TABLE OF CONTENTS

From the Desk of the State Chief Information Officer (CIO) ................................................................. 3

AST Guiding Principles ................................................................................................................................. 3

Executive Summary ..................................................................................................................................... 4

Strategy 1: Enhance security and privacy capabilities .................................................................................. 5
  Objective 1: Implement a cybersecurity framework policy ................................................................. 6
  Objective 2: Improve situational awareness ......................................................................................... 7
  Objective 3: Develop a robust enterprise security incident response program ............................... 8

Strategy 2: Enhance the Enterprise IT environment ....................................................................................... 9
  Objective 1: Invest in core enterprise enhancement ........................................................................ 10
  Objective 2: Develop and implement application rationalization process ..................................... 11

Strategy 3: Define the roadmap for maturing IT Processes and Strategic Business Alignment ... 12
  Objective 1: Strengthen project assurance and ensure project oversight ...................................... 13
  Objective 2: Coordinate multi-agency enterprise initiatives ............................................................ 14

For More Information .................................................................................................................................. 15

Close ............................................................................................................................................................ 16
From the Desk of the State CIO, Jason M. Allison

As the Agency for State Technology (AST) enters the second year of its three-year Strategic Security Plan, the focus remains on building enterprise security into the core composition of every information technology (IT) initiative. Florida has proven attractive to businesses and citizens, resulting in rapid growth. This growth goes hand-in-hand with state agencies offering more online services and generating more data which has become more appealing to hackers. Cybersecurity is at the forefront of AST’s efforts to build more efficient and effective systems and processes.

This plan will show the progress AST has made in the past year and outline the next steps that will enable AST to continue on the path to enhanced cybersecurity. AST’s focus remains on establishing new capabilities, supporting hardened infrastructure, and better aligning Florida's strategic initiatives for all state agencies. As is necessary for all strategic planning activities, AST has flexibility and expertise to accommodate for needs that exist within each of the state’s major program areas. As the plan evolves, new goals will be added and forward-looking strategies formulated. AST’s Strategic Security Plan positions Florida to undertake more aggressive, innovative solutions. In order to meet Florida’s ever-changing needs, AST’s strategies must be flexible and adaptive. AST will continue to help position Florida as a hub for innovation in order to drive economic success for the state, its citizens, and businesses.

AST Guiding Principles

AST is constantly raising the bar and promoting initiatives that are:

- Strategic
- Enterprise-focused
- Reliable
- Value-adding
- Innovative
- Collaborative
- Efficient
Executive Summary

Protecting information technology is vital to delivering effective government services. Enhancing security and infrastructure capabilities as well as establishing a roadmap for strategic alignment are at the core of AST efforts. AST has the ability to influence, for the good of the citizens of Florida, the security, efficiency, and direction of IT strategy. Now, more than ever before, there is an understanding that symbiotic relationships, based on shared goals, benefit all involved. Lessons learned over the years prove that IT enables efficiencies and innovation alike.

AST created a three-year Strategic Security Plan that evolves year-over-year to establish an innovative, yet flexible, platform to build a solid foundation for future state initiatives. Key to a rigorous information security plan is the protection of the confidentiality, integrity, and availability of the state's IT resources. All AST strategies and objectives address at least one of these tenants.

Strategy One

Establish a strong cybersecurity framework, cultivating partnerships for response efforts, and improve situational awareness to empower information security personnel.

Strategy Two

Establish objectives for assessing and enhancing the state's data center infrastructure.

Strategy Three

Establish objectives for project assurance and oversight and promote strategic business alignment by collaborating with state agencies to understand and support their mission-specific strategies.
Strategy 1: Enhance Security and Privacy Capabilities

Objective 1: Implement Cybersecurity Framework Policy

Objective 2: Improve Situational Awareness

Objective 3: Develop a Robust Enterprise Security Incident Response Program

Visitors to Florida in 2014 – 83.2 million (domestic)/11.3 million overseas
Objective 1: Implement a Cybersecurity Framework Policy

Protecting Florida’s information systems is a critical element in providing efficient government and cost effective delivery of services to the state’s citizens. Securing these vital systems requires a sound framework to guide the state’s workforce and promote efficiency.

Accomplishments:

- Filed new Florida Cybersecurity Standards (FCS)
- Led a multi-agency IT risk assessment
- Developed FCS guidance to help agencies address risk assessment recommendations
- Hosted risk assessment training for agency security professionals

Next Steps:

- Develop artifacts for compliance with the new FCS
- Prepare a Schedule IV-B for risk assessment remediation
- Establish an enterprise cybersecurity governance structure

The National Institute of Standards and Technology (NIST) Cybersecurity framework provides 356 informative references to help government organizations tackle cybersecurity.
Objective 2: Improve situational awareness

Florida's state agencies serve more than 20 million citizens. Every day Florida's information systems face threats on a global scale. To protect Florida's technology, state IT professionals must receive and share the most up-to-date threat information available. AST will pursue information sharing relationships that improve awareness of the cyber threat landscape.

Accomplishments:

- Held routine information sharing meetings with Agency IT Security Managers and Inspectors General
- Submitted LBR for information security training
- Maintained inventories of free information security resources
- Hosted the first AST and National Guard Cyber Range Exercise

Next Steps:

- Enhance community interactions through outreach
- Develop a partnership with the Florida Center for Cybersecurity (FC2)
- Pursue training opportunities that promote situational awareness
- Continue to develop high quality information security resources

In 2015, after manufacturing, government was the second most targeted industry of cyber-espionage campaigns.¹
Objective 3: Develop a Robust Enterprise Security Incident Response Program

The evolution of cyber threats creates challenges for how state agencies respond to incidents. AST will build partnerships that help predict and prevent compromise. While AST promotes initiatives to establish and maintain robust and in-depth defenses, it will also pursue an effective incident response program.

