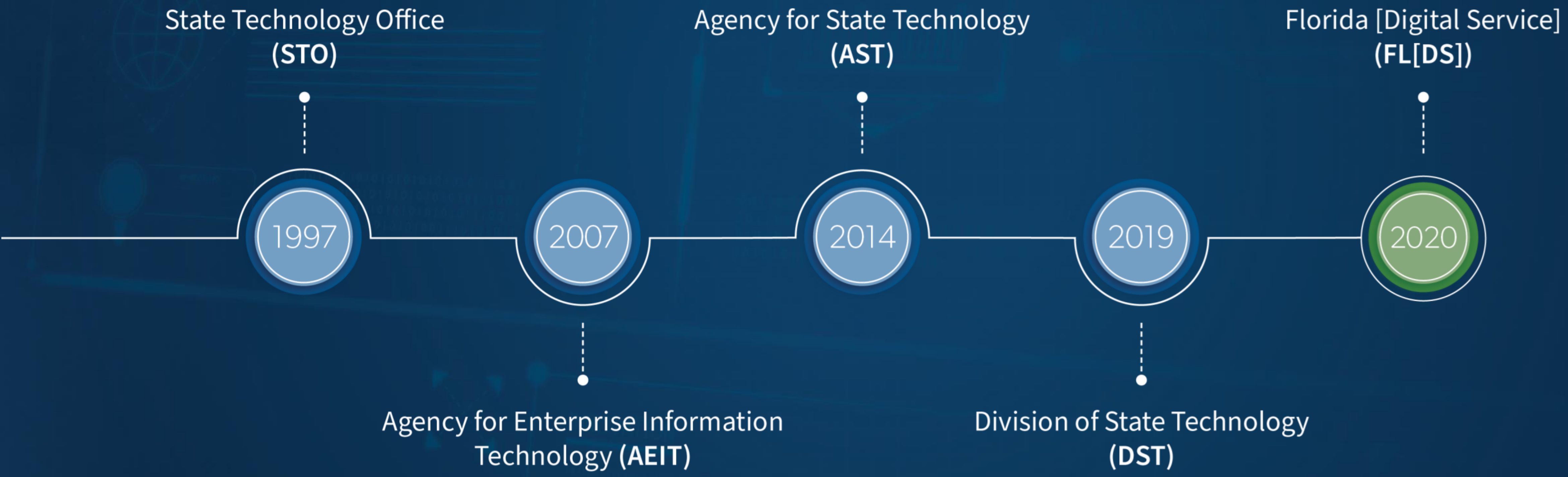
Florida [Digital Service]

CYBERSECURITY IN STATE GOVERNMENT

The Lead Entity for Cybersecurity in Florida

The History of Florida's State Technology Office

So Different it has Defied the Law of Bureaucracy



1997 — State Technology Office **(STO)**

2007 — Agency for Enterprise Information Technology **(AEIT)**

2014 — Agency for State Technology **(AST)**

2019 — Division of State Technology **(DST)**

2020 — Florida [Digital Service] **(FL[DS])**

FLORIDA [DIGITAL SERVICE]

- Established in 2020.
- Charged with creating innovative solutions that securely modernize state government.
- Partners with all state agencies to lead state technology into the future.
- Transforming government technology to better serve Floridians.
- Leveraging partnerships with other government entities to serve Florida.

OUR MISSION

To deliver better government services and transparency to Floridians through design and technology.

Cybersecurity in the 2022 Legislative Session

Legislation: HB 1297 (2021)

- Serving as the Lead Entity for Enterprise Cybersecurity.
- Designating Additional State Chief Information Security Officer Responsibilities.
- Creating the Florida Cybersecurity Advisory Council.
- Cybersecurity Operations Center ("CSOC").
  - Threat clearinghouse and response coordination.
  - Standardizing reporting policies and procedures.
  - ESF-20.
- Cybersecurity Training.
  - Providing training to all state agencies to develop, assess, and document skill level.

Enterprise Cybersecurity Resiliency

- $30 million provided to implement the recommendations of the Florida Cybersecurity Task Force Final Report.
- FL[DS], as the lead entity on cybersecurity, is spearheading projects to strengthen cybersecurity across the enterprise.
- Solutions and services are offered to all enterprise agencies .

Enterprise Cybersecurity: Launch Initiatives

Initiative one: Enterprise Threat Protection and End User Defense

- $15.9 million invested on 20+ agencies.
- Telemetry data being shared across participating agencies.
- Leverages buying power to create 25% savings for the state.

Initiative two: State of Florida’s Cybersecurity Operations Center (CSOC)

- Centralized monitoring and response, asset discovery, endpoint protection, content delivery network, managed security services, risk assessments, license access controls, workforce training, and incident response.

Cybersecurity in the 2022 Legislative Session

Cybersecurity Policy

- HB 7055
  - Ransomware Incident reporting and prohibition against payment.
  - Requiring local governments to adopt security standards.
  - Reporting and training enhancements.
- HB 7057: Exempting Public Records for all Agencies (state and local)
  - Coverage limits and deductibles.
  - Information relating to critical infrastructure.
  - Network schematics, hardware and software configurations, and response practices.

Cybersecurity Funding

- Funding to the Florida [Digital Service] ($85.4 million)
  - $50 million to continue and scale Enterprise Cybersecurity Program.
  - $30 million to launch a competitive grant program to fund cybersecurity initiatives in cities and counties.
  - $5.4 million to administer federal grant funds.
- Funding to Florida Center for Cybersecurity at USF ($37 million)
  - $7 million to perform a comprehensive risk assessment of critical infrastructure.
  - $30 million to provide statewide training opportunities.

Training Grants: $37 million to Cyber Florida at USF

$30 million to conduct cybersecurity training for state and local government executive, managerial, technical, and general staff.

- Training will be done in consultation with the Cybersecurity Advisory Council.
- Baseline training for enterprise security personnel requires a cyber range that facilitates structured and free-range training opportunities.
- Criteria for the cyber ranges is as follows:
  - The ability to provide the physical infrastructure necessary to meet enterprise needs.
  - The ability to replicate the design of the CSOC to make training as pragmatic as possible.
  - Curriculum and training content to facilitate additional training and skills development.
  - The ability to support additional educational opportunities in the higher education and K-12 environments.

$7 million to perform a comprehensive risk assessment of critical infrastructure and provide recommendations to support actionable improvements of the state's preparedness and resilience to significant cybersecurity incidents.

Technical Grants: $30 million to FL[DS]

A competitive grant fund to be designed by the State Chief Information Security Officer.

- The criteria and process are currently being developed.
  - Intention to align to the strategic design of the State CSOC.
  - Recognition that threat actors and nation states don't recognize geographical boundaries, separations of power, or levels of government.
  - Understanding that $30 million won't meet all the needs.
  - Aligned to training funding.
- Areas of Emphasis:
  - Centralized monitoring and response.
  - Asset discovery.
  - Endpoint protection.
  - Content Delivery Network.
  - Managed Security Services.
  - Incident response.

QUESTIONS?