



State Administration & Technology Appropriations Subcommittee

**Wednesday, January 10, 2024
8:30 AM - 10:00 AM
Webster Hall (212 Knott)**

MEETING PACKET

Committee Meeting Notice

HOUSE OF REPRESENTATIVES

State Administration & Technology Appropriations Subcommittee

Start Date and Time: Wednesday, January 10, 2024 08:30 am
End Date and Time: Wednesday, January 10, 2024 10:00 am
Location: Webster Hall (212 Knott)
Duration: 1.50 hrs

Artificial Intelligence (AI) Presentations and Panel Discussion

Cybersecurity Training and Critical Infrastructure Assessment Update

To submit an electronic appearance form, and for information about attending or testifying at a committee meeting, please see the "Visiting the House" tab at www.myfloridahouse.gov

NOTICE FINALIZED on 01/08/2024 4:00PM by EHP

State Administration & Technology Appropriation Subcommittee
January 10, 2024
Webster Hall (212 Knott Building)

Presenters

Cybersecurity Updates:

- Jim Aldrich, Associate Director for Education & Training, Cyber Florida, University of South Florida
- Brian Langley, Senior Executive Advisor, Cyber Florida, University of South Florida
- Melinda Miguel, Florida Chief Inspector General, Executive Office of the Governor

Artificial Intelligence:

- David Clark, Florida Technology Council
- Brian Fonseca, Director, Jack D. Gordon Institute for Public Policy, Florida International University
- Jimmie Harrell, Chief Information Officer, Department of Revenue
- Jim Zingale, Executive Director, Department of Revenue
- Ann Coffin, Director, Child Support Program, Department of Revenue

Cyber Florida
University of South Florida

Cyber Florida Programming Update

Session 2024
State Administration and Technology Appropriations
Subcommittee
January 10th, 2024

Cyber Florida Team

Ernie Ferraresso
Director of Cyber Florida

Jim Aldrich
Associate Director for Education and Training

Bryan Langley
Sr. Executive Advisor, Critical Infrastructure
Risk Assessment

James Jacobs
Associate Director of Partnerships and Policy

Cyber Florida

Created by the Florida State Legislature in 2014.

The University of South Florida serves as our host institution, but we work with the entire SUS on behalf of the State of Florida.

Mission: Help Florida become a national leader in cybersecurity education, academic and practical research, and community outreach and engagement.

CyberSecureFlorida Training Program

GOAL: Train state and local government employees in cybersecurity

The CyberSecureFlorida Training Program Offers:

- ❖ Flexible training options: in-person, virtual synchronous, virtual asynchronous, and self-paced.
- ❖ Continuous outreach and communications
- ❖ Engagement with institutional leadership
- ❖ Incentivized training through recognition efforts (digital badges).



Partner Institutions & Course Offerings

Cyber Florida currently offers over 40 courses.

- Cybersecurity Awareness Certificate for Florida State and Local Government Employees
 - This course covers all the topics included in the curriculum of “Cybersecurity Awareness Training” as described in The Local Government Cybersecurity Resource Packet provided by FL[DS].
- Executive Seminar in Cybersecurity Leadership and Strategy for Public Sector Leaders
- Non-Technical Comprehensive Cybersecurity Leadership and Strategy Professional Education Program for Public Sector Leaders and Managers
- Cybersecurity Leadership and Strategy Professional Education Program for Public Sector Leaders and Managers
- CompTIA PenTest + Exam Prep
- CompTIA Security+ Exam Prep
- ISC2 Certified Information Systems Security Professional (CISSP) Exam Prep
- CompTIA Cloud+ Exam Prep
- CompTIA Network+ Exam Prep
- CompTIA Advanced Security Practitioner (CASP+) Exam Prep
- Introduction to AI and Machine Learning for Cybersecurity
- Penetration Testing
- NIST Frameworks and Standards
- Implementing the Risk Management Framework



Visit www.cyberflorida.org for a complete list of course offerings.

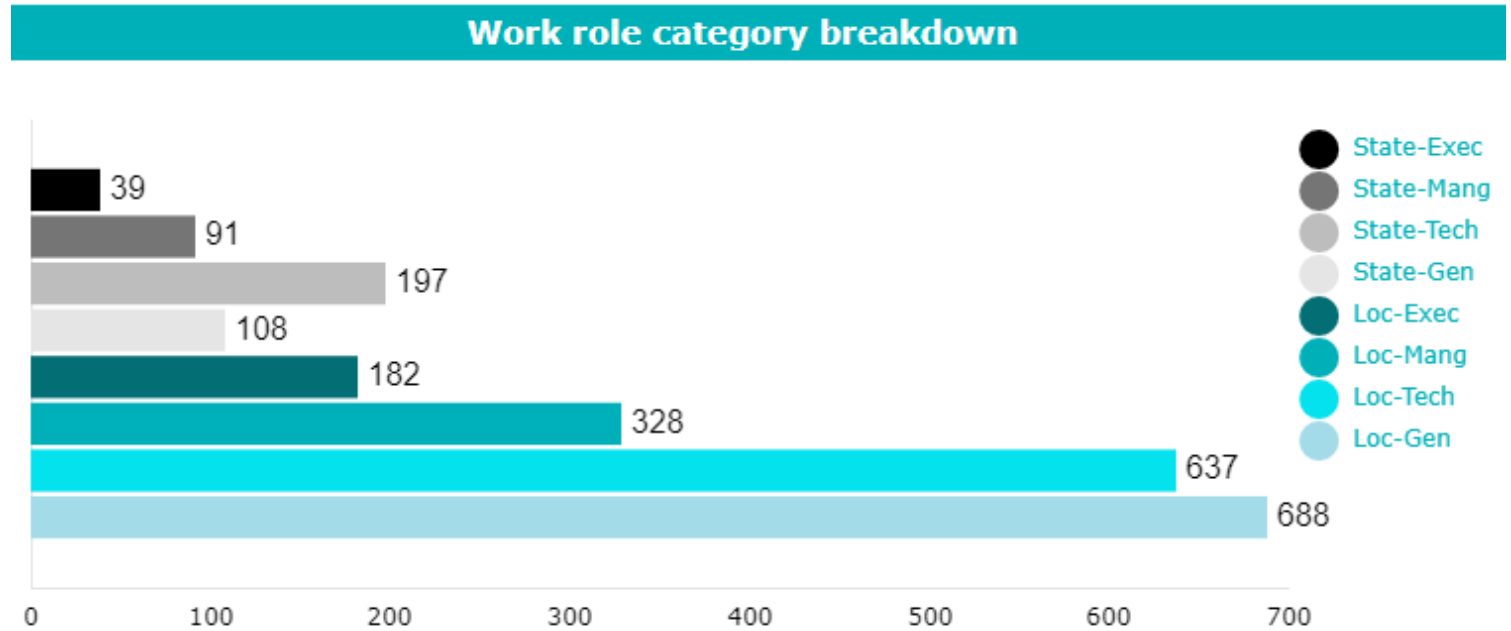
Metrics as of 12/31/2023:

Total Employees Trained

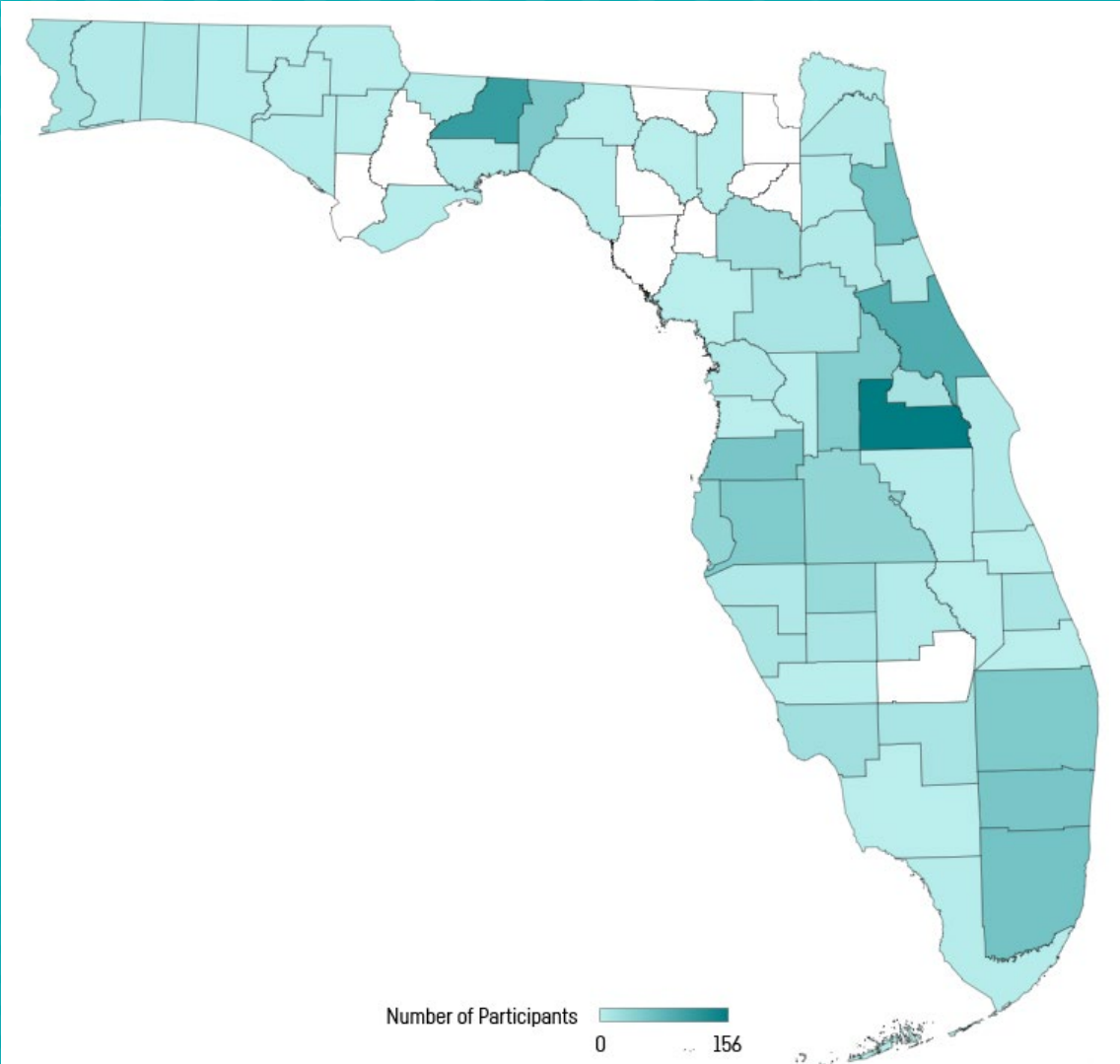
3028

Total Course Registrations

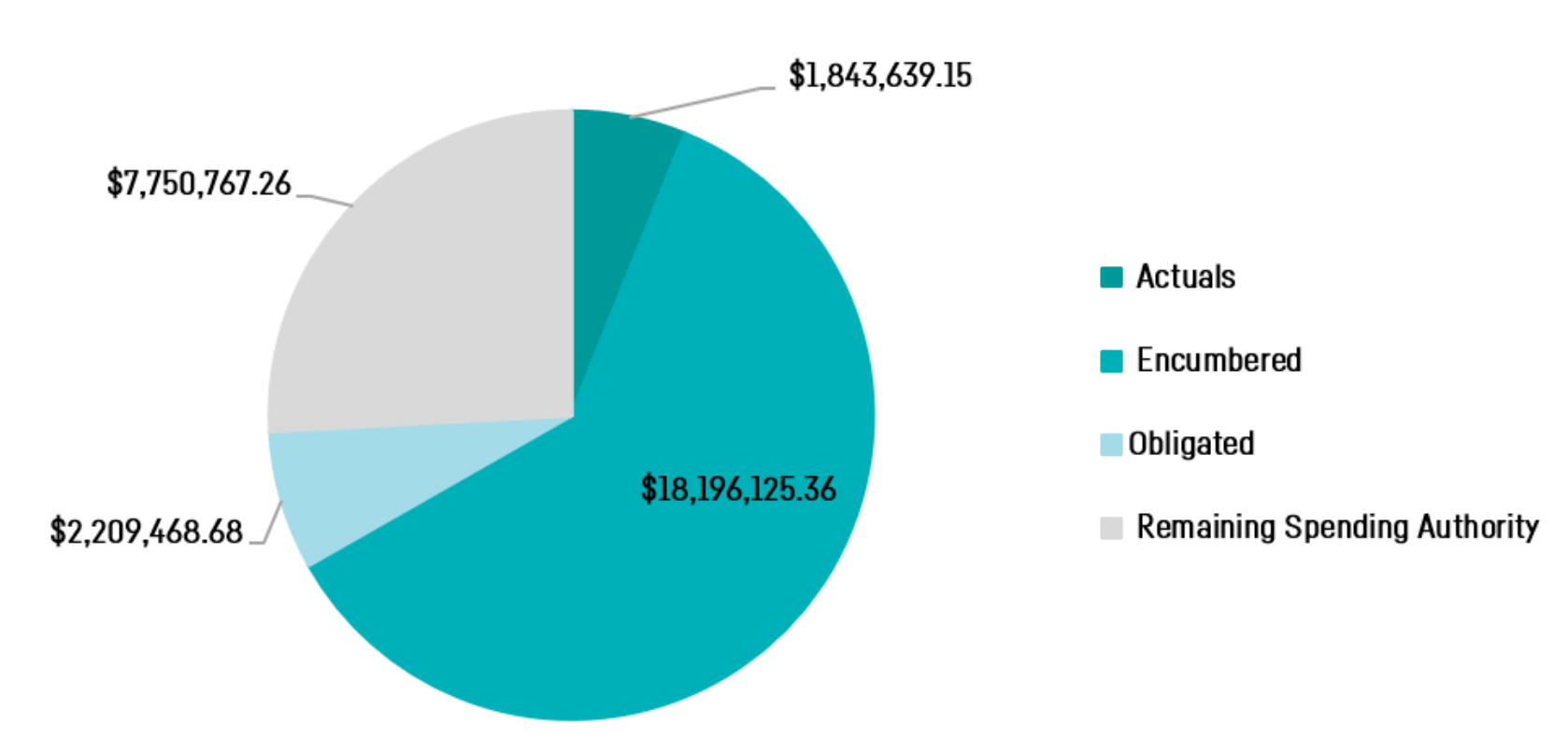
3796



CyberSecureFlorida
Training programs
now reach **87%** of
Florida's counties
(58 out of 67).



