RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: Law-W08

Cybersecurity: Federalism as Defense-in-Depth

MODERATOR: **Gregory von Lehmen**
Special Assistant to the President, Cybersecurity
University of Maryland University College (UMUC)

PANELISTS: **Brian Ray**
Professor of Law & Co-director, Center for Cybersecurity and Privacy Protection
Cleveland Marshall School of Law, Cleveland State University

Chetrice Mosley
Cybersecurity Program Director
Indiana Department of Homeland Security Office of Technology

Frank Grimmelmann
President & CEO
Arizona Cyber Threat Response Alliance (ACTRA)

Session Objectives

- Understand the role of state and state-level private action in addressing national cybersecurity issues
- Learn why state action, even if not uniform, can have national consequences
- Forecast state-level action for the next 3 - 5 years

RSAConference2019

State Legislative Initiatives

Brian Ray: Ohio

Incentivizing Private Sector Investment in Security
Ohio Data Protection Act (2017/2018, SB 220)

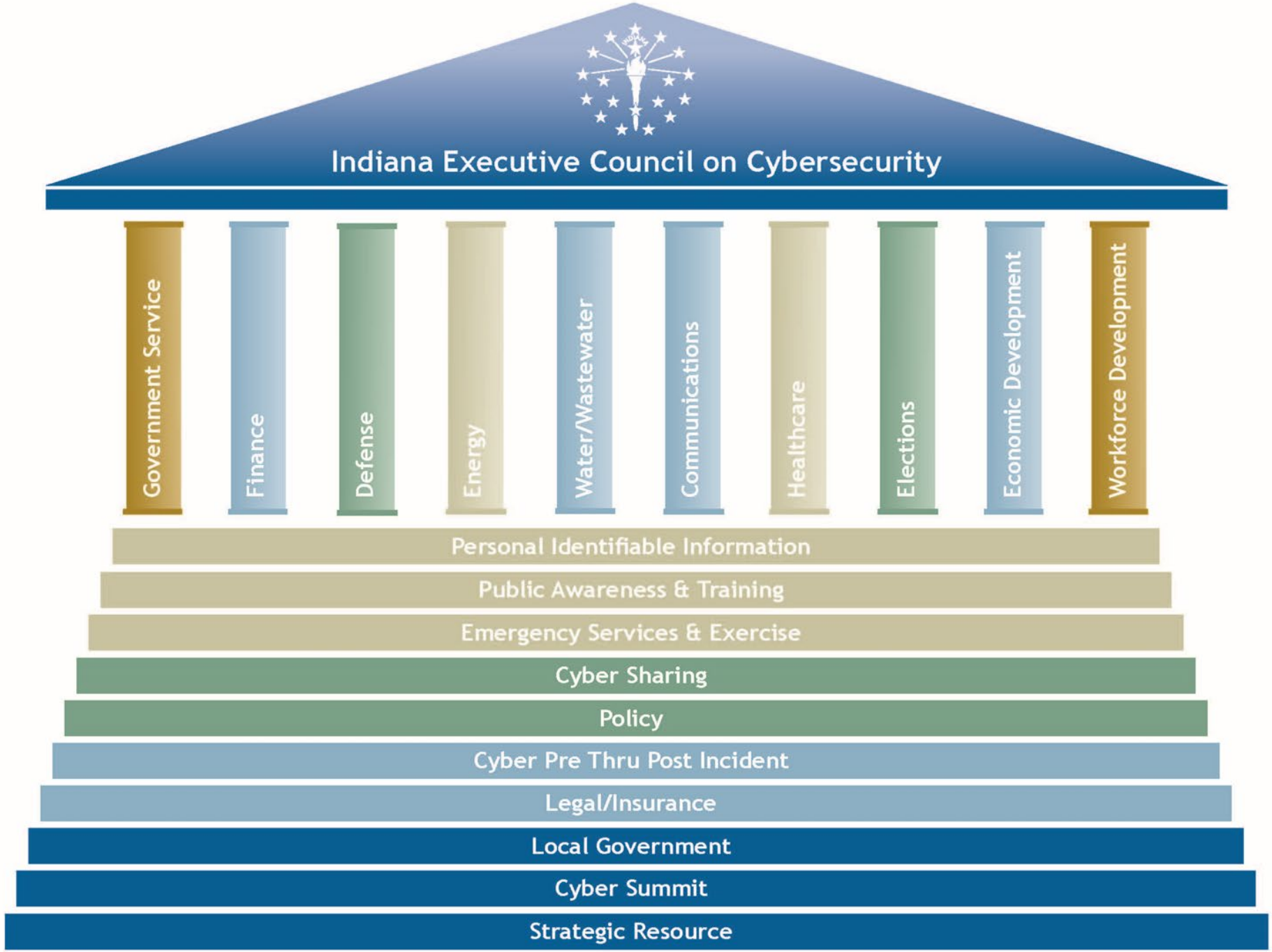
Legal Safe Harbor	Affirmative defense to a cause of action sounding in tort related to data breach
	Applies to all businesses that implement a cybersecurity program that complies with specified regulatory frameworks found in the statute
Business Incentive	Acts as an incentive to encourage cybersecurity within the business community
	DOES NOT create a minimum cybersecurity standard or private of action

