Senate Study Committee on the Creation of a Georgia Cybersecurity Force

Chairman Jason Anavitarte

September 13, 2022

Georgia Tech

The Changing Landscape of Cybersecurity

- **Moderator:**
  - Skeet Spillane, *President Pillar Technologies Partners CISO*

- **Panelists:**
  - David Levine, *CISO, Ricoh USA*

  - Curley Henry, *Vice President and Deputy CISO of Cybersecurity Strategy & Architecture at Southern Company*

Georgia Tech

Understanding Impact - Cybersecurity Challenges

- **Moderator:**
  - Raheem Beyah, *Dean, College of Engineering, Georgia Tech*

- **Panelists:**
  - Dr. Michael Bailey, *Chair, School of Cybersecurity and Privacy, Georgia Tech*

  - Daren Hubbard, *Vice President of Information Technology and Chief Information Officer, Georgia Tech*

Georgia Tech

GTRI Research in Cybersecurity – National and State Security

- **Moderator:**
  - William Robinson, *Deputy Director of Research, Information, and Cyber Sciences Directorate*

- **Panelists:**
  - Matt Guinn, *Lead, Network Operations Group, Command and Control Mission Assurance (C2MA) Division, CIPHER Lab, GTRI*
  - *Jessica Inman, Division Chief, Assured Software and Information Division, CIPHER Lab, GTRI*
  - Sam Litchfield, *Lead, Cybersecurity of Critical Infrastructure Strategic Energy Institute, Georgia Tech and Research Engineer, Embedded Systems Vulnerability Division, CIPHER Lab, GTRI*
  - Mike Ruiz, *Associate Chief of the Trusted Microelectronics Program Office and Student Initiative Lead, CIPHER Lab, GTRI*

Georgia Tech

Georgia Technology Authority

Shawnzia Thomas,
Executive Director

David Allen, *State CISO*

Georgia Tech

GEORGIA TECHNOLOGY AUTHORITY

Cybersecurity Force Exploration

Georgia General Assembly

OUR VISION

A transparent, integrated enterprise where technology decisions are made with the citizen in mind

—

OUR MISSION

To provide technology leadership to the state of Georgia for sound IT enterprise management

September 13th, 2022

Agenda

- Introduction
- GTA Overview
- Incident Response in GA
- Current Civilian Cyber Corps and Considerations
- Questions / Discussion

