


Update on the FY2020 Key Security Initiatives Implementation Roadmap

60x30TX
Texas Higher Education Coordinating Board

Zhenzhen Sun
Assistant Commissioner/CIO
Information Solutions and Services

Peter Donton
Information Security Officer
Information Solutions and Services

AOC – July 22, 2020



1

Agenda

This presentation will cover the following topics:


- Overview
- FY2020 Security Initiatives Implementation Roadmap
- Progress Report
- Next Steps



2

2

Overview




3

3

Agency Cybersecurity Framework

The diagram illustrates the Agency Cybersecurity Framework. At the center is a blue oval labeled "THECB Cybersecurity Framework". Surrounding it are five colored circles representing the stages of the framework: "Identify" (orange) at the top, "Protect" (grey) on the right, "Detect" (yellow) at the bottom, "Respond" (blue) on the left, and "Recover" (green) at the top-left. Arrows connect these circles in a clockwise cycle: Identify to Protect, Protect to Detect, Detect to Respond, Respond to Recover, and Recover to Identify. The entire cycle is supported by three pillars: "People" on the left, "Process" on the right, and "Technology" at the bottom.



4

4

Biennial Agency Cybersecurity Framework Assessment

- The agency is required by the statute to go through a biennial review of its information security program for compliance with the standards set forth by the Texas Cybersecurity Framework.
- The most recent assessment was conducted by AT&T Cybersecurity during May and July 2019.
- The current maturity level of the agency security framework is 3, which means the agency has well-documented policies and procedures that cover all the controls outlined in the framework.

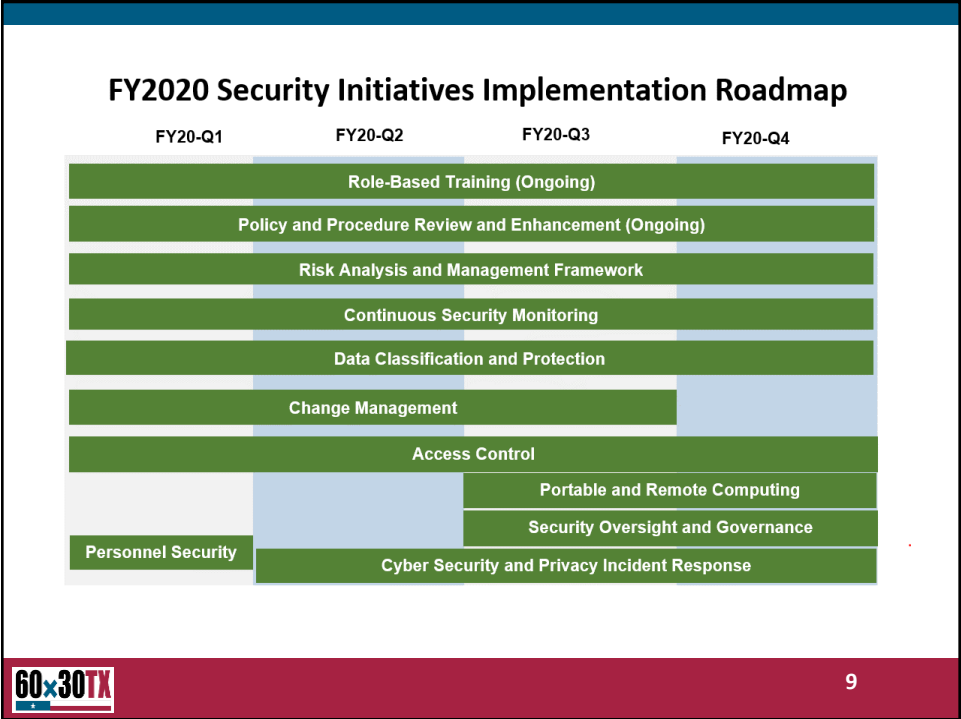
Key Recommendations

- Enforce appropriate protections for data based on classification levels
- Develop an enterprise level Risk Management Program
- Establish performance measures for the agency Information Security Program

