Bloomberg Federal Assistance e311 Content Workshop:

Cybersecurity Funding and Solutions

Bloomberg Philanthropies

THE UNITED STATES CONFERENCE OF MAYORS

E311 Workshop | Panelists & Subject Matter Experts

Trent Frazier
Deputy Assistant Director for Stakeholder Engagement Division, Cybersecurity & Infrastructure Security Agency

Bess Mitchell
Grants Branch Chief, Cybersecurity & Infrastructure Security Agency

Christopher Terry
Senior Manager Forensic & Integrity Services, EY

Chris Apple
Product Manager, Cybersecurity Solutions, Global Cyber Alliance

Bloomberg Philanthropies

THE UNITED STATES CONFERENCE OF MAYORS

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

EY Building a better working world

GLOBAL CYBER ALLIANCE

Workshop Goals

- *Provide cities with an understanding of how to access funding opportunities including the State and Local Cybersecurity Grant Program (SLCGP) and other funds available in the Bipartisan Infrastructure Law (IIJA), the application processes, and methods to optimize funding.*
- *Provide an overview of cybersecurity risks and tools that cities can use to build up their defenses and mitigate risk.*

Agenda

Part One: SLCGP

Presented by: Cybersecurity & Infrastructure Security Agency (CISA)

Introduction: CISA/FEMA Roles/Responsibilities

Update: Summary of the State and Local Cybersecurity Grant Program

Next Steps: Program Requirements and Engagement

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM

FEMA

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%

FEMA

Grant Program Goal & Objectives

- **GOAL: Assist SLTT governments with managing and reducing systemic cyber risk.**
  - Objective 1-Governance & Planning
  - Objective 2-Assessment & Evaluation
  - Objective 3-Mitigation
  - Objective 4-Workforce Development
- **Detailed information regarding the Goal and Objectives can be found in the NOFO**

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 jurisdictions (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

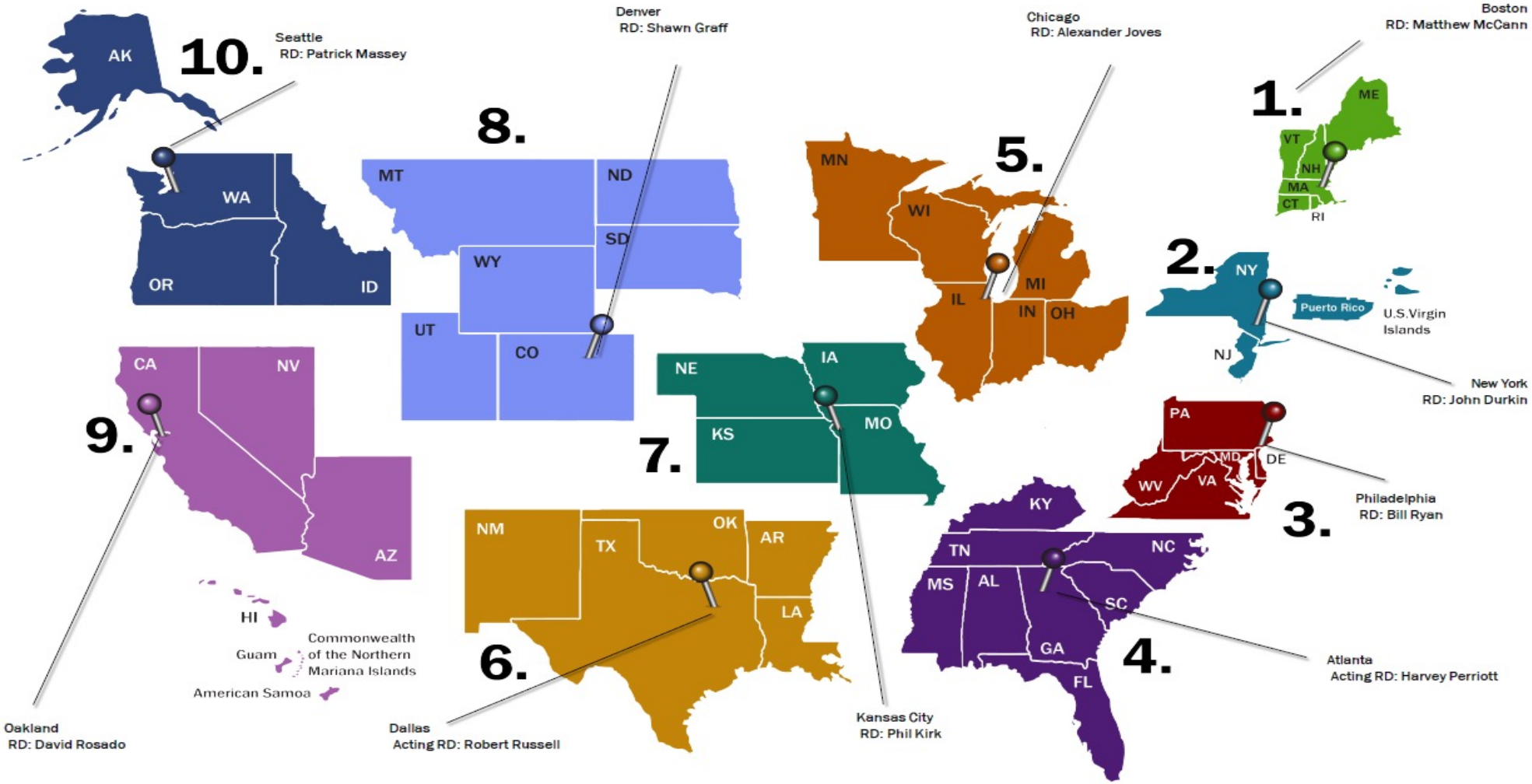
Notice of Funding Opportunity (NOFO)

