


June 29, 2022

MEMORANDUM

TO: M. Katherine Banks, Ph.D.
President

FROM: Ed Pierson 
Working Group Chair

SUBJECT: Implementation Memo – Working Group # 37

Recommendations to be Implemented: Prioritize cybersecurity to ensure campus services are not compromised.

Strategic Considerations:

The working group sub-groups addressed 4 categories of recommendations:

- Identity and Access Security
- Device Security
- Research Security
- Application Security

The summary recommendations per sub-group are presented below with the full subgroup report presented in the attached document.

Logistical Issues Addressed:

Identity and Access Security:

1. Recommendation 1: **Centralize on a single, modern, robust IAM service.** This means that there is a single identity (NetID) for each campus member, and that the infrastructure to support those identities is robust, reliable, and built on commercial-grade software.
2. Recommendation 2: **Build a sustainable IAM team.** Understaffing a critical area like Identity and Access Management (IAM) creates a significant security risk for the institution and jeopardizes our ability to deliver effective technology services at scale. The IAM team is a part of security and while it is properly positioned, it does need to be properly resourced.
3. Recommendation 3: **Address IAM concerns related to distributed and cloud services.** The increased usage of cloud services across many different campus units, especially Software-as-a-Service (SaaS) platforms, creates challenges in monitoring and securing access to university data and resources.

Device Security:

4. Recommendation 4: **Implementation of centralized endpoint deployment workflows.** These workflows will result in a more secure configuration from the onset, as IT cannot appropriately configure, secure, and manage what they are not aware of. These workflows should also include automated, initially-compliant defaults that are configured before startup as well as manual and automated validation of endpoint controls to ensure ongoing compliance with University, A&M System, and State information security requirements. All endpoints, regardless of how or where they are provisioned should be registered with a centralized asset tracking system.
5. Recommendation 5: **Standardize on a modern and centralized IT asset management system.** This system would contain a comprehensive, real-time inventory of IT assets, controls on each asset, and software on each asset, in use by the university. *This recommendation will also go a long way in creating a more streamlined and less intrusive annual risk assessment process and audit preparedness for all colleges and divisions across the university.*
6. Recommendation 6: **Standardized on a set of effective and centrally managed tools** for endpoint security and endpoint management. This would help provide the ability to centrally, efficiently, and effectively manage and secure endpoints. This will also allow for more effective monitoring whilst reducing cost due to duplication. These tools will continuously be evaluated and updated as new, better, and less expensive options hit the market. Where centralized tools cannot be deployed or used (i.e., industrial control systems or telemetric devices), subject matter experts should be available to assist with remediating and alternative controls. Validation that these tools are in place and functional should be a continuous and automated function.

Critical Dependency for Device Security: Implementation of a more modern and well thought out network infrastructure design that leverages identity and role-based network access controls, as well as purpose-built networks that are separated from the campus' "general use" network.

Research Security:

7. Recommendation 7: **Creation of a small Research Security Function/Team within Cybersecurity** of professionals dedicated to ensuring Texas A&M University retains and increases its grant competitiveness.

Application Security:

8. Recommendation 8: **Create a Secure SDLC program within Cybersecurity.**
This Secure SDLC program is intended to implement a mostly-automated pipeline ensuring the many critical and large security gaps in the thousands of applications and software used by Texas A&M are closed and we move rapidly towards a continuously shrinking attack surface on the application front.

Major Challenges Encountered and Resolutions:

These recommendations will be challenging technically, politically, and from a personnel and time resource perspective. To be successful, there will need to be a well-defined IAM service and clear processes and support mechanisms in place for migrating from distributed directories to a central directory. There will likely be some hesitancy by groups or individuals to give up their distributed directory services as it will be perceived as losing autonomy or capability as well as changing existing business processes. Service transition preparation will help alleviate those concerns. If there are legitimate obstacles to using the central IAM service, there should be an exception request process in place. Also, to be successful IT personnel will have to be able to allocate the time to work with the IAM team to migrate information resources tied to distributed directories to the central IAM service.

