TEXAS HIGHER EDUCATION
COORDINATING BOARD

P.O. Box 12788 Austin, Texas 78711

512/ 427-6101
Fax 512/ 427-6127

Web site:
http://www.thecb.state.tx.us

September 24, 2018

Dr. Raymund A. Paredes
Commissioner of Higher Education
1200 E. Anderson Lane
Austin, TX 78752

Dear Dr. Paredes:

The July 2018 status report provided by management to the Agency Operations Committee was accurate regarding actions taken to implement the recommendations in the *NTT Texas Cyber Security Assessment Report* at the Texas Higher Education Coordinating Board, issued June 2017 (*see Appendix 1)*.

Our review focused on assessing the accuracy of management's most recent report of corrective action status, dated July 2018. The assessment also considered actions taken between the last official report in July 2018, and our fieldwork in August/September 2018.

Our status assessment provides an outside evaluation of the agency's information security program as required on a biennial basis by Texas Administrative Code Chapter 202 Information Security. Our audit included reviewing the NTT assessment and obtaining a status update with relevant documentation to determine the implementation status.

We conducted this audit in conformance with the *International Standards for the Professional Practice of Internal Auditing.* Additionally, we conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our audit objectives.

The NTT assessment provided 72 recommendations divided into five categories. The most significant recommendations related to areas where the "**maturity**" of a scored element was at level two, on a scale of zero to level

five. NTT scored 34 of 72 of its recommendations as level two maturity. Maturity levels zero to five are defined in *Appendix 2*.

Details	# of Recommendations
Recommendations Reported by NTT Data at Level 2	34
Areas Remaining at Level 2, Verified by Internal Audit	16
Recommendations Reported by NTT Data at Level 3	38
Areas Remaining at Level 3, Verified by Internal Audit	32

The cooperation of your staff during this review was greatly appreciated. If you have any comments or concerns on the conduct of this review, please let me know.

Sincerely,

Mark A. Poehl

Mark A. Poehl, CPA, CIA, CISA, CFE
Director, Internal Audit and Compliance

PERFORMED BY:

Aporajita Ahmed, CPA, CFE, CITP, CGMA, CICA, Cyber Security Professional, Internal Audit Lead

cc:

THECB

Board Members

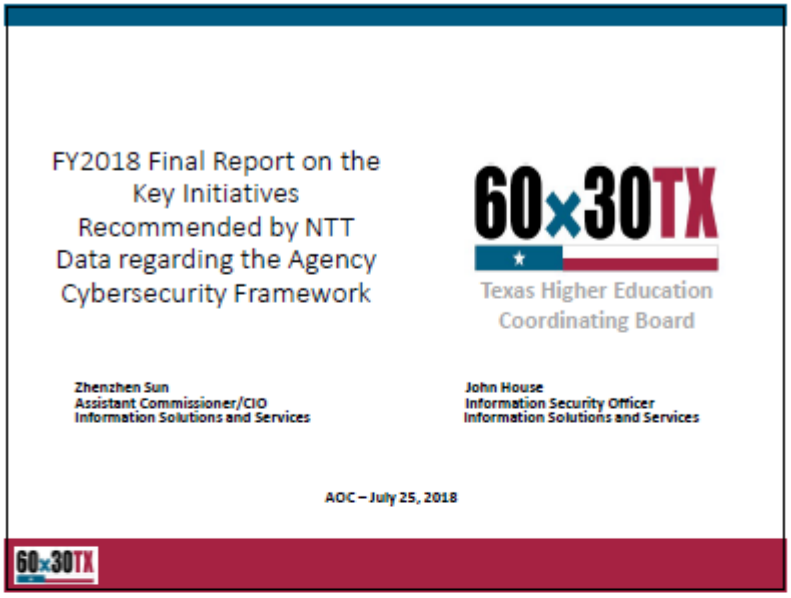
Commissioner's Office
Ms. Linda Battles, Deputy Commissioner for Agency Operations and Communication and COO
Dr. David Gardner, Deputy Commissioner for Academic Planning and Policy
Mr. William Franz, General Counsel
Ms. Zhenzhen Sun, Assistant Commissioner for Information Solutions and Services

STATUTORY DISTRIBUTION REQUIREMENT

Legislative Budget Board
Ms. Julie Ivie
Governor's Office of Budget & Planning
Mr. John Colyandro
State Auditor's Office
Internal Audit Coordinator
Sunset Advisory Commission
Ms. Jennifer Jones