- NIST Cybersecurity Framework, 800-53, 53A, or 800-171
- Federal Risk and Authorization Management Program (FEDRAMP)
- Center for Internet Security Critical Security Controls (CIS CSC)
- ISO/IEC 27000 Family
- HIPAA Security Rule Subpart C or HITECH
- GLBA Title V
- Federal Information Security Modernization (FISMA)
- Payment Card Industry standard (PCI) plus another listed framework

RSAConference2019

States Securing Themselves

Cheryl Mosley: Indiana


Indiana Executive Council on Cybersecurity
Government Service
Finance
Defense
Energy
Water/Wastewater
Communications
Healthcare
Elections
Economic Development
Workforce Development
Personal Identifiable Information
Public Awareness & Training
Emergency Services & Exercise
Cyber Sharing
Policy
Cyber Pre Thru Post Incident
Legal/Insurance
Local Government
Cyber Summit
Strategic Resource

YEAR 1 IN REVIEW

- More than 200 members
- 20 teams; 1 Council
- Completed Four Phases
  - Research
  - Planning
  - Implementation
  - Evaluation

YEAR 1 IN REVIEW

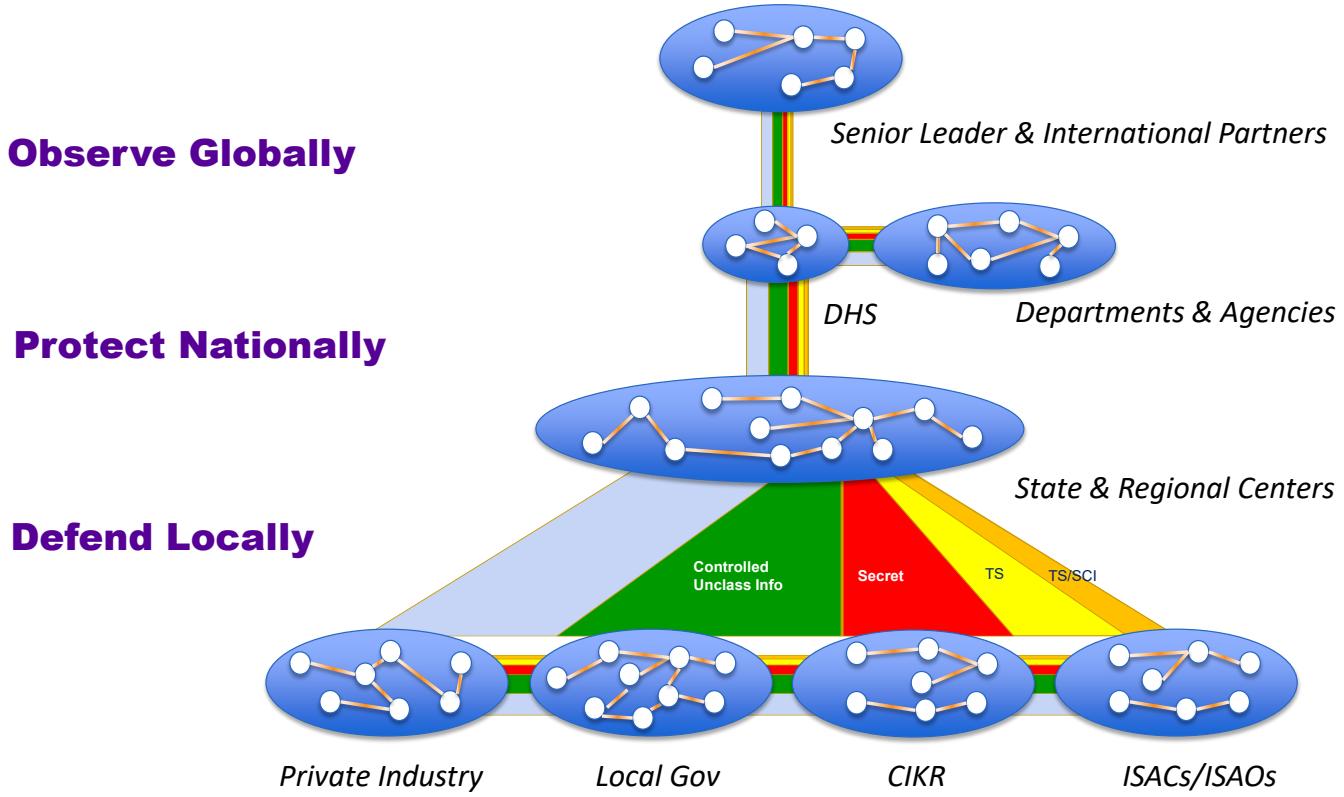
- Developed 20 Strategic Plans for 69 Deliverables with 120 Objectives
  - Completed 19 deliverables (27.5%)
  - Completed 38 objectives (31.6%)