Distribution of Project Funds



Encumbered and obligated funds reflect the contracted services of partners and Cyber Florida for providing training through June 2024.


The approx. \$7.7 million remaining will be used to expand course offerings and address program needs as they are identified during that time.

This funding extends to include FY 2024-2025.

Next Steps




Increase Marketing Efforts




Continue ongoing program assessment to identify workforce needs



Seek Endorsement from State and Local Organizations



Engage Additional Partners to Expand Course Subject Matter Areas



Expand Course Offerings from Existing Partners

Critical Infrastructure Risk Assessment



Highlights of findings

- Meeting state and federal requirements and guidelines across all 16 sectors, to include government, county, and city to support their cybersecurity efforts and programs.
- Assessment show 7 out of 10 vulnerabilities were Risk Management which is an area in need of investment and support. (See chart below)
- 77% of participants meet the Basic Level for Ransomware Readiness.

Top 10 Weaknesses Observed Among Florida's CI Providers

Rank (weighted)	Category	Sub-Category	Question	% "Yes" (unweighted)
1	Identify	Risk Management	Response and recovery planning and testing are conducted with suppliers and third-party providers.	28%
2	Identify	Risk Management	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	35%
3	Identify	Risk Management	Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.	39%
4	Identify	Risk Management Strategy	Organizational risk tolerance is determined and clearly expressed.	46%
5	Identify	Risk Management	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.	43%
6	Protect	Information Protection Processes and Procedures	Response and recovery plans are tested.	53%
7	Protect	Information Protection Processes and Procedures	A System Development Life Cycle to manage systems is implemented.	53%
8	Protect	Data Security	Integrity checking mechanisms are used to verify hardware integrity.	56%
9	Protect	Information Protection Processes and Procedures	A vulnerability management plan is developed and implemented.	62%
10	Identify	Risk Management	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	50%

Recommendations

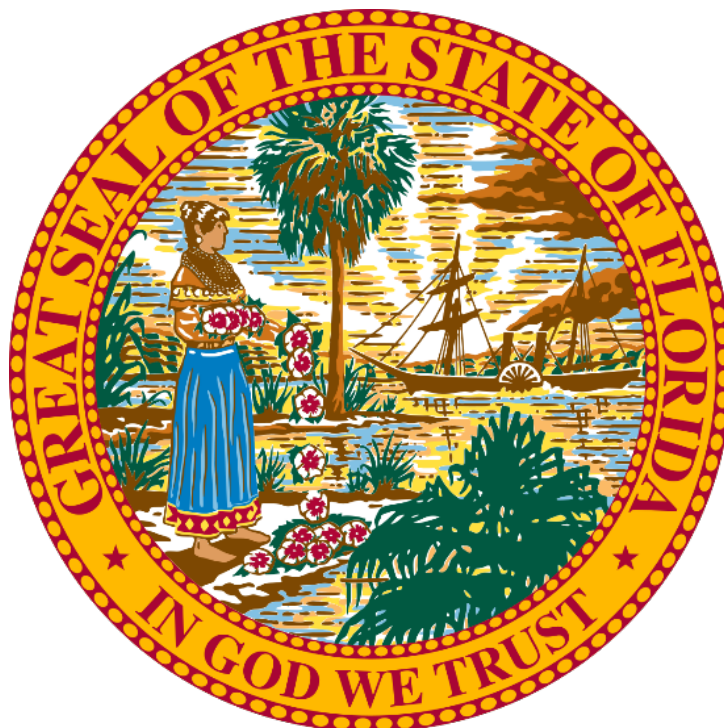
- Adopt and implement a Florida-Specific Cybersecurity Maturity Model for critical infrastructure providers by the end of 2024.
- Close the maturity gap for “basic” ransomware readiness by the end of 2025.
- Establish 2022 GAA Specific Appropriation 2944B as a recurring program informed by other legislatively mandated efforts.
- Formalize and increase investments in critical infrastructure cybersecurity workforce development across the public and private sectors.
- Continue to expand and mature existing critical infrastructure cybersecurity initiatives.
- Construct and maintain a comprehensive list of critical infrastructure entities operating in the state for sampling and communication purposes.
- Continue to provide cybersecurity risk assessments to Florida’s CI providers



Questions

**Cyber Pathways Program
Chief Inspector General**

EXECUTIVE OFFICE OF THE GOVERNOR OFFICE OF THE CHIEF INSPECTOR GENERAL



Update on Cyber Pathways Program and Enterprise Audit Activities

The Honorable Ron DeSantis
Governor of Florida

Melinda M. Miguel
Chief Inspector General



Agenda

- Discuss Cyber Pathways Program
 - Implementation of Specific Cyber Audits
 - Training and Micro-Learning (Just-In-Time Learning)
 - Enterprise Cybersecurity Audits



Created Cyber Pathways Program

Florida Inspectors General adopted a multi-featured cyber resilience pathways program supported by the Office of the Chief Inspector General. This program creates “**pathways**” to cyber competency and fulfills expectations associated with amendments to the Florida IG Act in 2021 (HB 1297) that requires **specific cyber audit plan (annually in each OIG)**.

The Cyber Pathways Program equips OIG staff with the fundamentals required to audit, investigate, inspect, and review cybersecurity risk management and cybersecurity operations, and assess agency compliance with government requirements such as NIST and following professional auditing standards.

