Securing the Enterprise

State of Florida

Agency for State Technology

Category: Cybersecurity

Project Initiation Date: July 1, 2014

Project Completion Date: December 31, 2016

Contact:

Eric Larson, Interim Executive Director/State CIO
Eric.Larson@ast.myflorida.com
850.412.6045

Executive Summary

The creation of the Agency for State Technology (AST) provided the State of Florida a centralized agency to pursue enterprise information technology (IT) initiatives and provide State of Florida agencies an advocate to promote interoperability and data sharing across the entire state enterprise. Perhaps more importantly, it positioned Florida to strengthen the security of the enterprise through strategic and operational initiatives. AST has successfully implemented many key initiatives to continue its mission of pursuing enterprise-wide improvements to the state's security posture while pursuing economies of scale. This nomination highlights initiatives that collectively support a cybersecurity program that consistently improves the cohesion of the state's cybersecurity posture.

By adopting the Florida Cybersecurity Standards (FCS) through promulgating Rule Chapter 74-2, Florida Administrative Code (FAC), AST ensured that each state agency follow a uniform standard for securing IT infrastructure. In addition, because the FCS aligns to the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, each agency's security posture aligns with an industry recognized standard.

To further the goals of meeting statutorily required reporting requirements and ensuring the State of Florida is consistently working toward common security goals while ensuring state agency autonomy, AST created two tools to aid agencies in completing statutory reporting. Florida Statute requires that state agencies complete and submit an agency strategic and operational plan (ASOP) annually and triennial risk assessments. To aid agencies in the completion of these required reports, AST developed assessment tools to give agencies an efficient process to measure and report improvements to their security posture.

The tools produce graphs through an aggregation of algorithms which support both tactical and strategic insight and align to the Florida Cybersecurity Standards, the NIST Cybersecurity Framework, and the Center for Internet Security Critical Security Controls. Collectively, the tools allow for a uniform reporting method enabling AST to perform aggregate reporting for both an agency and at the enterprise level.

Concept

There was tremendous growth in the State of Florida's enterprise approach to cybersecurity in December 2015. The Agency for State Technology's multi-agency approach to cybersecurity, with a centralized and interoperable approach to security, has set the stage for large scale improvements to the state's security posture while pursuing economies of scale in resource procurement.

AST's Creation

There was a two-year gap in having a centralized IT organization which included no centralized IT oversight between July 2012 and July 2014. This gap in oversight included significant leadership shortfalls with the absence of both a state Chief Information Officer (CIO) and Chief Information Security Officer (CISO). The same two-year window saw numerous financial institutions, retail stores, government agencies, and the entertainment industry experience a variety of significant cybersecurity incidents.

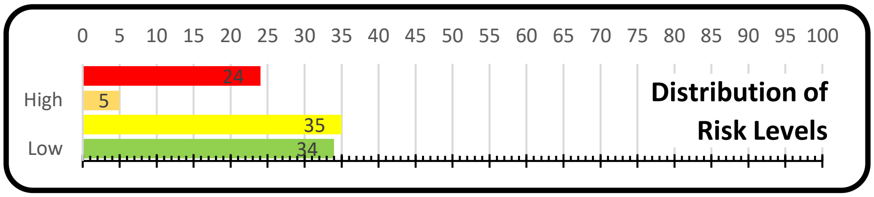
In response to the absence of centralized oversight of state IT, the Florida Legislature established the AST in July 2014. AST's task was to develop and publish IT policy for the management of state information technology resources, oversight of state technical projects, and management of the State Data Center.

AST's creation gave the state one centralized agency to pursue enterprise IT initiatives. One of AST's main initiatives is a centralized approach to security involving multiple government agencies. Before AST, the lack of centralization required each agency to pursue security in an ad hoc manner. Security standards, reporting, threat detection, intelligence sharing, and situational awareness lacked consistency or standards.

Florida's cybersecurity efforts, which include 36 government agencies and a smaller number of partner agencies, now have a cybersecurity advocate and organization focused on pulling together disparate efforts to promote interoperability and data sharing across the entire enterprise of Florida's state government. Many initiatives occurred in the 2016 calendar year that improved the cohesion of the state's cybersecurity posture.

Florida Cybersecurity Standards

To align the state's security posture the adoption of an industry recognized cybersecurity standard was needed. In March 2016, AST promulgated Rule Chapter 74-2, FAC, known as the *Florida Cybersecurity Standards (FCS)*. Each executive branch state agency is required to follow the standard for securing its IT infrastructure. Notably, the *Florida Cybersecurity Standards* align to the NIST Cybersecurity Framework, giving



Florida agencies accepted and authoritatively developed content. Each agency now shares a common and concise vernacular allowing each to work toward similar policy, technology, and training implementations while maintaining agency autonomy.

Data center Consolidation

Prior legislative mandates required most State of Florida agencies to consolidate into a primary data center rather than maintain data center operations within individual agencies. This approach facilitates unified management, procurement, and technological efficiencies for cybersecurity.

Reporting Requirements

Florida statutes requires that agencies submit two required security reports to AST. One annually and the other triennially. AST recognizes that the reports should serve not only to report agency activities, but that they should also inform decision making and high-level policy making. The goal is to better align resources and realize cost savings through economies of scale.