RSAConference2019

Threat Information Sharing: Private-Public Partnerships

Frank Grimmelman: Arizona

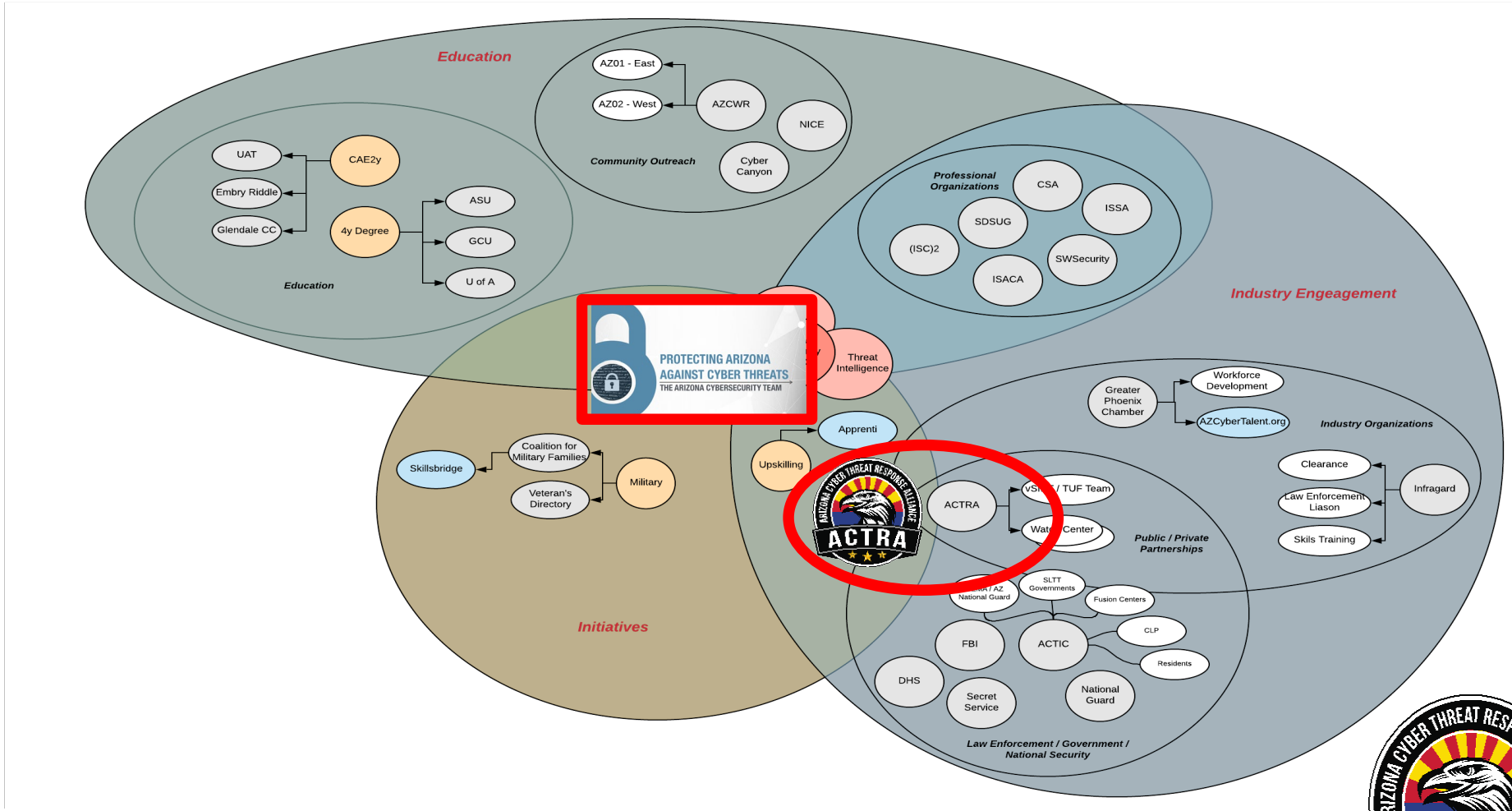
Whole of Nation Cyber Defense



Ability to evolve the cyber defense timelines of our critical infrastructure from "months to minutes to seconds" through:

- **PPP and Broader Cyber Threat Intelligence Sharing**
- **Fusion and Enrichment Constructs**
- **Automated Indicators and Response Mechanisms**
- **Integrated Adaptive Cyber Defense Approaches**

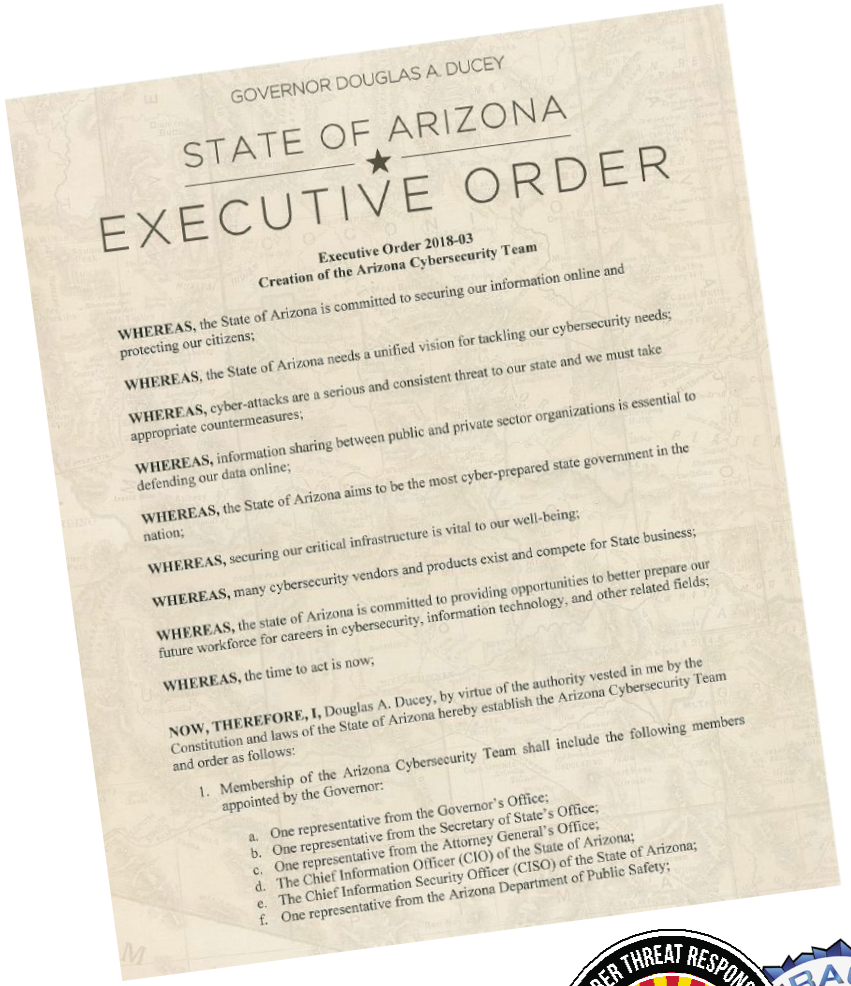
Arizona Cybersecurity Ecosystem



Governor Ducey's 3/7/18 Executive Order

PROTECTING ARIZONA AGAINST CYBER THREATS
THE ARIZONA CYBERSECURITY TEAM

- State of Arizona is committed to securing our information online and protecting our citizens
- Cyber-attacks are serious and consistent to our state and we must take appropriate countermeasures
- Arizona aims to be most cyber prepared in nation
- Securing critical infrastructure is vital
- Information sharing between public and private sector is essential



GOVERNOR DOUGLAS A. DUCEY

STATE OF ARIZONA

EXECUTIVE ORDER

Executive Order 2018-03
Creation of the Arizona Cybersecurity Team

WHEREAS, the State of Arizona is committed to securing our information online and protecting our citizens;

WHEREAS, the State of Arizona needs a unified vision for tackling our cybersecurity needs;

WHEREAS, cyber-attacks are a serious and consistent threat to our state and we must take appropriate countermeasures;

WHEREAS, information sharing between public and private sector organizations is essential to defending our data online;

WHEREAS, the State of Arizona aims to be the most cyber-prepared state government in the nation;

WHEREAS, securing our critical infrastructure is vital to our well-being;

WHEREAS, many cybersecurity vendors and products exist and compete for State business;