- **The State and Local Cybersecurity Grant Program (SLCGP) NOFO was released Friday, September 16**
  - Included detailed allocations for all 56 State and Territories
  - Eligible entities have 60 days to submit applications, due November 15
  - NOFO outlines administrative and programmatic requirements
  - Applications will be reviewed by CISA and FEMA with awards being made NLT December 31
    - Completed Cybersecurity Plans are NOT required to be submitted with application
  - Tribal consultation is ongoing, Tribal Cybersecurity NOFO will be released at a later date

Program Next Steps

- Eligible Entities engage with CISA staff on programmatic questions, and FEMA staff for administrative questions:
  - To contact CISA: SLCGPinfo@cisa.dhs.gov or www.CISA.gov/cybergrants
  - To contact FEMA: ASKCSID@fema.dhs.gov
- During the application development process, SAA's should identify members of Statewide Cybersecurity Planning Committees in accordance with NOFO requirements, and begin developing Statewide Cybersecurity Plans
  - Eligible entities should reach out to CISA Regional Staff for assistance in establishing these committees

CISA Regional Structure



FEMA

Agenda

Part Two: IIJA

Presented by: EY

IIJA Cybersecurity-Specific Funding

Other IIJA Funding Programs With Cybersecurity Components

Key Activities to Optimize Funding

Best Practices Spotlight

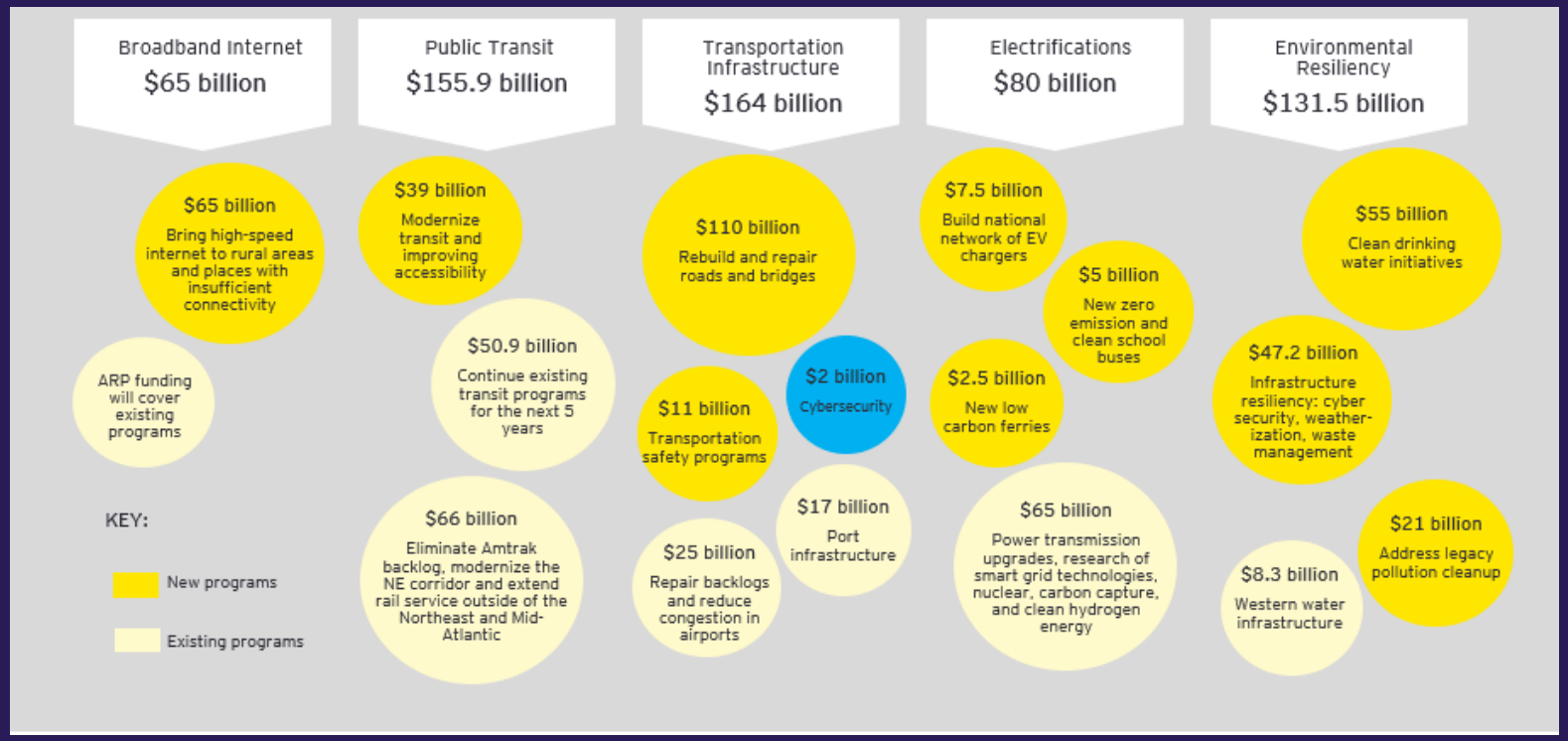
Bloomberg Philanthropies

THE UNITED STATES CONFERENCE OF MAYORS

EY Building a better working world

The Infrastructure Investment and Jobs Act Components

Authorized a historic $1.2T level of funding to states, territories, tribes and localities to address pressing infrastructure needs, **with substantial attention to broadband expansion and cybersecurity concerns, and to that end, appropriated $2B over the next several years to cybersecurity programs specifically.**

