Florida's Information Technology Security Plan

State of Florida

Agency for State Technology

Category: Cybersecurity

Project Initiation Date: November 2014

Project Completion Date: December 2015

Contact:

Jason M. Allison, Executive Director/State CIO
Jason.allison@ast.myflorida.com
850.412.6050

Executive Summary

Pursuant to section 282.318(3)(a), Florida Statutes, the Florida Agency for State Technology (AST) published a comprehensive information technology (IT) security plan in February 2015. The *Statewide Information Technology Security Plan* is a result of Florida's commitment to establishing standards and processes consistent with cybersecurity best practices and adopting rules to safeguard agencies' data and IT resources to ensure the availability, confidentiality, and integrity of these assets.

The plan offers technology guidance for 32 executive branch agencies and includes three aggressive strategies to enhance visibility into agencies' security accomplishments, align agencies' efforts to achieve greater economies of scale, and establish a roadmap for future information security development. In March 2015, AST leveraged the plan's roadmap by beginning the development of the Florida Cybersecurity Standards (FCS), subsequently incorporated and promulgated into Chapter 74-2, Florida Administrative Code, in March 2016.

These hallmark cybersecurity standards align with the National Institute of Standards and Technology's (NIST) Framework and are based on industry standards, guidelines, and practices that promote the protection of critical infrastructure.

In June 2015, AST further leveraged the plan's roadmap by completing a statewide risk assessment designed to assess the maturity of the state's data centers and its customer agencies' security practices. Through collaborative planning and purposeful action, Florida has the recipe to become the nation's leader in state government cybersecurity.

Concept

The Florida State Legislature established the Agency for State Technology (AST) in July 2014. Included in the legislation was the requirement for AST to submit an initial statewide IT security strategic plan by February 1, 2015, and annually thereafter.

Developing and socializing this security plan was a top priority for AST and its newly hired Chief Information Security Officer (CISO). With less than three months from the CISO's hiring date to the security plan's required due date, AST was able to successfully meet this aggressive submission schedule through effective collaboration and active communication with key stakeholders.

AST's plan focuses on three long-term strategies spanning 2015 through 2018 and emphasizes year one objectives designed to build security into the very fabric of state IT operations and processes (Figure 1). These foundational strategies will position AST to pursue initiatives in a collaborative, organized and secure manner.

Strategy One enhances security and privacy capabilities by establishing objectives for adopting a strong cybersecurity framework, cultivating collaborative partnerships for critical response efforts, and focusing on situational awareness to empower the state workforce.

Strategy Two enhances the enterprise IT environment by establishing objectives for assessing and enhancing the state's data center infrastructure, which includes application rationalization.

Strategy Three defines the roadmap for maturing IT processes and strategic business alignment through IT project assurance and oversight, and promotes strategic business alignment by partnering with state agencies to understand and support their mission-specific strategies.

Figure 1 – AST Statewide Information Technology Security Plan Roadmap

Significance

With the abolishment of the former Agency for Enterprise Information Technology (AEIT) in July 2012, and prior to the creation of AST in July 2014, Florida experienced a two year void in centralized IT oversight. This leadership gap included the absence of both a state Chief Information Officer (CIO) and a state CISO during a time when financial institutions, large retail chain stores, government agencies, and the entertainment industry experienced a variety of cybersecurity incidents. Reestablishing a state CISO and creating the 2014 *Statewide Information Technology Security Plan* were two critical steps Florida took to increase security awareness and harden its critical infrastructure. The plan demonstrates Florida's commitment to safeguarding and protecting IT resources, while embracing new capabilities to ensure protection for citizens and businesses throughout the state.

Developing the *Statewide Information Technology Security Plan* is a significant accomplishment for AST in that it sets the vision for cybersecurity in Florida and offers guidance to 32 executive branch agencies.

This centralized approach to cybersecurity allows the state to realize significant benefits and outcomes:

- Increases agency and AST visibility into the security posture of the state
- Supports efforts to harden the state's technology infrastructure
- Promotes economies of scale in technology purchases
- Improves threat information-sharing across state agencies
- Promotes the development of consistent security practices throughout the state
- Increases the state's ability to train its security personnel

Impact

The *Statewide Information Technology Security Plan* paved the way for the formation of a multi-agency work group created by AST to assist with developing the Florida Cybersecurity Standards.

The administrative rule establishes the Florida Cybersecurity Standards which state agencies must comply with in the management and operation of state resources. This rule is modeled after the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014, and the Federal Information Security Management Act of 2002 (44 U.S.C. §3541, et seq.).

In June 2015, AST further leveraged the Statewide Information Technology Security Plan's roadmap by completing a security risk assessment designed to assess the overall security maturity level of AST and its customers. The assessment evaluated agencies across ten security control categories (Table 2).

Table 2 – Security Control Categories

Governance	Process & Operations
Planning and Budgeting	Communications, Awareness & Training
Organization, Roles & Responsibilities	Event Detection & Response
Controls Framework	Threat & Vulnerability Management
Architecture	Risk & Controls Assessment

The results of the security risk assessment provides AST with a valuable baseline to measure all future cybersecurity initiatives and also supports and validates the principles outlined in the *Statewide Information Technology Security Plan*.

With the creation of AST in July 2014, the publication of the *Statewide Information Technology Security Plan* in February 2015, the findings of the 2015 security risk assessment, and the promulgation of the Florida Cybersecurity Standards in March 2016, Florida is well on its way to fulfilling its aggressive cybersecurity agenda.

References:

Link to AST Information Technology Security Plan:

http://ast.myflorida.com/doc%20library/2015-18%20Strategic%20Security%20Plan_1.29.15.pdf?AgyID=7298