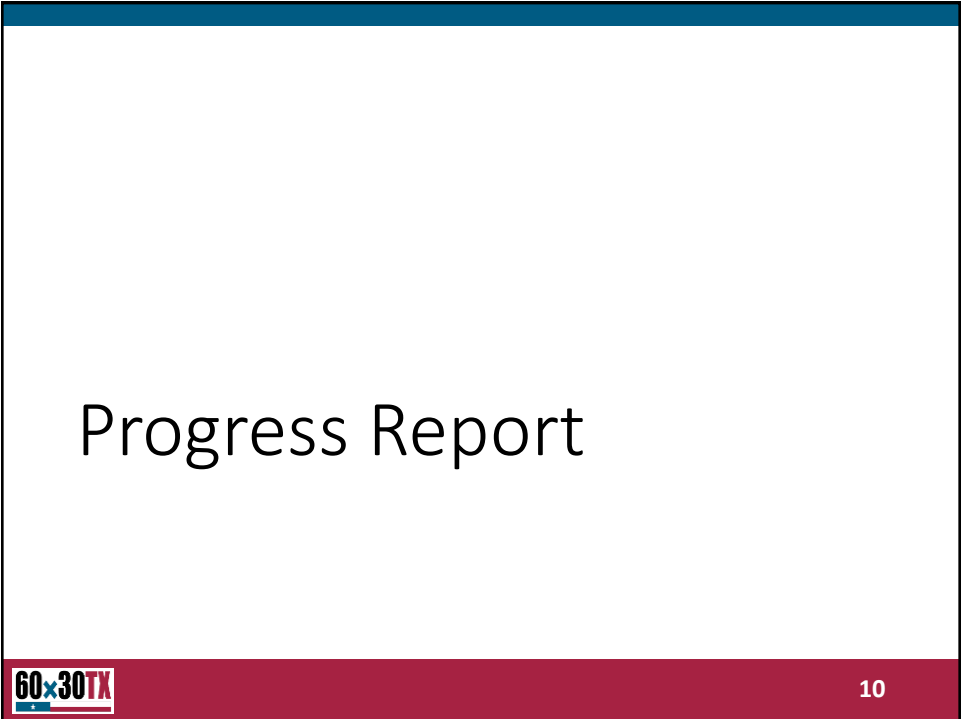
FY2020 Security Initiatives Implementation Roadmap

Our Strategy to Mature the Agency Cybersecurity Framework

- Information Solutions and Services division publishes the *Security Initiatives Implementation Roadmap* at the beginning of each fiscal year.
- **Input**
 - Agency business goals and priorities
 - Recommendations from the biennial assessments
 - Maturity level of the control objectives
 - Agency environment: assets, people, business processes and risks
- **Output**
 - A prioritized list of projects
 - A relevant and actionable implementation roadmap



9



10

Progress Report

Procurement and Deployment of Web Application Firewall (WAF)

- Obtained legislative appropriation, procured, deployed and managed through the Managed Security Services (MSS) at the State Data Center
- The first agency to deploy WAF at the State Data Center
- Project completed in Q2 FY20
- Ongoing effort to place agency websites under its protection
- Remediates web application vulnerabilities without software redevelopment

Procurement and Deployment of Security Incident and Event Management (SIEM)

- Obtained legislative appropriation, procured, deployed and managed through the MSS
- Project completed in Q1 FY20
- Tuning data collection and reporting
- Tool to inform the new agency Risk Management Framework



Progress Report

Deployment of Multi-Factor Authentication for Office 365 resources

- For all user types
- Achieved in Q2 FY20

Developed end-user training for Data Classification and Data Loss Prevention

- Phased rollout beginning in Q4 FY20

Security Awareness Training

- Among the first five state agencies to gain certification in Q1 FY20
- Continuing to fine tune procedures to ensure compliance with HB3834



FY2020 Maturity Level Forecasting

Objective	Control Area	FY2019	Aug 2020
Identify	Data Classification	3	3.50
Identify	Enterprise Security Policy, Standards and Guidelines	3	3.00
Identify	Control Oversight and Safeguard Assurance	3	3.00
Identify	Information Security Risk Management	3	3.25
Identify	Security Assessment and Authorization	3	3.00
Identify	External Vendors and Third Party Providers	3	3.50
Identify	Security Oversight and Governance	3	3.25
Protect	Cryptography	3	3.00
Protect	Change Management	3	3.00
Protect	Security Systems Management	3	3.00
Protect	Security Awareness and Training	3	3.50
Protect	Privacy Awareness and Training	3	3.25
Protect	Secure Configuration Management	3	3.00
Protect	Physical and Environmental Protection	3	3.50
Protect	Personnel Security	3	3.00
Detect	Security Monitoring and Event Analysis	3	3.50
Respond	Cyber-Security Incident Response	3	3.50
Respond	Privacy Incident Response	3	3.00

60x30TX
13

13

Next Steps

60x30TX
14

14

Next Steps

Retain current appropriation levels for Manage Security Services and Cybersecurity Initiatives

- \$440K appropriated by the 86th legislative session for FY20-21
- Security Incident Event Management
- Web Application Firewall
- Security Assessments
- Identity and Access Management

Designate a Privacy Officer

- Role is essential to support agency strategic goal of becoming a data resource for the higher education institutions and the general public

Next Steps

Implement Risk Management Program to support resource allocation decisions.

- A “dashboard” for the IT Steering Committee and the executive management to support decision making process
- Key to achieving level 4 Capability Maturity

Deploy Data Classification and Data Loss Prevention controls

- Co-deployment with migration to SharePoint and OneDrive Online

Review governance on policy process

- Remote work policy and implement related controls

Thank you