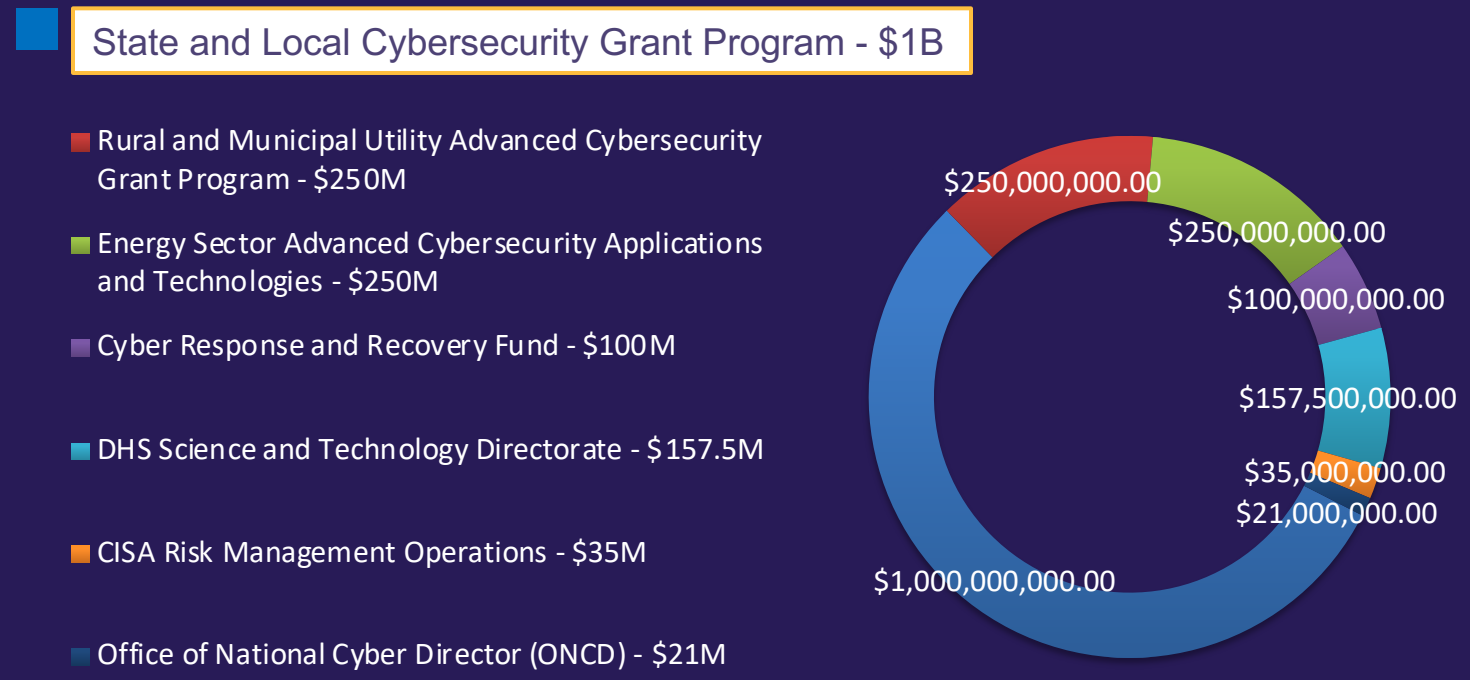


Bloomberg Philanthropies

THE UNITED STATES CONFERENCE OF MAYORS

IIJA Cybersecurity-Specific Funding

Breakdown of the $2B for Cybersecurity authorized by the IIJA, includes grants to improve the