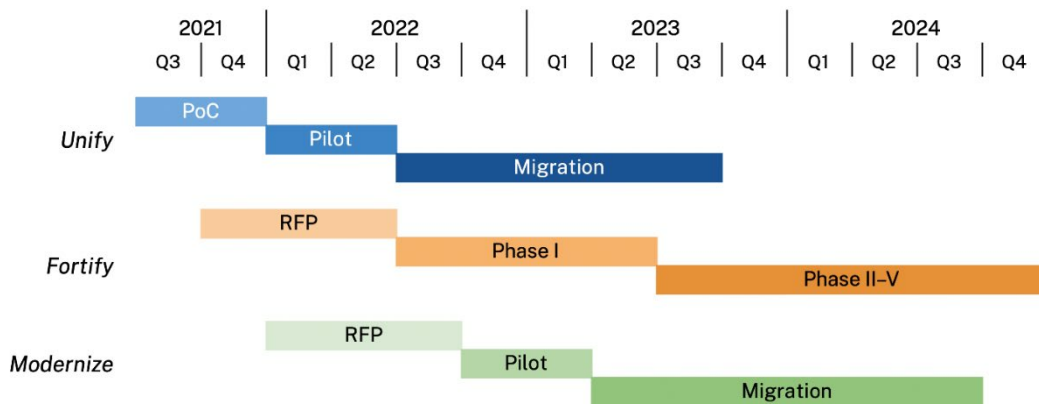
There will be a need to hire a few cybersecurity positions to address some of the recommendations in this proposal. However, to a large extent, the human resources needed for most of the recommendations already exist in the TAMU security team as well as college and division IT teams. There will need to be additional resources allocated to licensing costs, as there will initially be a need to purchase additional licenses for current central security and manageability tools that will be deployed to a larger audience. However as more endpoints begin converting to the usage of a centralized set of tools, they will discontinue the purchase of the many duplicative tools currently being paid for and used. The only additional licensing cost will be for devices that currently have no security or manageability tools at all.

Key Logistical Issues to be Completed and Timeline:

Identity and Access Security:

Based on previous consultant recommendations the following timeline is recommended.

1. Q2 2023 - Fortify — Replace the legacy Division of IT “Merge” (phase 1 of 5)
2. Q3 2023 - Unify — Active Directory consolidation complete
3. Q3 2024 - Modernize — Single Sign-On (SSO) Re-platform complete
4. Q4 2024 - Fortify — Enhance functionality of “Merge” replacement (phases 2 to 5)



Device Security:

- Resources identified: June 1, 2022
- Program design begins (tools and process identified): August 1, 2022
- Task force setup and feedback loop initiated: September 1, 2022
- Implementation for Initial College: October 1, 2022
 - Lessons Learned and revisit of design
- Phase two colleges implemented: December 1, 2023
 - Lessons Learned and revisit of design
- Phase three colleges implemented: March 1, 2023
- Year two repeat and review of entire program: June 1, 2023-June 1, 2024

Research Security:

- Program design begins: June 1, 2022
- Resources onboarded and active by: August 1, 2022
- Program Beta Kickoff by: September 1, 2022
- Program in full swing and feedback loop active via task force by: October 1, 2022
- Program Review and revision: March 1, 2023

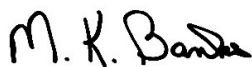
Application Security:

- Phase 1: Set up the tools and resources needed July 1, 2022
- Phase 2: Design and implement a mature, versatile, and mostly-automated pipeline and process. September 1, 2022
- Phase 3: A rapid implement-fail-learn-redo phase with a diverse sample set of developers and applications. December 1, 2022
- Phase 4: Market the matured program University and system-wide and subsequently begin full production activity. May 1, 2023

Summary

The outcomes stated in the attached sub-group reports should positively impact the academic and research focuses of the university by standardizing and streamlining security controls, improving the overall campus and researcher experience while increasing security. It is possible that during the implementation of the recommendations there could be short-term inconveniences as information resources are transitioned. However, implementing these recommendations will reduce the University’s overall cybersecurity risk footprint. The University will become more grant competitive, and small to moderate financial gains should be realized as costs associated with redundancy of efforts, licensing, and systems as well as costly mistakes and chaotic unplanned processes will be greatly reduced.

Approved:



August 13, 2022

M. Katherine Banks, Ph.D.
President

Date

APPENDIX of Sub-Group Reports

Working Group 37: Subgroup 1: Identity and Access Management

Recommendation Overview

Recommendation #3: Prioritize cybersecurity to ensure campus services are not compromised.

