Center for Internet Security®

SLTT Artificial Intelligence Safety and Governance Challenges and Workforce Implications

Part of the MS-ISAC AI Safety and Governance Webinar Series

James Globe
VP Strategic Advisor Cybersecurity Capabilities
james.globe@cisecurity.org

May 17, 2024

Center for Internet Security

An Independent, Community Driven Not-for-Profit

Who We Are:

CIS Center for Internet Security®

501(c)(3) nonprofit, ~400+ employees

Our Mission:

To create confidence in the connected world

Home of the:

- **CIS Critical Security Controls**
- **CIS Community Defense Model**
- **CIS Benchmarks**

- **Multi-State ISAC**
- **Elections Infrastructure ISAC**

We Are Your Cybersecurity Advisors

Multi-State Information Sharing & Analysis Center

The MS-ISAC

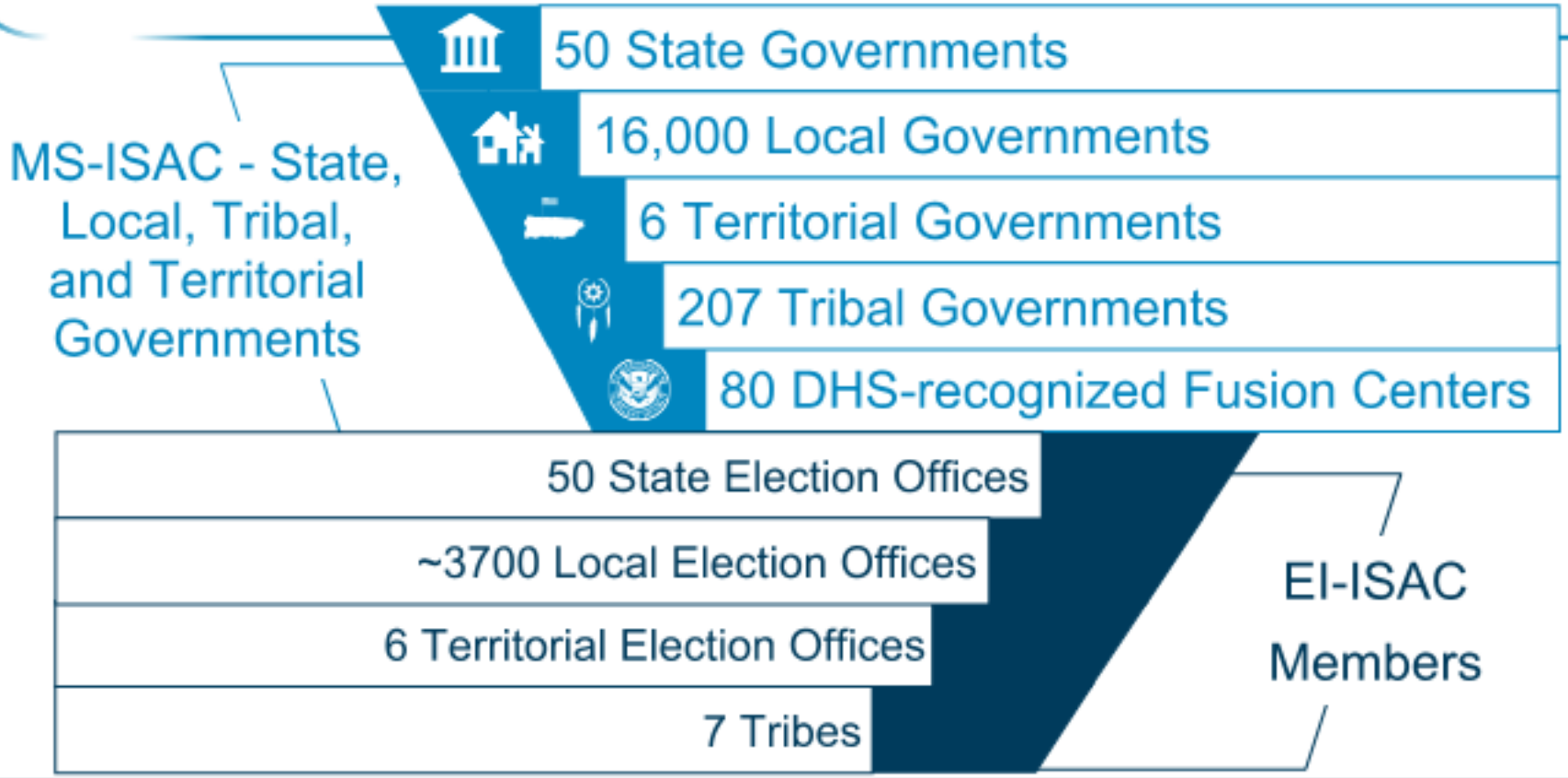
- Designated by the Cybersecurity & Infrastructure Security Agency (CISA) as a key resource for cyber threat prevention, protection, response and recovery for all U.S. State, Local, Tribal and Territorial (SLTT) governments

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

Missions at a Glance

CISA, CIS, MS/EI-ISAC

Who We Serve



No-Cost MS\EI-ISAC Benefits to SLTTs

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

Cyber Threat Intelligence

- Cyber Alerts & Advisories
- Quarterly Threat Report
- Regular Indicators of Compromise (IOCs)
- White Papers
- Cyber Threat Briefings
- Real-Time Intelligence Feeds

Cybersecurity Services

- 24x7x365 Security Operations Center (SOC)
- Cyber Incident Response Team (CIRT)
- ISAC Threat Notification Service (IP & Domain Monitoring)
- Malicious Domain Blocking & Reporting (MDBR)
- Endpoint Detection & Response (EDR) *(EI-ISAC only)*

Cyber Framework & Best Practices

- Nationwide Cybersecurity Review (NCSR)
- CIS SecureSuite Membership
  - *Tools to implement the CIS Critical Security Controls and CIS Benchmarks*

Other Member Resources

- MS\EI-ISAC Webinars
- MS-ISAC Working Groups
- CIS CyberMarket
- Virtual Service Reviews
- Homeland Security Information Network (HSIN)
- Vulnerability Disclosure Program *(EI-ISAC only)*
- Situational Awareness Room *(EI-ISAC only)*

Why Am I Here?

Agenda

01

AGENDA ITEM 01

Defense in Depth and Defining Reasonable Cybersecurity – A CIS Cyber Reasonableness Initiative

02

AGENDA ITEM 02

SLTT Organizations AI Safety and Governance Challenges – A CIS AI Safety Initiative