WHEREAS, the state of Arizona is committed to providing opportunities to better prepare our future workforce for careers in cybersecurity, information technology, and other related fields;

WHEREAS, the time to act is now;

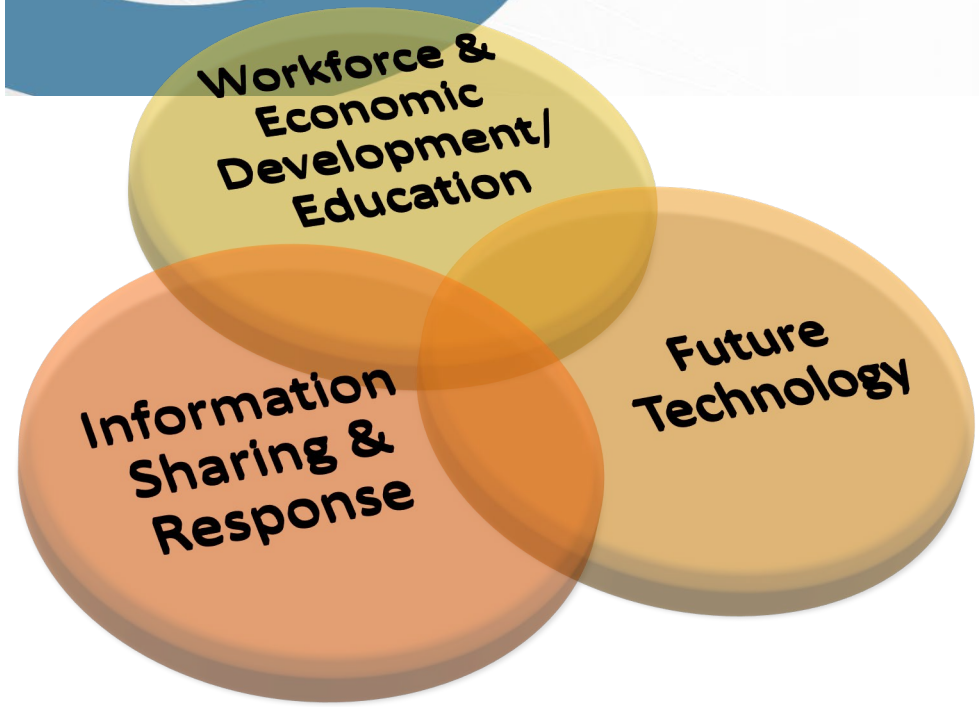
NOW, THEREFORE, I, Douglas A. Ducey, by virtue of the authority vested in me by the Constitution and laws of the State of Arizona hereby establish the Arizona Cybersecurity Team and order as follows:

1. Membership of the Arizona Cybersecurity Team shall include the following members appointed by the Governor:
   a. One representative from the Governor's Office;
   b. One representative from the Secretary of State's Office;
   c. One representative from the Attorney General's Office;
   d. The Chief Information Officer (CIO) of the State of Arizona;
   e. The Chief Information Security Officer (CISO) of the State of Arizona;
   f. One representative from the Arizona Department of Public Safety;