Introductions

September 13, 2022

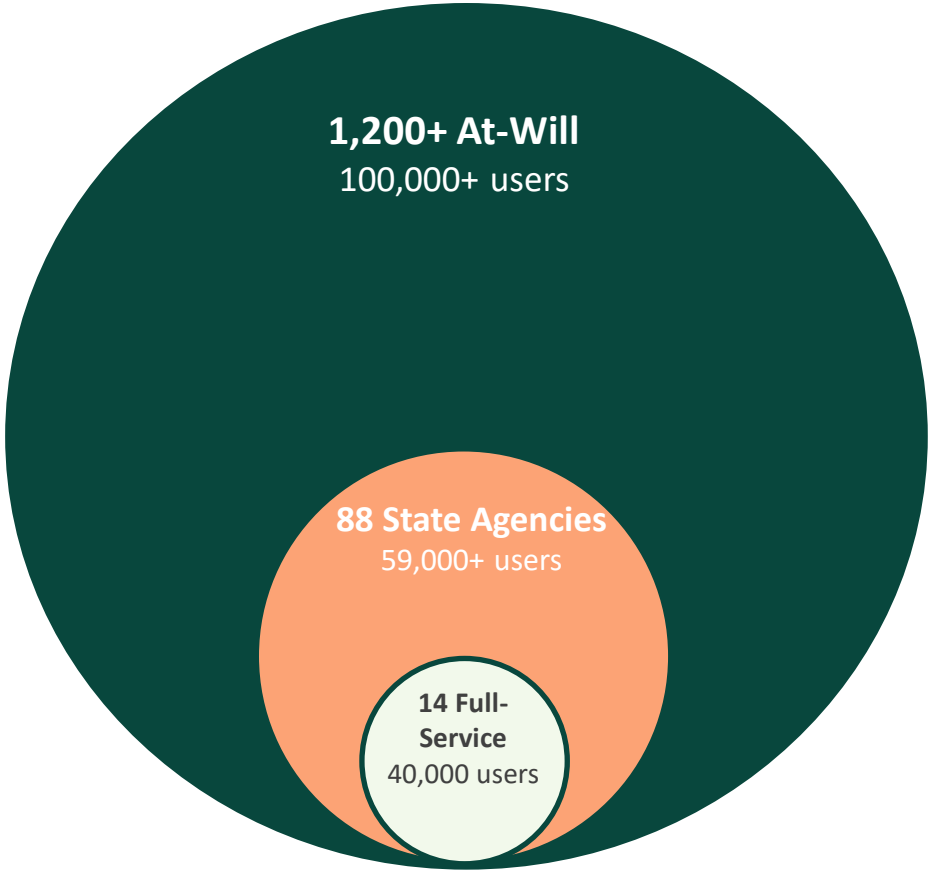
GTA Overview

Shawnzia Thomas
CIO and Executive Director

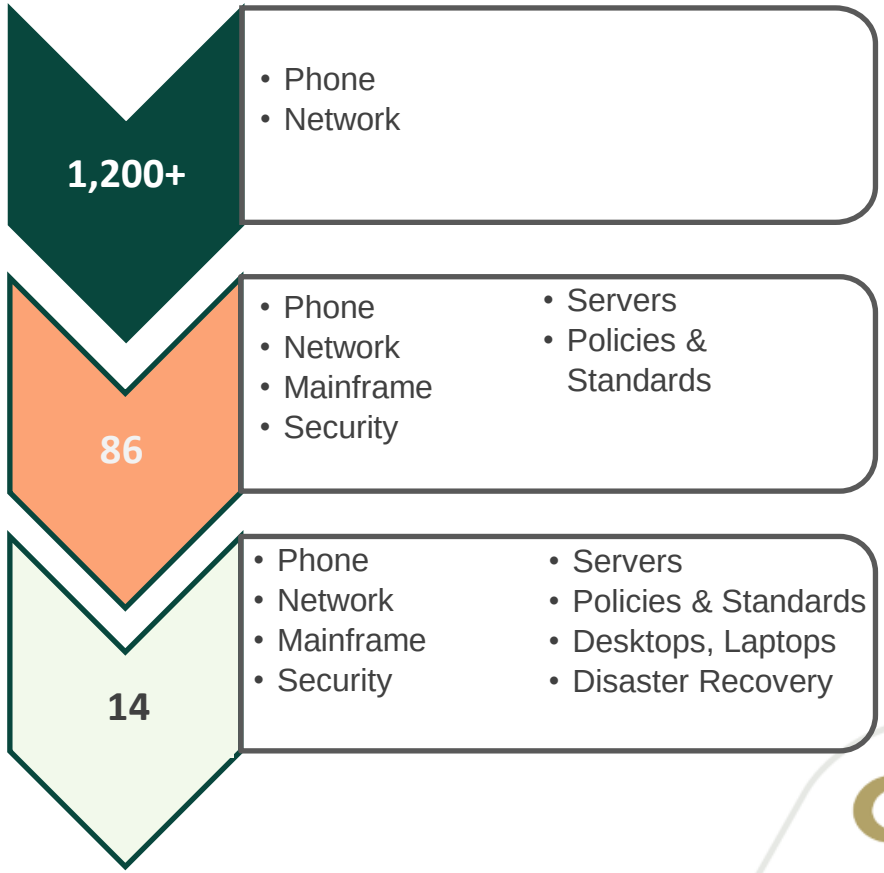
September 13, 2022

Georgia Technology Authority Scope

Which agencies are served?
(segmented by services consumed)



Which services do they get?
(varies from all services to one or two)



