# Joint Committee on
# Cybersecurity, Information Technology, and Biotechnology
## Tuesday, November 9, 2021, 10:00 a.m.
## Meeting via Zoom

---

**Opening Remarks**

**Maryland Cybersecurity Council Report Findings (Part 1)**

*Dr. Greg von Lehman, University of Maryland Global Campus – Staff to the Maryland Cybersecurity Council*

*Chip Stewart, Department of Information Technology - State Chief Information Security Officer*

**Maryland Cybersecurity Council Report Findings (Part 2)**

*Ben Yelin, University of Maryland Center for Health and Homeland Security – Program Director for Public Policy & External Affairs*

*Russel Strickland, Department of Emergency Management – Acting Secretary*

*Laura Corcoran, Maryland Cybersecurity Council – National Security Agency Fellow*

**Hazard Planning and Information Sharing**

*Russel Strickland, Department of Emergency Management – Acting Secretary*

*Jay Kaine, Motorola Solutions Cybersecurity – Director of the Cyber Threat Fusion Center*

*Kyle Bryans, MS ISAC – Senior Program Specialist*

**Closing Remarks**

Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

# Task II
# Review of State Cybersecurity
# State Chief Information Security Officer
# Chip Stewart

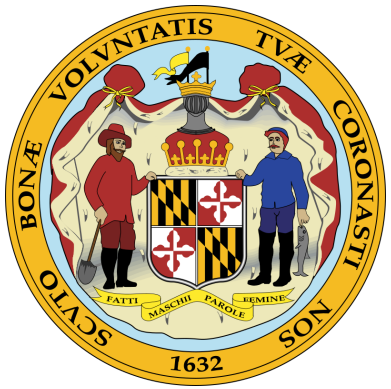
# Annapolis Cybersecurity Summit

- Maryland Data Privacy Executive Order
- Chief Data Officer Executive Order
- New Partnership with National Security Agency
- Established the Maryland Institute for Innovative Computing through a partnership with the University of Maryland Baltimore County
- MD THINK Executive Order

# Survey Data and Format

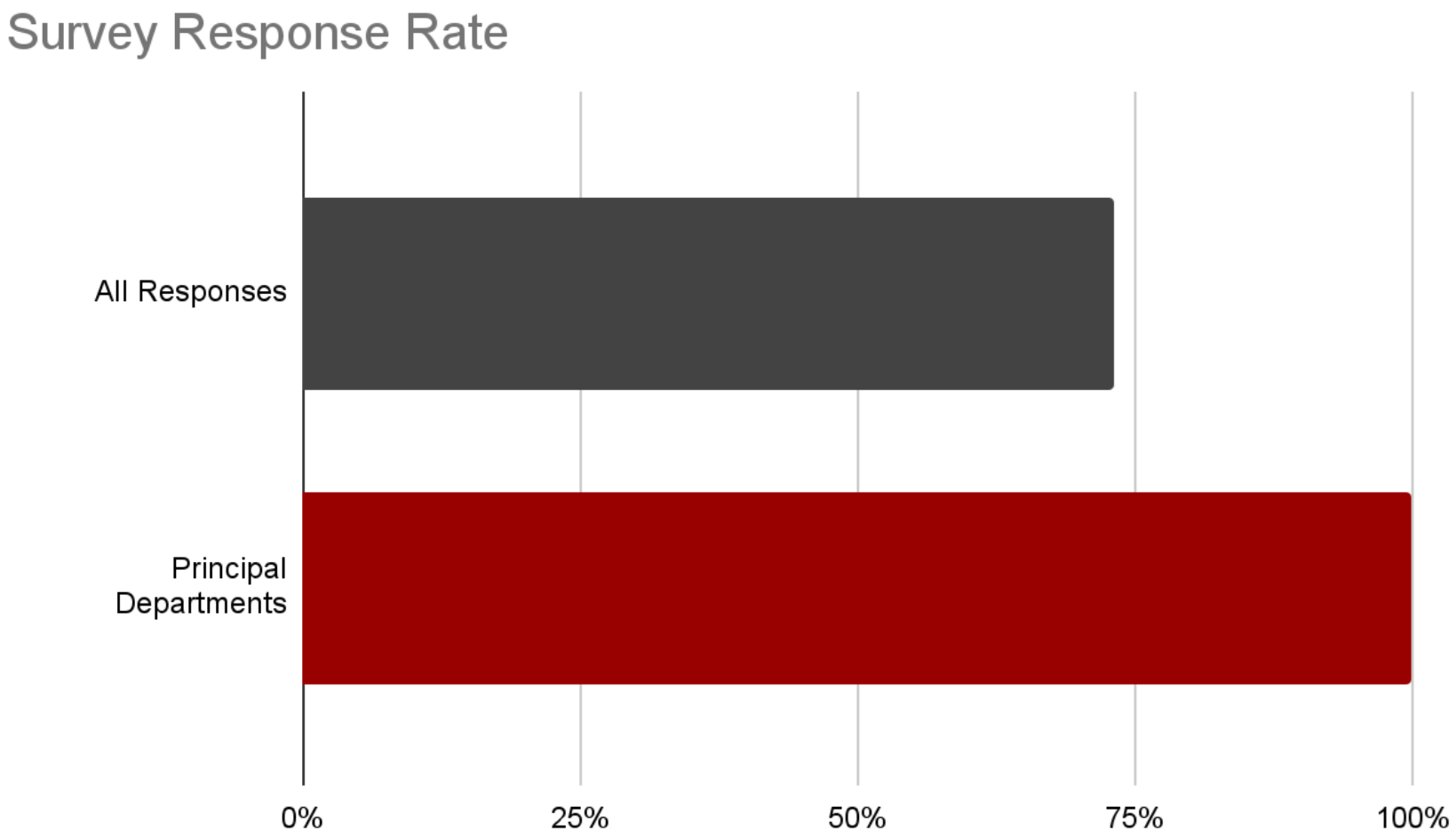
Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