The Cyber Pathways Program includes the following:

1. **Training** (Two-hour, one day, two days, one week, certification courses and other training courses) = Est. \$400,000.00
2. **Tools** (Audit Program with Bi-Weekly Support and other Technical Assistance) = Est. \$300,000.00
3. **Audit Enablement** (Subject Matter Expertise/Consulting Services) = Est. \$300,000.00



Training Investment

- Introduction to Cyber Fundamentals
- ISACA Certified Information Systems Auditor (CISA) certification training classes for senior internal audit staff.
- ISACA Certified Governance of Enterprise Technology (CGEIT) certification training for senior internal audit staff.
- FBI Cybersecurity Boot Camp Two-Day Training for auditors and investigators
- SkillSets Training Subscription
- Identity and Access Management Training
- IIA – CIA Exam Prep
- Anatomy of an Attack
- Introduction to Cloud Computing
- CompTIA Security+
- Introduction to Cybersecurity Investigations Training
- Incident Response and Recovery Training
- CSIRT Exercises – Observation activities across 34 agencies



Technology Related Certifications

Certification	Certification Holders (Actual #) FY 20-21	Certification Holders (Estimated #) FY 23-24
Certified Information Systems Auditor (CISA)	8	31
Certified in the Governance of Enterprise IT (CGEIT)	0	8
Certified Internal Auditor (CIA)	20	31

Source: Florida Inspectors General Expertise System as of November 30, 2023



Florida Cybersecurity Standards (FCS) – Rule 60GG-2

The Florida Cybersecurity Standards are based on the NIST Cybersecurity Framework (CSF) and is in sync with the CSF version 1.1

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications



FY 21-22 Enterprise Audit

1 - Identify

2 - Protect

3 - Detect

4 - Respond

5 - Recover

Detect

DE.AE - Anomalies and Events

DE.CM - Security Continuous Monitoring

DE.DP - Detection Processes

DE-CM

1 - Networking Monitoring

2 - Physical Monitoring

3 - Personal Activity

4 - Detect Malicious Code

5 - Detect Unauthorized Mobile Code

6 - Monitor External Service Providers

7 - Monitor for Unauthorized Personnel, Software, Connections & Devices

8 - Perform Vulnerability Scans as part of SDLC



FY 22-23 Enterprise Audit

1 - Identify

2 - Protect

3 - Detect

4 - Respond

5 - Recover

Protect

PR.AC - Identity Management and Access Control

PR.AT - Awareness and Training

PR.DS - Data Security

PR.IP - Information Protection Processes and Procedures

PR.MA - Maintenance

PR.PT - Protective Technology

PR-AC

1 - Identities and credentials are managed for authorized devices and users.

2 - Physical access to assets is managed and protected.

3 - Remote access is managed.

4 - Access permissions are managed, incorporating the principles of least privilege and separation of duties.

5 - Network integrity is protected, incorporating network segregation where appropriate.

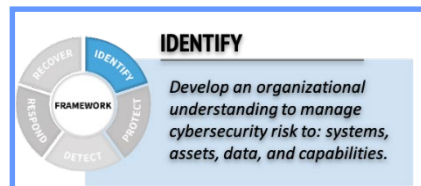
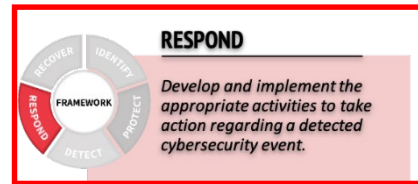
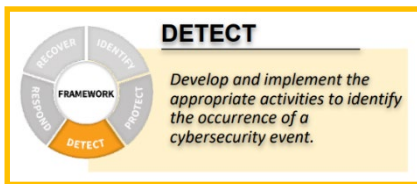
6 - Identities are proofed and bound to credentials and asserted in interactions.

7 - Users, devices, and other assets are authenticated.



FY 23-24 Enterprise Audit

Incident Response, Reporting, and Recovery



Phase 1: Preparation

Phase 2: Detection and Analysis

Phase 3: Containment, Eradication, & Recovery

Phase 4: Post-Incident Activity

Phase 5: Coordination



FY 24/25 Enterprise Audit

- Audit Topic Selected By January 2024
 - Based on Risk Assessment, Audit Coverage, Other Factors
- Create Audit Program with Testing
 - Distribute to CIO/ISM – June 2024
- Kick Off Audit for FY 24/25 in July 2024
 - Initiate and Conduct Fieldwork
 - Develop Findings and Recommendations
 - Prepare and Distribute Report
 - Conduct Follow-Up



THANK YOU



AI
Florida Technology Council



ARTIFICIAL INTELLIGENCE

**Florida House of Representatives
State Administration & Technology
Appropriations Subcommittee**

January 10, 2024

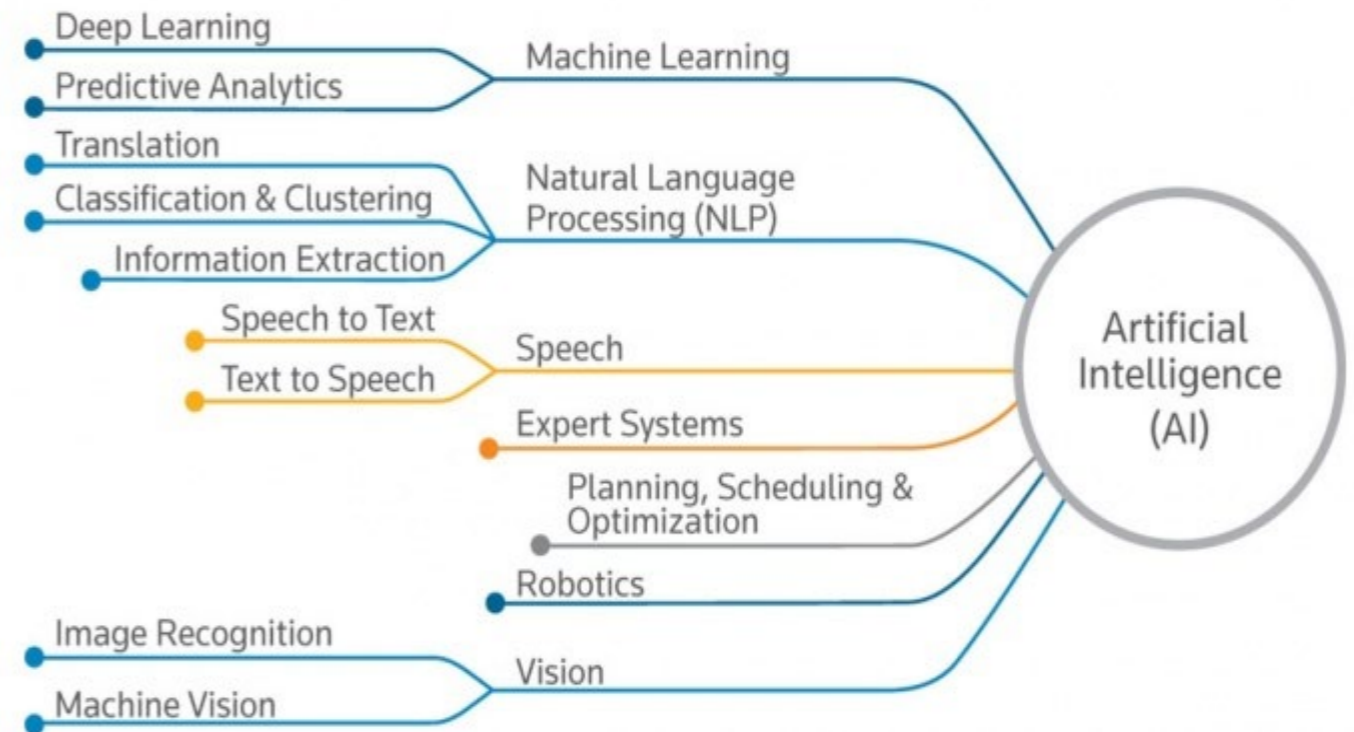
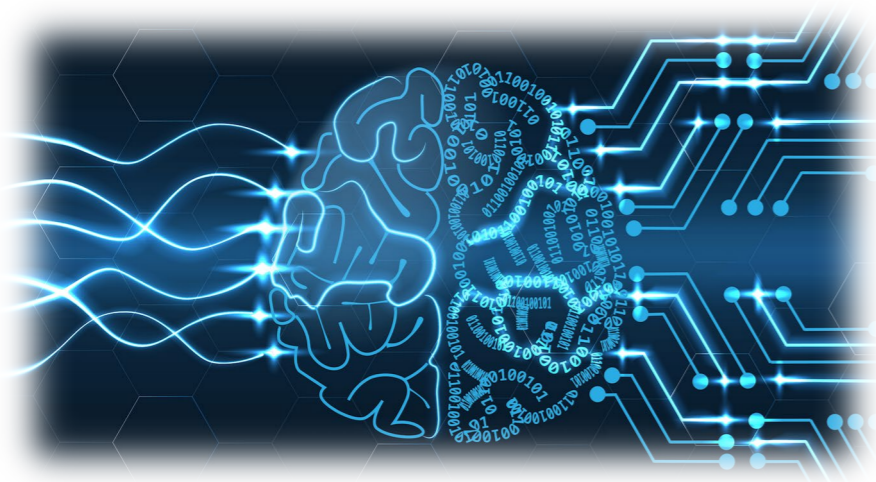