cybersecurity architecture of state and local schools, hospitals, parks, etc., through 2025.



Bloomberg Philanthropies

THE UNITED STATES CONFERENCE OF MAYORS

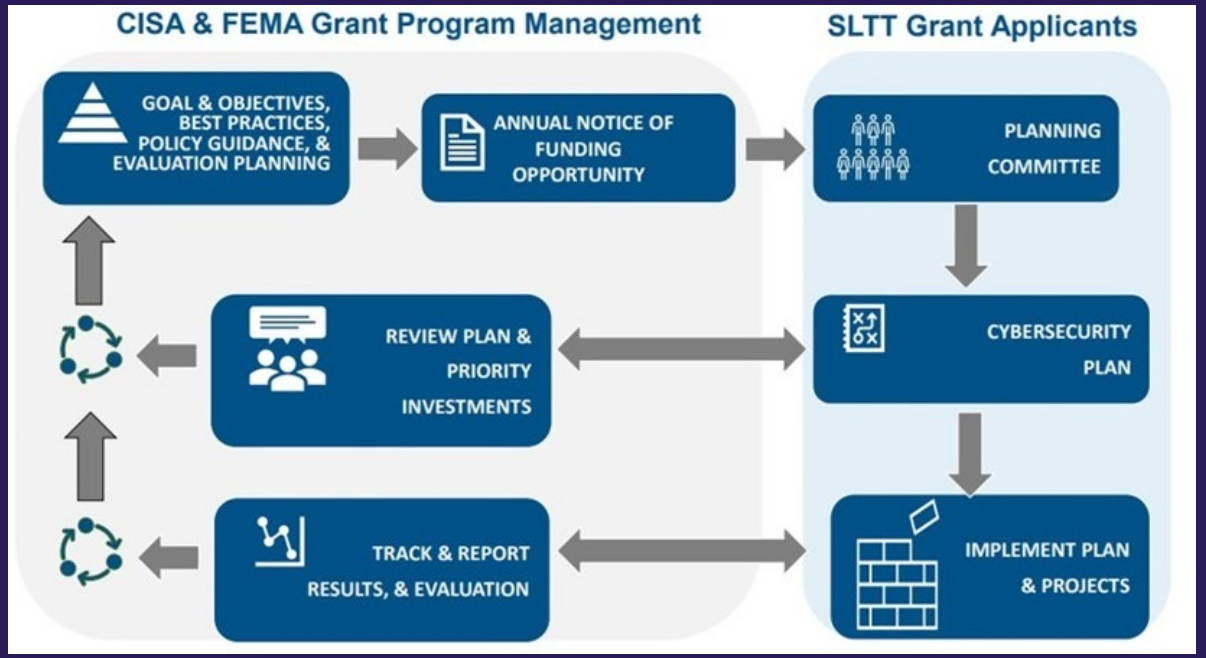
Other IIJA Programs with Cybersecurity Components