MARYLAND
OFFICE OF THE ATTORNEY GENERAL

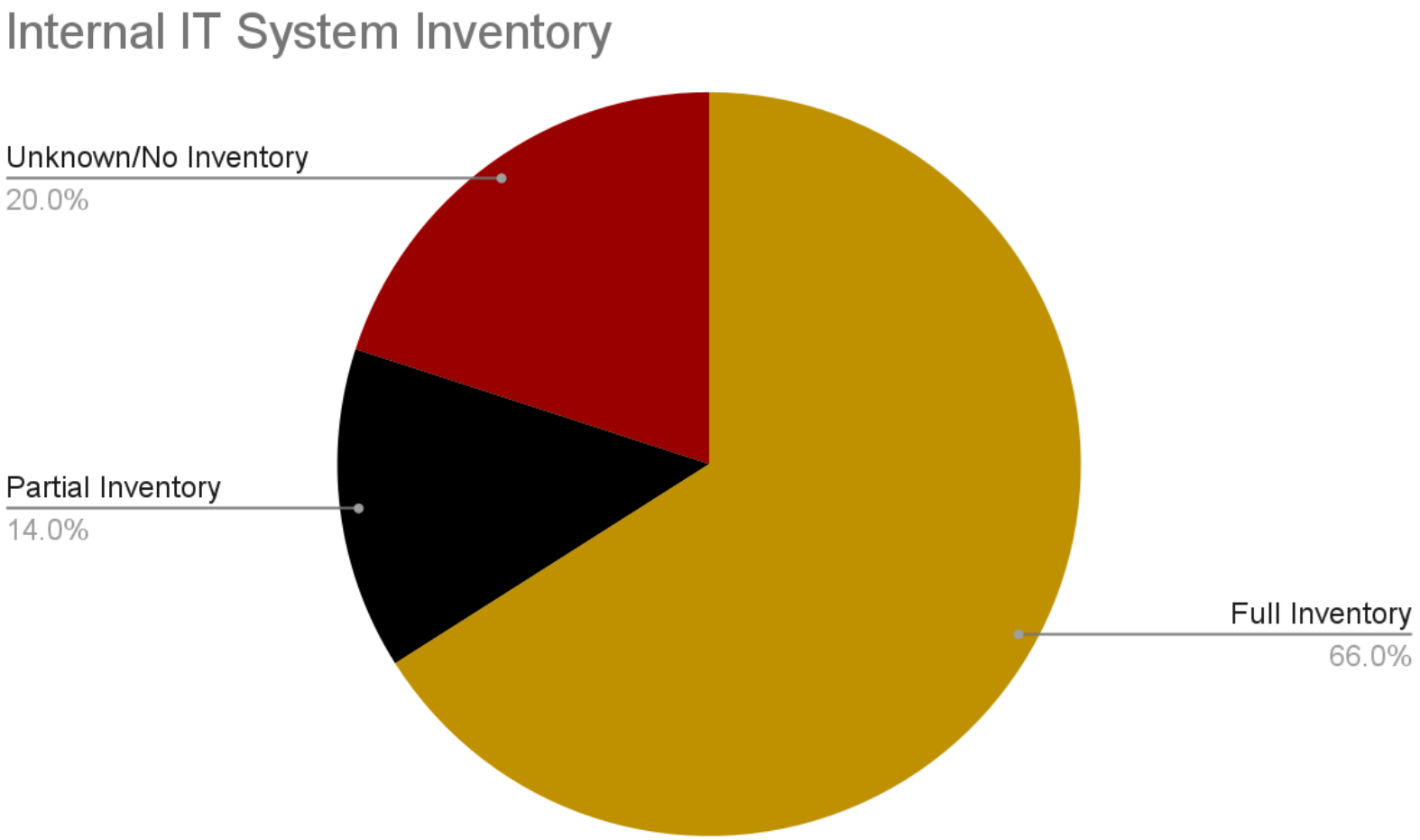



UNIVERSITY OF MARYLAND
18 56

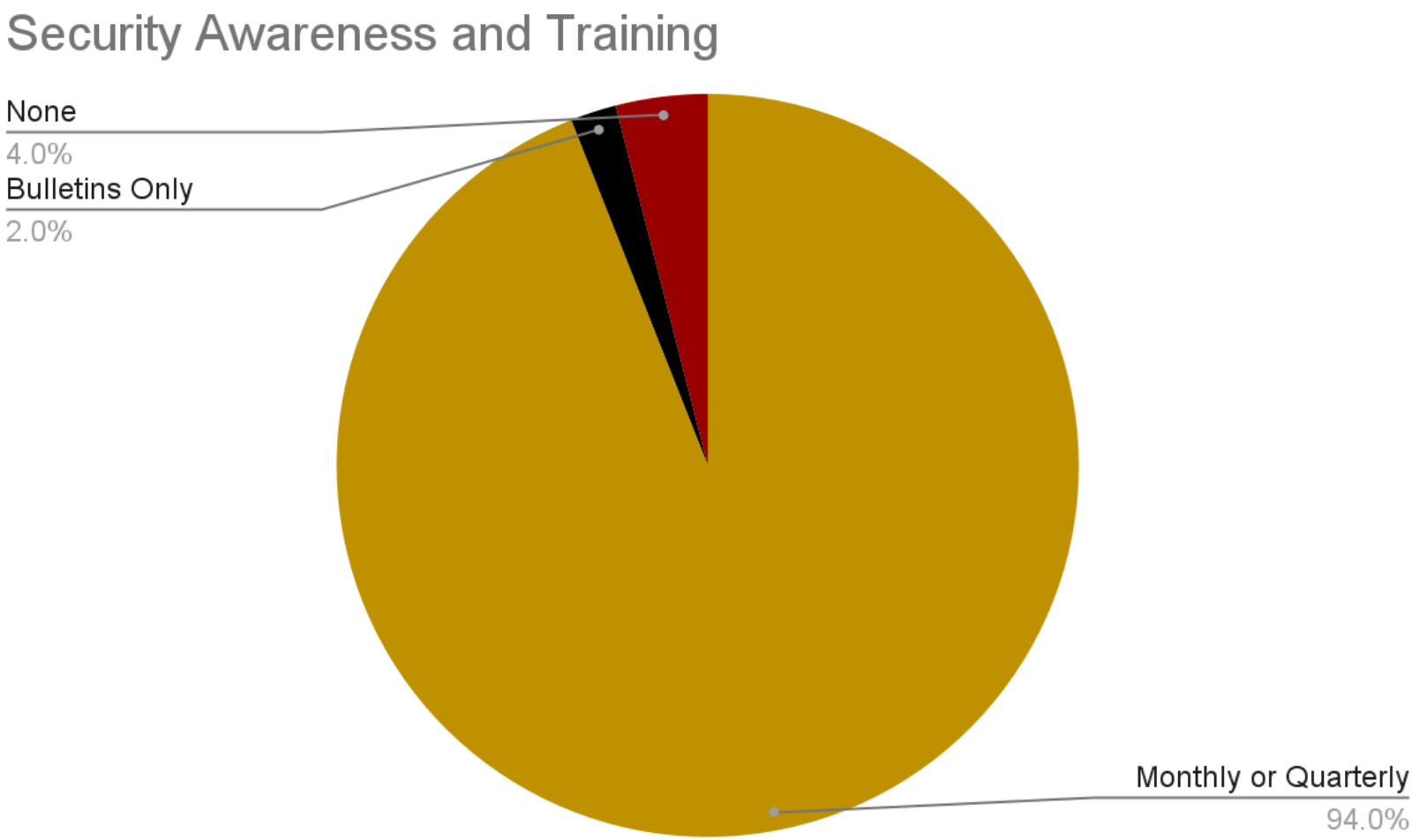
# Report Response Rates



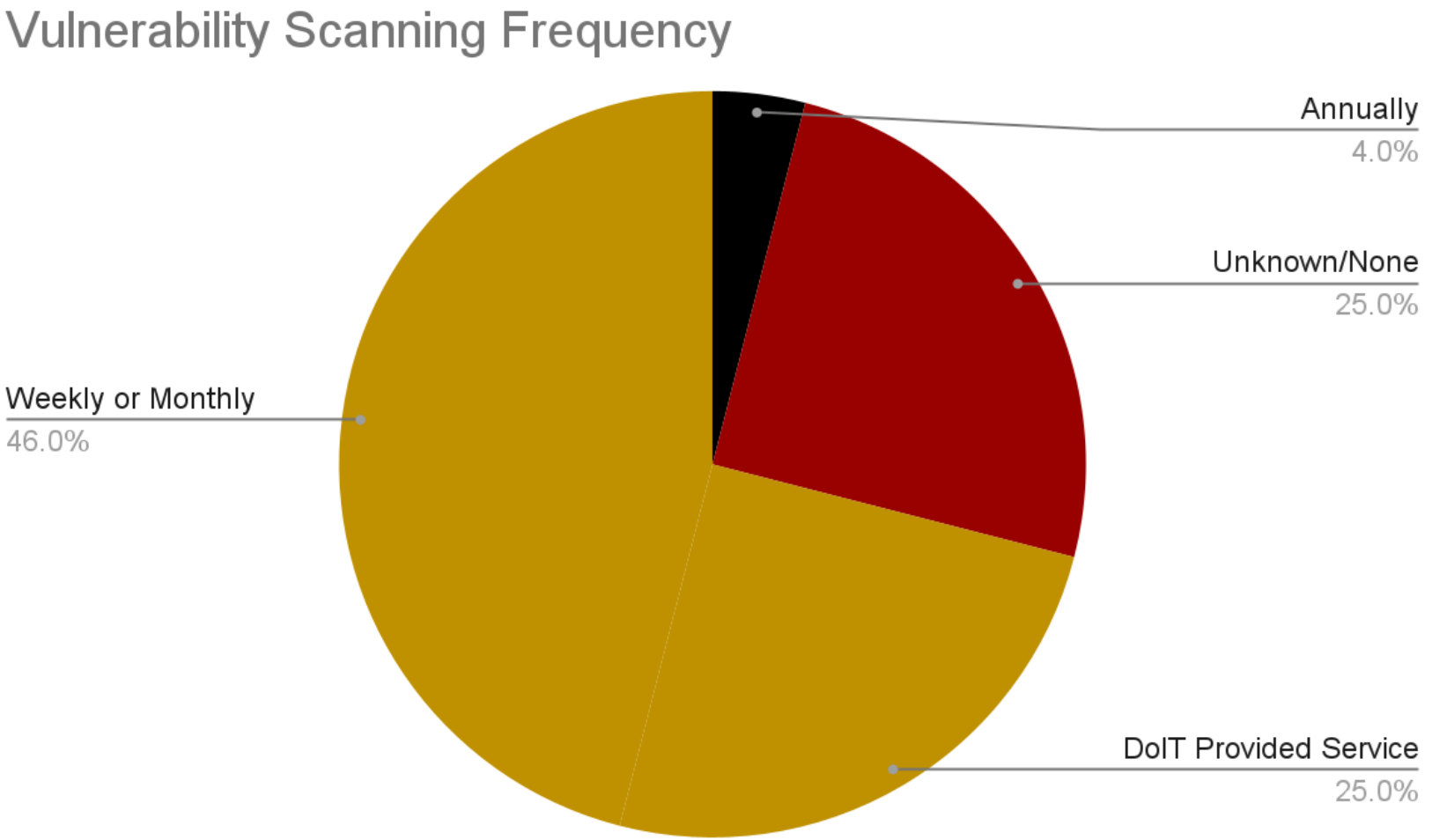
# Identify
# Asset Management



# Protect
# Security Training



# Protect
# Vulnerability Scanning



# Protect
# Risk Management

1

## External Vulnerability Assessment

Resources engaged in consistent vulnerability scanning, evaluation, and mitigation of the State's networks and systems.

2

## Threat Intelligence Management

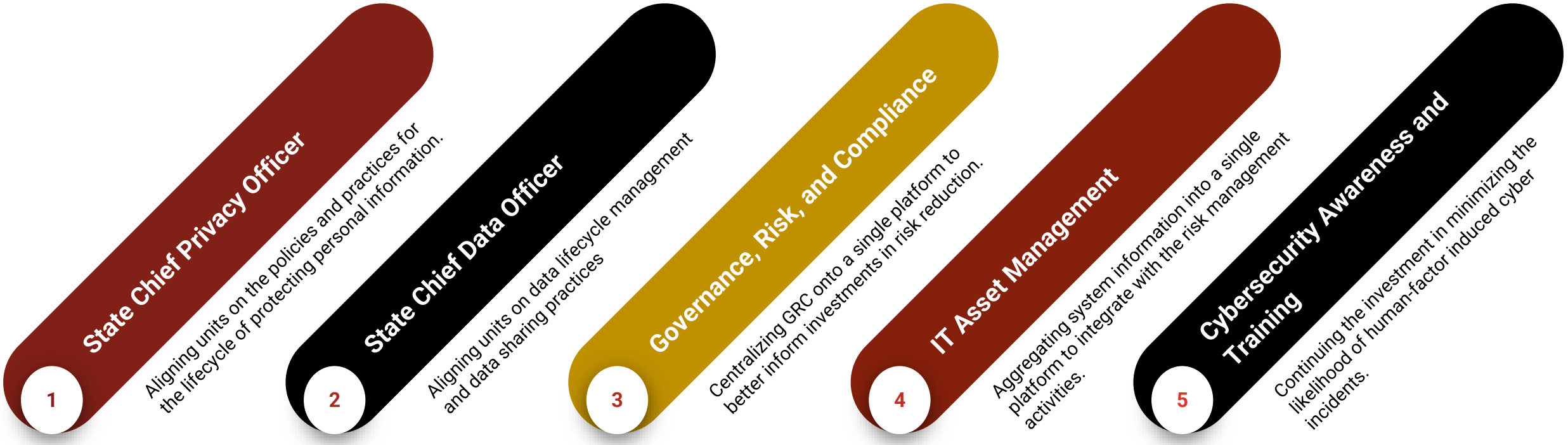
Pulling information from the dark web and other sources to connect dots from threat actors to vulnerability

3

## Ongoing Risk Assessment

Heavy focus on adversarial external threats at the state-wide level.

# Ongoing Initiatives



# New Initiatives

1

## Backups

Having and being able to restore backups is crucial for recovering from cyberattacks and other disasters.

2

## Multi-Factor Authentication

Passwords are no longer enough to secure accounts. Centralized multi-factor authentication is one of the most effective ways to prevent access through a valid account.

3

## Vulnerability Management

Implementing vulnerability management tools, continuously scanning for vulnerabilities, and prioritizing response is one of the most impactful ways to reduce risk.

Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

# Questions

# State Cybersecurity Study
# Ad Hoc Working Group
## CONVENED BY THE MARYLAND CYBERSECURITY COUNCIL

# Study Steering Committee

Co-chairs

- Ben Yelin, Center for Health and Homeland Security, Carey School of Law, University of Maryland, Baltimore, & Senator Katie Fry Hester (District 9, Carroll & Howard Counties)

Members

- Delegate Ned Carey (District 31A, Anne Arundel County)
- Kevin Kinnally, Legislative Director, Maryland Association of Counties
- Senator Susan Lee (District 16, Montgomery County)
- Chip Stewart, State CISO, Maryland Department of Information Technology
- Acting Secretary Russell Strickland, Maryland Department of Emergency Management
- Dr. Greg von Lehmen, University of Maryland Global Campus, Staff to the Maryland Cybersecurity Council

# Study Steering Committee

- CHHS Legal Externs/Interns Serving as Research Associates
  - Serena Chenery
  - Robert Layne
  - Gavin Rader
  - Alek Stathakis
  - Stephanie Vangellow
  - Mike Rovetto
  - Makenzie Donaldson

# Study Structure

- Task 1
  - Questions about cybersecurity governance
- Task 2
  - State agency questions
- Task 3
  - Local units of government questions

# Task 1

GOVERNANCE

# Questions

- What are the cybersecurity roles in managing risk (SCISO, DoIT, MDEM, local jurisdictions)? How can the State foster more collaboration?
- How can the State better collaborate with the federal government, other states and the private sector to leverage resources, share best practices, and better understand emerging cyber threats?
- How can the State improve its cybersecurity governance to consider county and municipal needs, respond to audit deficiencies, and increase awareness of State strategy and standards?
- What are the implications of the State's current fee-for-service and decentralized model for cyber risk? Other models?
- How does Maryland's IT strategy and security manual compare with other states? What are the opportunities for improvement?

# Task 1 Technical Consultations

Other States

- Daniel Dister (CISO, State of New Hampshire)
- Kevin Ford (former CISO, State of North Dakota)
- Michael Geraghty (CISO, State of New Jersey)
- Shawn Riley (CIO, State of North Dakota)

Related associations

- John Guerriero (Senior Policy Analyst, NGA)
- Mathew Pincus (Director of Government Affairs, NASCIO)
- Tony Sager, Brian DeVallance, and Curtis Dukes (Center for Internet Security),
- Jamie Ward (Account Executive, Center of Internet Security Services, Multi-State Information Sharing and Analysis Center),

Private Sector

- Kirk Herath (recently retired Associate General Counsel and Chief Privacy Officer, Nationwide Insurance).

Maryland

- Chip Stewart (State CISO)
- Acting Secretary Russell Strickland (MDEM)

# Five Major Themes to Reduce Cyber Risk

- Centralizing Executive Branch IT and cybersecurity management
- Supplementing procurement rules to enhance supply chain risk management
- Maturing the strategic risk management role of the Maryland Cybersecurity Coordinating Council
- Creating public accountability for cybersecurity spending as a measure of effort
- Leveraging other resources to reduce the cost of cybersecurity
- Enhancing strategic plans to provide more information about goals and objectives

# Centralization

Core Recommendations

- That the General Assembly codify the key elements of the EO (Maryland Cyber Defense Imitative), viz. the SCISO's position, the SCISO's the Office of Security Management, the authorities outlined in the EO consistent with two recent Executive Orders (Maryland Data Privacy) and (State Chief Data Officer), and the Maryland Cybersecurity Coordinating Council
- That  the IT functions of all agencies in the Executive Branch be centralized in DoIT and brought into the "enterprise". All IT budgets would become part of DoIT's budget and agency IT staff would report to the DoIT Secretary
- Similarly, that the cybersecurity functions of the Executive Branch agencies be centralized and made part of the "enterprise". All agency cybersecurity budgets would become part of one cybersecurity budget and agency cybersecurity staff would report to the SCISO.
- That the SCISO continue to be appointed by the Governor and that the Governor consider whether DoIT is the appropriate place for the SCISO

# Rationale for Centralization

- Permits unified operational direction of the State Executive Branch IT cybersecurity
- Provides complete visibility into agency IT and cybersecurity, eliminating  shadow IT
- Creates opportunity to achieve greater economies of scale
- Enables staffing flexibility, i.e., temporary reassignment of IT or cybersecurity staff from one agency to another to address emergencies
- Strengthens the SCISO role across the Executive Branch enterprise by retaining appointment by the Governor

# Supply Chain Risk Management

Core Recommendations

- That the State mandate basic security requirements as part of the procurement process for State contractors who will have access to State databases or systems consistent with a widely recognized standard such as NIST SP 800-171 or ISO 27001, CIS Controls, Cybersecurity Maturity Model Certification (CMMC), or other.
- That State agencies implement the intake procedure for all procurements of systems or devices, including procurements under $50,000, that connect to networks to ensure that IT solutions have a verified level of trust.

# Maturing Strategic Enterprise Risk Management: The Maryland Cybersecurity Coordinating Council

- Chaired by the SCISO
- Meets at least once a quarter
- Membership:
  - The Director of the Governor's Office of Homeland Security
  - The Secretary of Budget and Management
  - The Secretary of General Services
  - The Secretary of Human Services
  - The Secretary of Public Safety and Correctional Services
  - The Secretary of Health
  - The Adjutant General
  - The Director of the Maryland Emergency Management Agency
  - The Superintendent of State Police
  - The Secretary of Transportation

# Value of Enterprise-Level Governance Group

- How security controls to ensure confidentiality, integrity, and availability of data and systems are implemented requires tradeoffs in light of agency business functions. Data access controls that are too restrictive, for example, could make it too difficult to effectively provide certain citizen services. Agencies are best positioned to inform the SCISO about how to implement controls aimed at confidentiality, integrity, and availability in the context of agency business needs.
- Engagement creates buy-in and makes implementation easier.
- Finally, an enterprise-wide stakeholder group is best positioned to perform strategic-level risk framing, assessment, monitoring, and response planning. One of the fruits of this activity are recommendations that prioritize cybersecurity risk across the enterprise and target where investments can buy down the most risk.

# That Is the Job MCCC Is Meant to Do

- The strategic risk management function is called out in the EO
- According to the EO, “the MCCC shall provide advice and recommendations to the SCISO about
  - i) *strategy* and implementation of cybersecurity initiatives and recommendations; and
  - ii) building and sustaining the State’s capability to *identify, mitigate, and detect cybersecurity risk,* and to respond to and recover from cybersecurity-related incidents”. (Section D (2)).

# For the MCCC to Grow into the Strategic Risk Management Role

Core Recommendations

- That the risk assessments required by the State Security Manual be performed, aggregated, and prioritized by agencies and used by the MCCC to prioritize risk across the Executive Branch to inform strategic planning and to connect priorities with the budgeting process, i.e., make corresponding recommendations for security investments that will have the greatest impact in buying down risk.
- That representatives of the legislature and the State judiciary be added as nonvoting member of the MCCC and that the chair have the prerogative to invite other members as appropriate to participate in MCCC meeting.
- That the meetings of the MCCC be exempt from the Open Meetings Act so that it can be an ongoing forum for sensitive discussions of cybersecurity strengths and challenges and for shaping recommendations to the SCISO.

# Cybersecurity Funding Model

Core Recommendation

- That the cybersecurity budget for the State enterprise should be appropriated and not be reliant on the charge-back model

Rationale

- The perspective of several professionals interviewed is that the charge-back model for cybersecurity puts agencies in a bind between their own tight budgets and priorities on the one hand, and cybersecurity needs on the other, causes them to do their own balancing, and results in a reluctance to take on other costs. The result: headwinds to the implementation of more robust security
- Finding is supported by NASCIO's biennial surveys of state CIOs over more than a decade.
  - Since 2010, *insufficient cybersecurity* budget ranks as the top challenge
  - In the 2020 survey, lack of a *dedicated* cybersecurity budget ranked as the fourth major challenge

# Reference Point: Federal Spending Cyber (Appropriation Model)

| | Actual FY 2019 | Estimated FY 2020 | Proposed FY 2021 |
|---|---|---|---|
| | Billions of Dollars | | |
| 1) Federal Government Cyber | 16.937 | 18.792 | 18.779 |
| 2) Less DoD Cyber | -8.527 | -10.075 | -9.846 |
| 3) Equals Total Cyber Civilian | 8.410 | 8.717 | 8.933 |
| 4) Divided by Total Civilian IT Budget | 51.877 | 52.925 | 53.358 |
| 5) Equals % Civilian Cyber to Civilian IT | 0.162 | 0.165 | 0.167 |

Office of Management and Budget. FY 2021: A Budget for America's Future. Analytical Perspectives: pp 220 and 268-269 at https://www.novoco.com/sites/default/files/atoms/files/fy_2021_analytical_perspectives_budget_021020_0.pdf

# State Spending on Cybersecurity?

- Difficult to know, but NASCIO staff estimate spending of states across the US to be between 1-3% of total IT spend
- What is it in the Maryland Executive Branch? Not published

# Related Recommendation: Accountability for Funding Effort

Core Recommendation

- That the Governor's annual budget overview:
  - Should include statistics on the IT budget and the cybersecurity budget across the State enterprise
  - Include a comparison of cybersecurity budget to the IT budget ala annual OMB overview of the President's budget submission to Congress

# Leveraging Other Resources to Reduce Cost & Risk

Core Recommendations

- Utilize the Critical Infrastructure Security Agency program to implement the .gov domain in all State agencies and political subdivisions
- Join the Multi-State Information Sharing and Analysis Center (MS-ISAC) for a wide range of security services at deeply discounted pricing
- State consideration of partnerships with other states to achieve greater buying power on contract vehicles that agencies and local units of government could use to obtain cybersecurity services

# Changes in Strategic Planning

Core Recommendations

- That there be a fully developed, cybersecurity strategic plan separate from the Maryland IT Master Plan and that both be informed by MCCC and consultations with pollical subdivisions
- That both the Maryland IT Master Plan and any cybersecurity strategic plan attach timelines and appropriate metrics to the plans' goals and objectives and
- That the cybersecurity strategic plan provide information about the maturity level of the State's cybersecurity and how goals and objectives will advance that maturity.

# Rationale

- Separate cybersecurity strategic plan would serve as a guide for a separate centralized cybersecurity budget for the Executive Branch.
- Metrics would better inform about timelines and what success looks like for both the IT Master Plan and a separate cybersecurity strategic plan
- Linking the cybersecurity strategic plan to a maturity model would show the coherence of discrete goals and objectives in advancing the cybersecurity of the State.

# Task 2

REVIEW OF STATE CYBERSECURITY

# Task 2: Recommendations

1. DoIT should conduct a **Bi-Annual Cybersecurity survey** of all state agencies every-other year.
2. Work with all the Chief Data Officer and state agencies to produce the first baseline report of specified state data.
3. Each state unit should complete a complete **inventory of their IT system** by the end of the year in order to successfully manage risk.
4. Each State unit should develop specific **Recovery Time Objectives/Recovery Point Objectives** to ensure system recovery and continuity of services in the event of a cybersecurity incident or other disaster.