**Presented by David Clark
Chair, Florida Technology Foundation**

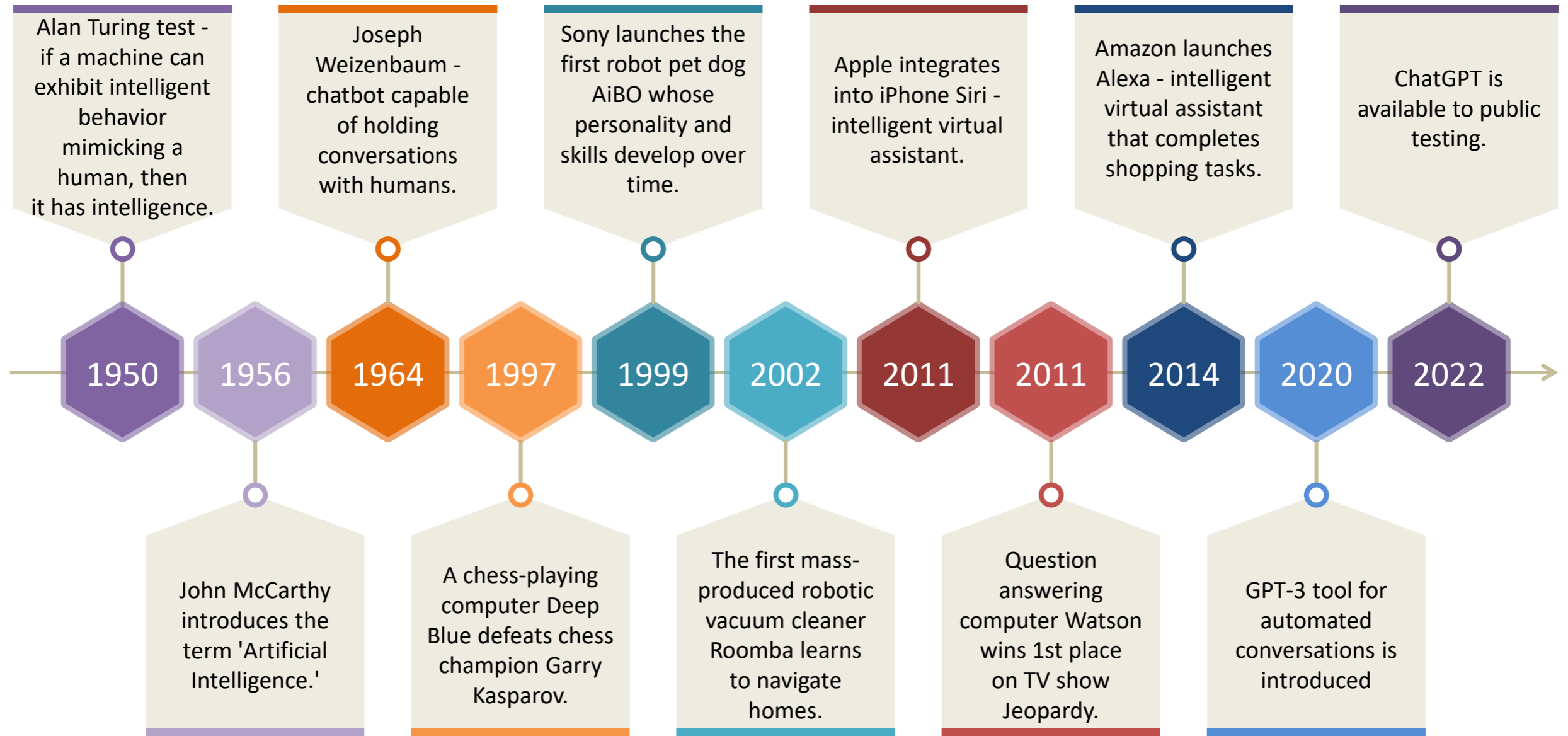
Artificial Intelligence - What is it?

Science and engineering of making intelligent machines, especially intelligent computer programs with the capability to imitate intelligent human behavior.