03

AGENDA ITEM 03

Addressing SLTT Cyber Workforce Demands

A Security Operations Center Apprenticeship Program (SOCAP) Initiative

CIS Center for Internet Security®

Defense in Depth and CIS Controls

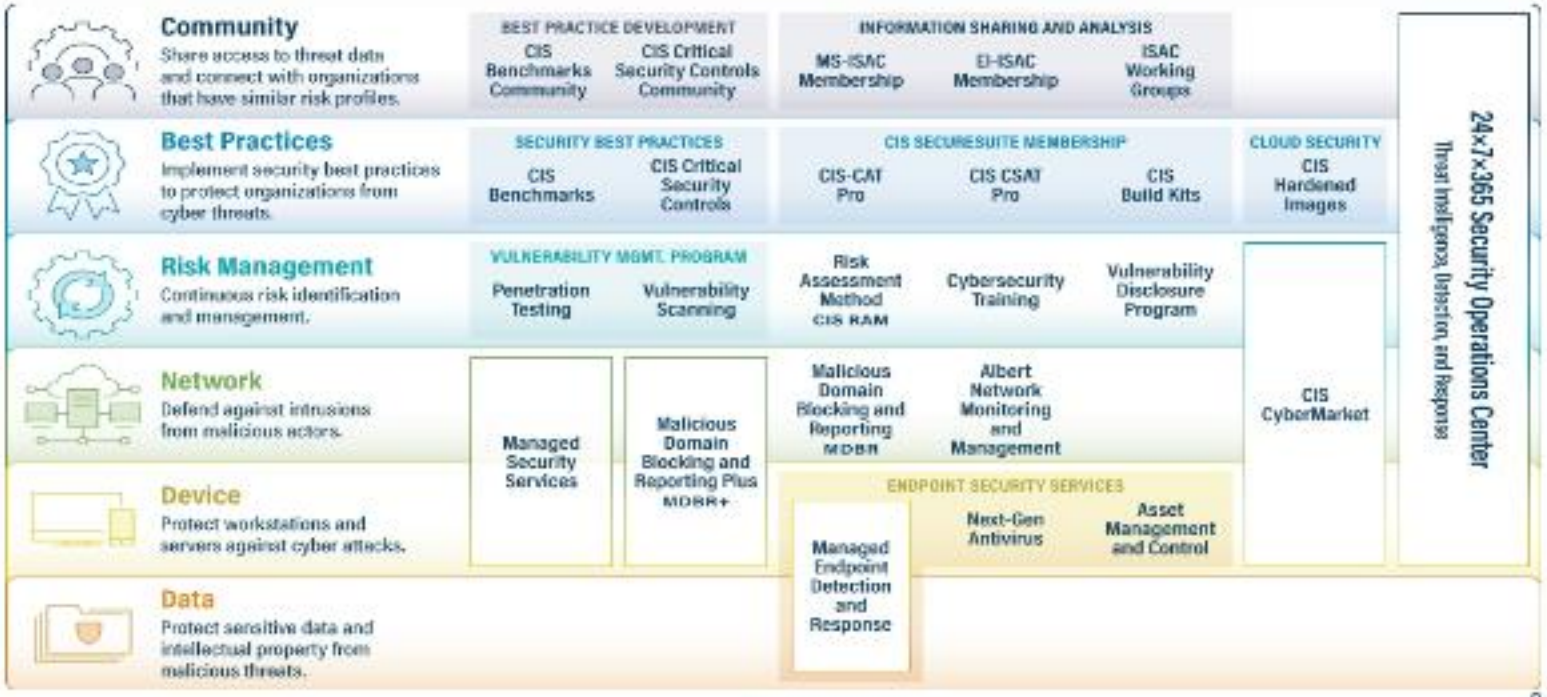
Cyber Reasonableness Initiative

General Release

CIS Defense in Depth Strategy

Suite of Products and Services to Increase Cyber Attacks Resilience

Defense-in-Depth Approach to Cybersecurity



CIS Critical Controls and Benchmarks

Offensive Security Increases Defensive Security

- Key Outcomes
  - Enhances Cyber Defenses
  - Effective Cyber Hygiene
  - Enables Phased Implementation
  - Enables Phased Assessments & Managed Risks
  - Vetted Secure Configurations of Operating Systems, Enterprise Applications, and Services Benchmarks

Control 1	Inventory and Control of Enterprise Assets
Control 2	Inventory and Control of Software Assets
Control 3	Data Protection
Control 4	Secure Configuration of Enterprise Assets and Software
Control 5	Account Management
Control 6	Access Control Management
Control 7	Continuous Vulnerability Management
Control 8	Audit Log Management
Control 9	Email and Web Browser Protections
Control 10	Malware Defenses
Control 11	Data Recovery
Control 12	Network Infrastructure Management
Control 13	Network Monitoring and Defense
Control 14	Security Awareness and Skills Training
Control 15	Service Provider Management
Control 16	Application Software Security
Control 17	Incident Response Management
Control 18	Penetration Testing

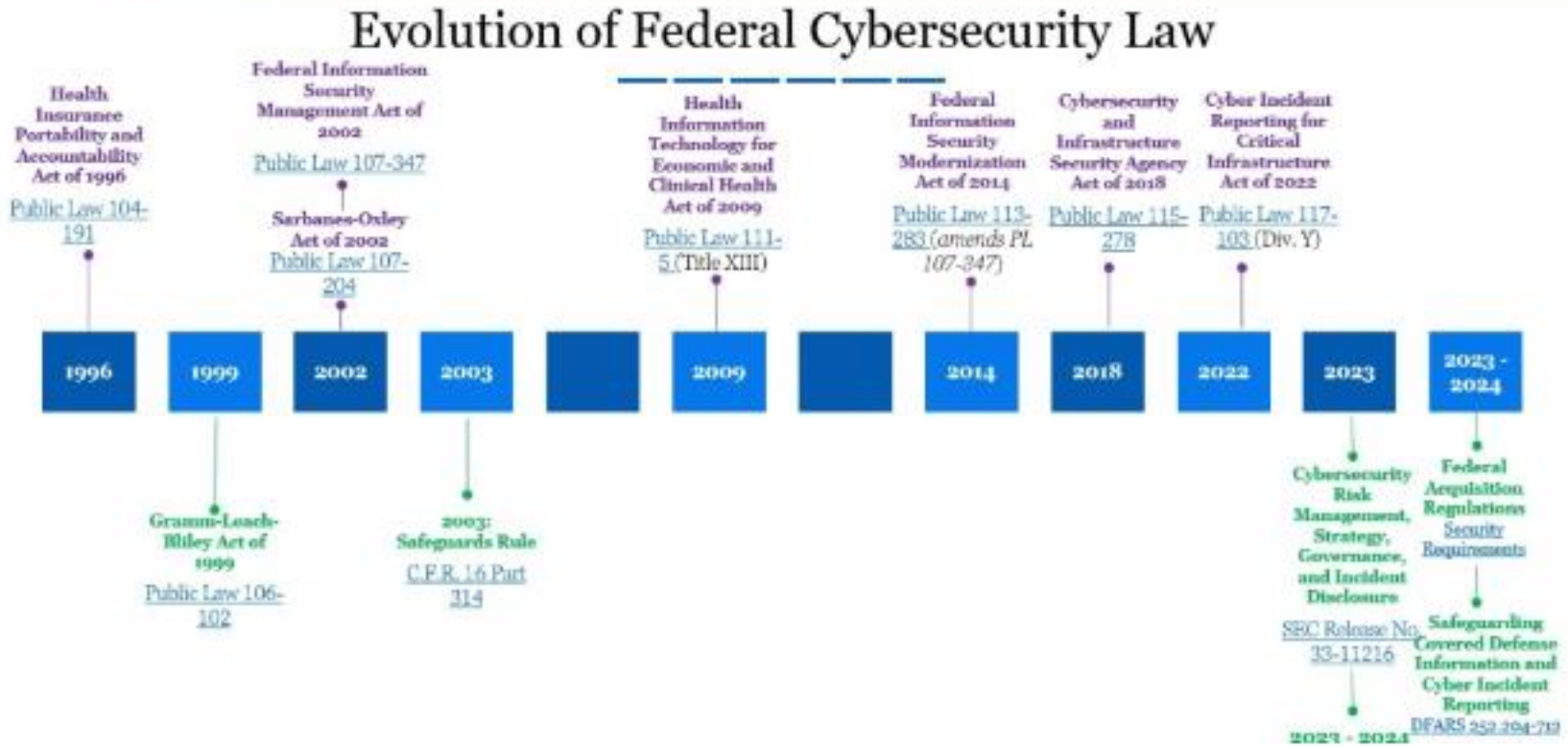
CIS Cyber Reasonableness

A New Initiative – To Define A Minimum Standard

- **No national law defining "What is" reasonable cybersecurity**
  - Cases litigated using common law negligence claims
  - Plaintiff must prove:
    - Legal Obligation (i.e., Duty of Care), and
    - Failed to meet obligation (i.e., Standard of Reasonableness)
- **Increasing convergence of Technology, Public Policy, and Economics**
- **CIS developed a guide to defining reasonable cybersecurity**
  - Target audience: Organizations, Regulators, and Litigators