# Task 2: Recommendations

7. The Office of Security Management should ensure that an **external vulnerability and risk assessment** is completed for each State unit once every other year.
8. The Chief Data Officer and the Chief Privacy Officer should work with agencies to **develop standards** to describe sensitive information and to establish information sharing and data use agreements.
9. All state units should conduct **regular backup operations** and more frequent restoration testing.
10. State agencies should operate with **multi-factor authentication practices** for remote access and email access.
11. All units of state government must conduct **cybersecurity training** that reflects best practices and is available for all regular and contractual employees.

# Task 2: Recommendations

12. All units of state government must complete **regular vulnerability scans**.
13. All units of state government should be able to describe the remediation objective-time for vulnerabilities of various severities.
14. Given the number of legacy systems in State units, the State should **prioritize funding for upgrades** and modernization efforts.
    - The General Assembly should consider bonding for a major investment in updating the state's technical deficit in a manner similar to that undertaken by the State of Massachusetts.
    - A new oversight board (similar to the BPW process, but specific for IT) should be charged with oversight of the investment.

# Task 3

## LOCAL UNITS OF GOVERNMENT QUESTIONS

# Task 3: Introduction & Overview

- Purpose was to evaluate cyber readiness and operational needs of the State's local governments and subdivisions, and determine how State could best improve cybersecurity posture at the local level.
- Risk assessment that evaluated the preparedness of **County Governments**, **municipal governments**, **local school districts**, and **emergency managers** to prepare for, and respond to, cyber incidents
- Varied surveys designed to solicit responses to some fundamental questions about local cybersecurity readiness:

**Risk Assessment**

**Risk Management**

**Awareness and Training**

# Task 3: Introduction & Overview

- **Task III Research Team Leader**: Ben Yelin, Program Director, Public Policy & External Affairs, University of Maryland Center for Health and Homeland Security
- **Support**: Research team of legal externs, current law students at the University of Maryland Francis King Carey School of Law

To assist in obtaining data, the team worked closely with liaisons for each of the entities:

**County Governments**: Kevin Kinnally, Legislative Director, Maryland Association of Counties

**Municipal Governments**: Justin Fiore, Government Relations Manager, Maryland Municipal League

**Local Emergency Managers**: Brian Bauer, Preparedness Branch Manager, and Paul Gump, Cyber Preparedness Unit Supervisor, at the Maryland Department of Emergency Management

**Local School Districts**: Mary Pat Fannon, the Executive Director of the Public School Superintendents Association of Maryland

# Task 3: Key Takeaways

- Units of local government for the most part are making great strides in cybersecurity preparedness efforts.
- Gaps in preparedness are related to significant staffing shortages, inadequate access to training and other resources, and the security risks of outdated legacy systems, frequently handed down by State agencies.
- State can

# Task 3: Survey Results

## 1. COUNTY IT DEPARTMENT SURVEY/FOCUS GROUP

### BALTIMORE COUNTY, WICOMICO COUNTY, SOMERSET COUNTY, GARRETT COUNTY, PRINCE GEORGE'S COUNTY

- Some counties are not allocating sufficient resources to cybersecurity. Need **clear standards** to evaluate the effectiveness of control systems.
- Desire for State to provide additional funding and assist the counties in obtaining resources (tools, software, hardware, and personnel).
- Many Counties rely on legacy systems provided by the State, so **vulnerabilities** that are introduced at the State flow down to the Counties.

# Task 3: Survey Results

## 2. APPOINTED LOCAL EMERGENCY MANAGER CYBER SURVEY

- Most common barriers identified to closing identified gaps, mitigating known vulnerabilities, and reducing cybersecurity risks were **time, staffing, resources, and outdated systems**.
- Jurisdictions listed funding, **training**, and resources as some of the top ways the State can support jurisdictions for non-technical cyber preparedness.
- 84.6% of surveyed jurisdictions maintain cyber insurance.
- More than 90% of surveyed jurisdictions conduct regular technical cybersecurity awareness training for the protection and mitigation of IT systems, networks, and resources.
- However, more than half of respondents do not have consequence management plans for cybersecurity incidents, nor Continuity of Operations (COOP) annexes dedicated to cybersecurity.

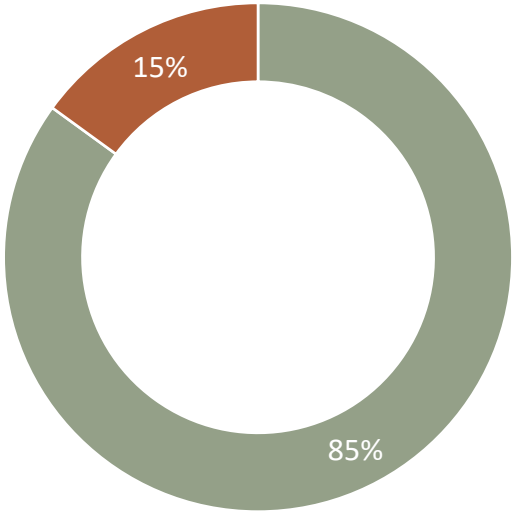



Figure 3. 85% of surveyed jurisdictions do not conduct and/or host training courses on cyber security and preparedness that focus on **emergency management and homeland security**

# Task 3: Survey Results

## 3. MD PUBLIC SCHOOL SYSTEM SURVEY ON CYBER SECURITY

- Only 31% of respondents indicated that their organization allocates sufficient resources to cybersecurity in their budget.
- Just 21% of respondents reported their LEA has a Disaster Recovery Plan and an Incident Response Plan, which have been tested within the past 12 months.
- There is a disparity between urban and rural communities. Rural districts have a difficult time recruiting and retaining talented staff.

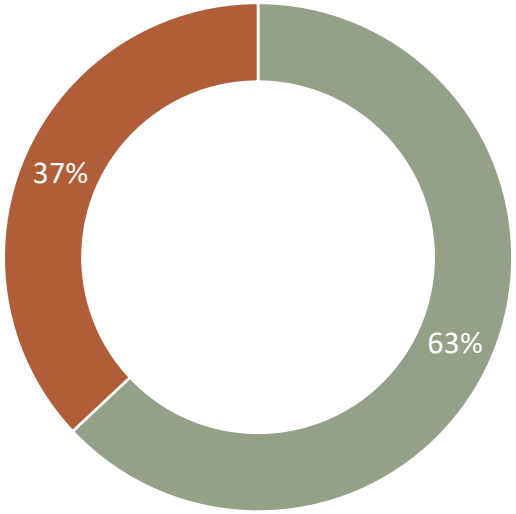



Figure 4. 63% of respondents had completed a recent vulnerability assessment for all internal information systems

# Task 3: Survey Results

## 4. MUNICIPALITIES CYBER SURVEY

- About 55% of respondents indicated their jurisdictions maintain cyber insurance.
- Almost 90% of respondents reported that their municipal government had not conducted a vulnerability assessment of jurisdiction IT infrastructure and network.
- None of the respondents reported that their jurisdictions conduct regular technical cybersecurity awareness training for the protection and mitigation of IT systems and networks.

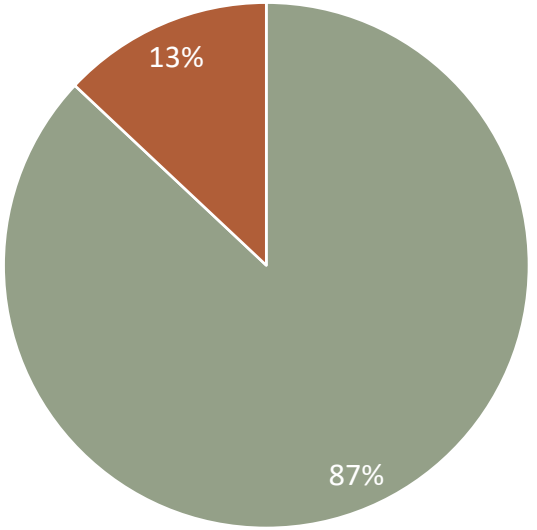



Figure 5. 87% of respondents reported their jurisdiction had not requested or completed a cyber assessment

# Task 3: Recommendations

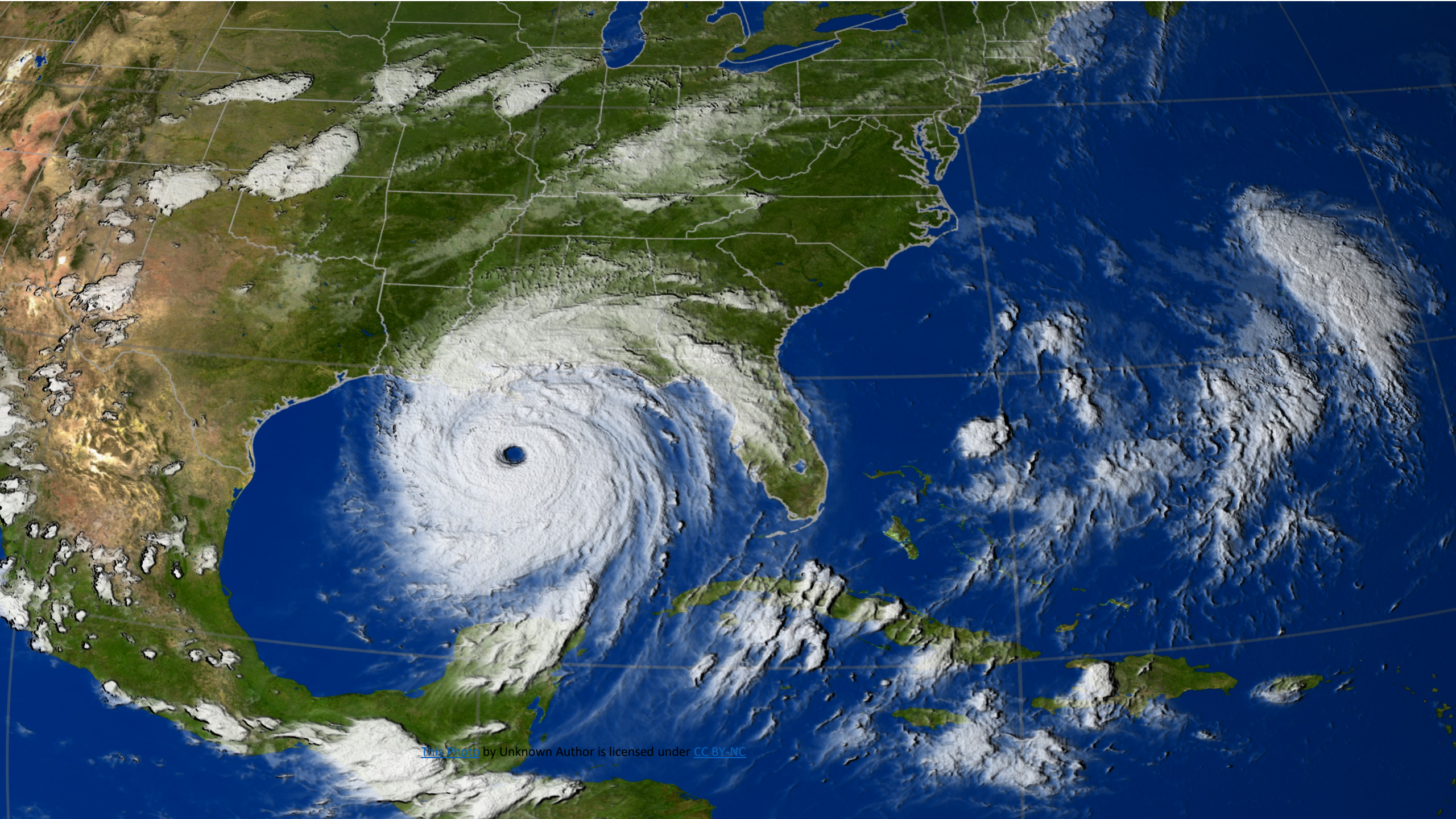
1. SCISO should support a bifurcated cybersecurity effort for units of local government. Division of duties between **DoIT** and **MDEM** will be based on previously agreed-upon matrix. In general, DoIT will be responsible for technical support, technical evaluation of prevention plans, and mitigation. MDEM will be responsible for communications, coordination, and resource allocation.
2. Fully fund, support and staff the **Cybersecurity Preparedness Unit**, within the Preparedness Branch of the Consequence Management Directorate of MDEM.
3. Review for efficiency and effectiveness, available **disaster relief funds** for cyber incidents (including the rainy day fund) to make sure that the State is equipped to respond to a cybersecurity attack.
4. Establish a **Local Cybersecurity Support Fund**, to be available to units of local government. Fund could be used for:
    1. Hardening current devices and networks, and purchasing new devices, hardware and software;
    2. Hiring new cybersecurity staff;
    3. Paying outside vendors for cybersecurity-related trainings