Strategic Considerations

The Identity and Access sub-working group was tasked to provide recommendations to ensure that Cybersecurity remains a top priority as it relates to Identity and Access. Sub-working group members recognized that significant effort and progress has recently been made toward improving Identity and Access Management (IAM) by IAM experts in TAMU Security with partnerships from across campus via working groups, and nationally recognized consultants that assessed and evaluated our current state in depth, conducted many interviews, and ultimately mapped out the exact steps needed. Members wanted to capitalize on that progress, making recommendations that would be an *enabler* for the campus community while providing *secure outcomes*.

Desired Outcomes

- An **optimized user experience** regarding number of accounts, provisioning workflows, and IAM support
- A **clearer and improved security posture** by having one place to know who has access to what while reducing overall attack surface
- A **central commercial IAM shared service** to increase innovation, automation, and capability to manage on-premises and cloud resources while reducing duplicate administrative effort

Recommendations

9. **Centralize on a single, modern, robust IAM service.** This means that there is a single identity (NetID) for each campus member, and that the infrastructure to support those identities is robust, reliable, and built on commercial-grade software. This solution would have the following properties:
 - a. The solution must address identity AND access. A current need in our IAM solution space is for a single pane of glass to manage and see who has access to what. Access controls should focus on RBAC (Role Based Access Control), zero-trust, and just-in-time concepts.
 - b. The solution should provide streamlined “orchestration” capabilities to university information resources. This means automated provisioning workflows (electronic routing with approvals) that include human resources, colleges and business divisions, and IT. This capability would enable faculty, staff, and students to gain access to information services that are appropriate for their roles in an efficient, secure manner. This includes the ability to interface with third-party applications and network access control capabilities.
 - c. The solution should include a common directory. This means that the university should look to eliminate unnecessary directory services, such as Active Directory (AD) domains. Currently there are many AD domains in divisions and colleges, and this duplication of effort is inefficient, and creates unnecessary security risks.

- d. The solution should use modern SSO technologies. This means we need to address the legacy CAS (Central Authentication Service) and Shibboleth services currently in place. These services will likely be necessary to support certain applications, but modern SSO solutions and protocols, such as Azure AD, should be preferred when possible.
 - e. The solution should be well managed. This means that in addition to the technology, there should be proper governance in place without creating bureaucracy. This will help ensure that current and future core business and customer facing needs are surfaced and met and that sufficient self-service capabilities are granted to appropriate IT professionals and non-IT employees. It should also ensure all aspects of IAM related people, processes, communication, and training are addressed.
10. **Build a sustainable IAM team.** Understaffing a critical area like Identity and Access Management creates a significant security risk for the institution and jeopardizes our ability to deliver effective technology services at scale. The IAM team is a part of security and while it is properly positioned, it does need to be properly resourced.
- a. Compared to our peer institutions, Texas A&M is dramatically understaffed in key areas. Using peer comparison data, and recommendations from industry consulting firms, IAM staffing should be raised to levels that can support the expertise and customer service targets the university expects. *Per the Identity of Tomorrow – Peer Institution Comparison whitepaper (see Appendix A), the IAM team FTE count should be raised from four to at least nine, meeting the median among our peer institutions.*
 - b. Additionally, this team must have the authority to design and manage the IAM services while working closely with other critical stakeholders. The IAM team will collaborate with those who have services that are dependent on or integrated with the IAM service, to ensure a flexible and sustainable design.
11. **Address IAM concerns related to distributed and cloud services.** The increased usage of cloud services across many different campus units, especially Software-as-a-Service (SaaS) platforms, creates challenges in monitoring and securing access to university data and resources.
- a. Policies should be developed to govern the configuration and use of identities on SaaS platforms. User provisioning should be connected to the central identity store and governed by the overall NetID lifecycle. This provides appropriate oversight for high-impact services that support university business functions.
 - b. Oversight of distributed applications and services should include regular assessments to enumerate and track essential attributes of the service, such as the service sponsor, application administrator(s), data stewards and managers, and the classification of any data managed, stored, or transmitted by that service.
 - c. In order to help application administrators meet compliance targets associated with IAM requirements, self-service tooling will be necessary for IT pros to implement identity and SSO solutions in their applications. Developer-focused tooling should

include resources such as API documentation, code samples and libraries, and self-service key/token management.

Logistical Issues Addressed

Anticipated challenges associated with the proposed recommendations. Mechanism for implementing the recommendations, Customer/stakeholder feedback mechanism. Budget impact if applicable.