Incident Response in GA

COL(R) David Allen – CISO, State of Georgia

September 13, 2022

Georgia Cyber Dependencies

Federal Partners

Capability Integration

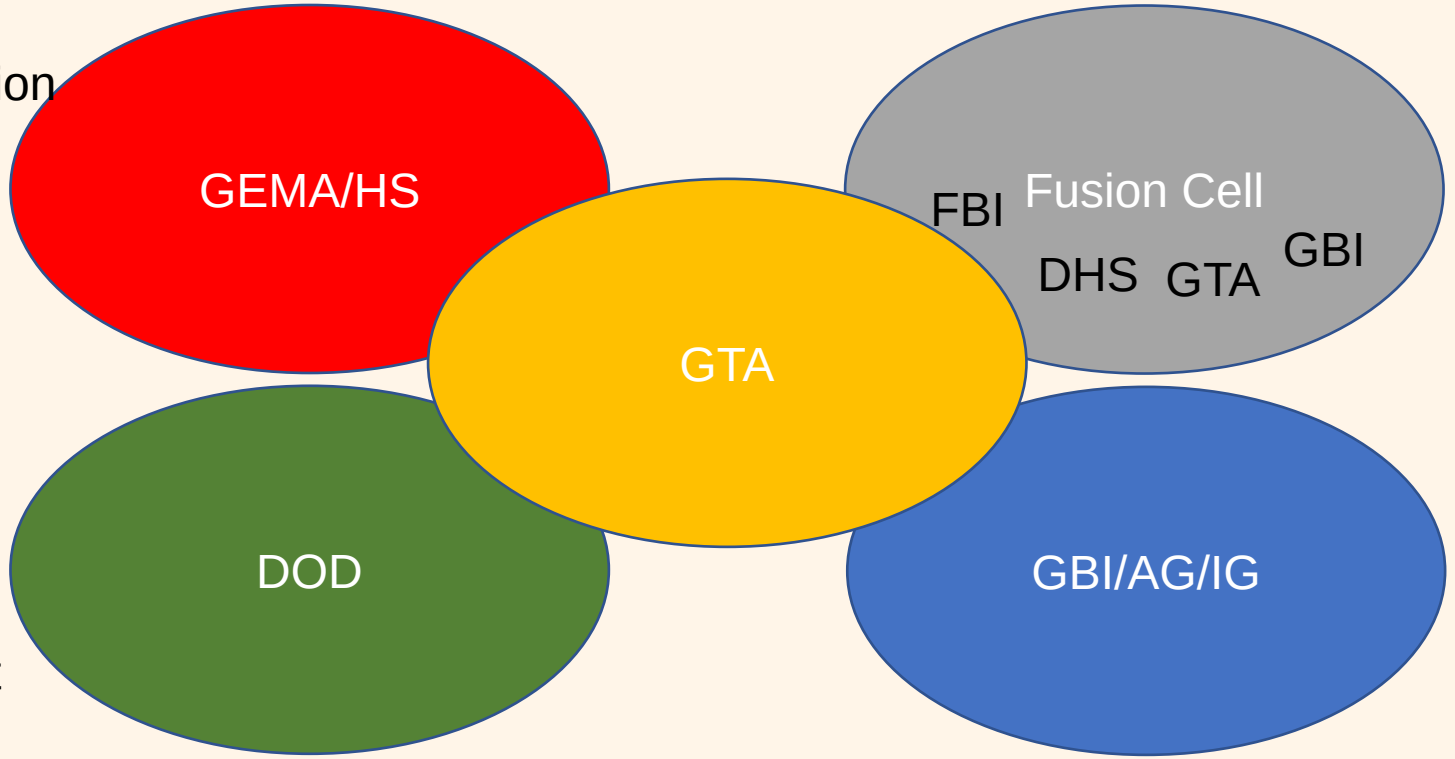
Disaster Response

Training

Outreach

Incident Response

Public Safety Support



Intel/Threat Sharing

Incident Response

Outreach

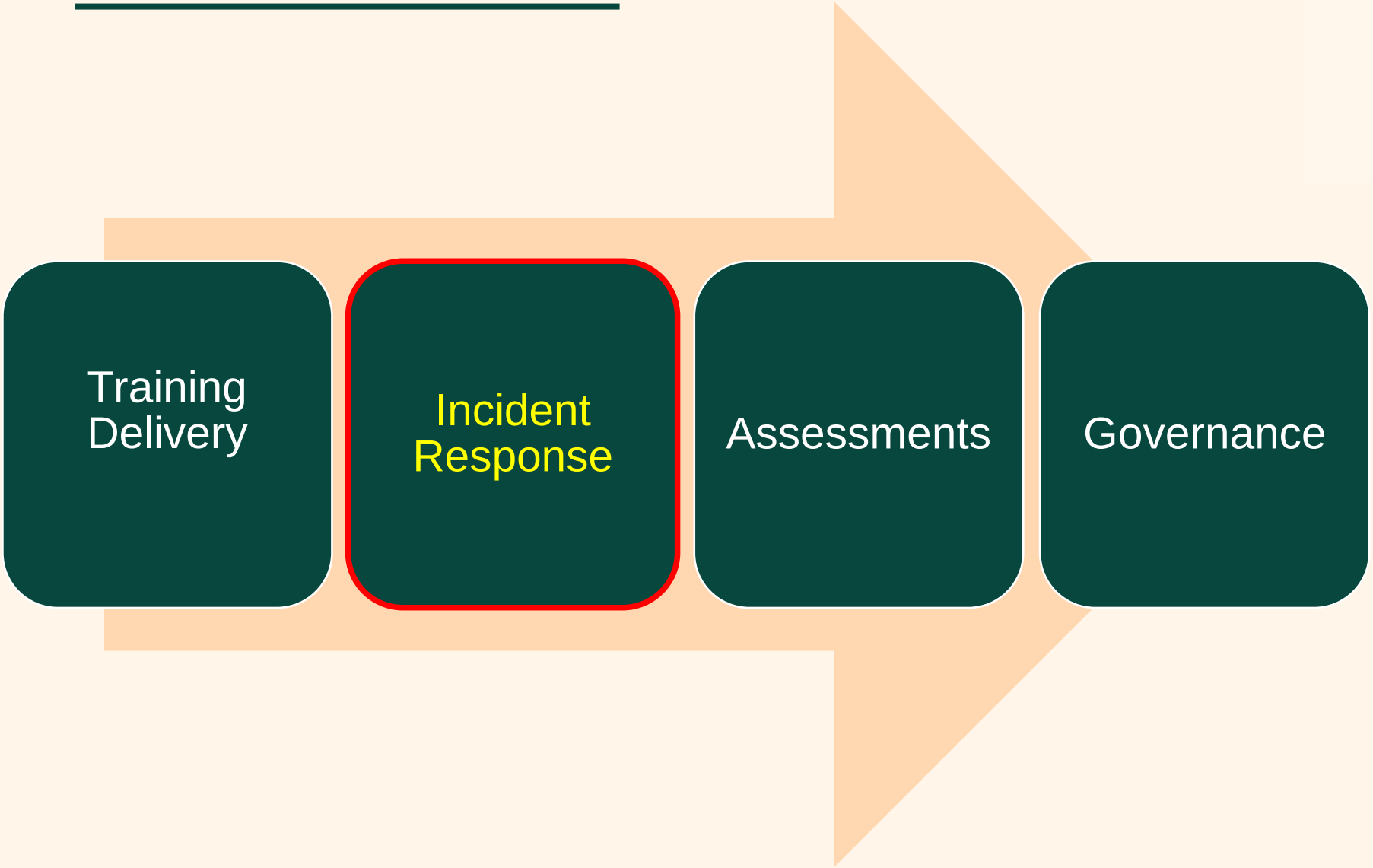
Training

Legal Facilitation

Disaster Response

Local Government / Education / Private Partners

OIS Lines of Effort



Culture of security, awareness, and resilience. Mature cybersecurity program and OIS as premier support organization

