CoALS Technology Security Committee
April 21st, 2021
1:00 p.m.

Attendance:

Members			
Kerry Pickens - Chair (Manager Policy & Compliance)	Tim Ramsey (Associate Director of IT)	_ name (PI CoALS Research)	Keith Wicker (Information Security Officer)
Gene Curtiss (Manager Systems & Infrastructure)	Barry Stratta (Manager Software & Applications)	Sushant Patil (Security Analyst – Security & Risk)	_ name (Title)
_ name (Title)	_ name (Title)	_ name (Title)	_ name (Title)

Also in Attendance:

Minutes

Item 1: **Approval of Minutes**
Description: Review and approval of minutes from previous meeting.

Item 2: **Governance Committee Reports** (5 mins)
Description: Note relevant information from available reports as applicable.

A. TAMU ITAC – N/A
B. AgriLife Computer Advisory Team – N/A
C. CoALS Council of Department Heads – N/A
D. AgriLife Technology Leadership Council -N/A
E. AIT Enterprise Technology Committee (ETC)
    - Information about new Agent password policy changes already in affect (12 characters minimum, 2 year expiration date)
    - Microsoft authentication APP
F. AIT Technology Compliance Committee (TCC)
    - You have a voice into forming compliance policy! (ex: implementation of security cameras, etc.)

Item 3: **Lessons Learned (10 mins)**
Description: As applicable from recent activities.

- Vulnerability scans –
    - Expired certificates on web servers. Forwarded to Barry if 02 and Gene if 06., then sent to Tim and Alex as leads for Research Computing Center
    - Remote service using an SSL Certificate that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks
        - Medium risk
        - Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm
        - Note that certificates in the chain that are contained in the Nessus CA database have been ignored
    - Remote service is accepting connections encrypted with SSL 2.0 and/ or SSL 3. Which is putting systems at HIGH risk (man-in-the-middle attacks)
        - These versions of SSL are affected by several cryptographic flaws including:
            - an insecure padding scheme with CBC ciphers

- insecure session renegotiation and resumption schemes

Item 4: **New Business / Special Topics (15 mins)**
Presenter: Kerry Pickens
Description: Differences between BFURD Audit and annual Risk Assessment

- BFURD Audit will include Research Computing Center and will be a continuous process
    - Purpose of BFURD is for the staff to learn how to produce audit records and there is a requirement by each department head that we provide them with a consumable document that details what they should be doing. BFURD captures the business requirements (the high level things they do across all departments)
        - https://firstcallhelp.tamu.edu/wp-content/uploads/2021/05/MicrosoftTeams-image.png
        - https://firstcallhelp.tamu.edu/wp-content/uploads/2021/05/TSC-May-Meeting-Proactive-vs-Reactive.png
    - When we do the RA, it'll be easier because they already answered all those questions in the BFURD, so it will speed up the process
- RA is supposed to be seasonal, but the project scope keeps creeping. We started late in 2020 because of the reorganization and staff turnover. The 2020 deadline for Phase 2 was September 2020 so we just finished Phase 3 Reporting.
- RA only includes the college assets (02), but IT RM tried to add HIPAA assessments. Refer any HIPAA assessments on 06 assets to Keith Wicker.
- 2021 RA will include the applications by impact level category such as
    - Source code
    - No source
    - Vendor hosted
- RA is based on NIST v4 low standards. BFURD is based on NIST v5 and includes emerging technologies (IoT, etc.). Not notified by IT RM when RA will include NIST v5.
- Purpose of BFURD is to prepare staff for TAMU system audit by preparing audit records for verification and validation. Auditors have their own system and may be using NIST v5. Example of audit record is risk register that includes audit findings, security remediations and vulnerability scans.
- Vet Lab complies with ISO standards so if we consolidate IT departments, will we go to ISO or stay with NIST?
- IT Security Progress
    - https://firstcallhelp.tamu.edu/wp-content/uploads/2021/05/BCBCP-IT-Security-Progress.pdf

Description: Business Continuity, Disaster Recovery and DR Testing
Audit records that need to be updated and tests scheduled annually

- Plan exists just needs to be updated and include references to other TAMU plans
- DR Exercises need to be scheduled
    - Testing backups, etc.

- Vendor contacts and staff/faculty contacts need to be updated
- Need incident response process documented
    - Flow chart is needed for this
- Business Impact Analysis for **each department**. Draft written by IT staff and then discussed with Dept Head. Include recovery times and objectives, and priority for recovery of assets.

Item 5: **Action Items**

A. Phase I RAIL inventory completed by June 4th
B. Phase II assessors assigned by DRAC
C. Business Continuity Plan and DR Plan updated – Sushant to complete by Sept 1
D. Incident Response Process - Sushant to complete by Sept 1
E. DR Tests Scheduled by Dec 31st

Item 6: **Close**

Description: Adjourn meeting on time noting actions and conclusions of meeting.
Next meeting: 3rd Wednesday of June at 1 p.m. (June 16th, 2021)