Programs That Permit Expenditure On Cybersecurity Measures

- U.S. Department of Commerce
  - Broadband Equity, Access, and Deployment Program (BEAD) - $42.5B
- U.S. Environmental Protection Agency
  - Clean Water and Drinking Water State Revolving Funds (SRF) - $11.7B
  - Drinking Water State Revolving Fund - $11.7B
- U.S. Department of Transportation Programs
  - Port Infrastructure Development Program - $2.25B

Key Activities to Optimize Funding

- Contact your State Administrative Agency (SAA) and State-wide Cybersecurity Planning Committee directly to offer input to your state's cybersecurity plan. (A full list of SAA contacts can be found at this link.)
- Understand policy areas of emphasis
  - Develop holistic approach to the Cybersecurity Plan
  - Target focused investments, sustainable over time
  - Establish strong planning committees
  - Support state role as leader and service provider



Bloomberg Philanthropies

THE UNITED STATES CONFERENCE OF MAYORS

Key Activities to Optimize Funding (continued)

- Keep in mind the following considerations when pursuing federal dollars for cybersecurity for mitigation measures:
  - 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
- Understand what other State, Local, Tribal, and Territorial (SLTT) governments are doing to prepare
- **Consider becoming members of MS-ISAC for access to numerous free cybersecurity resources (membership link in chat)**

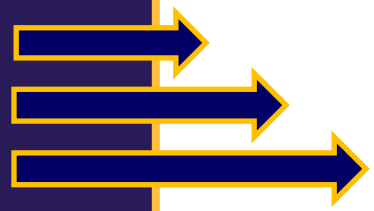
What Some State, Local, Tribal and Territorial (SLTT) Governments are Doing to Prepare

Federal Cybersecurity Grant Subrecipients in New Mexico

- New Mexico Gov. Michelle Lujan Grisham established a Cybersecurity Planning Committee to guide New Mexico's initiatives to protect the state's information security and privacy
- The committee will perform the following functions:
  - plan and develop a robust cyberinfrastructure to address risks and threats to information systems owned by state and local governments
  - advise the governor regarding necessary cybersecurity legislation and support applications to receive federal funding to address cybersecurity needs and challenges
- The committee will include cybersecurity professionals, to be appointed by the governor, from state agencies, school districts, counties, cities and tribal communities

How Cities Should Work With States

- Cities should coordinate with cybersecurity planning committees and state CISO directly to offer assistance in providing input to the statewide cybersecurity plan
- Cities should also consider participating on the planning committee itself



Bloomberg Philanthropies

THE UNITED STATES CONFERENCE OF MAYORS

Other Cybersecurity Funding Best Practice

ARPA Cybersecurity Grant Subrecipients in Texas

- Federal cybersecurity grant subrecipients in Texas fared best in securing federal funding when they coordinated expeditiously in preparing detailed applications, budget estimates, and project scope.