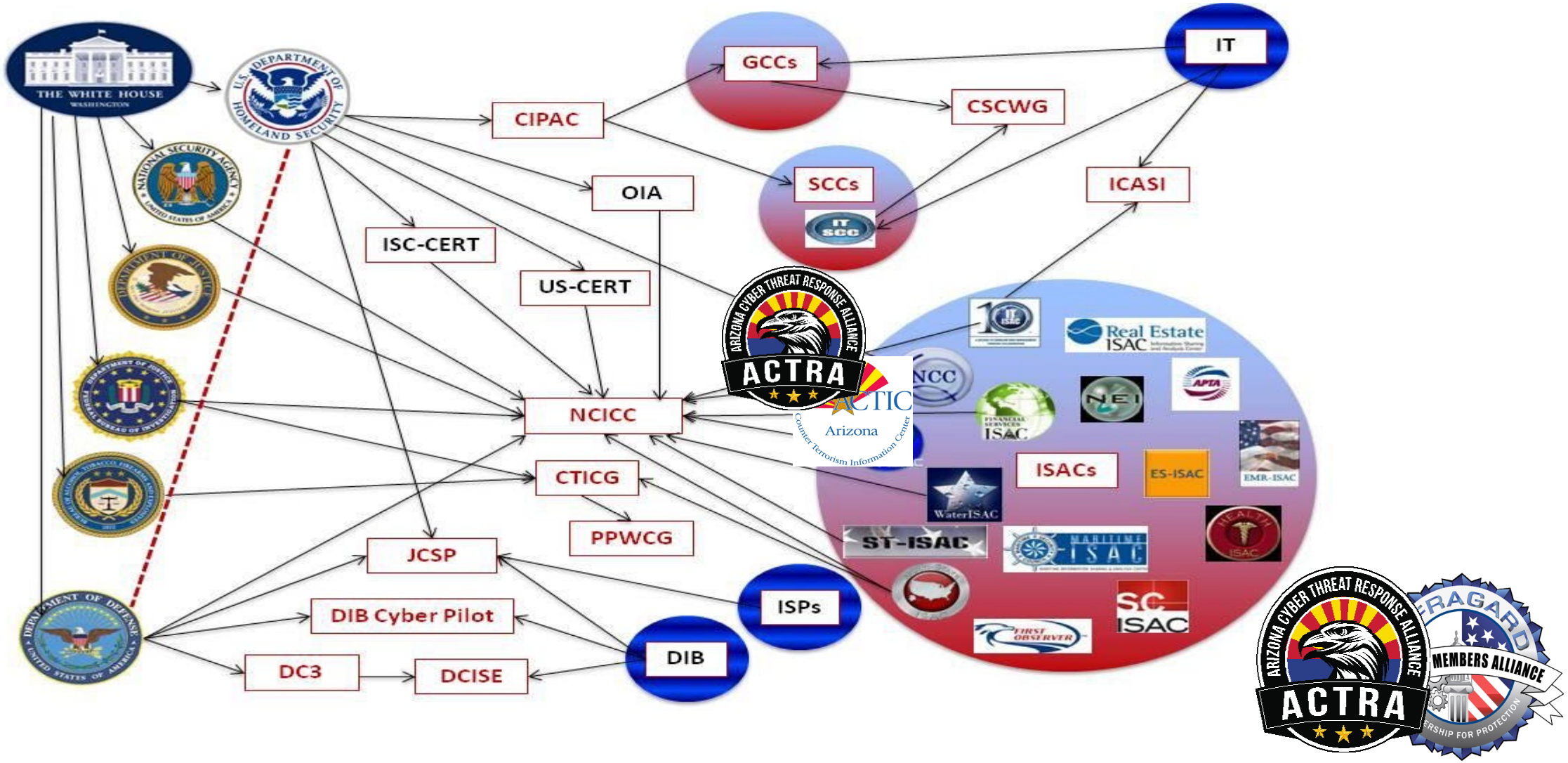
ACT's Members (23)

Governor's Office	Secretary of State Office	Attorney General's Office	AZ CIO	AZ CISO
AZ Dept of Public Safety	AZ Dept of Homeland Security	AZ Dept of Emergency & Military Affairs	AZ Commerce Authority	Info Sharing & Analysis Organization
Critical Infrastructure	US Congress	Private Sector (2)	AZ Legislature (2)	Federal LEO (2)
	Local Govt (2)	Universities/ Colleges (3)		