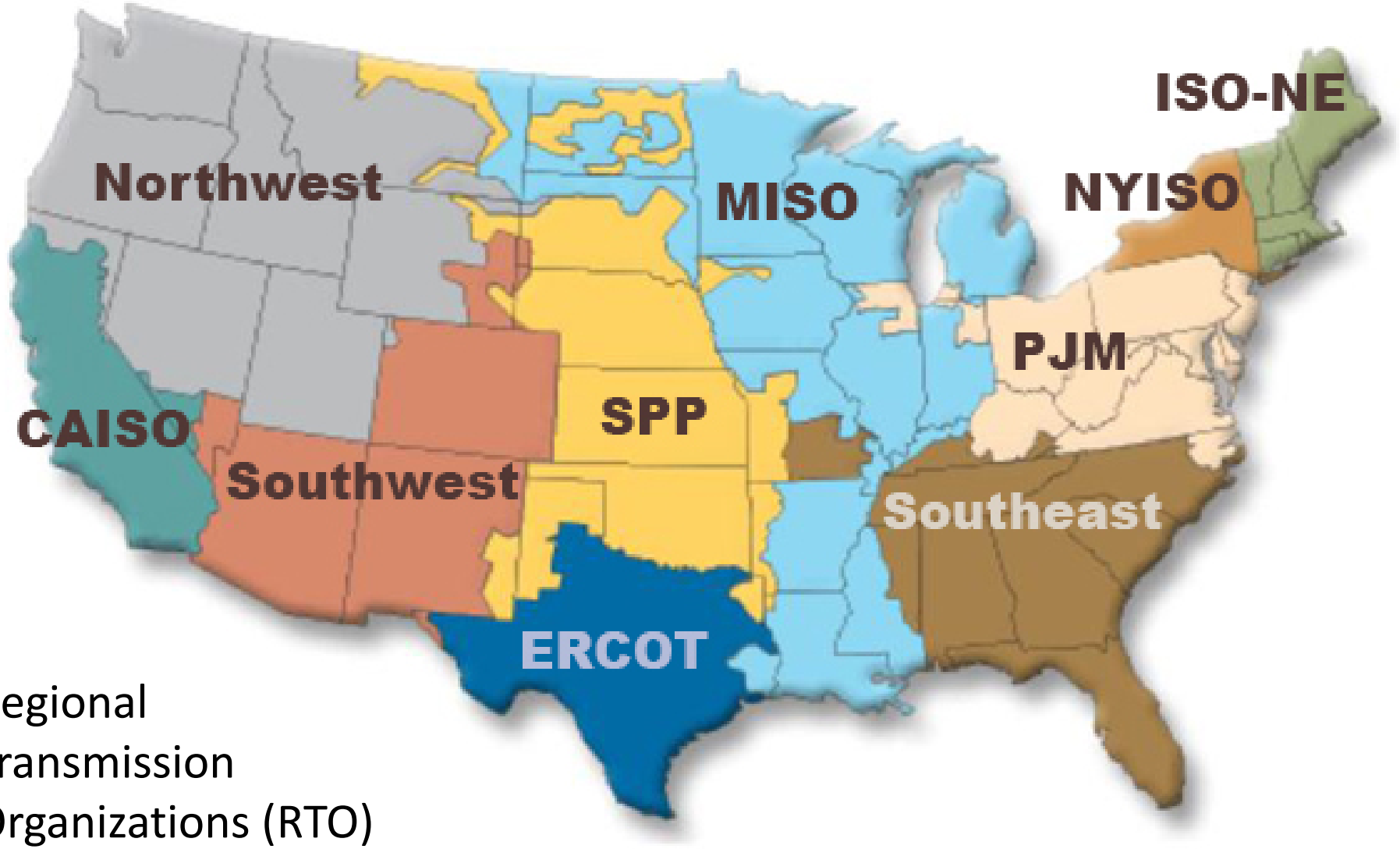
# Thank You

# Cybersecurity for the Maryland Electric Grid

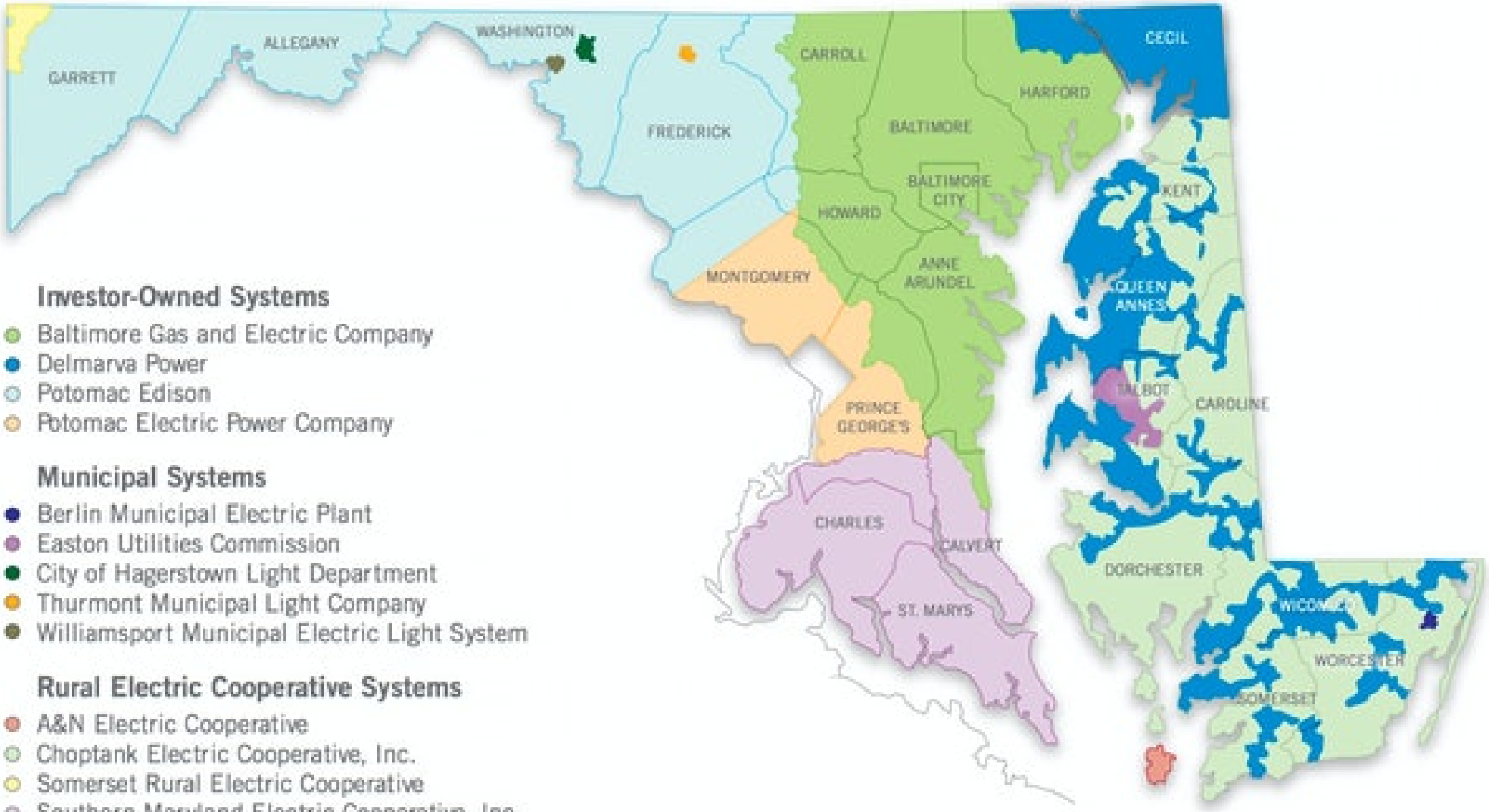
Observations and Recommendations

November 9, 2021






Regional Transmission Organizations (RTO)




**Investor-Owned Systems**

- Baltimore Gas and Electric Company
- Delmarva Power
- Potomac Edison
- Potomac Electric Power Company