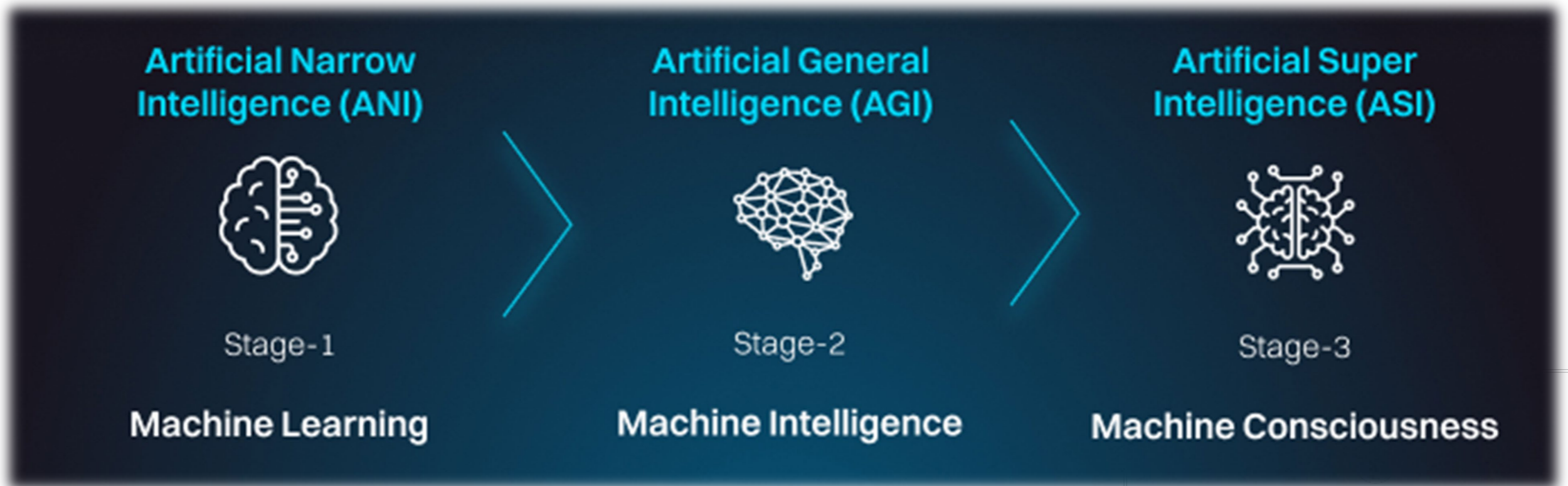
AI is a machine's ability to perform the cognitive functions we associate with human minds, such as perceiving, reasoning, learning, interacting with an environment, problem solving, and even exercising creativity.







Artificial Intelligence Development History



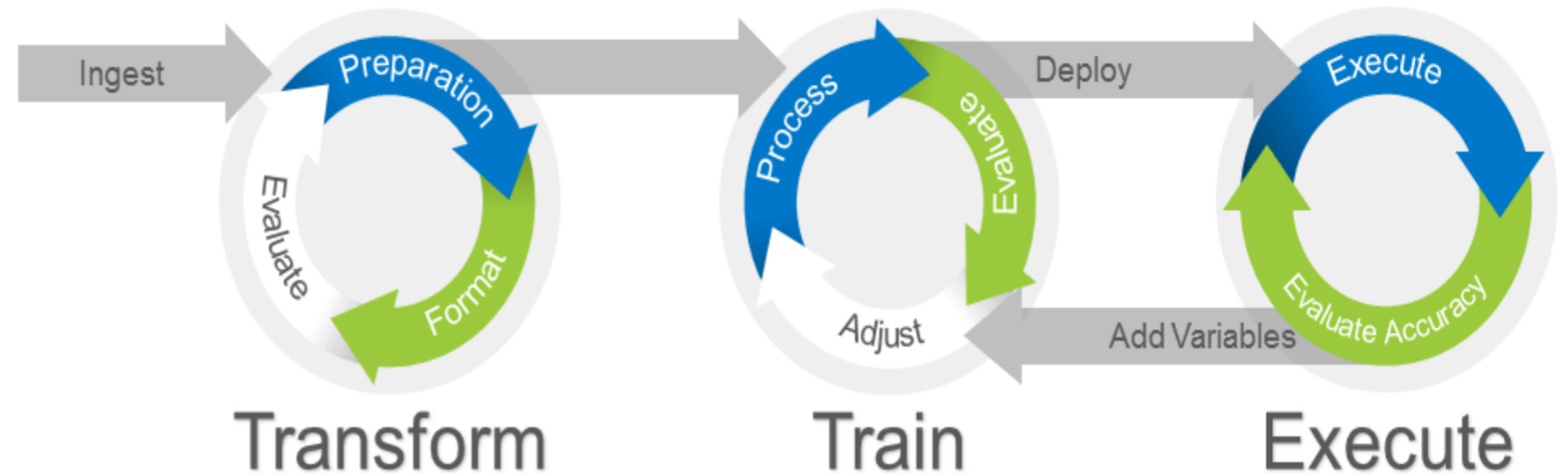
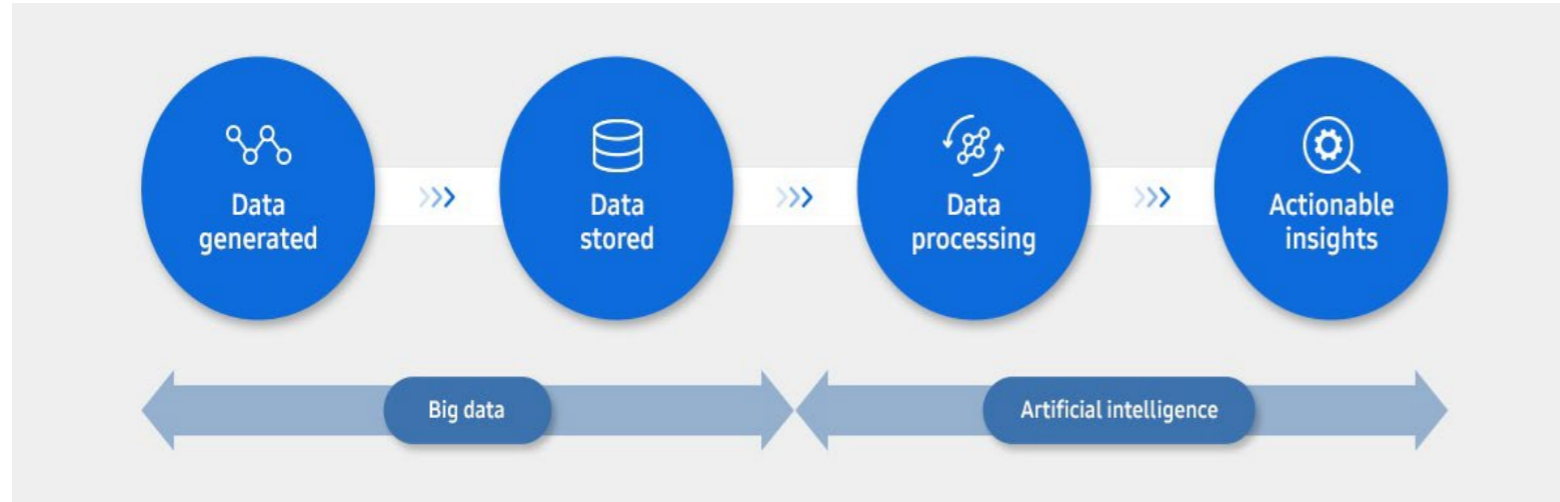
Stages of AI



Types of AI

Reactive AI	Limited memory	Theory of mind	Self-aware
<ul style="list-style-type: none">◦ Good for simple classification and pattern recognition tasks◦ Great for scenarios where all parameters are known; can beat humans because it can make calculations much faster◦ Incapable of dealing with scenarios including imperfect information or requiring historical understanding	<ul style="list-style-type: none">◦ Can handle complex classification tasks◦ Able to use historical data to make predictions◦ Capable of complex tasks such as self-driving cars, but still vulnerable to outliers or adversarial examples◦ This is the current state of AI, and some say we have hit a wall	<ul style="list-style-type: none">◦ Able to understand human motives and reasoning. Can deliver personal experience to everyone based on their motives and needs.◦ Able to learn with fewer examples because it understands motive and intent◦ Considered the next milestone for AI's evolution	<ul style="list-style-type: none">◦ Human-level intelligence that can bypass our intelligence, too
			

How AI Works



Examples of AI

As it stands, 90% of well-known companies invest in AI, and 83% of them think AI will help them maintain or gain a competitive edge.