Current Cybersecurity Laws and Regulations

Federal



Current Cybersecurity Laws and Regulations

State

- State and Territories have Data Breach Laws
  - All 50 States
  - DC, Guam, Puerto Rico, and US Virgin Islands
- States have enacted both Data Protection and Data Privacy Laws
  - 6 States have Data Protection Laws
    - Safe Harbor
    - State Departments and Agencies
- 19 States have Data Privacy Laws
- State Executive Branch Regulations

State Comprehensive Data Privacy Statutes

California. California Consumer Privacy Act as amended by the California Privacy Rights Act

Colorado. S. B. 21-190, Colorado Privacy Act

Connecticut. S. B. 6: An Act Concerning Personal Data Privacy and Online Monitoring

Delaware. H. B. 154, Delaware Personal Data Privacy Act

Florida. S. B. 262, Florida Digital Bill of Rights

Indiana. S. B. 5, Consumer Data Protection

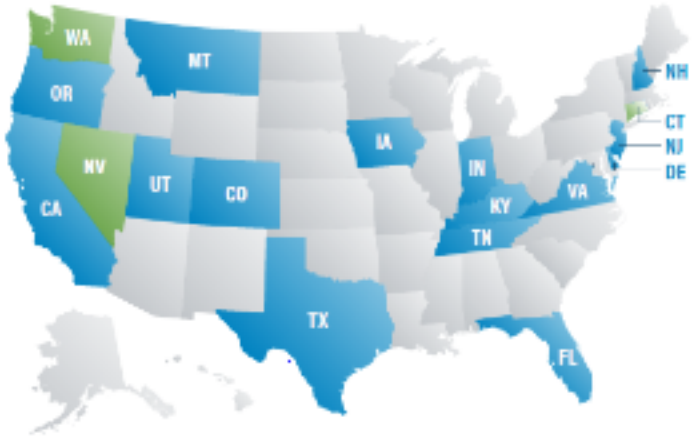
Iowa. S. F. 262, Consumer Data Protection Act

Kentucky. H. B. 15, Kentucky Consumer Data Protection Act

Montana. S. B. 384, Consumer Data Privacy Act

New Hampshire. S. B. 255, Consumer Expectation of Privacy

New Jersey. S. 332, An Act Concerning Commercial Internet Websites, Consumers, and Personally Identifiable Information



Oregon. S. B. 619, Relating to Protections for the Personal Data of Consumers.

Tennessee. H. B. 1181, Tennessee Information Protection Act

Texas. H. B. 4, Texas Data Privacy and Security Act

Utah. S. B. 227, the Consumer Privacy Act

Virginia. Consumer Data Protection Act

State Health Data Privacy Statutes

Connecticut. S. B. 3, An Act Concerning Online Privacy, Data and Safety Protections

Nevada. S. B. 370, Health Data Privacy Law

Washington. H. B. 1155, Washington My Health, My Data Act

Defining Reasonable Cybersecurity

A New Initiative – To Define A Minimum Standard

- **No National law defines reasonable cybersecurity involving data breaches**
- **Various Statutes, Regulations, and Case law**
  - Data Breach Notification
  - Data Privacy
  - Safe Harbor Incentivization
- **CIS guidance supports the objective of defining and helping organizations meet reasonable cybersecurity**
  - Using the CIS Critical Security Controls

CIS's Reasonable Cybersecurity Guideline

Next Steps

- **Kickoff Briefing at RSA 2024**
  - May 9, 2024
- **Download the Guide here**
  - https://www.cisecurity.org/insights/white-papers/reasonable-cybersecurity-guide
- **CIS Hosted Webinar**
  - To be scheduled
- **Panel Discussion at MS-/EI-ISAC Annual Conference**
  - June 24-26, 2024
- **Potential International Conference**
  - Briefing to NCSL General Forum to be scheduled

Center for Internet Security®

SLTT Organizations

AI Safety and Governance Initiatives and Challenges

General Release

What is Artificial Intelligence?

Do We Agree on a Common Definition?

Artificial Intelligence is generally understood to include "engineered or machine-based **systems** designed to **operate with varying levels of autonomy** and **generate outputs** (such as content, predictions, recommendations or decisions), for a **set of explicit or implicit objectives**."

But there is no universally accepted definition . . .

"The science of making machines do things that would require intelligence if done by men."

– Marvin Minsky

"An umbrella term for the science of making machines smart.

– Royal Society

"The field of computer science dedicated to solving cognitive problems commonly associated with human intelligence, such as learning, problem solving, and pattern recognition."

– Amazon

"At base, for a system to exhibit artificial intelligence, it should be able to learn in some manner and then take actions based on that learning. These actions are new behaviors or features of the system evolved from the learnings."

– Omar Abdelwahed

What is Artificial Intelligence?

Types of AI Technologies

NARROW AI

A system capable of demonstrating intelligence in relation to one particular task.

Popular AI Development Approach

Machine Learning

Teaching a computer to identify and recognize patterns by example, rather than programming specific, predetermined rules.

Supervised Learning

Training the system using labeled data to help identify patterns.

Unsupervised Learning

Training the system using unlabeled data requiring self-identification of patterns.

Reinforcement Learning

Training the system by rewarding correct decisions and punishing incorrect ones.

GENERAL AI

A system that is functionally equal (or superior) to human intelligence and can exhibit the full range of human cognitive abilities.

Example Tests

Turing Test

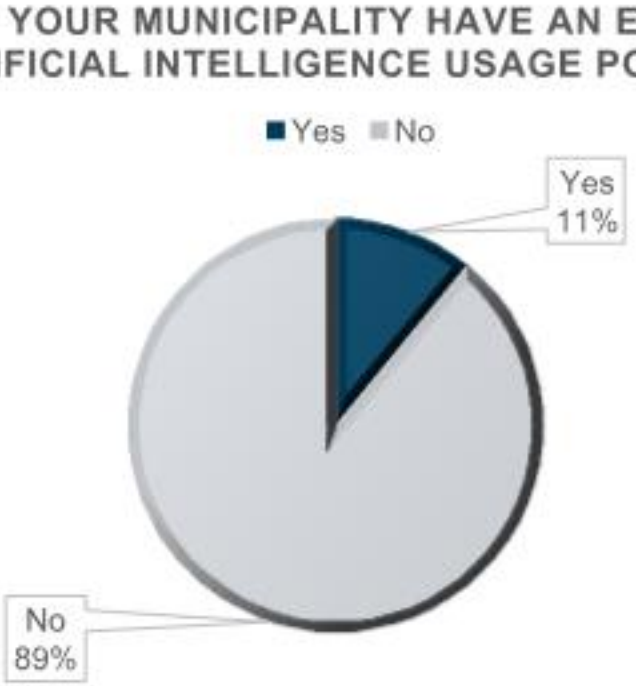
In conversation with a human, can the machine convince a bystander it is the human?