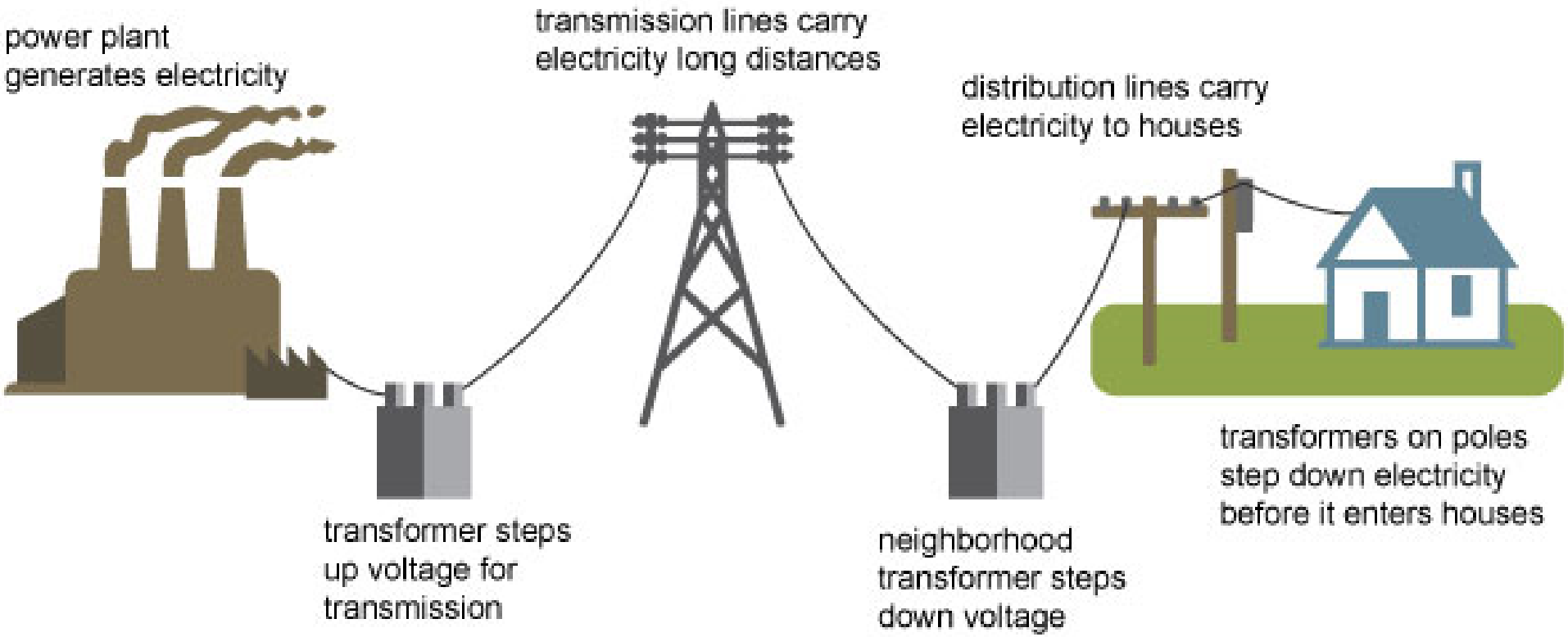
**Municipal Systems**

- Berlin Municipal Electric Plant
- Easton Utilities Commission
- City of Hagerstown Light Department
- Thurmont Municipal Light Company
- Williamsport Municipal Electric Light System

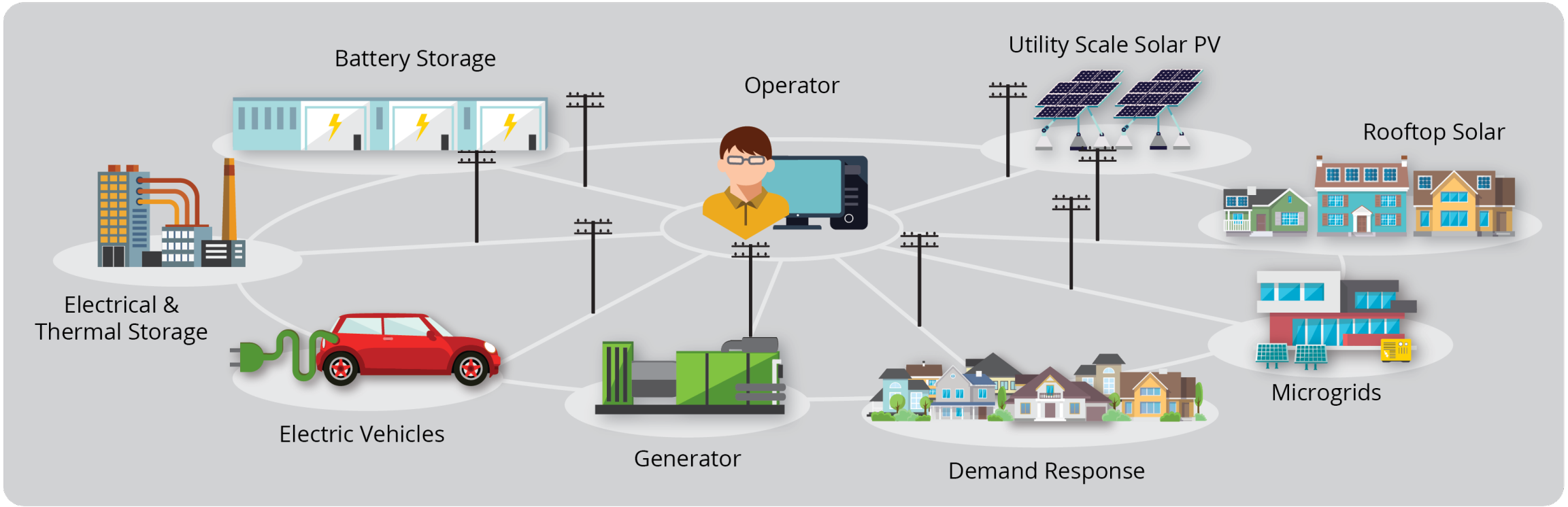
**Rural Electric Cooperative Systems**

- A&N Electric Cooperative
- Choptank Electric Cooperative, Inc.
- Somerset Rural Electric Cooperative
- Southern Maryland Electric Cooperative, Inc.

# Electricity generation, transmission, and distribution




Source: Adapted from National Energy Education Development Project (public domain)



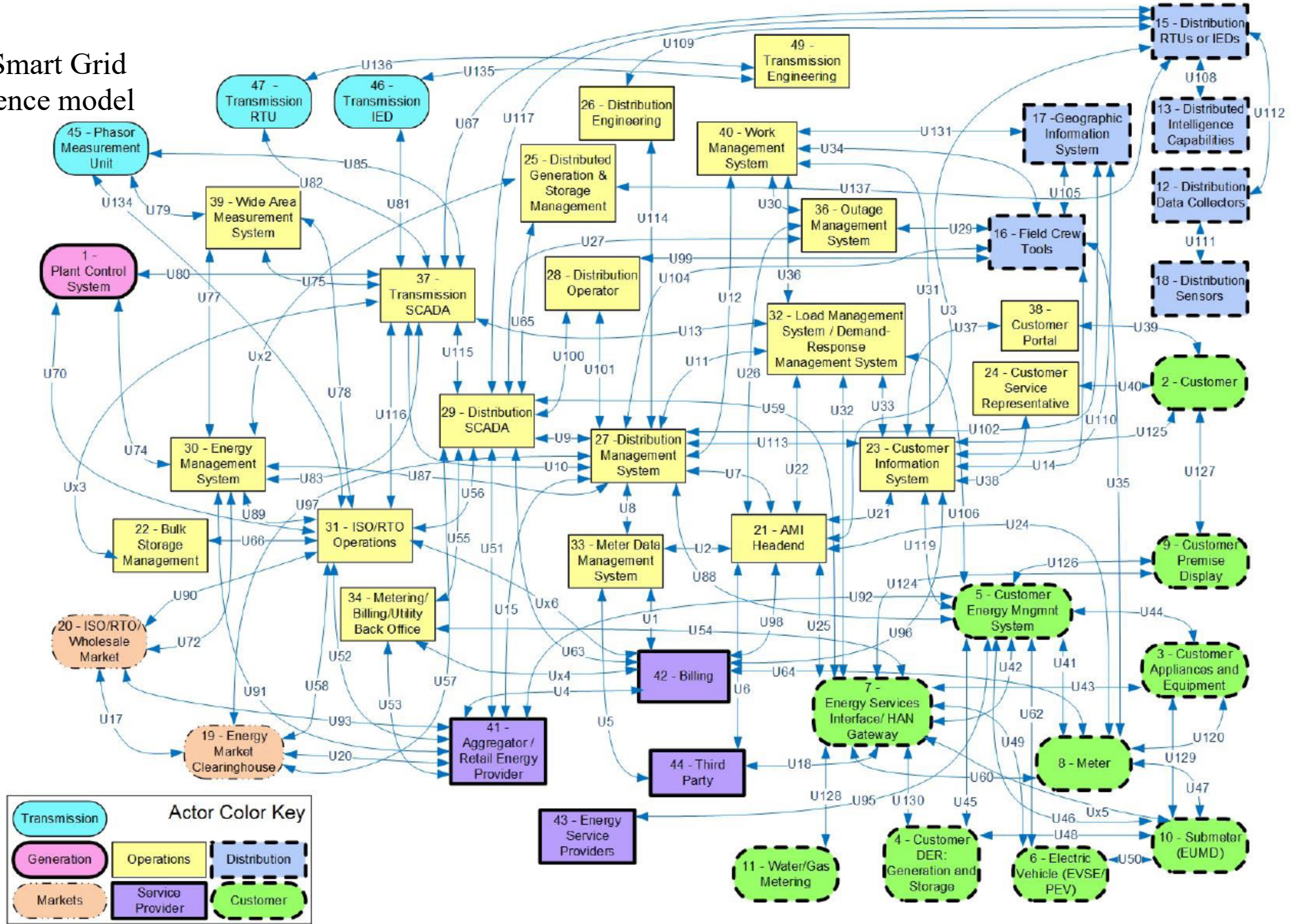

# DER = distributed energy resource


kV2c
Power Supply FITZALL™
BGE
0704
USA
0114
TEG159833985SG006
3Ø G 159 833 985 AMI


YASKAWA


TESLA

2014 NIST Smart Grid logical reference model



# Recommendations

# Regulatory Goals

- high levels of service quality and reliability
- cost-effective
- objective and verifiable standards
- accountability

# Regulatory Goals

**MD Code, Public Utilities, § 7-213.**
**Service quality and reliability standards**

**Scope of regulations**

(e)(1) The regulations adopted under subsection (d) of this section shall:
(i) include service quality and reliability standards, including standards relating to:
1. service interruption;
2. downed wire response;
3. customer communications;
4. vegetation management;
5. periodic equipment inspections;
6. annual reliability reporting; and
7. any other standards established by the Commission;

Add “cyber resiliency”

# Building Cyber Resiliency

# Building Cyber Resiliency

Require utility providers to incrementally implement zero trust principles, process changes, and technology solutions that protect data assets and business functions by use case. Develop and maintain dynamic risk-based policies for resource access. Authenticate all connections and encrypt data. Design cybersecurity of newly interconnected resources around zero-trust principles.