Incidents reported to the GEMA/HS website
https://gema.georgia.gov/

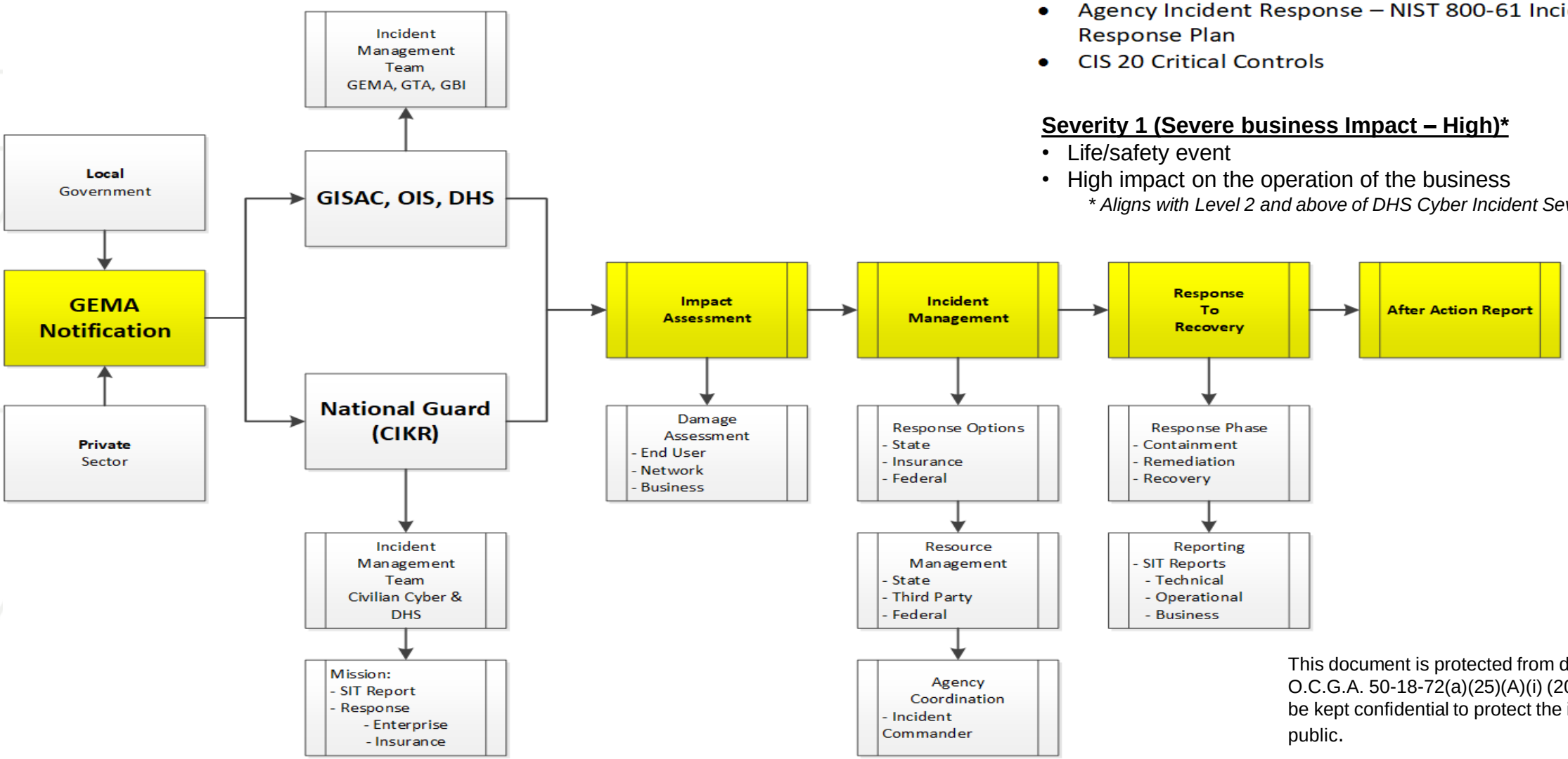
State-Wide Incident Management Process
Escalate to GEMA: Severity 1 Incidents

- National Incident Management System (NIMS)
- Agency Incident Response – NIST 800-61 Incident Response Plan
- CIS 20 Critical Controls

Severity 1 (Severe business Impact – High)*

- Life/safety event
- High impact on the operation of the business

** Aligns with Level 2 and above of DHS Cyber Incident Severity Schema*



Civilian Cyber Corps

September 13, 2022

State Examples with existing civilian cyber capabilities

Cyber_Civilian_Corps_14June2022.pdf (nga.org)

1. Ohio passed legislation creating cyber force within the NG
    - *The Ohio House voted unanimously to create a civilian cyber force within the Ohio National Guard to respond to cyberattacks against elections systems, governments, businesses, and critical infrastructure.*
    - Ohio Cyber Reserve

2. Michigan existing legislation
    - DTMB - Michigan Cyber Civilian Corps (MiC3)
    - ***The Michigan Cyber Civilian Corps (MiC3) is a group of trained, civilian technical experts who individually volunteer to provide rapid response assistance to the State of Michigan in the event of a critical cyber incident.***

Georgia Tech

Georgia State Defense Force

O.C.G.A. § 38-2-50 (2012)

TITLE 38. MILITARY, EMERGENCY MANAGEMENT, AND VETERANS AFFAIRS
CHAPTER 2. MILITARY AFFAIRS
ARTICLE 1. STATE MILITIA GENERALLY
PART 3. STATE DEFENSE FORCE

The Georgia State Defense Force is an auxiliary unit of the Georgia Department of Defense, serving in support of the national and state constitutions under direction of the Governor and the Adjutant General of Georgia.

- *When ordered by the Adjutant General, provide an organized, trained, disciplined, rapid response volunteer force to assist state and local government agencies, and civil relief organizations in impending or actual emergencies to assure the welfare and safety of the citizens of Georgia.*
- https://paonews.net/

Analysis and Additional Considerations

OIS has reviewed the legislation from Ohio, as well as those from other states (MI, WI, IN, and NY). If structured properly, we feel there is the potential for a volunteer cyber response team to be an overall benefit to the state, especially for local government and critical infrastructure.

There are areas that will need to be addressed.

1. Liability – Protecting the volunteer from potential liability should be considered when passing legislation. Volunteers accessing private property or systems should not be held liable while serving on behalf of the state.
2. Background Checks – All volunteers should be required to pass a background check before serving in this capacity.
3. Reimbursements –If Georgia were to establish this program under the State Defense Force, like that of Ohio, it could create a conflict whereas current SDF members in Georgia are not paid for their service. Ohio's legislation allows for cyber volunteers to be paid during their deployment.
4. Sustainability – Significant administrative overhead and funding considerations as the program grows.

Additional Considerations not discussed:

Additional incentives for recruitment (USG and TCSG program students)

Universities w/ cyber programs: Augusta, Columbus State, Georgia State, Georgia Tech, Kennesaw State, North Georgia

Georgia Tech

Discussion

September 13, 2022

Fortinet – A Path to CIPA Compliance

Jim Finger, *Major Accounts Manager*

Georgia Tech

FORTINET

A Path to CIPA Compliance

Content Filtering Best Practices

Jim Finger / Jason Matthews – GA State/Local/Education

Legal Disclaimer

We are not attorneys, and this is not legal advice. The information and materials presented are for general information purposes only.