Coffee Test

Can the machine enter an average American home and figure out how to make coffee?

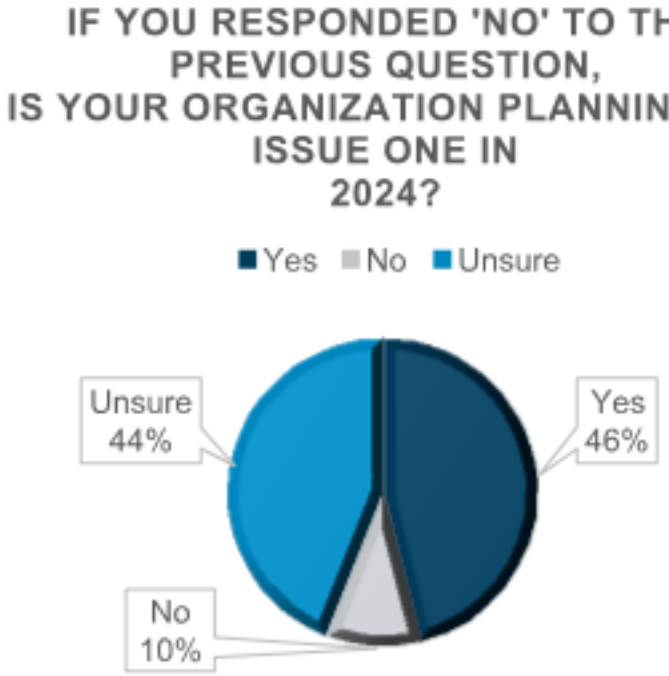
SLTT's AI Safety and Governance

AI Usage Policy Development – Questionnaire Results (January 2024)



SLTT's AI Safety and Governance

AI Usage Policy Development – Questionnaire Results (January 2024)



Analysis Implications

- Shadow IT\AI within SLTT IT Ecosystems
- Pilots and POC Initiatives
- Use Case Development
- Business Needs Justification
- Research
- Lack of Resources

SLTT's AI Safety and Governance

AI Usage Policy Development – 2024 Questionnaire Results (April 2024)

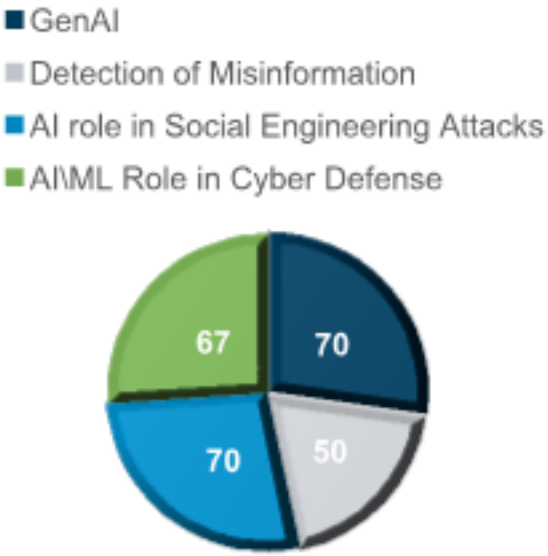
Analysis Implications

- 6% Increase in Created Policies
- 56% Increase in SLTT organizations actively working on policies

SLTT's AI Safety and Governance

AI Usage Policy Development – Questionnaire Results (January 2024)

WHICH AI OR ML TOPICS ARE YOU INTERESTED IN?

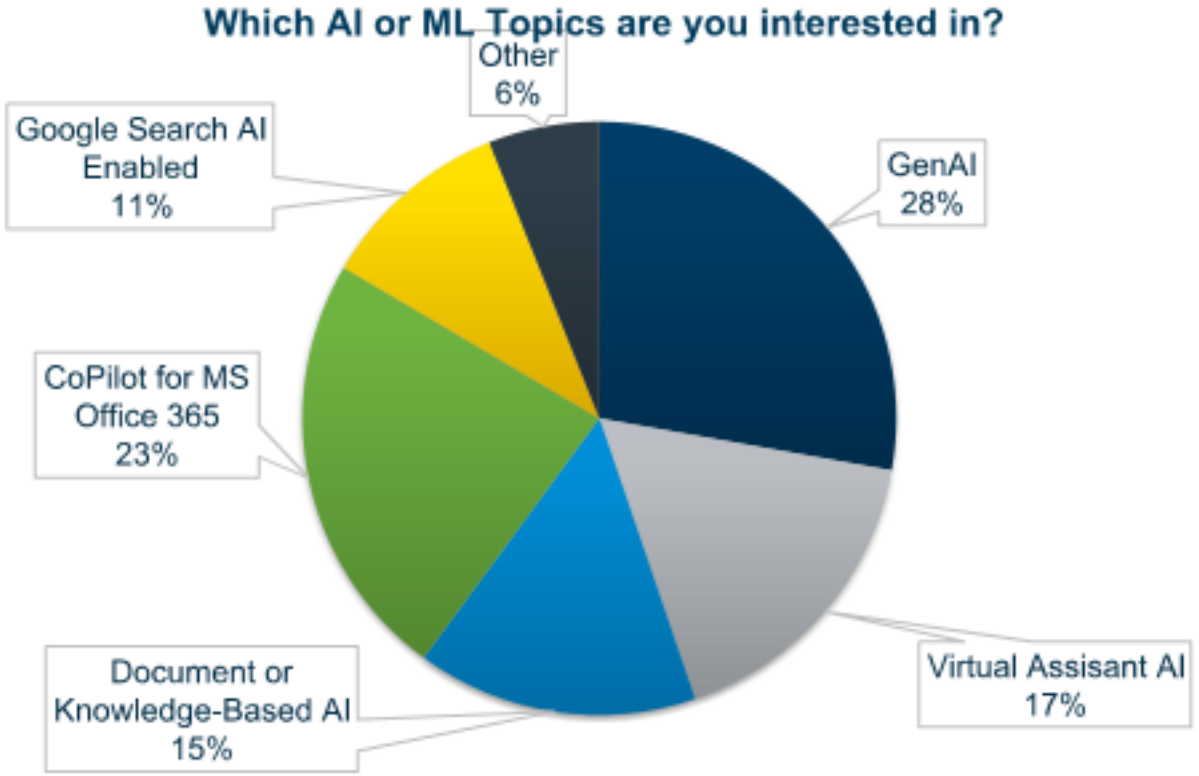


Analysis Implications

- Concerns around development of GenAI Use Cases
- Concerns around GenAI Acceptable Usage
- Concerns for implementation of appropriate GenAI controls
- GenAI Ethics and legal Guidelines
- Concerns for detecting ShadowAI already in their IT Environments