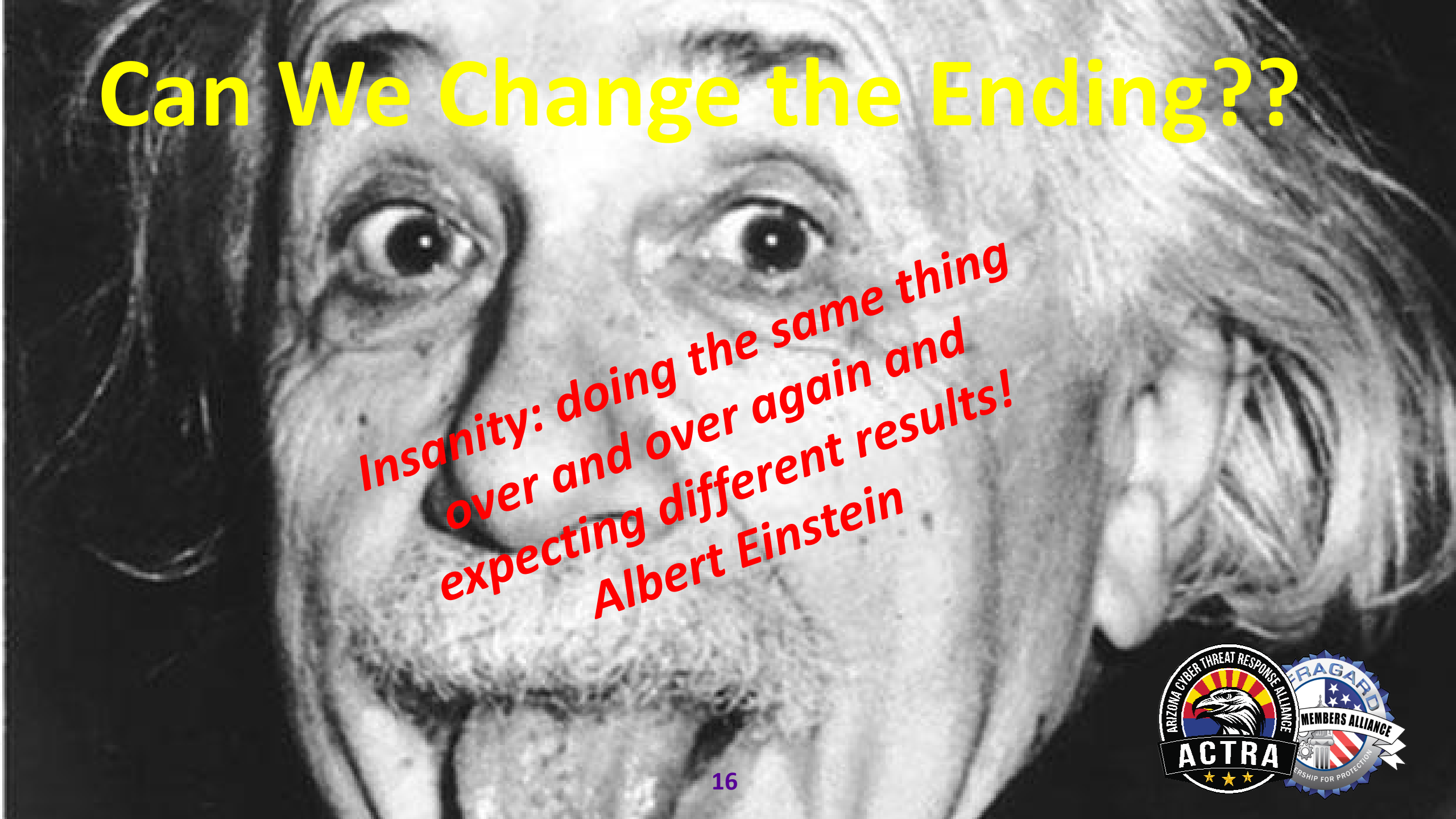
ACT Sub-Groups



Key Institutions in the Cybersecurity PPP Landscape



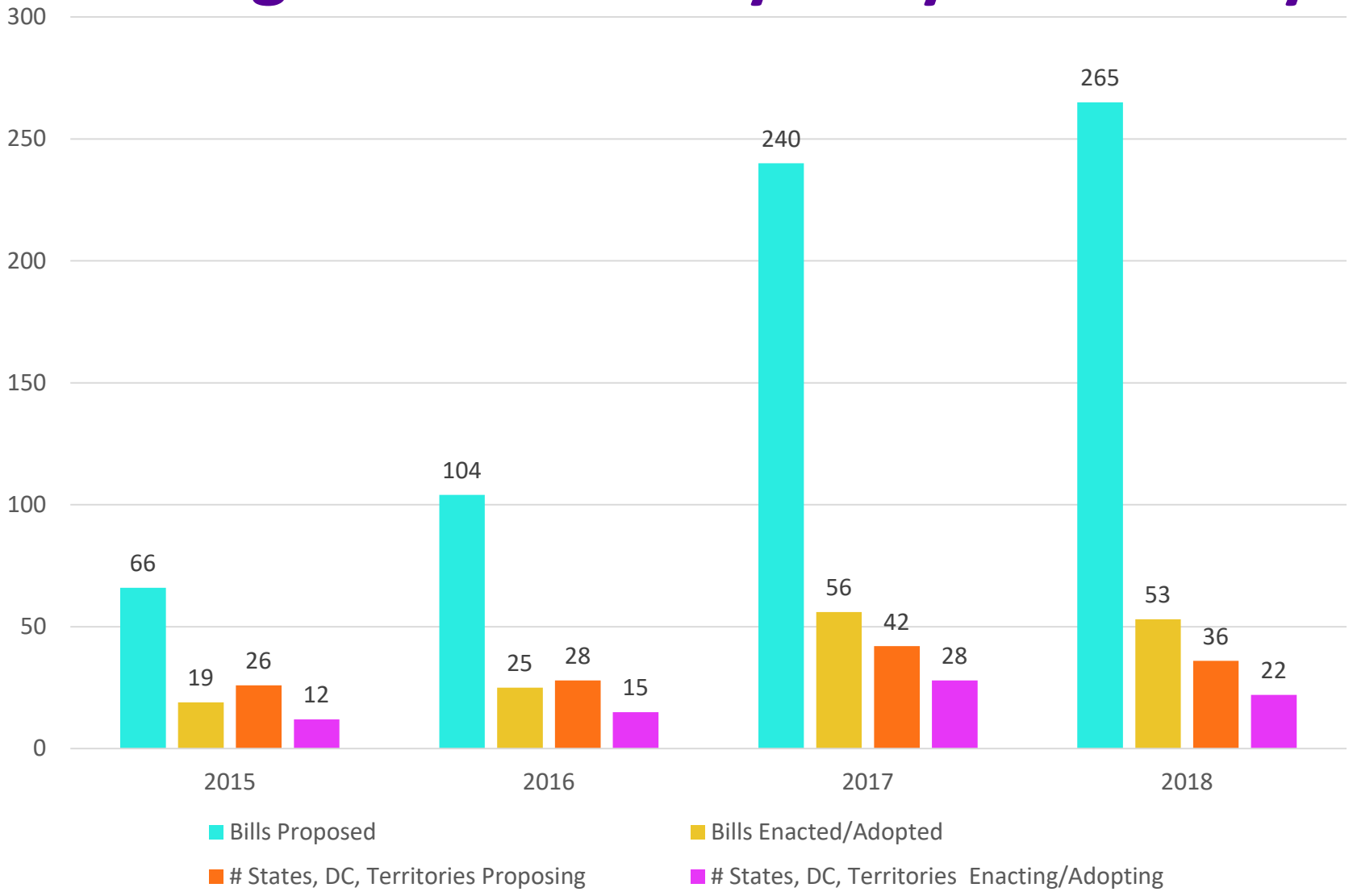
Can We Change the Ending??