Georgia Tech

Objectives

Describe	Describe the basic requirements of CIPA
Discuss	Discuss filtering best practices and various technologies that can be used
Review	Review consequences of noncompliance and potential risks

Who is Fortinet?

Georgia Tech

Who is Fortinet?

For over 20 years, Fortinet's mission has been to secure people, devices, and data everywhere.

We have been a driving force in the evolution of cybersecurity and the convergence of networking and security. Our network security solutions are the most deployed, most patented, and among the most validated in the industry.

CIPA Overview

Georgia Tech

Protecting Children Online

A Brief History

Act	Year	Description	Constitutional?
Communications Decency Act (CDA)	1996	Filtering tied to federal funds, part of the Telecommunications Act of 1996, created E-rate funding	No (1997)
Child Online Protection Act (COPA)	1998	Filtering tied to federal funds, never went into effect	No (2007)
Children's Online Privacy Protection Act (COPPA)	2000	Regulates how commercial websites collect personal information from children under the age of 13. Doesn't apply to K-12	Yes
Children's Internet Protection Act (CIPA)	**2000**	**Filtering tied to federal funds**	**Yes**

Georgia Tech

The Children's Internet Protection Act

"The Children's Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet."

Neighborhood Children's Internet Protection Act

Passed into law at the same time as CIPA

CIPA defines requirement for filtering and policy

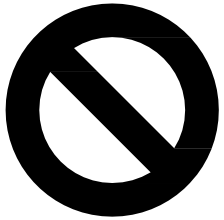
NCIPA defines what's *inside* the policy

What Do We Need To Protect?

Required

- Any device used to access the internet
- Applies both to adults & minors, organization-wide
- Categories:
  - Obscene
  - Pornographic
  - Harmful to Minors

Not Required



- Audio/Text
- Social Media
- Exceptions for bona fide research

Technology is Changing!

Schools are a Target

- Loads of data, tons of technology

Mobile Devices, 1-to-1, Hotspots

- Students have multiple devices connected at all times

Encryption

- SSL/TLS, VPN

Malware, ransomware, very broad attack surface

Georgia Tech

A Path to CIPA Compliance

Georgia Tech

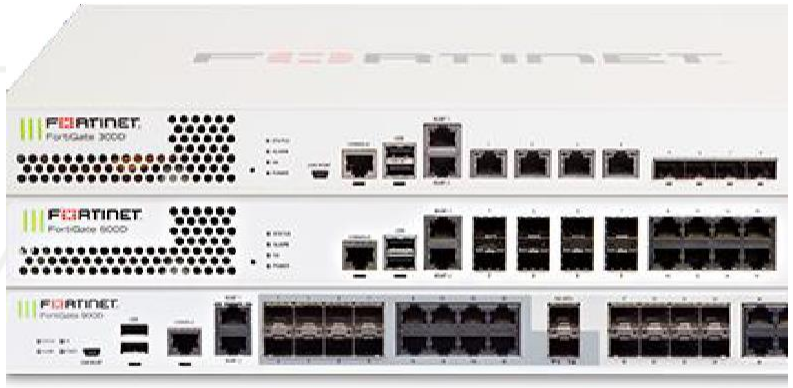
3 Steps to CIPA Compliance

Technology Protection Measure

Internet Safety Policy

Notice and Public Meeting

Technology Protection Measure



Hardware
(Fortigate Firewall, FortiProxy)

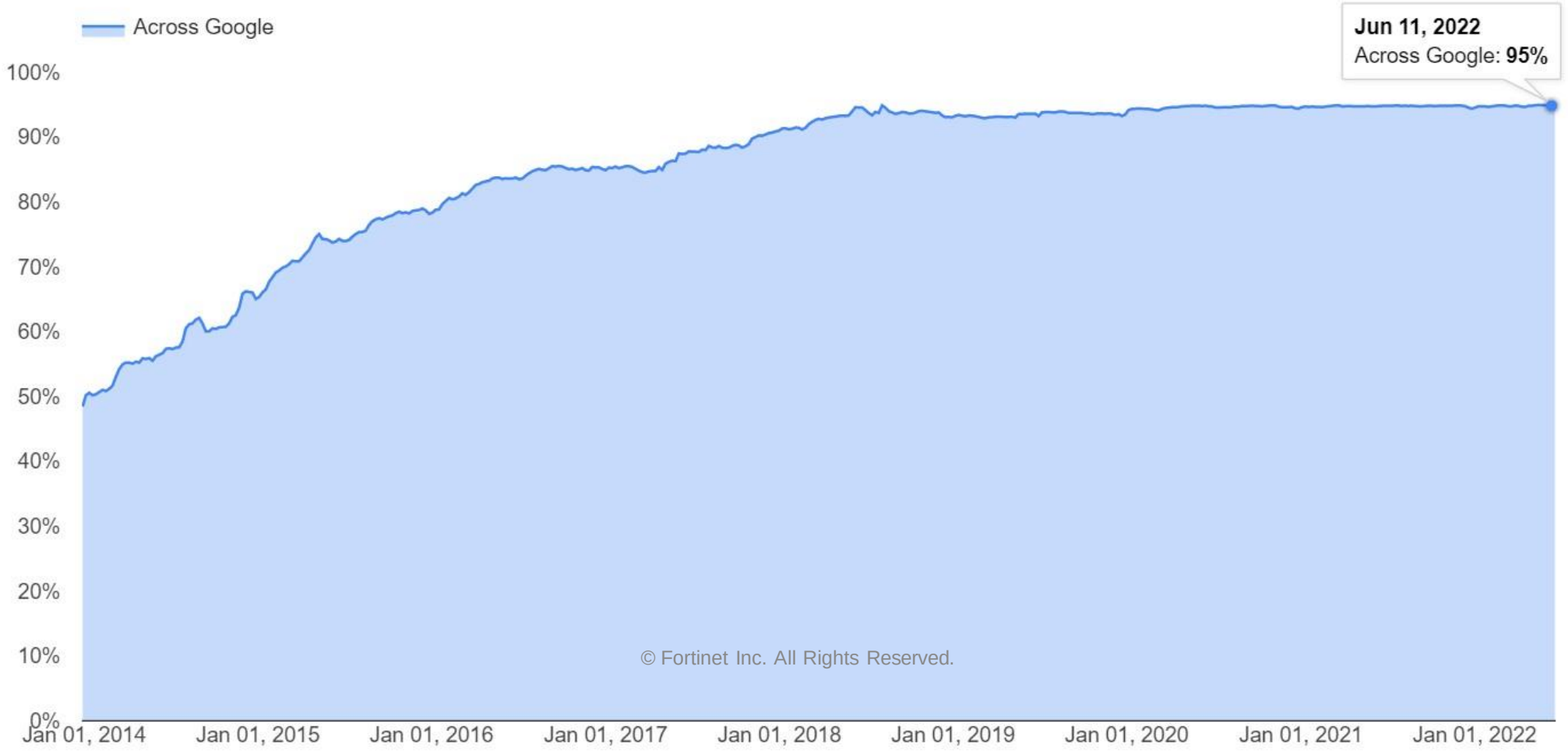
Software
(FortiClient/EMS, FortiEDR)