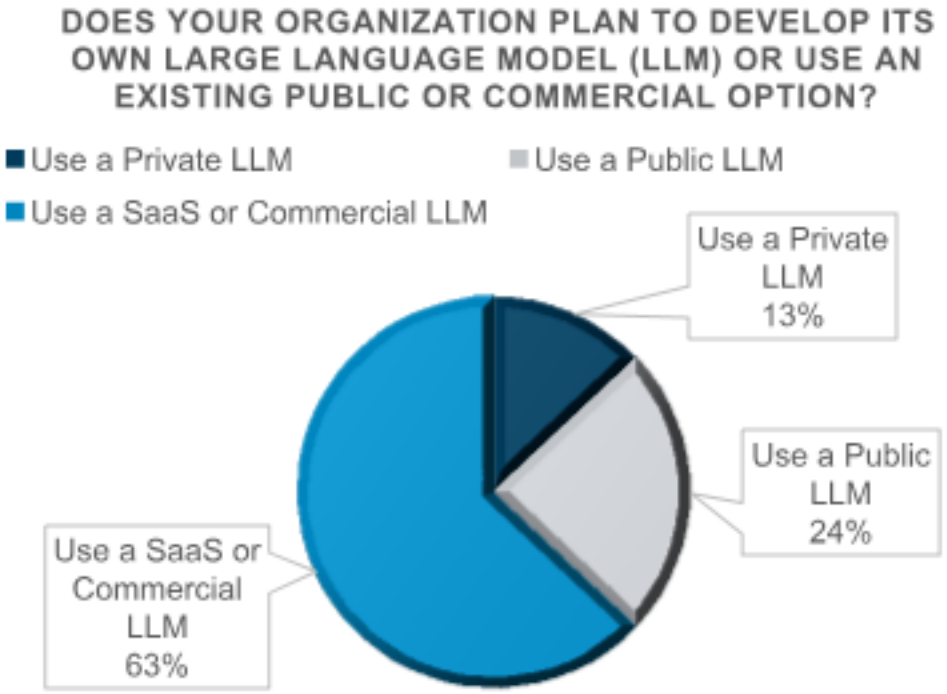
SLTT's AI Safety and Governance

AI Usage Policy Development – Questionnaire Results (April 2024)



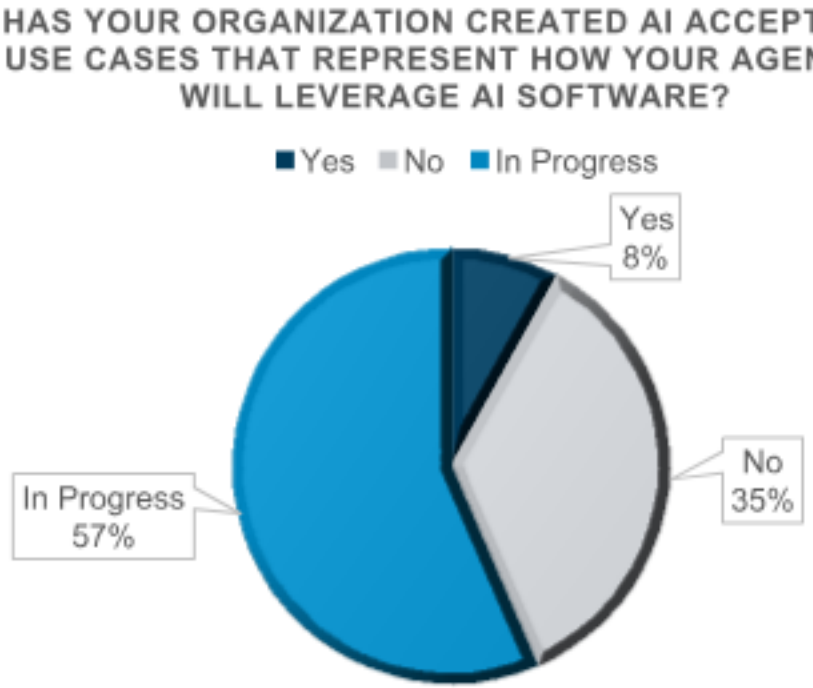
SLTT's AI Safety and Governance

AI Usage Policy Development – 2024 Questionnaire Results (April 2024)



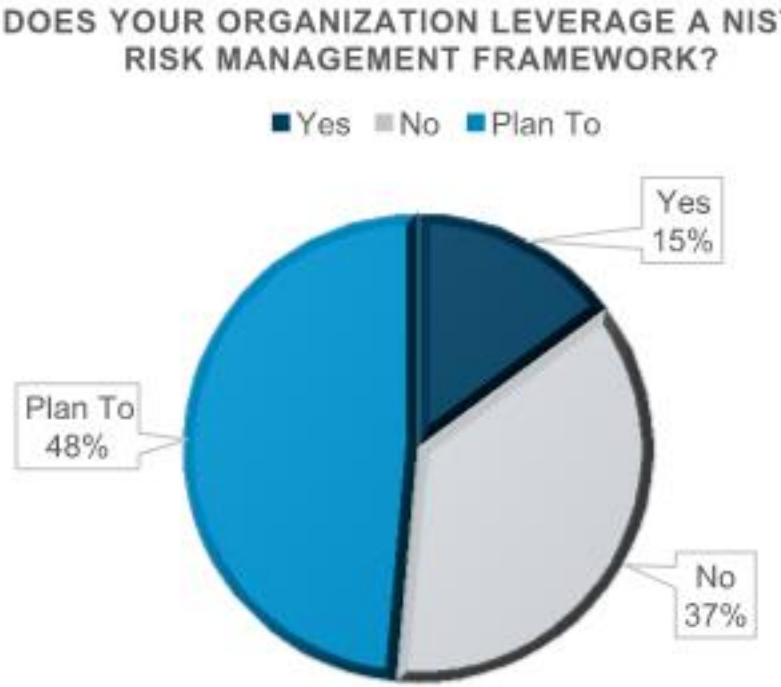
SLTT's AI Safety and Governance

AI Usage Policy Development – 2024 Questionnaire Results (April 2024)



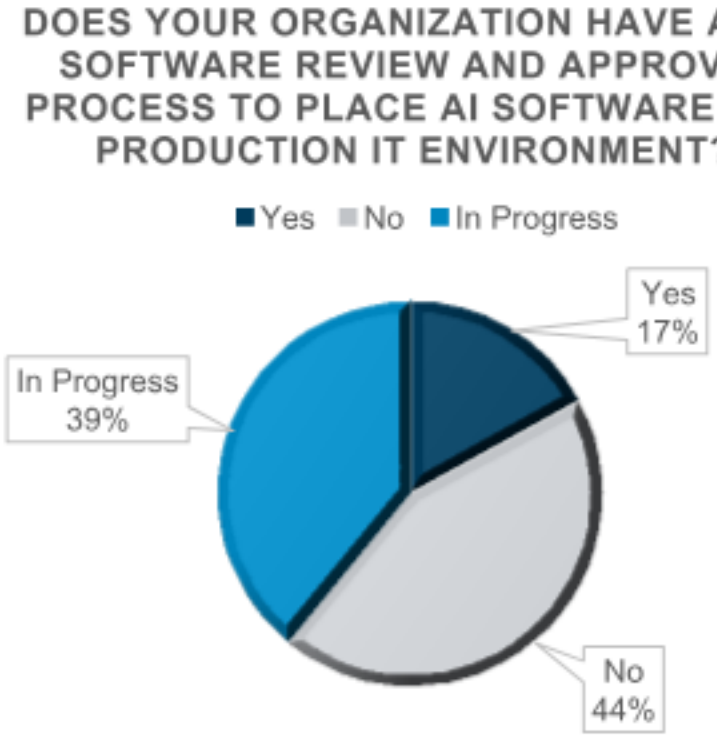
SLTT's AI Safety and Governance

AI Usage Policy Development – 2024 Questionnaire Results (April 2024)



SLTT's AI Safety and Governance

AI Usage Policy Development – 2024 Questionnaire Results (April 2024)



CIS Center for Internet Security®

Addressing SLTT Cyber Workforce Demands

A Security Operations Center Apprenticeship Program (SOCAP) Initiative

General Release

Why are more Cyber Apprenticeship programs needed?