Lessons Learned

- Detailed project scope that aligned to program areas of emphasis
- Detailed budget, included itemization of capital versus operational costs
- Coordinated with other cities and counties to form a multi-group project
- Sustainability considerations made
- Coordinated multiple funding options and supplantation

Bloomberg Philanthropies

THE UNITED STATES CONFERENCE OF MAYORS

City Spotlight: Albany, New York

Mayor Kathy Sheehan

Albany, New York

- Highlighting cybersecurity risks and solutions in real-time experience by the City of Albany
- 2019 Ransomware Attack: Lessons Learned

ALBANY
NEW YORK | EST. 1686

Bloomberg Philanthropies

THE UNITED STATES CONFERENCE OF MAYORS

Agenda

Part Three: Solutions

Presented by: Global Cyber Alliance (GCA)

Cities are Easy Prey for Cyber Criminals

Update Your Defenses with Cybersecurity Funding

Reminders & Understanding Your Controls

GLOBAL CYBER ALLIANCE™

Bloomberg Philanthropies

THE UNITED STATES CONFERENCE OF MAYORS

Cities are Easy Prey for Cyber Criminals

Real World Consequences

- Disruption of critical services to residents (e.g., cyber attacks on 911 call centers, electric grids, traffic signals, hospitals)
- Financial loss
- Breach of sensitive/residents' information
- Risk to public safety
- Mis/disinformation planted on websites or social media

Vulnerability Reminders

- Loopholes, open doors, unguarded entryways
- Phishing emails and social engineering
- Flaws in software or operating systems
- Use of malware and ransomware
- User complacency

Bloomberg Philanthropies

THE UNITED STATES CONFERENCE OF MAYORS

Update Your Defenses with Cybersecurity Funding

Root out knowledge gaps in your own cyber environment:

- What is in your IT environment?
- Who is on your network and what is connected to the Internet?
- Where is your most sensitive data?
- Do any access levels unknowingly enable malicious actions?
- Does legacy access exist?
- Is your network segmented? Are networked systems regularly patched?
- Who has remote network access, and do they need it?
- Do you have periodic reviews of the above?
- Do you manage and monitor critical social media accounts?

Use identified gaps or deficiencies to craft specific, effective grant applications.

Bloomberg Philanthropies

THE UNITED STATES CONFERENCE OF MAYORS

Reminders & Understanding Your Controls

Most ransomware attacks target state & local governments

Password Vulnerabilities

- Are you using Multifactor Authentication (MFA) everywhere that you should?
- Do you conduct security awareness training?
- Do you mandate strong passwords?
- Do you conduct phishing tests?

Phishing, Malware, Ransomware

- Do you mandate the installation of AV software, and is it auto-updated? How do you detect and contain unprotected devices?
- Have you implemented DNS security to prevent access to malicious domains?
- Do you allow unvalidated USB devices to be used?

Backup & Recovery Issues

- Do you maintain both online and offline backups?
- How are both types of backups secured?
- Is backup frequency sufficient to minimize data loss and ensure adequate recovery time?

By answering these questions, cities can identify vulnerabilities that can become opportunities for the use of federal funds.

Bloomberg Philanthropies

THE UNITED STATES CONFERENCE OF MAYORS

Resources

For more information, visit:

https://bloombergcities.jhu.edu/program/e311

Connect with today's panelists & subject matter experts online to learn more:

Cybersecurity Infrastructure & Security Agency SLCGPinfo@cisa.dhs.gov or www.CISA.gov/cybergrants

EY: https://www.ey.com/en_us

Global Cyber Alliance: https://www.globalcyberalliance.org/

Additional Resources:

Federal Emergency Management Agency: ASKCSID@fema.dhs.gov

To contact your SAA: https://www.fema.gov/grants/preparedness/about/state-administrative-agency-contacts

To learn more about the MS-ISAC or to become a member: https://www.cisecurity.org/ms-isac

Bloomberg Philanthropies

THE UNITED STATES CONFERENCE OF MAYORS

Q&A

Bloomberg Philanthropies

THE UNITED STATES CONFERENCE OF MAYORS