ISP
(Linksys HomeWRK Hotspot)

Georgia Tech

SSL Decryption + Inspection

https://transparencyreport.google.com/



Why Linksys HomeWRK for Education

Secure & Reliable Connectivity

Greater coverage and reception with nationwide coverage from top carrier networks

Meet CIPA Requirements

Safe and secure internet access from homes with leading Fortinet security technologies

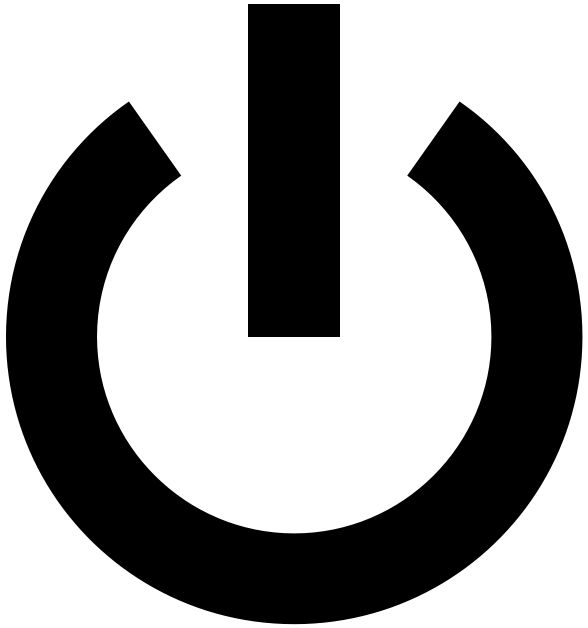
Qualified for Govt. funding

Affordable hardware and subscription plans, paid through available Govt funded programs

Government programs available for all schools to immediately take advantage of this solution

Georgia Tech

Disabling Your Filter



- Filtering needs to be easily disabled upon request
- Critical for constitutionality

Internet Safety Policy

Must enforce a policy, must be adopted at a public meeting

Must address the NCIPA requirements

Must provide for educating minors about appropriate online behavior

Internet Safety Policy

NCIPA Requirements

1. Prevent minors from accessing inappropriate matter on the internet and World Wide Web
2. Address the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications
3. Prevent unauthorized access, including “hacking” and other unlawful activities by minors online
4. Prevent unauthorized disclosure, use, and dissemination of personally identifiable information (PII) regarding minors
5. Address measures designed to restrict minors’ access to materials that are harmful to minors

Fortigate Firewall

FortiProxy

FortiMail

FortiEDR

FortiClient/EMS

Linksys HomeWRK

Georgia Tech

Public Hearing

- Must provide reasonable public notice
- Can be school board meeting, etc.
- Only needs to occur one time
- Keep records, add to end of policy

Risks of Noncompliance

Georgia Tech

Penalties for Noncompliance

Failure to Submit Certification

Any library or school that fails to submit the certification requirements described above shall be ineligible for funding under the E-rate program

Failure to Comply with Certification

Not only loses eligibility for funding, must reimburse the E-rate fund for discounts received

FCC has complaint hotline!

Remedies

Can re-apply after implementing safeguards and certifying compliance

Resources

- Sample Internet Safety Policies
  - https://e-ratecentral.com
  - https://concordiacharter.org/wp-content/uploads/2016/02/CCS-Internet-Safety-Policy.pdf
- E-Rate Information
  - https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/Flyer-Education-E-Rate.pdf
- Test your web filter
  - https://www.fortiguard.com/webfilter/categories