RSAConference2019

Moderated Panel Discussion

State Legislative Activity in Cybersecurity



Source: National Council of State Legislatures: Annual Cybersecurity Legislation Summary

Consumer Privacy

California Consumer Protection Act (AB 375)
(Effective January 1, 2020)

- **Notice**: Guarantees consumers the right to know what data is being collected
- **Consent:** Guarantees consumers the right to opt out of data being sold
- **Deletion**: Guarantees consumers the right to delete all their private data, with exceptions
- **Access**: Guarantees consumers the rights to access, download, or transfer their data
- **Kids' Rights**: Kids under 16 must opt in to consent to the sale of their data
- **Enforcement**: The attorney general can levy fines, consumers can sue for breaches

Raising the Security Standards of IoT Devices
Information Privacy: Connected Devices (California AB 1908)
(Effective January 1, 2020)

The act requires “reasonable” security features in “connected devices”.

- “Connected device” means any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address.

- A security feature is “reasonable” if either each device manufactured has a unique password, or the device requires the user to generate a new means of authentication before access is granted for the first time.

Breach Notification
& Incentivizing Consumers to Protect their Identity

- **Maryland Personal Information Protection Act (HB 974)**
  - Range of PII, including biometric data
  - Notification within 45 days
  - Firm makes determination whether breach occurred and whether there is likelihood of harm
  - Encrypted data is per se exempted from notification
  - State statute defers to HIPPA and Graham-Leach-Bliley for entities covered by those federal statutes

- **Maryland Credit Report Security Freezes – Notice and Fees Act** (**SB 202**)
  - Prohibits credit reporting agencies from charging breach victims' fees for a credit freeze & thaws.

Maryland Legislation
Workforce Development

- **Cybersecurity Workforce Development (2018, SB 204)**
  - State-level scholarship-for-service program for full-time undergraduate and graduate students

New York Financial Sector Regulations (23 NYCRR 500) (Not Legislation but Significant State Action)

Covered entities: any person operating under a license or other authority under the banking, insurance, or financial services laws of New York.

Exemptions include firms with fewer than 10 employees, or less than $5 million gross revenues in each of the last three years, or less than $10 million in end-of-year total assets.

Major headings address requirements:

- Cybersecurity program
- Cybersecurity policy
- Implementation
- Pen testing & vuln assessment
- Audit trails
- Access privileges
- Application security
- Risk Assessment
- Staffing and threat intelligence
- Third-party provider policy
- Multifactor authentication
- Data retention
- Others

But We're Making Progress

- According to the 2018 NASCIO Survey:
  - All 50 states have enterprise-level CISO roles (established by legislation in 31 states)
  - In 25 states CISO's have senior-level reporting, either to the governor or to a cabinet secretary
  - 45 states have approved cybersecurity strategy and governance plans
  - 47 states have established awareness training programs for state employees

Next 3 – 5 Years

“There will be greater recognition of SLTT governments’ role in the nation’s cybersecurity efforts.”

2018 SLTT Government Outlook (MS-ISAC)

RSAConference2019

Audience Questions?

RSAConference2019

Thank you!