Cyber Apprenticeship Programs targeting Public Sector Organizations

There are very few public sector national apprenticeship programs that focus on SLTT organizations

CIS will provide leadership to support national apprenticeship programs focused on the public sector

SLTTs have limited resources to recruit, train and mentor cyber staff

CIS will leverage its expertise and partners to address the increased technical demands on SLTT governments

Lack of sufficient cyber workforce continues to weaken cyber defenses in SLTT organizations

CIS will leverage its trusted relationships with SLTT organizations to understand job needs

Cyber Workforce Trends

Fortinet 2022 Global Cybersecurity Skills Gap Survey

Cybersecurity affects every organization

80% of organizations experienced one or more breaches during the last 12 months.

19% confirm five or more breaches.

Almost 40% suffered breaches that cost more than a million dollars USD to remediate.

Recruitment and retention of talent is a problem

67% of respondents agree that the skills shortage creates additional cyber risks for their organization. As such, 76% of organizations now have a board of directors who explicitly recommend increases in IT and cybersecurity headcount.

However, 60% of organizations struggle to recruit cybersecurity talent and 52% struggle to retain it.

Organizations are looking for individuals with certified skills

95% of decision-makers believe technology-focused certifications positively impact both their role and their team. As such, 81% of leaders prefer to hire people with certifications.

However, 78% indicate it's hard to find certified people, which is why 91% of organizations are willing to pay for the training and certification of their employees.

Organizations are looking for more diversity

7 out of 10 leaders worldwide say hiring women and new graduates are among their top three challenges.

61% say hiring minorities is also a top three challenge.

Despite the challenges, or perhaps because of it, 3 out of 4 organizations implemented formal processes to hire more women, and 9 out of 10 actively engaged women and new graduates during the last three years.

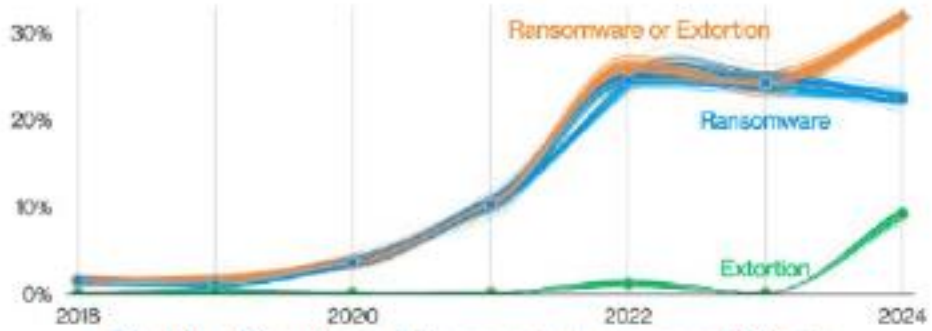
Raising cybersecurity awareness remains a key challenge

87% of organizations implemented a training program to increase cyber awareness. However, 52% of leaders continue to believe their employees still lack the necessary knowledge. This raises the question of the effectiveness of these programs.

66% of organizations that don't have a program intend to set one up.

Cyber Workforce Trends

2024 Verizon Data Breach and Incidents Report



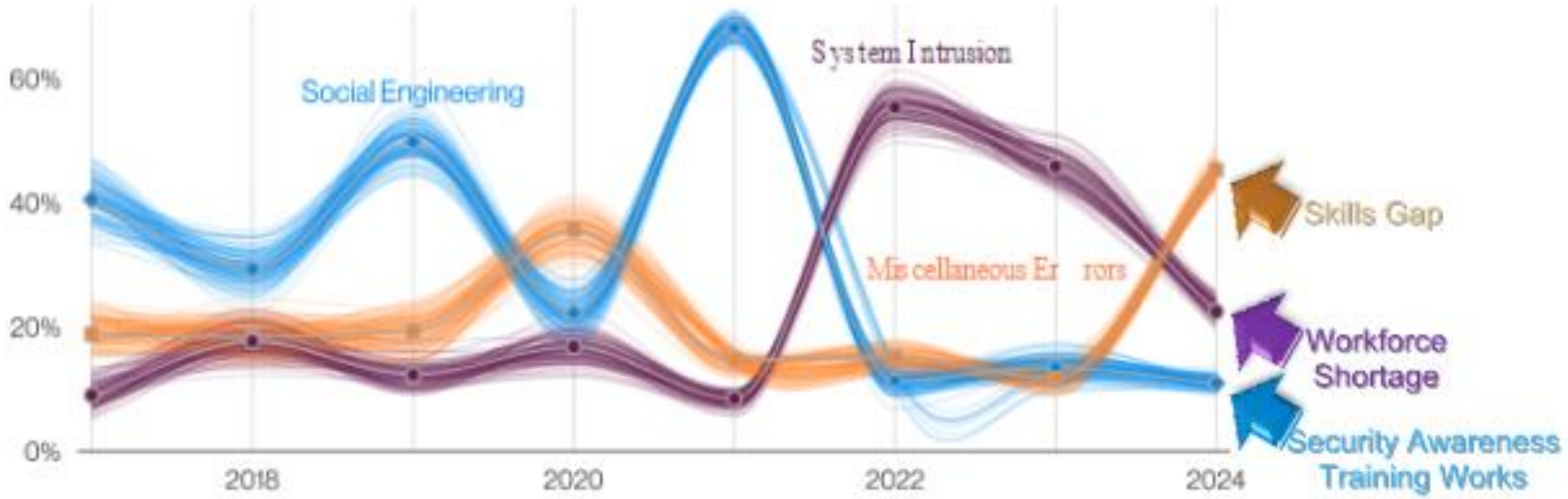
Public Sectors Ransomware and Data Breaches over Time

Frequency	12,217 incidents, 1,086 with confirmed data disclosure
Top patterns	Miscellaneous Errors, System Intrusion and Social Engineering represent 78% of breaches
Threat actors	Internal (59%), External (41%) (breaches)
Actor motives	Financial (71%), Espionage (29%) (breaches)
Data compromised	Personal (72%), Internal (37%), Other (31%), Credentials (17%) (breaches)
What is the same?	System Intrusion and Social Engineering remain top attack patterns in this sector.