Recommendation #1 will require the acquisition of new technology services which will have reoccurring budget implications. To successfully design, implement, and migrate to the new IAM service and its workflows, the IAM team will need to conduct meetings and collaborate regularly with stakeholders like human resources, colleges and business divisions, and IT to ensure they meet university business and staff/faculty/student needs. They should also have mechanisms in place for stakeholders to request changes or new features to the IAM service, its workflows and processes.

Recommendation #2 will require additional staffing and potentially new skills for the IAM team and related support teams. Staffing could be addressed through a combination of new positions being created which has budget implications and/or the reassignment of existing IT personnel as part of the IT consolidation who are interested and have experience or skills. New skills could be identified and require professional development funding for training.

Recommendation #3 likely requires the engagement of the cloud vendors and the customers who procured their services. For cloud services not already using a campus SSO service or to move to a more modern, campus preferred SSO service, there could be time, budgetary and/or contractual implications for the customer to make those changes. ***Future contracts and renewals should include language reinforcing the utilization of SSO.*** It is possible that some cloud services do not support SSO or only a limited SSO mechanism.

Major Challenges Encountered and Resolution

Resources needed, resistance from stakeholders to be overcome, impact on stakeholders.

Recommendation #1 will be challenging technically, politically, and from a personnel and time resource perspective. To be successful, there will need to be a well-defined IAM service and clear processes and support mechanisms in place for migrating from distributed directories to a central directory. There will likely be some hesitancy by groups or individuals to give up their distributed directory services as it will be perceived as losing autonomy or capability as well as changing existing business processes. Service transition preparation will help alleviate those concerns. If there are legitimate obstacles to using the central IAM service, there should be an exception request process in place. Also, to be successful IT personnel will have to be able to allocate the time to work with the IAM team to migrate information resources tied to distributed directories to the central IAM service.

Key Logistical Issues and Proposed Timeline

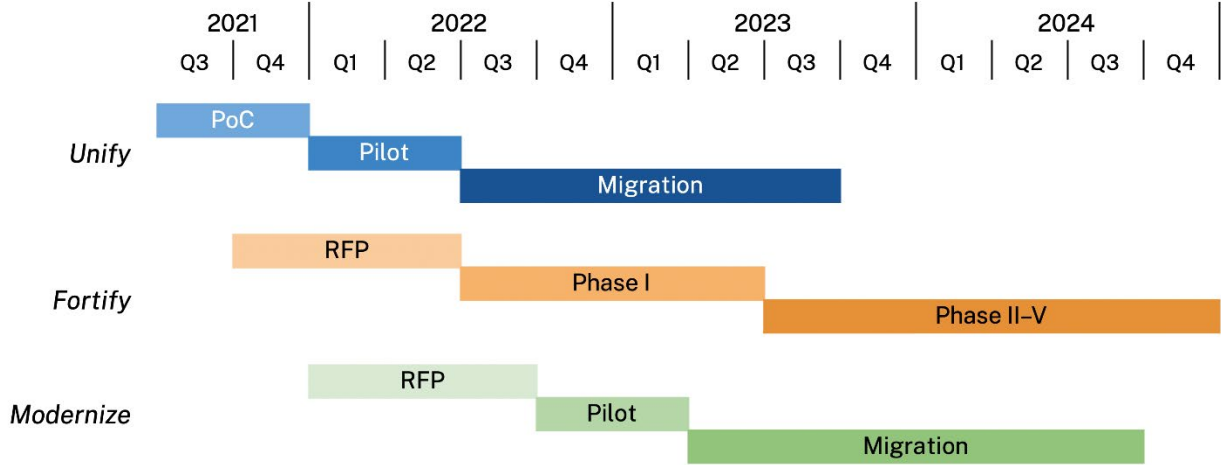
Rules/SAP needed, organizational structures impacted, any Academic impact, any Research impact. Performance metrics to showcase success.

Proposed Timeline

Based on previous consultant recommendations the following timeline is recommended.

5. Q4 2023 - Fortify — Replace the legacy Division of IT “Merge” (phase 1 of 5)

- 6. Q2 2024 - Unify — Active Directory consolidation complete
- 7. Q3 2024 - Modernize — Single Sign-On (SSO) Re-platform complete
- 8. Q4 2024 - Fortify — Enhance functionality of “Merge” replacement (phases 2 to 5)



Rules/SAPs

For the most part, the existing university security controls are sufficient. These recommendations should reinforce those controls and help improve the security posture of the university. However, as previously stated in recommendation #3, policies should be developed to govern the configuration and use of identities on SaaS platforms.