Georgia Tech

Georgia Bureau of Investigation

Steve Foster, *Special Agent Charge, Georgia Cyber Crime Center*

Georgia Tech

SHI

Marc Yoder, *Chief Information Security Officer*

Georgia Tech

SHI | ASG

Building a Sustainable Cybersecurity Force

Agenda

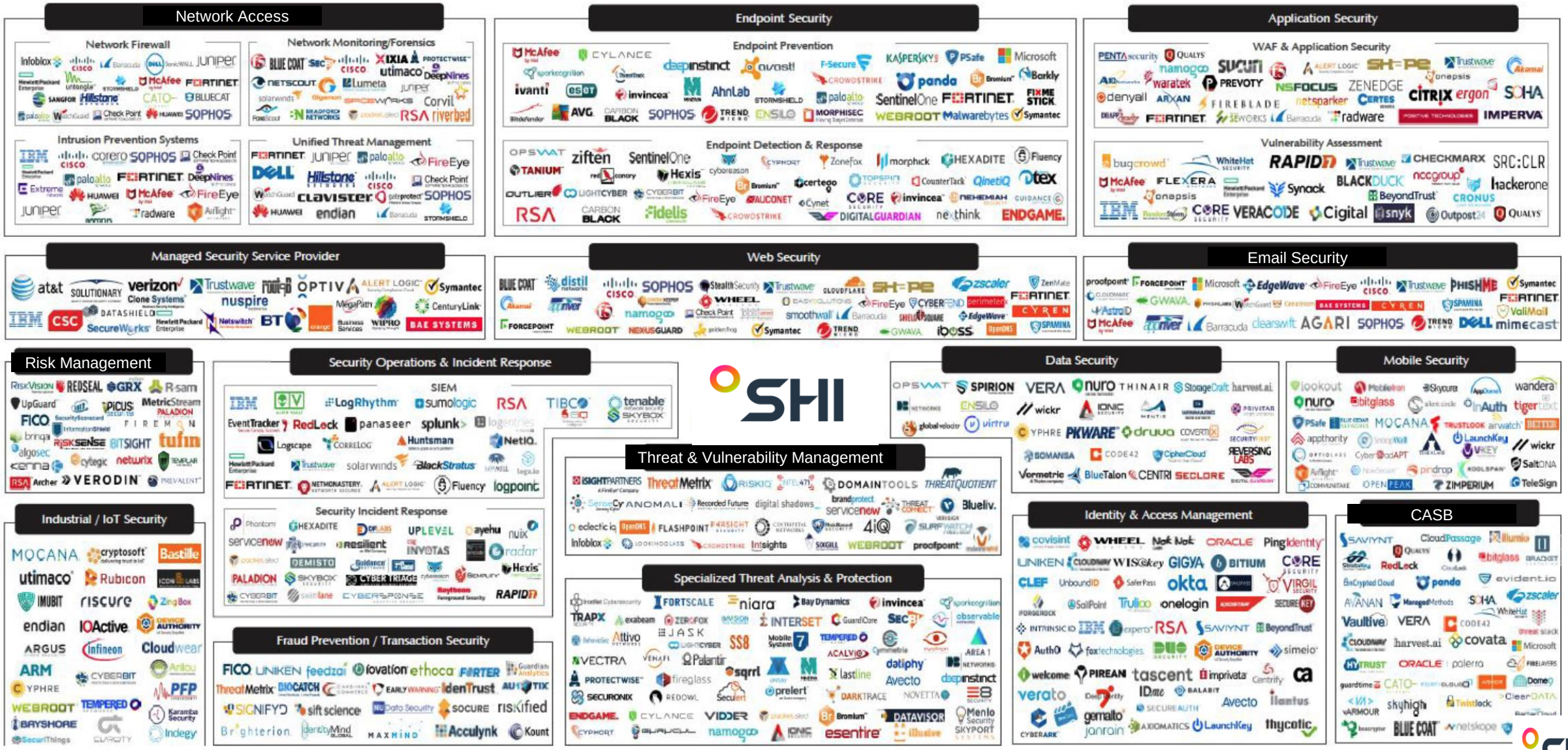
01. Build Right
02. Buy Right
03. Sustainability

WE NEED TO HAVE A DIFFERENT KIND OF CONVERSATION

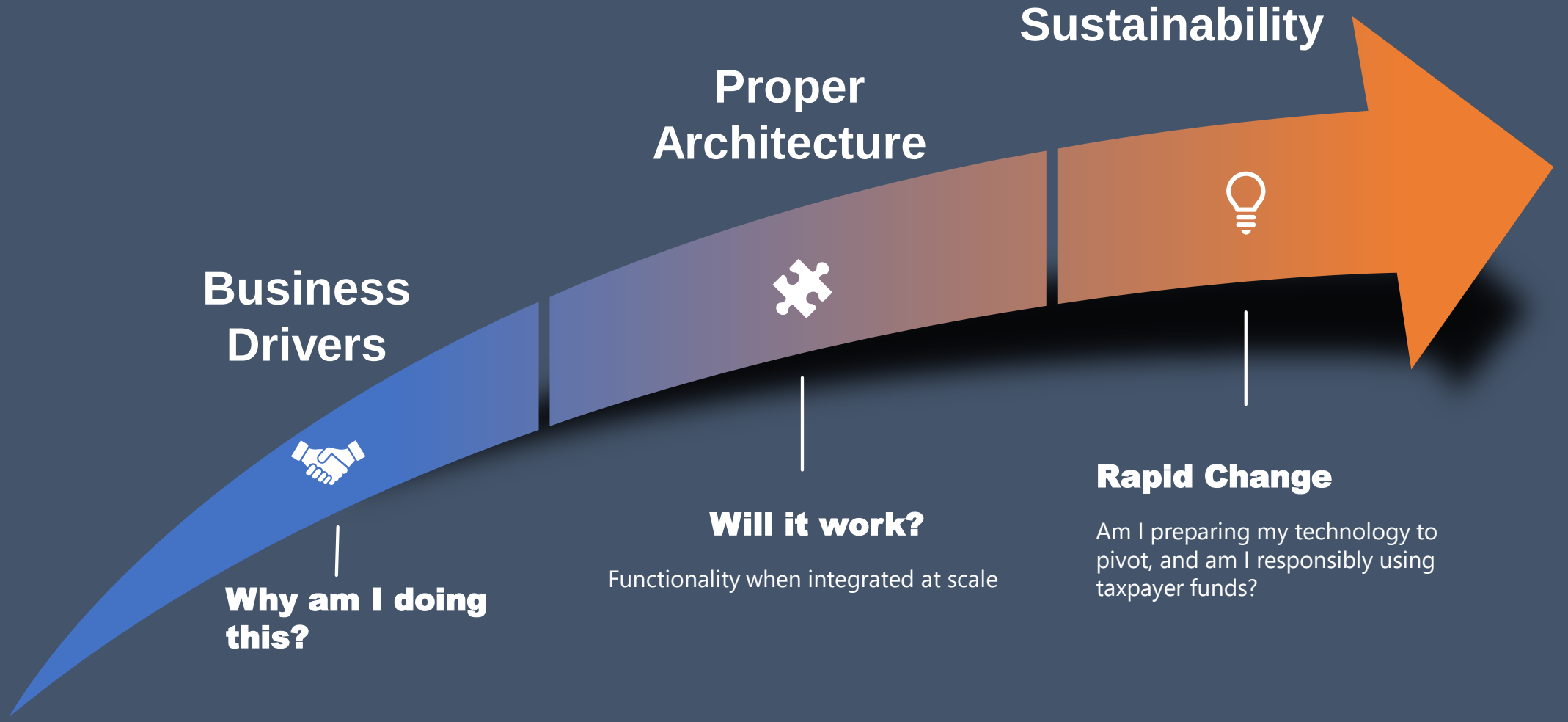
Common Challenges	Ever Changing Threat Landscape	Reduced Visibility	People & Skills Shortages	Vendor Sprawl
Traditional Environments	Static Policies/Rules	Single Location / Campus	Siloed Operations	Point Products
⬇	⬇	⬇	⬇	⬇
Modern Enterprise Environments	**Dynamic & Intelligent**	**Hybrid Applications and Remote Workforce**	**Automated and Managed**	**Deploy Strategic Solutions**