Appendix 1

Status Update by THECB Management in July 25, 2018



2017 Agency Cybersecurity Framework Assessment Results

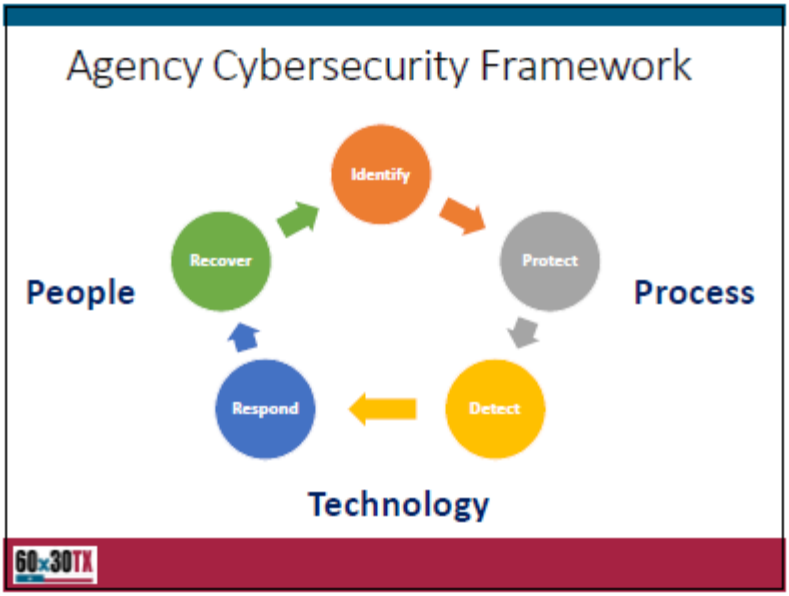
- Between April and June 2017 NTT Data, Inc., vendor contracted by the Department of Information Resources, performed an assessment of the THECB's cybersecurity infrastructure.
- NTT presented their findings and over 70 recommendations to the Board in a Special Called Board meeting on June 28th, 2017.
- Among the 40 objectives of the TX Cybersecurity Framework:
  - ❑ THECB scored higher than the state agency average in 34 objectives
  - ❑ 3 objectives received scores equal to the state agency average
  - ❑ 3 objectives received scores lower than the state agency average

60x30TX

THECB Control Objective Maturity Scores

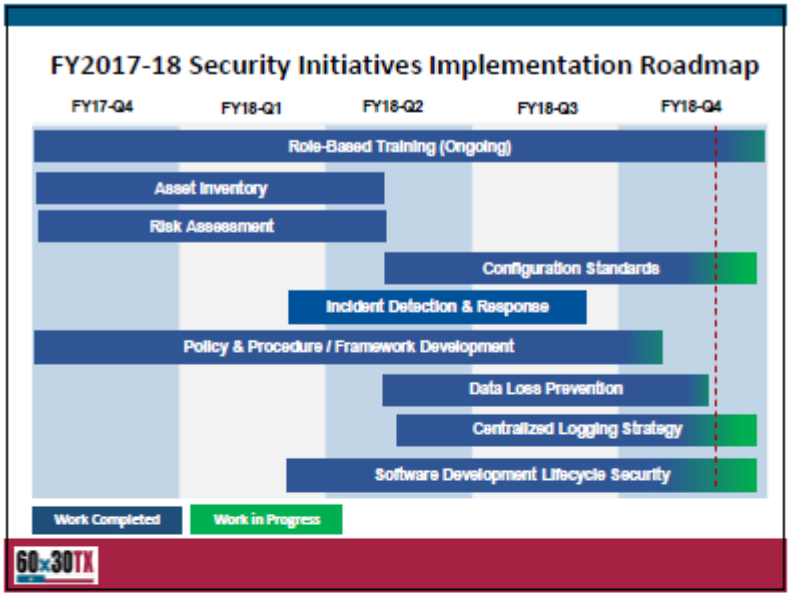
Maturity Level	Number of Objectives
Level 3	24
Level 2	16
Total	40

60x30TX



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**
  - Recommendations made by NTT Data
  - Control objective maturity scores
  - Business priorities, assets, people and risks
- **Output**
  - A prioritized list of projects
  - A relevant and actionable implementation roadmap


FY2017-18 Security Initiatives Implementation Roadmap
FY17-Q4
FY18-Q1
FY18-Q2
FY18-Q3
FY18-Q4
Role-Based Training (Ongoing)
Asset Inventory
Risk Assessment
Configuration Standards
Incident Detection & Response
Policy & Procedure / Framework Development
Data Loss Prevention
Centralized Logging Strategy
Software Development Lifecycle Security
Work Completed
Work in Progress
60x30TX