Impacts

The desired outcomes previously stated should ultimately positively impact the academic and research focuses of the university by simplifying their overall campus identity experience while increasing security. It is possible that during the implementation of the recommendations there could be short-term inconveniences as information resources are transitioned to the IAM service and/or their individual account credentials used are transitioned to the NetID.

Working Group 37: Subgroup 2: Endpoint Security

Recommendation Overview

Recommendation #3: Prioritize cybersecurity to ensure campus services are not compromised.

Strategic Considerations

Endpoints are usually the entryway of malicious cyber-attacks into an organization. Whether due to activities such as websites visited, emails read, or the many applications installed with vulnerabilities, securing endpoints throughout their lifecycle is one of the most important functions an organization can conduct to prevent detrimental cyberattacks from becoming successful.

One of the first steps in endpoint security is the proper management of endpoints. Endpoints in this context are network-connected compute devices, whether physical or virtual. A well-managed and hardened endpoint is much less likely to become an unwilling vector of attack into the organization.

Whether the goal is securing endpoints or managing endpoints properly, a distributed model will always fail. Endpoint security must be based on a standard set of tools used by all endpoints across the organization providing the needed correlated signal and information to the security team for both proactive and reactive measures. Security cannot be properly conducted in pieces or disjointed but rather must be as close to an ecosystem as possible. Using standardized tools for both endpoint security and endpoint management gets the organization closer to the desired secure ecosystem.

The most important step is always gaining visibility, and the first vital tool needed to gain visibility, is a single unified security asset management system that can automatically and continuously distinguish between “managed/secured” and “unmanaged/not secured” endpoints; moving the organization continuously closer to a wider security coverage via real-time data that displays TAMU asset locations and the state of each endpoint’s security and manageability.

By implementing these recommendations Texas A&M University will be taking an immense step forward towards a drastic increase in our security posture as well as simultaneously reducing and managing the cost of endpoint security and endpoint management.

The Recommendations are:

Implementation of centralized endpoint deployment workflows. These workflows will result in a more secure configuration from the onset, as IT cannot appropriately configure, secure, and manage what they are not aware of. These workflows should also include automated, initially-compliant defaults that are configured before startup as well as manual and automated validation of endpoint controls to ensure ongoing compliance with University, TAMU System, and State information security requirements. All endpoints, regardless of how or where they are provisioned should be registered with a centralized asset tracking system.

Standardize on a modern and centralized IT asset management system. This system would contain a comprehensive, real-time inventory of IT assets, controls on each asset, and software on each asset, in use by the university. This recommendation will also go a long way in creating a more streamlined and

less intrusive annual risk assessment process and audit preparedness for all colleges and divisions across the university. This solution would:

1. Largely rely on automated processes through connections with required endpoint and existing network visibility tools.
2. Also have a manual process of finding endpoints / IT assets as needed initially (specially for devices that have been “shelved” and/or not connected to the TAMU network).

Standardized on a set of effective and centrally managed tools for endpoint security and endpoint management. This would help provide the ability to centrally, efficiently, and effectively manage and secure endpoints. This will also allow for more effective monitoring whilst reducing cost due to duplication. These tools will continuously be evaluated and updated as new, better, and less expensive options hit the market. Where centralized tools cannot be deployed or used (i.e., industrial control systems or telemetric devices), subject matter experts should be available to assist with remediating and alternative controls. Validation that these tools are in place and functional should be a continuous and automated function. See proposed timeline.

Critical Dependency: *Implementation of a more modern and well thought out network infrastructure design that leverages identity and role-based network access controls, as well as purpose-built networks that are separated from the campus’ “general use” network. This would address security at the network level, allowing access based upon one’s role at the University, providing access only to networks and services one requires access to. This network would not allow end-users on the general use network to access devices they do not require access to, such as security cameras, HVAC systems, and other sensitive networks and/or devices.*

Logistical Issues Addressed

The proposed recommendations will be part of a 2-year program and implemented a college/division at a time. At the end of the 2-year Program (planning and implementation), the entire activity is continued year-over-year as an operational activity.

As the initial part of this program, a granular planning stage is needed to ensure each group of stakeholders and users as well as their “business” needs are taken into consideration before implementation and ensuring a mature exception process is in place. A major part of the planning phase is to ensure the right balance is held between securing endpoints and ensuring the business of the University is not disrupted.