Manufacturing Robots

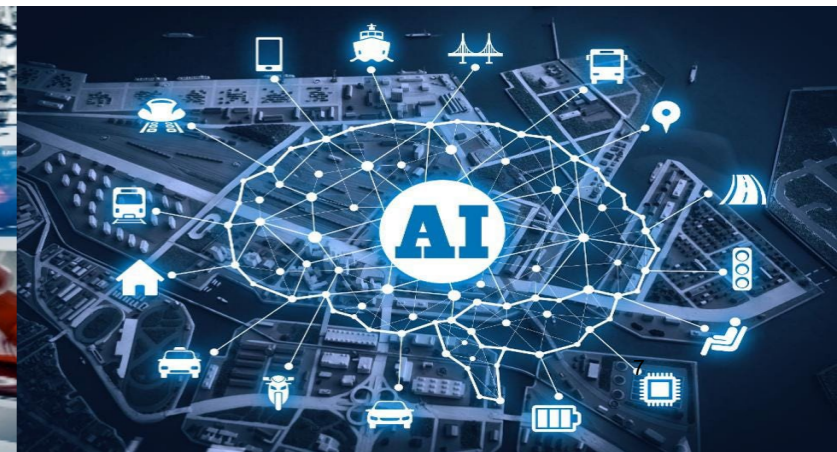
Disease Mapping

Conversation Bots

Smart Assistants

Self-Driving Cars

Social Media Monitor



AI in Our Daily Lives



AI Powered Smart Devices



Smartphones



Drones



Media Streaming



Smart Home
& Security



AI Business



Targeted
Marketing



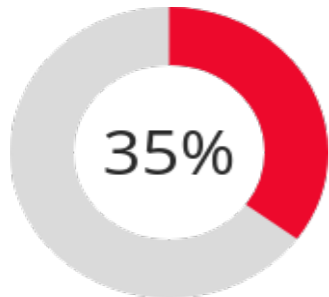
Customer Service
and Support



Smart Supply
Management



Quality Control
and Assurance



Of businesses have already
implemented some form of AI in
their workplace.

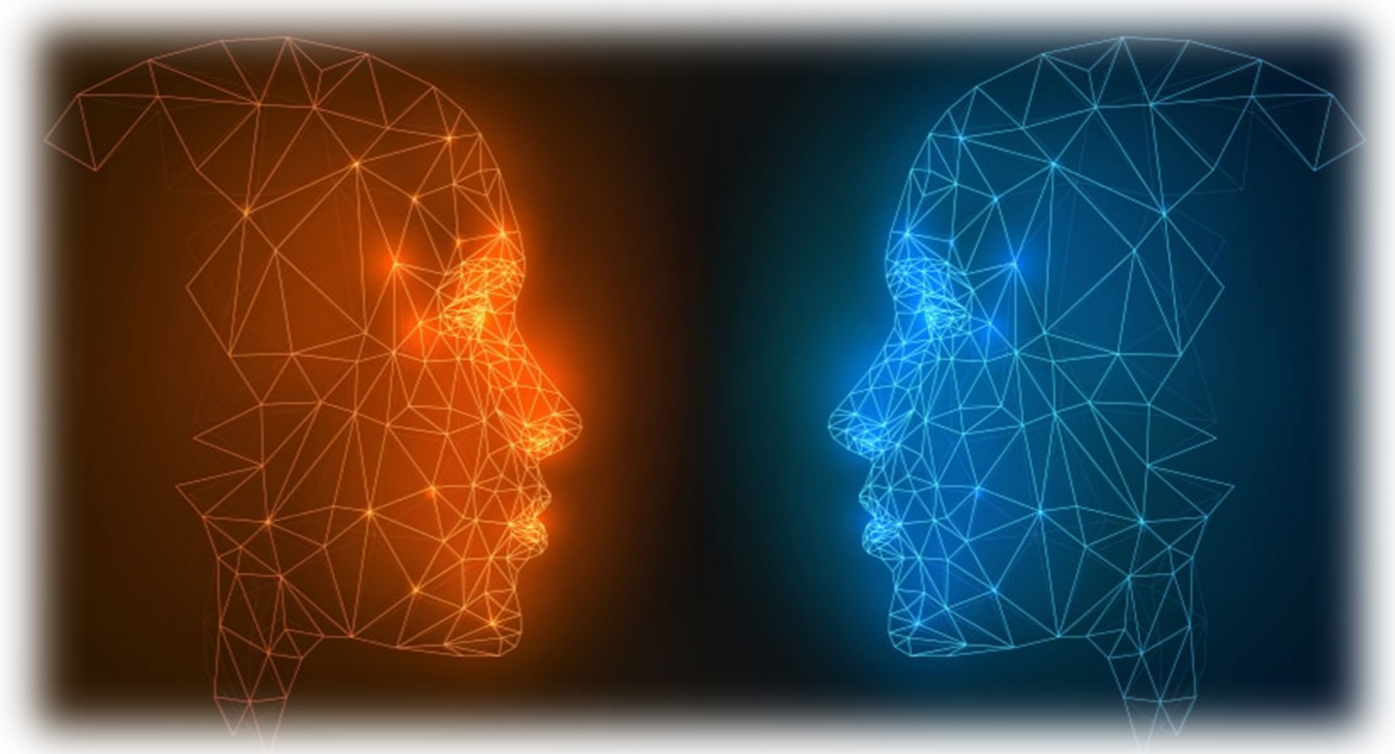
McKinsey predicts AI will ADD \$13
Trillion to the global economy by
2030



Good or Something Else Choose Wisely

As you can see in many ways AI is being used behind the scenes to impact our daily lives and it will continue to benefit our modern society.

However, along with good, negative consequences will arrive. The sooner governance is address regarding the opportunities and challenges involved in AI, the better equipped society will be to appropriately leverage the many lifechanging positives and mitigate and manage the negative outcomes.



Now What?

We have a choice to be engaged and involved. It is here and cannot be ignored.

Smart governance of the entities and people who develop and control the AI systems.

The future we create is ours and how we develop and govern the technologies around us, especially AI, will determine the future we and our children live in.



Thank you



David Clark
Chair, Florida Technology
Foundation



Brian Fonseca
Director, Jack D. Gordon Institute for Public Policy
Executive Director, Cybersecurity@FIU

January 10, 2024

Public Sector Adoption

Policymakers should consider legislation that guides how to best implement AI technologies that enhance public services, improve efficiencies, and reduce costs.