# Incorporating Security by Design

# Incorporating Security by Design

Include a formal requirement for all state funded grant recipients working on electric grid resilience or modernization to address cybersecurity risk both in the design and reporting phases of their work.

# Conclusions

Motorola Solutions, Inc.
500 W Monroe Street, Ste 4400
Chicago, IL 60661-3781
USA

## Director, Cyber Threat Fusion Center

Jay Kaine serves as the Director of the Motorola Solutions Cyber Threat Fusion Center. He is responsible for the establishment, implementation, and operation of a center that will inform and protect public safety organizations globally against cybersecurity threats. Before joining Motorola, Jay served as a Program Manager at Science Applications International Corporation (SAIC), supporting the Office of the Principal Cyber Advisor to the Secretary of Defense. In this capacity, Jay supported implementation of the Department of Defense Cyber Strategy and various strategy and policy initiatives including cybersecurity of the defense industrial base.

Before joining SAIC, Jay served as an officer in the U.S. Army for 25 years, retiring from the U.S. Army Cyber Branch in 2018. Jay's service in uniform is marked by decades of experience in strategy, planning, and supporting global intelligence-driven operations designed to disrupt complex geopolitical, economic, and informational threats.

Jay holds a Bachelor of Science degree from the United States Military Academy at West Point, a Master of Arts degree from the U.S. Marine Corps Command and Staff College, he completed a postgraduate fellowship through the Massachusetts Institute of Technology, and he is a Certified Information Systems Security Professional.

# MOTOROLA SOLUTIONS CYBERSECURITY

JOINT COMMITTEE
CYBERSECURITY, IT, & BIO TECH

Jay Kaine
Director, Cyber Threat Fusion Center
Motorola Solutions

MOTOROLA SOLUTIONS

# PUBLIC SAFETY CYBER THREAT FUSION CENTER

## Cyber Platform Overview

- Fusion center leveraging intelligence gathered through protection of public safety customers
- Threat data and advanced notification of threats/remediation tactics in place today
- Extending platform to include a collaborative mix of public and private entities
- Global reach to inform proactive local action

## Threat Sharing through Collaborative Approach

- Engaged with Federal/S&L/Enterprise partners to participate
- Engaging State of Maryland to participate and leverage existing fusion center
- Focused on implementing best practices already in place for existing ISACs and State Cyber functions

## Focused on Providing Protection Mechanisms to Mid/Small Organizations

- Combination of intelligence sharing and protection mechanisms to reduce Cyber risk
- Protection mechanisms range from $150k to $250k per location

# CYBER OBSERVATIONS

## CRITICAL SHORTAGE OF CYBER CAPABILITY IN THE PUBLIC SAFETY MARKET

### Lack of Personnel

- IT/Safety personnel filling Cyber roles
- Unable to recruit
- Knowledge base focused on internal network security vs. cloud

### Remote Access Challenges

- Endpoints (mobile and external connected devices) create security gaps
- Home based office use straining access security guidelines
- Security protocols lessened to enable usage outside of office networks

### Inadequate Monitoring

- Security monitoring only limited to core network assets while applications are exposed
- Lack of 24x7 support capabilities
- Lack of global visibility and insights
- Even with security information, limited ability to address threats in a proactive or reactive manner

# INFORMATION SHARING + CAPABILITIES

## STRATEGY: PARTNER WITH PUBLIC SAFETY TO INFORM AND PROTECT


### THREAT ADVISORY

Information sharing platform focused on current and future threat to Public Safety Domain leveraging collaboration between public and private entities

### TRAINING

Training and certification for cloud security, response management, risk management, and privacy planning.

### SECURITY MONITORING

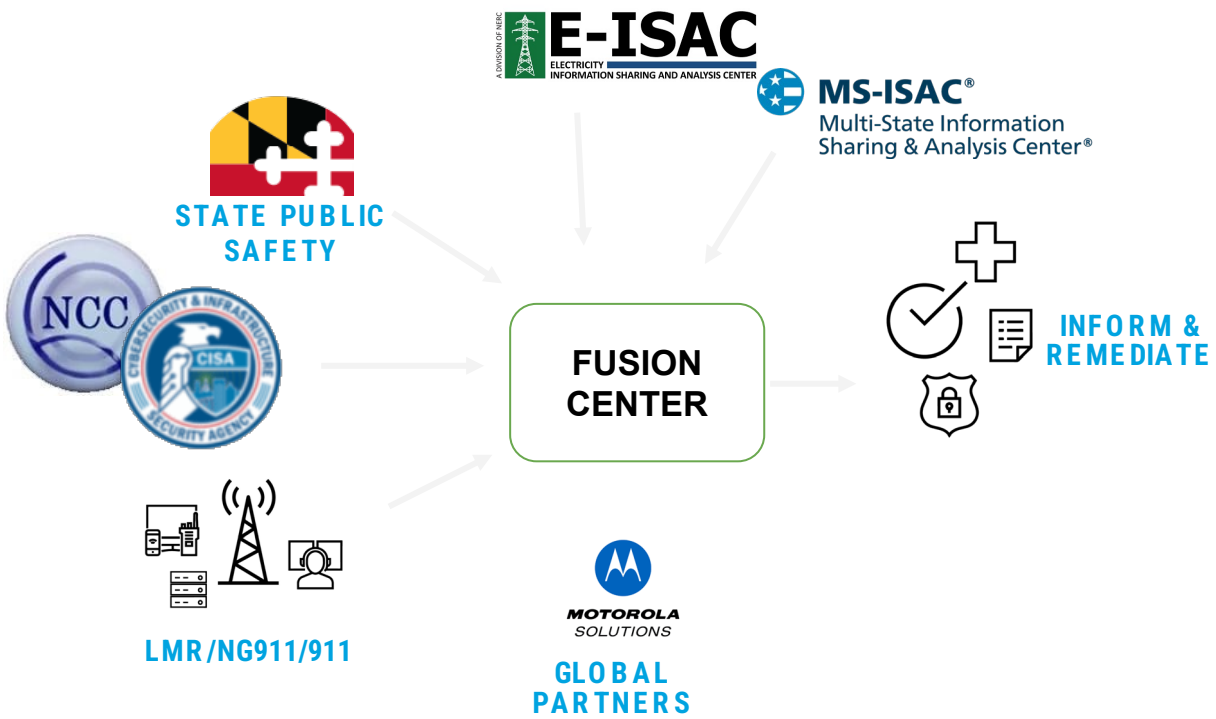
24x7 monitoring of network, applications and all assets, with incident management, reporting, advanced threat detection and response, and security patching.

### INCIDENT RESPONSE

Business continuity and major incident response planning, system recovery, post-incident planning analysis.

# PUBLIC SAFETY CYBER COLLABORATION

## CONTINUOUS ATTACK SURFACE INSIGHTS, ADVANCED THREAT DETECTION & RESPONSE




## Overview

### Collaboration with Fed/S&L/ISACs

- Analyst exchanges
- Anonymized reporting/sharing
- Webinars / table top exercises

### Program Currently Underway

- Strategic/operational assessments
- Secure portal in development
- Strategy in progress

