurity Advisor
Region 5 – Minnesota District
Phone: 612-716-3044
Email: christopher.gabbard@cisa.dhs.gov