Accomplishments:

- Submitted a LBR and supported agency requests for managed security services
- Hosted an overview of emerging identity and access management technology
- Established working relationships with incident response partners
- Posted incident response guidelines in information security manager portal

Next Steps:

- Enhance enterprise visibility into state infrastructure and network traffic
- Create and launch an enterprise incident reporting portal
- Establish working groups to populate the state cybersecurity framework
- Develop the Florida Cyber Disruption Strategy

70% of organizations report having been compromised by a successful cyberattack in the past 12 months.²
Strategy 2: Enhance the Enterprise IT Environment

Objective 1: Invest in Core Enterprise Enhancement

Objective 2: Develop and Implement Application Rationalization Process

Economic Impact of Florida’s Tourism Industry in 2014:
- Tourism Spending - $82 billion
- Tax Revenue Generated by Tourism - $4.9 billion

Florida is 5th in high-tech employment and ranks at the top for employment in communications equipment manufacturing, internet and telecommunications, engineering services, computer systems design.
More than a means of automation, IT promotes innovation, supports trade, and encourages investment in Florida. However, aging information systems create risk and increased expense as they become difficult to secure. AST will pursue modern, consistent, and standardized service offerings. System upgrades and consolidation will improve security, lower costs, and enhance disaster recovery capabilities for state agencies.

Accomplishments:
- Completed a Data Center Operational Assessment
- Established a consistent disaster recovery (DR) platform strategy and completed infrastructure readiness testing of DR site
- Replaced end-of-life equipment and updated network security equipment
- Consolidated AST-North and AST-South service catalogs

Next Steps:
- Continue the physical consolidation of the AST-North and AST-South data centers
- Enhance activity auditing, logging framework and authentication capabilities
- Improve mitigation strategies for Distributed Denial of Service (DDoS) attacks
- Establish Managed Security Service in the Data Center

The third quarter of 2015 saw a 180% more DDoS attacks over the same period in 2014 with one record setting attack of 222 Mpps (million packets per second.) ³
Securing an enterprise environment requires knowing which applications are used and how they interact. AST will develop an application rationalization process to identify the state application portfolio and its associated security risks. AST and state agencies can then prioritize initiatives to increase security, reduce complexities, and lower the cost of new applications.

**Accomplishments:**
- Completed the Cloud Readiness Study
- Adopted the application rationalization technique and methodology established through the course of the Cloud Readiness Study

**Next Steps:**
- Begin application dependency mapping
- Implement application performance monitoring toolset
- Begin software asset inventory to support license and version control

173 days: The average investigation time from infiltration to discovery.
Strategy 3: Define the Roadmap for Maturing IT Processes and Strategic Business Alignment

Objective 1: Strengthen Project Assurance and Ensure Project Oversight

Objective 2: Coordinate Multi-agency Enterprise Initiatives

Top Reasons why your company should be in Florida, too:
- Over 26,000 IT companies have significant operations in Florida

The forecast average loss for a breach of 1,000 records is between $52,000 and $87,000.¹
Considering security early in the project management lifecycle helps identify security services and tools that agencies can share. Not only does this offer cost savings, it also promotes security at all stages of a project. Working with state agencies, AST will help develop consistent project management standards to improve efficiencies, minimize project risks, and facilitate successful projects across the state.

**Accomplishments:**

- Performed oversight of 11 projects
- Promulgated the Florida IT Project Management and Oversight Standards (FITPMOS)
- Provided training, templates, and guidance on FITPMOS
- Promoted collaboration and knowledge-sharing through bi-monthly Chief Planning Officer (CPO) meetings

**Next Steps:**

- Align FITPMOS to the FCS, and make other improvements to the FITPMOS
- If funded in the budget, implement a project monitoring tool
- Continue to advance the state’s project management maturity
- Offer training to project management professionals and the vendor community

Research & development activities worth nearly $8 billion annually happen in Florida. Innovation & research excellence in IT fields ranging from photonics/optics and modeling, simulation & training, to nanotechnology and material science.¹
Objective 2: Coordinate multi-agency enterprise initiatives

Collaboration between agencies promotes business alignment. AST will work with agencies to find ways to lower costs, use existing information in innovative ways, and develop ways to share business processes. AST will continue to host workshops that promote conversations between agencies to identify technology that agencies can share.

Accomplishments:
- Promoted an enterprise approach to IT
- Assisted agencies with Legislative Budget Request reviews to promote alignment
- Identified, with agency input, data sharing opportunities between agencies

Next Steps:
- Deliver IT service standardization and consolidation recommendations
- Inventory current enterprise architecture and develop a road map for improvement

Verizon experts predict that there will be over five BILLION IoT (Internet of things) devices by the end of this decade.¹
For More Information

1 2015 Verizon Data Breach Report

2 2015 NetIQ Cyberthreat Defense Report North America & Europe
(Requires Registration)

3 Akamai Q3 2015 State of the Internet Report


2015-2018
Statewide Strategic IT Security Plan
Agency for state Technology

Updated February 1, 2016

For more information visit ast.myflorida.com