Public Sectors Data Incidents Summary

Cyber Workforce Trends

2024 Verizon Data Breach and Incidents Report

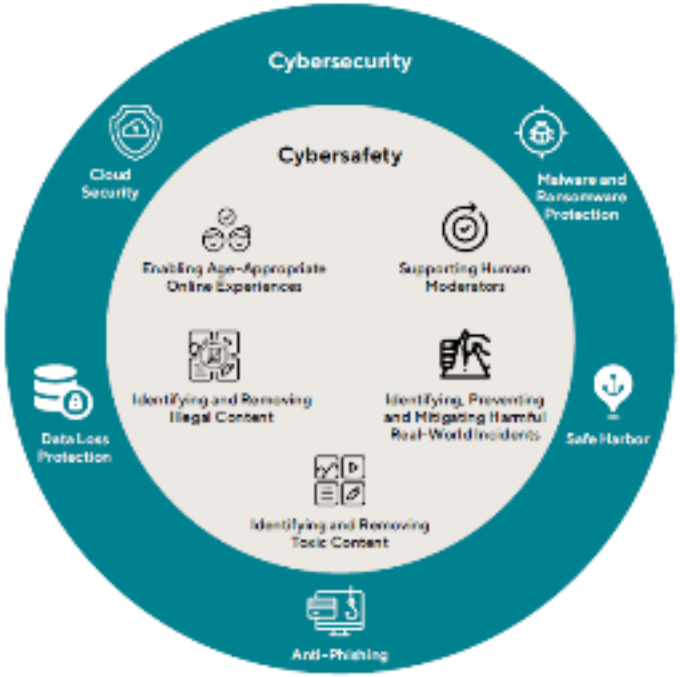


Top Attack Patterns over Time

Cyber Workforce Trends

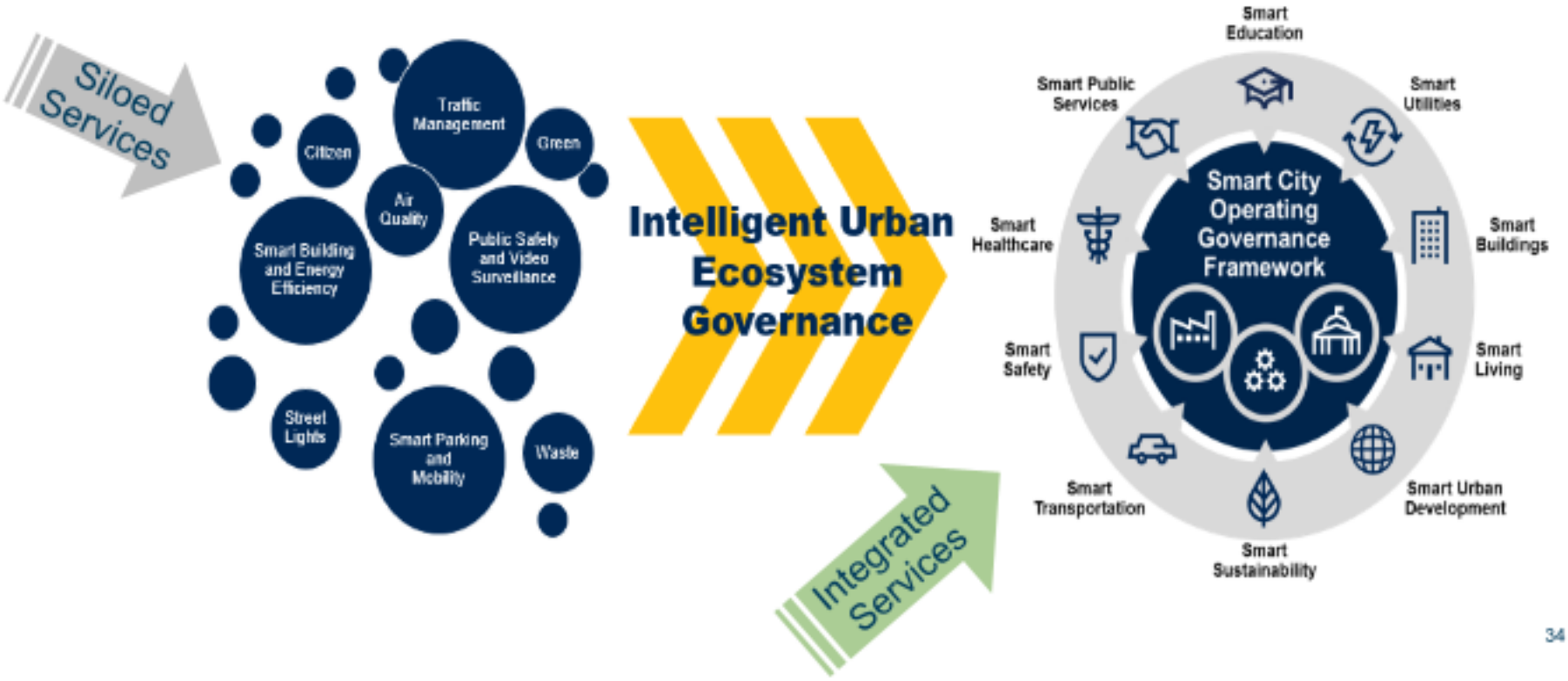
Expanding Attack Vectors and Skills Requirements

- **Cybersecurity and Cybersafety Expanding Skills Demands**
  - Generative Artificial Intelligence (AI) Attacks
  - Misinformation
  - Disinformation
  - Social Engineering
  - Deepfakes
  - Hybrid Threats
    - Diplomatic
    - Military
    - Economic
    - Technological
      - Cyber Attacks



Cyber Workforce Trends

Smart City and Digital Transformation Projects



Cyber Workforce Trends

Cyber Clinic Services and Students Security Operation Centers (SOCs)

Hands-On Experience Opportunities

Rise in Student and Government SOCs

State-based, local municipalities, universities, colleges, community colleges as well as HBCUs and HSI are standing up dedicated SOCs.

Rise in Academia-based Cyber Clinic Services

Colleges and universities are providing vulnerability assessment, penetration testing, and cyber advisory services to public sector and small businesses.

Rise in Artificial Intelligence and Machine Learning Enabled Services

Generative AI and ML projects in support of threat correlation and analysis in support of security operations is on the rise. Both AI and ML technologies are used for threat detection, behavioral-based normalization and anomaly detection, deepfakes detection, misinformation identification, and more.

What the Numbers Say

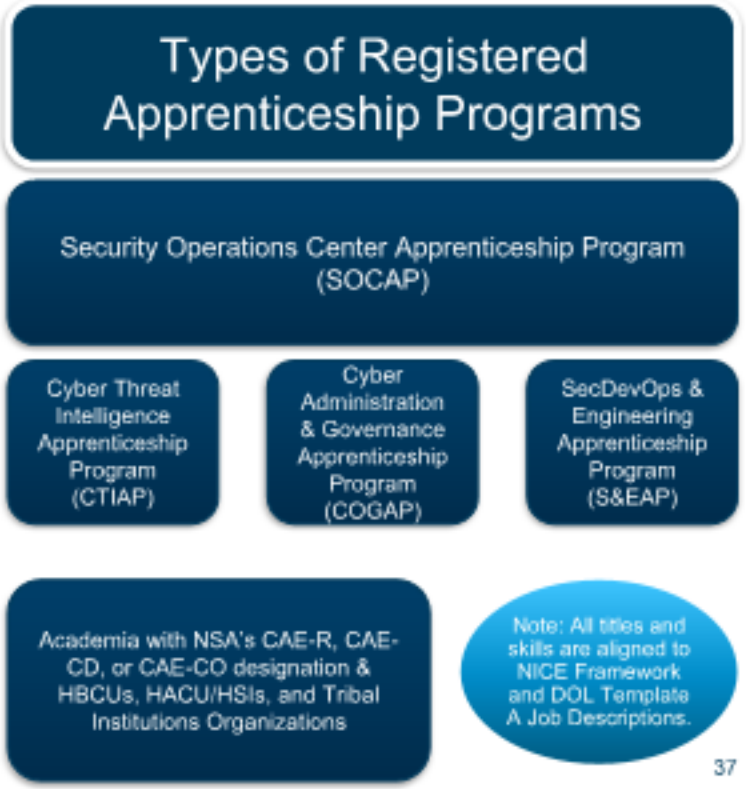
Feedback from SLTT Organizations Questionnaire

WHAT ARE YOUR CURRENT SECURITY OPERATIONS STAFFING NEEDS?