### Remediation Options

- Network, endpoint and cloud monitoring
- Incident response
- Threat hunting


THANK YOU

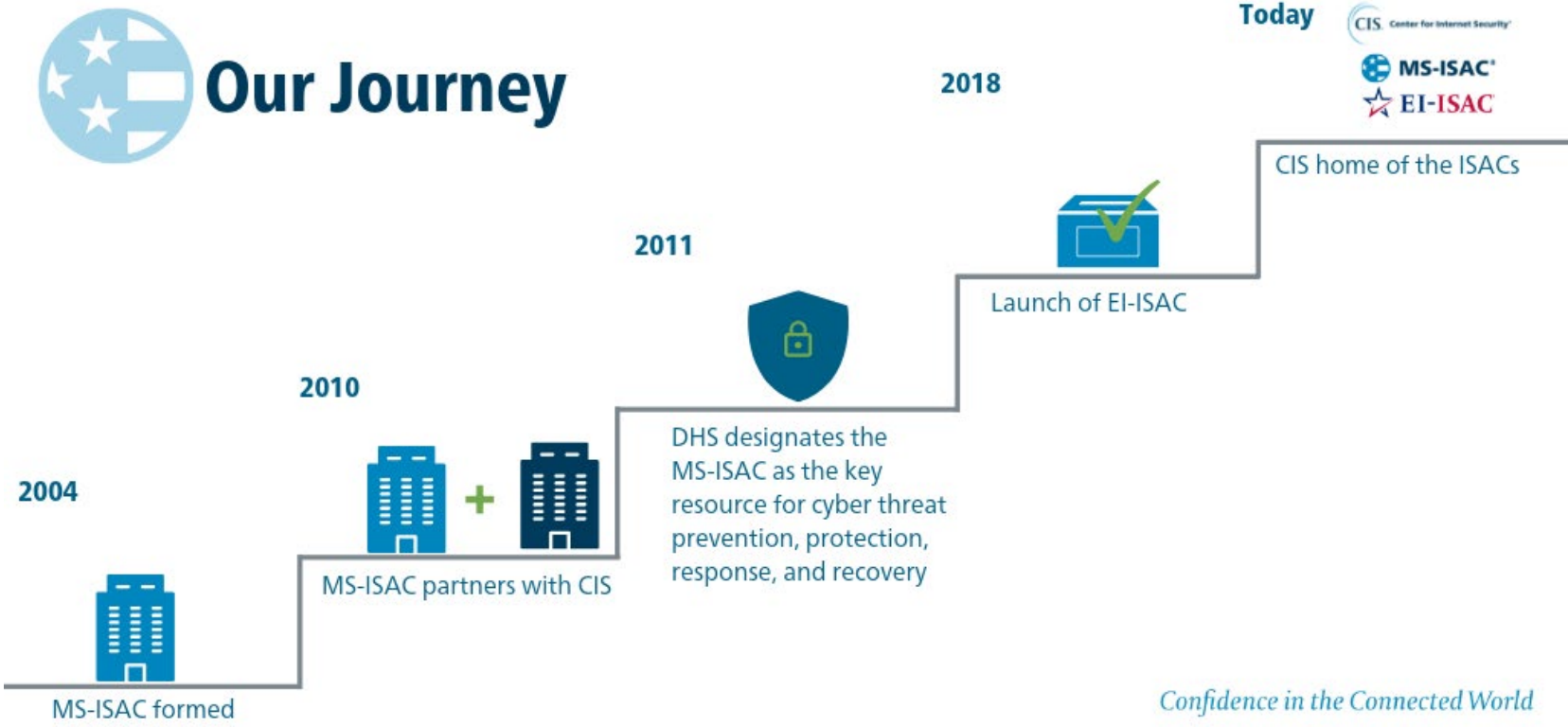
# No-Cost Resources With the MS-ISAC

Kyle Bryans

Senior Program Specialist

MS-ISAC®
EI-ISAC

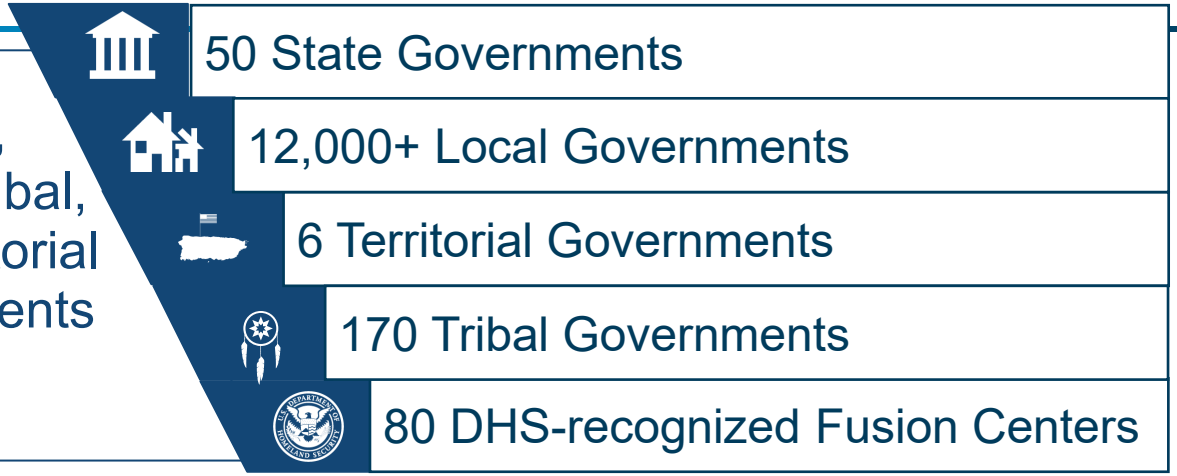
# Our Journey




*Confidence in the Connected World*

# Who We Serve

State, Local, Tribal, and Territorial Governments




99 Members in the State of MD

10 Towns and Cities in MD

13 K-12 School Districts in MD

21 Counties in MD

# Benefits of MS-ISAC Membership

## The Home Field Advantage

### No Cost Benefits To You

→ 24×7×365 Security Operations Center (SOC)
→ Passive IP & Domain Monitoring
→ Malicious Domain Blocking & Reporting (MDBR)
→ Cybersecurity exercises
→ Cybersecurity advisories
→ Cyber event notifications
→ Education and awareness materials
→ CIS SecureSuite® Membership
→ Incident response resources

→ Malicious Code Analysis Platform (MCAP)
→ Monthly newsletters, webinars and threat briefings
→ Homeland Security Information Network (HSIN) *access, including portals for communication and document sharing*
→ Deloitte Cyber Detect Cyber Respond Portal
→ Nationwide Cybersecurity Review (NCSR)
→ Discounts on training
→ Vulnerability assessment services

**https://learn.cisecurity.org/ms-isac-registration**

# Security Operations Center

**24/7 support for:**

- ✓ Network Monitoring Services
- ✓ Research and Analysis

**24/7 analysis and monitoring of:**

- ✓ Threats
- ✓ Vulnerabilities
- ✓ Attacks

**24/7 reporting:**

- ✓ Cyber Alerts & Advisories
- ✓ Web Defacements
- ✓ Account Compromises
- ✓ Hacktivist Notifications

To report an incident or request assistance:

**Phone**: 1-866-787-4722

**Email**: soc@cisecurity.org

# Malicious Domain Blocking and Reporting (MDBR)

**Security Focused DNS service:**

Blocks malicious domain requests before a connection is even established!

**Simple Implementation:**

No new hardware or software required

**Helps limit infections related to:**

- Known Malware
- Ransomware
- Phishing
- Other cyber threats

# Malicious Domain Blocking and Reporting (MDBR)

## How does it work?

- Proactively blocks network traffic to known harmful web domains.
- Weekly reports sent to organization.

## Register for MDBR:

- https://mdbr.cisecurity.org/

## For more information, review the FAQ:

- https://www.cisecurity.org/ms-isac/services/mdbr/mdbr-faq/

# Disseminations & Alerts

MS-ISAC Advisory  Michael Aliperti

MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Various Cisco Products Could Allow for Administrator Privileges - PATCH: NOW - TLP: WHITE

Retention Policy  Default 2 year move to archive (2 years)  Expires 7/3/2022

This message was sent with High importance.

**TLP: WHITE**
**MS-ISAC CYBERSECURITY ADVISORY**

**MS-ISAC ADVISORY NUMBER:**
2020-089

**DATE(S) ISSUED:**
07/03/2020

**SUBJECT:**
Multiple Vulnerabilities in Cisco Products Could Allow for Administrator Privileges

**OVERVIEW:**
Multiple vulnerabilities have been discovered in Cisco products, the most severe of which could allow for an attacker gaining administrator pr
exploitation of the most severe of these vulnerabilities could result in an attacker gaining administrator privileges. Depending on the privilege
data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be les

**THREAT INTELLIGENCE:**
There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEMS AFFECTED:**
- Cisco AnyConnect Secure Mobility Client for Mac OS releases earlier than 4.9.00086
- Cisco Digital Network Architecture Center releases earlier than 1.2.10
- Cisco Identity Services Engine releases earlier than 2.6 Patch 7
- Cisco 250 Series Smart Switches


Volume 15, Issue 7 • July 2020  Monthly Security Tips Newsletter

From the desk of
Michael Aliperti
MS-ISAC Chair

## 6 Common Elderly Scams to Watch Out For and How to Stay Safe

A scam can be initiated via the computer (email, internet, social media), text, postal mail, in person, or a phone call. No matter the origin of the scam, the characteristics are the same:

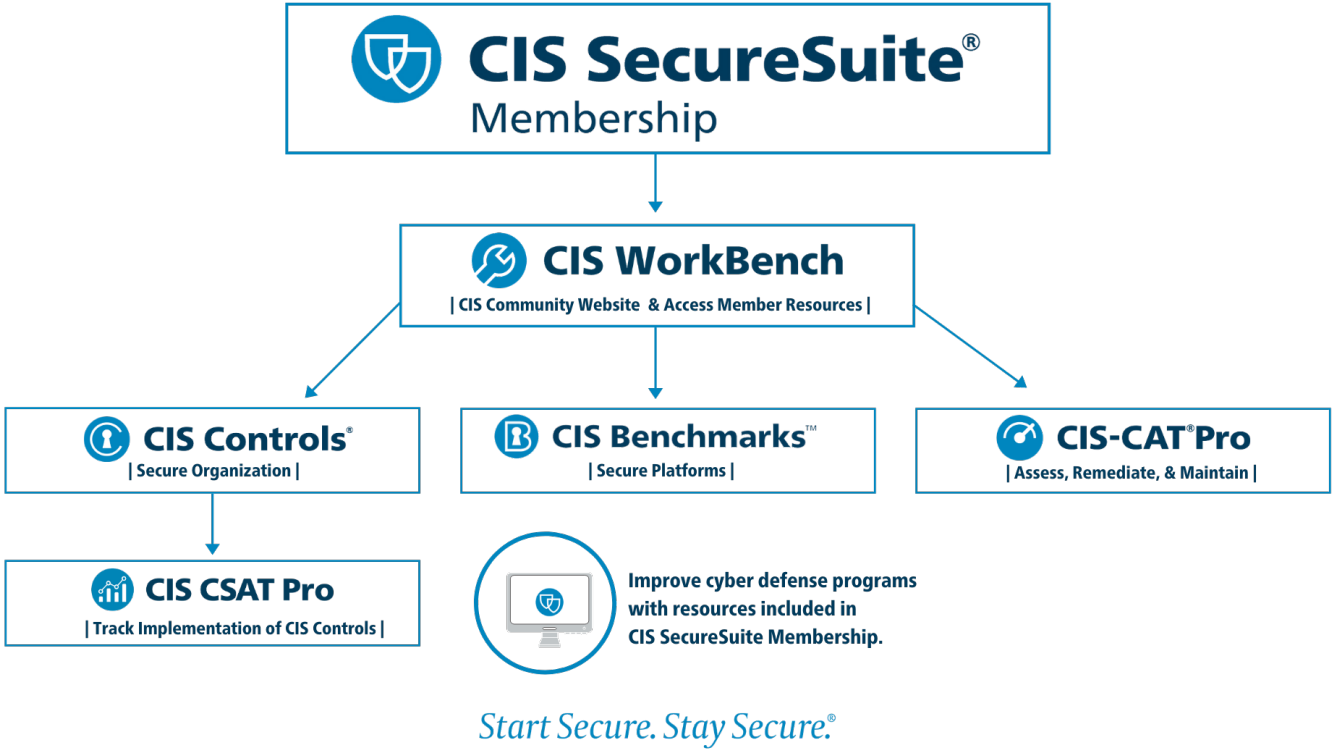
- First, there is something to pique your interest – someone in trouble, big discount offers, lottery win.
- Second, the individual contacting you seems trustworthy, super friendly, and seems to care about you.
- Third, there's a deadline associated with the offer – act fast, act now.

There will always be scams, particularly those targeted at seniors. This month's newsletter identifies some common scams and some tips to help you take control of the situation and stay safe and stay in control.

**Grandparent Scam**

One of the most common scams presented to seniors is the Grandparent Scam. The caller claims to be a relative, a grandson or granddaughter, and the call is urgent. Typically, the grandchild is out of

# CIS SecureSuite Membership




*Start Secure. Stay Secure.®*

MS-ISAC®

EI-ISAC®

Thank you!

# Contact Us


**Security Operations Center**
24/7 Phone Number
1-866-787-4722
**soc@cisecurity.org**

**Kyle Bryans**
Senior Program Specialist
518-880-0747
Kyle.Bryans@cisecurity.org