Significance

Risk Assessments

In Fiscal Year 2016-17 the Florida Legislature provided funding for 16 state agencies to complete third party risk assessments and tasked AST with establishing a risk assessment methodology and procurement approach for the initiative. The presence of an office dedicated to enterprise security and the recognition of the Florida Cybersecurity Standards created a ready-made path toward procurement and completion. Proviso required that AST use uniform criteria based on industry best practices, identify risk with severity, recommend and prioritize remediation strategies, and estimate a cost and schedule of remediation for each agency.

In response to the legislation, AST developed a Request for Quote (RFQ) template that included all requisite requirements that agencies could then customize to address their unique needs. Agencies could proceed to release their customized RFQ to potential contractors and select the best value for their agency needs. Each agency had the ability to work with their chosen contractor to add to the base requirements dictated by the legislature, while also reporting back to AST in a standard reporting tool created by AST for that purpose.

FCS Reporting Tool

To collect uniform assessments from disparate risk assessors and agencies, AST created a form in Microsoft Excel that aligns to the FCS and, by extension, the NIST Cybersecurity Framework. The tool addresses all cyber security domains and uses risk aggregation to group together remediation strategies which then map to one of the 22 security categories within the framework. Agency employees, contractors, or any organization aligned with the NIST Cybersecurity Framework, may freely download and complete the Risk Assessment Tool. The tool is currently available via download from AST's website. In addition, NIST included the tool as an industry resource on its Cybersecurity Framework website. The tool allows for an assessor to gauge an organization's maturity in each of the 98 subcategories of the FCS (and NIST Cybersecurity Framework). Input in each subcategory feeds executive and operational graphs that highlight top risks, quickest and least expensive wins, and cost and time estimates to remediate the organization's security shortfalls.

Economies-of-Scale

While AST recognizes that each agency is unique with specific needs, the enterprise approach to security has shown that agencies often have parallel needs that a single technology or process may address through similarity of need, similarity of regulatory requirement, or improve security within the data center environment they share.

AST procures services that multiple agencies may purchase at a reduced cost through an enterprise pricing model. The ability to negotiate costs at an enterprise level provides smaller agencies that do not have the budgetary resources to engage vendors with additional procurement resources through their partnership with AST.

Consolidation of Incident Reporting

Section 282.318(4)(d), Florida Statutes, requires that agencies develop procedures to report information technology security incidents and breaches to the Florida Department of Law Enforcement's (FDLE) Cyber Crime Office and AST. To facilitate the reporting of incidents while reducing the duplication of reporting efforts, AST created the incident reporting portal to allow agency security workers a compliant method to report incidents to both AST and FDLE. Reports submitted to the portal generate alerts to both AST and FDLE. In addition to satisfying mandatory reporting requirements, the portal allows agencies to monitor attack trends through anonymized statewide incident counts, shown by type.

Agency Security Plans

Florida statutes requires that each state agency annually submit an Agency Strategic and Operational Plan (ASOP) for information technology security. The plan must cover a three-year period, define security goals, intermediate objectives, and projected agency costs for the strategic issues of agency information security policy, risk management, security training, security incident response, and disaster recovery. Agencies must base their plans on the statewide IT security strategic plan created by AST. By statute, the plans must include performance metrics that agencies can objectively measure to reflect progress toward security goals and objectives as identified in the agency's strategic information security plan. Further, the plan must include a progress report that objectively measures progress made towards the prior year's operational information technology security plan with a project plan that includes activities, timelines, and deliverables for security objectives that the state agency will implement during the coming fiscal year.

AST designed an assessment tool to assist agencies with completing and submitting the required annual assessments while ensuring a uniform reporting structure. The Excel based tool provides agencies with an efficient and effective process to measure improvements to their security posture, while also ensuring the report provides agencies the ability to respond to the assessments in a concise, uniform matter. The reports produced by the tool serve to inform at both an agency and enterprise level. The tool affords security personnel within each agency clear reports that may be used to inform executive decision making. In addition, AST can readily consolidate multiple agency reports to inform policy makers.

An added benefit to the tool is that many of the assessment categories align with the Center for Internet Security's Critical Security Controls. This allows agencies to measure their maturity against an industry accepted and well documented framework.

While agencies did not have baseline figures to compare to, a number of agencies reported time savings with the new tool. Based on agency responses, an estimated five hours of work time was saved per agency utilizing the ASOP tool. Five hours across 36 state agencies completing the ASOP tool resulted in a time savings statewide of approximately 180 hours.

Impact

Common Security Goals

AST leverages the cohesion realized by a common operating paradigm to plan, purchase, and drive security improvements, training, and contract vehicles to better defend Florida's cyber landscape. Common security goals across agencies allow the realization of cost and time savings.

Policy Alignment

The NIST Cybersecurity Framework and the Center for Internet Security Critical Security Controls are both widely adopted and well documented. Agencies may now repurpose literature developed by those organizations, as well as similar organizations, avoiding development and creation hurdles.

Similarity of Need

Because of similarity of need across multiple agencies, the state realizes cost savings by entering negotiations with increasing buying power. Purchases as diverse as network monitoring systems and training meet the needs of multiple agencies. AST pursued many cost saving purchases that both realized cost savings and set the stage for future cost savings.

In 2016, the Florida Legislature provided AST funds to train agency security professionals. To address the training requirement, AST began the process of procuring training aligning with the CIS Critical Controls. The goal being to allow agency security staff to implement each of the controls and then audit their progress toward alignment.