Registered Apprenticeship Programs

DOL Registered Apprenticeship Program Overview

- **What is a Registered Apprenticeship Program?**
  - A sponsor employs staff within their home state
  - Register at least 20 apprentices within two years
    - Each Apprentice completes 2000+ hands-on activities
    - Each Apprentice completes 166 hours of training
  - Sponsor ensures the occupations in each Apprenticeship Program align to DOL's Template D standards



Program Offering Details

Key Occupations By Apprenticeship Program

- **Security Operations Center Apprenticeship Program (SOCAP)**
  - Cyber Defense Operator
  - Cyber Defense Incident Responder
  - Cyber Defense Forensics Analyst
  - Vulnerability Assessment Analyst
- **Cyber Threat Intelligence Apprenticeship Program (CTIAP)**
  - Cyber Defense Analyst
  - Threat/Warning Analyst
  - Exploitation Analyst
  - All-Source Analyst

- **Note: All titles and skills are aligned to NICE Framework and DOL Template A Job Descriptions.**

Program Offering Details

Key Occupations By Apprenticeship Program

- **SecDevOps & Engineering Apprenticeship Program (S&EAP)**
  - Software Developer
  - Secure Software Assessor
  - System Testing and Evaluation Specialist
  - Information Systems Security Developer
  - Data Analyst
  - Technical Support Specialist
  - Network Operations Specialist
  - Systems Security Analyst
  - Cyber Defense Infrastructure Support Specialist

- **Note: All titles and skills are aligned to NICE Framework and DOL Template A Job Descriptions.**

Program Offering Details

Key Occupations By Apprenticeship Program

- **Cyber Administration & Governance Apprenticeship Program (CAGAP)**
  - Cyber Policy and Strategy Planner
  - IT Project Manager
  - Cyber Ops Planner
  - Cyber Intel Planner
  - Privacy Officer/Privacy Compliance Manager
  - Cyber Legal Advisor

- **Note: All titles and skills are aligned to NICE Framework and DOL Template A Job Descriptions.**

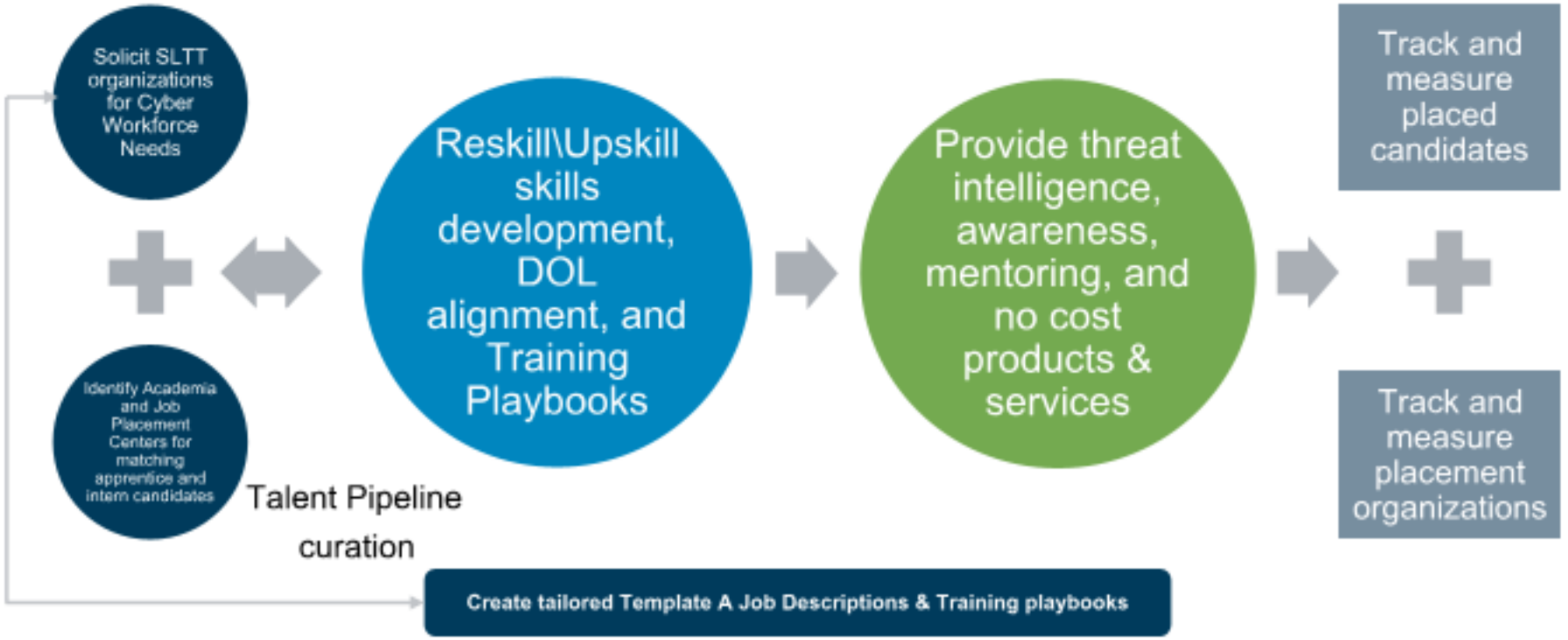
How CIS Can Help

Why should CIS get involved?

- MS-ISAC has over 1500 higher education entities as members, and more than 200 of those entities have NSA's Center of Academic Excellence (CAE) designation in cybersecurity research, operations, and/or defense that represent a talent pipeline to public organizations.
- CIS has trusted relationships with CIOs, IT Leadership, and CISOs of all 56 states, as well as thousands of local municipalities, territories and tribal organizations.
- CIS will identify and facilitate the injection of top cyber talent into the over 16,000 State, Local, Tribal, Territorial, and Election public sector organizations that are members of the MS-ISAC and EI-ISAC.

How CIS Can Help

Why should CIS get involved?



How can NCSL help?

Four Actionable Takeaways

1. **Download the Reasonable Cybersecurity Guide and give it a voice within your chambers**
   - https://www.cisecurity.org/insights/white-papers/reasonable-cybersecurity-guide
2. **AI Safety, Ethical Usage, and Understanding LLMs**
   - How LLM aggregate and share metadata with LLM Service Providers\Brokers
   - How LLMs stitch data points together “to learn” and “to answer questions”
   - Procurement and Data Governance Requirements for LLM
3. **Champion SLTT Apprenticeship Programs targeting**
   - Programs that focus on Reskilling and Upskilling existing staff
   - Advocate skills-based job description and hiring
4. **Understand the impacts of handling Deepfake Incidents on your municipalities and brand (trust)**

CIS Center for Internet Security®

Questions?

James Globe
VP Strategic Advisor Cybersecurity Capabilities
james.globe@cisecurity.org