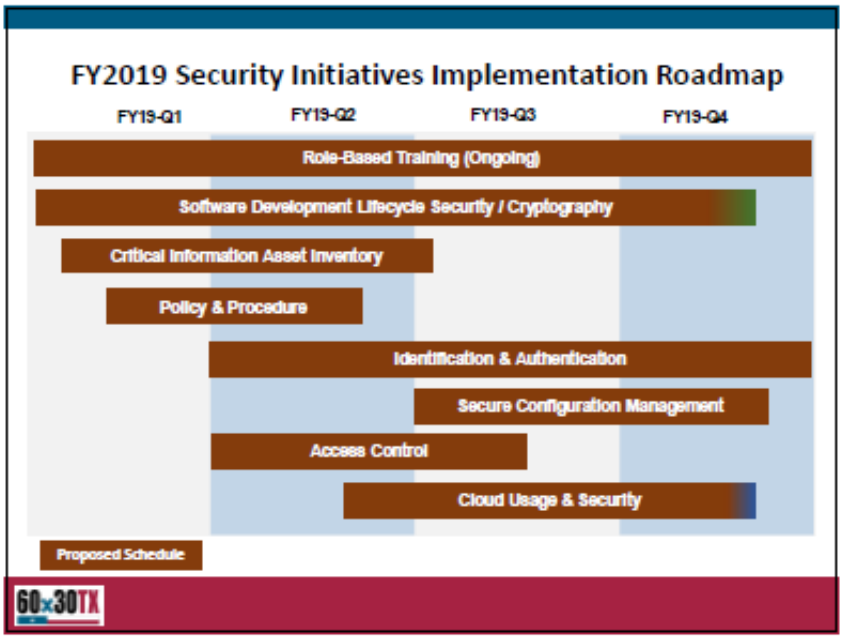

Progress Report – Completed in Q3
▪Configuration Hardening Standards
▪Acquired Vulnerability Management tool through Data Center Services Managed Security Services (MSS)
▪Policy & Procedure
▪Data Loss Prevention procedures updated, training developed
▪Data Loss Prevention tool deployed on workstations
▪Updated Section HH IT policies – to be posted pending approval
▪Completed Enterprise Architecture Strategy Document & Training
▪Software Development Lifecycle Security
▪Security checklist and frameworks for developers published
▪Role Based Training
▪Office 365 Data Loss Prevention Training
▪Updates to Security Awareness training library
60x30TX

Cybersecurity Control Area Improvement

Objective	Control Area	2017	08/2018
Identify	Critical Information Asset Inventory	2	3
Identify	Information Security Risk Management	2	3
Identify	Security Compliance and Regulatory Requirements Management	2	3
Protect	Enterprise Architecture, Roadmap & Emerging Technology	2	3
Protect	Secure System Services, Acquisition and Development	2	3
Protect	Security Awareness and Training	2	3
Protect	Privacy Awareness and Training	2	3
Protect	Secure Configuration Management	2	3
Protect	Media	2	3
Protect	System Configuration Hardening & Patch Management	2	3
Protect	Data Loss Prevention	2	3
Protect	Identification & Authentication	2	3
Protect	System Communications Protection	2	3
Detect	Security Monitoring and Event Analysis	2	3
Respond	Cyber-Security Incident Response	2	3
Respond	Privacy Incident Response	2	3

Q4 Initiatives Still in Progress

- Configuration Hardening Standards
  - Implement MSS Vulnerability Management – use Qualys scans to prioritize remediation & reduce vulnerabilities
  - System Security Plans for critical applications
- Software Development Lifecycle Security
  - MSS Fortinet Web Application Firewall operational on agency websites
  - MSS Application Vulnerability Scanning integrated in the software development lifecycle
- Centralized Logging Strategy
  - MSS Security Incident & Event Management – Implement acquired services


FY2019 Security Initiatives Implementation Roadmap
FY19-Q1
FY19-Q2
FY19-Q3
FY19-Q4
Role-Based Training (Ongoing)
Software Development Lifecycle Security / Cryptography
Critical Information Asset Inventory
Policy & Procedure
Identification & Authentication
Secure Configuration Management
Access Control
Cloud Usage & Security
Proposed Schedule
60x30TX

Appendix 2

Capability Maturity Model as developed by Department of Information Resources

Maturity Levels					
LEVEL 0: Non-Existent. There is no evidence of the organization meeting the objective.	**LEVEL 1: Initial.** The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.	**LEVEL 2: Repeatable.** The organization has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.	**LEVEL 3: Defined.** The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.	**LEVEL 4: Managed.** The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.	**LEVEL 5: Optimized.** The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.
Control Objective Maturity Indicators					
0	1	2	3	4	5