SHI | ASG

The Cybersecurity Landscape – Tool Sprawl

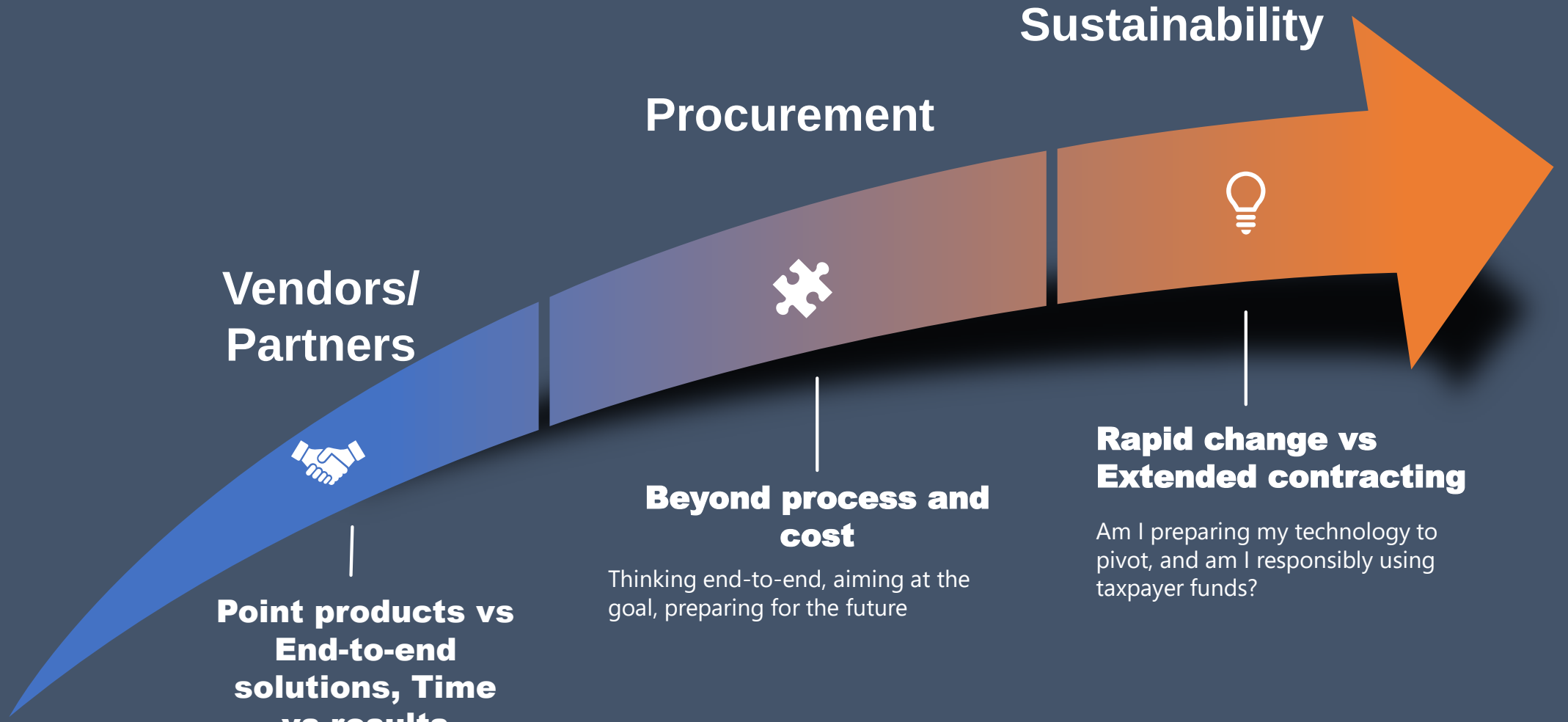


Build Right



SHI | ASG

Buy Right



SHI | ASG

Sustainability

What do I have?

- Infrastructure
- Licensing
- Configuration
- Costs

How am I protecting it?

- Framework
- Policy
- Controls
- Technology

How am I doing?

- Legislative and Compliance Drivers
- Assessments
  - Internal
  - External
  - Tempo

SHI | ASG

SHI | ASG

Thank You