- Discussions on funding
- Partnerships with technology companies
- Ensuring equitable access to improved services

Economic Impact and Workforce Transformation

Policymakers should consider legislation that inform strategies to manage the economic shifts caused by AI.

- Workforce retraining
- Boost education and research
- Support sectors most at-risk

Ethical Use and Regulation of AI

Policymakers should consider legislation that establishes ethical guidelines and regulatory guardrails to ensure responsible use.

- Combat misinformation
- Purge algorithmic and computational biases
- Protect privacy and civil rights

Florida **AI** Policy Summit

JANUARY **19**, 2024

FIU

Jack D. Gordon Institute for Public Policy
Steven J. Green School of International & Public Affairs



**CYBER
FLORIDA**
at the UNIVERSITY OF SOUTH FLORIDA



**Miami Dade
College**

AI
Department of Revenue

Department of Revenue Technology Automation Projects

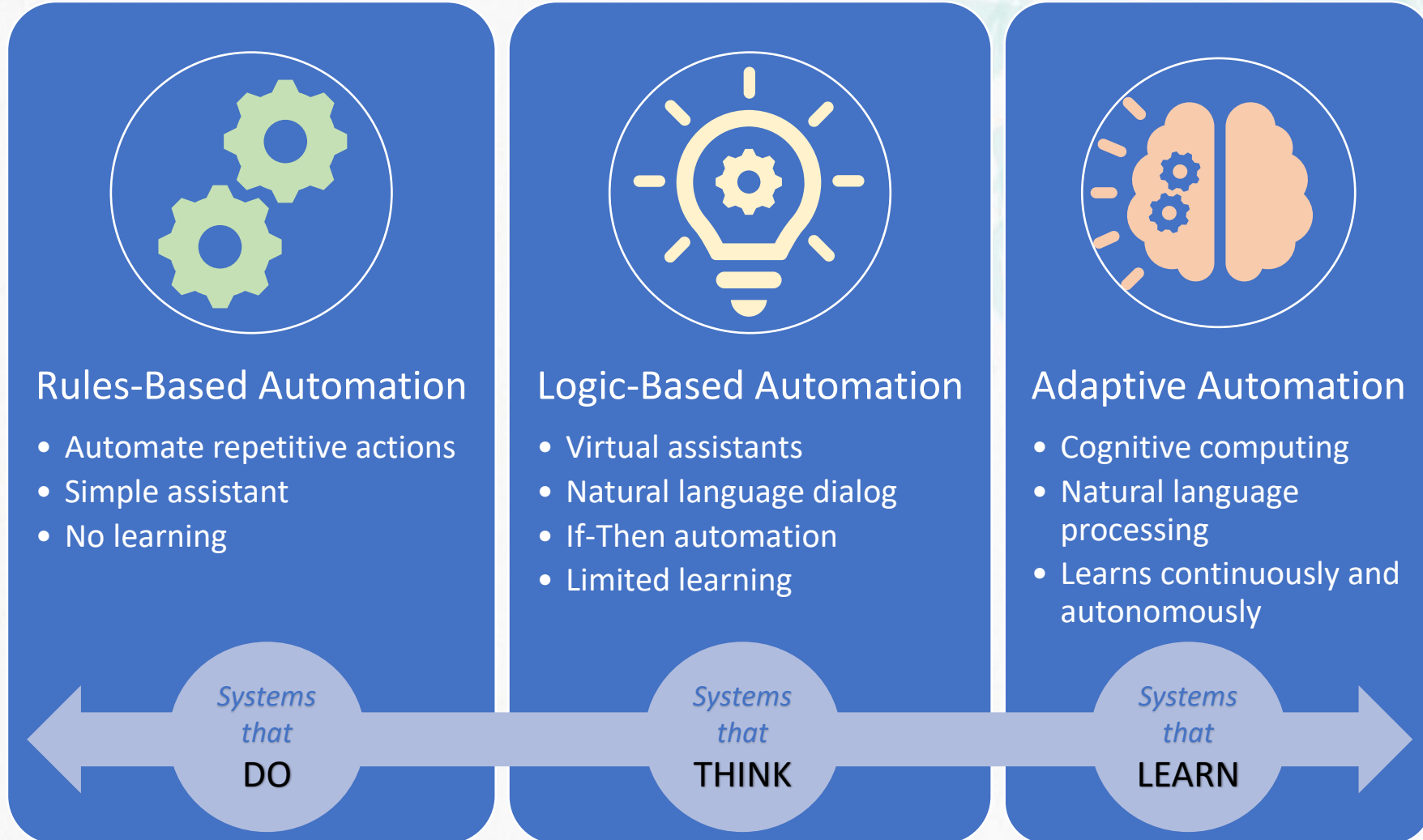
January 10, 2024



Objectives

- Describe virtual assistant use and proposed expansion
- Highlight current and possible future automation and artificial intelligence projects

Artificial Intelligence Spectrum of Ability



Child Support Virtual Assistant

- **DORA** – Department of Revenue Answers
- Conversational Artificial Intelligence Platform
- Answers over 200 non-case specific questions on a variety of topics
- Available on 19 public webpages



When you establish paternity, you identify the legal father of the child. Other, the father and the child.

Child are:

by
or her father
to identify
parent, if available
support and medical

fits, military allowances

What to:

In the child

related to each other has a legal father. Married parents and their



What is
Genetic Testing?

Genetic testing identifies a
child's biological father.

[LEARN MORE >](#)

Have a question
about genetic
testing?

 Click on me!

Child Support Virtual Assistant

The image displays two screenshots of the Child Support Virtual Assistant chat interface. The left screenshot shows a user asking "How do I get my license reinstated?" and receiving a detailed response with options to pay online, at court, or by mail, and a "View More" button. The right screenshot shows a user asking "How do I make a payment?" and receiving a response with options to pay online, with cash, or by mail, and a "Did this answer your question?" prompt.

- Revenue staff create the content, not the platform
- Revenue staff monitor conversations to
 - Identify searched topics to create and improve content
 - Teach the platform when there is a better response available
- The platform uses both staff monitoring and customer feedback to improve responses to similar questions in the future
- DORA offers three possible responses if no assigned response is available
- 50 interactions daily, with average of 2.5 questions with each interaction

Virtual Assistant Expansion

- Legislative Budget Request
 - \$125,127 recurring (and \$215,978 nonrecurring)
- General Tax public webpages
- Financial Management employee-facing virtual assistant to assist with payroll, vendor payments, purchasing, and similar topics
- Revenue's internal information technology Service Desk to assist with common technology questions
- Revenue will have one solution used by all programs and will be scalable with different knowledge bases/libraries

Current and Future Automation and AI Projects

Current

- Rules-based case processing
- Batch program scheduling, initiation, and monitoring
- Code migration
- Automation of data entry
- Document scanning and processing
- Vulnerability management
- IT system monitoring
- AI utilization policy

Future

- Expansion of DORA
- Automated application testing
- Automate access management to SAP systems
- Automate external communication with Department customers

Questions?