Representatives from colleges and divisions will be part of the initial phase planning sessions and will also have a channel to provide continuous feedback from users and stakeholders informing how we should pivot at any given moment during this multi-phased program. The initial phase will cover a majority of end-user endpoints, and then another phase may focus on endpoints with more intricate requirements, and then possibly another phase to address any other endpoints.

The anticipated annual cost of the initial two-year program is estimated at \$300,000.00-400,000.00 per year. This cost includes the software licensing and needed staffing. However, as licensing costs of sunset tools drop off and staffing resources are identified across the University IT community, there will be a net reduction in overall and all-encompassing spend across the University.

Major Challenges Encountered and Resolution

An anticipated challenge will be convincing faculty and staff, that do not currently use any sort of managed or secured devices, to begin using secured and well-managed devices moving forth.

Another challenge is in the arena of procurement. University employees, whether faculty or staff, that do not follow appropriate purchasing processes and/or involve their IT personnel for the procurement of IT assets and services may be resistant to utilizing a unified and well-managed process for the procurement of endpoints and/or related services.

The human resources needed already, and to a large extent, exist in the TAMU security team as well as college and division IT teams. The resources that may not currently exist are in the area of licensing. There will initially be a need to purchase additional licenses for current central security and manageability tools that will be deployed to a larger audience. However as more endpoints begin converting to the usage of a centralized set of tools, they will discontinue the purchase of the many duplicative tools currently being paid for and used. The only additional licensing cost will be for devices that currently have no security or manageability tools at all.

Key Logistical Issues and Proposed Timeline

The University Controls affected are in the following categories:

- Access Control (AC)
- System and Service Acquisition (SA)
- System and Communication Protections (SC)
- Risk Assessment (RA)

These University SAPs and Controls will need very minor adjustment to indicate stronger language on the use of standard endpoint protection and tools.

Performance metrics will focus on:

- Time series Increase in visibility
- Rate of coverage
- Increase in blocked malware
- VOC (voice of the customer) surveys and results
- Reduction in the number of disparate duplicative tools

Proposed Timeline

- | | |
|---|---------------------------|
| • Resources identified: | June 1, 2022 |
| • Program design begins (tools and process identified): | August 1, 2022 |
| • Task force setup and feedback loop initiated: | September 1, 2022 |
| • Implementation for Initial College: | October 1, 2022 |
| ○ Lessons Learned and revisit of design | |
| • Phase two colleges implemented: | December 1, 2023 |
| ○ Lessons Learned and revisit of design | |
| • Phase three colleges implemented: | March 1, 2023 |
| • Year two repeat and review of entire program: | June 1, 2023-June 1, 2024 |

Working Group 37: Subgroup 3: Research Security

Recommendation Overview

Recommendation #3: Prioritize cybersecurity to ensure campus services are not compromised.

Strategic Considerations:

With over a Billion dollars in research expenditures, Texas A&M University conducts research across healthcare, policy, infrastructure, global health and security, energy, food and water, defense, and many other areas and industries. With such a large footprint in the national research landscape the many national, state, and private granting agencies and entities are requiring more and more stringent security controls.

Ensuring that cybersecurity and the security of research data and systems are properly accounted for in the grant proposal and the conducting of funded research can be a daunting and expensive endeavor, at times causing less competitive grant proposals by Texas A&M researchers.

To date there has not been an organized effort to advise and assist faculty across all colleges with their research cybersecurity and IT risk management needs by providing standard tools, programs, policies, and processes combined with close consultations.

The recommendations (section above) in this document are focused on solving the existing gap spanning all areas of research and colleges by providing researchers with the focused and practical resources, tools, and consultations they need to increase grant competitiveness, ensure compliance to granting agency and contractual requirements, as well as reduce overall duplicative effort and spend.

The Recommendations are:

1. Creation of a small team of Cybersecurity/IT Risk Management professionals dedicated to ensuring Texas A&M University retains and increases its grant competitiveness by:
 - Ensuring contractual and federal granting agency security requirements are being completely met. Security requirements by granting agencies are rapidly increasing and becoming more stringent.
 - Ensuring researchers have required, robust, and centrally provided tools and services that would go a long way in eliminating the need for technology duplication, grant cost duplication, and unnecessary consumption of researcher time and effort.
 - Providing advisory services to researchers where needed from pre-grant proposal to post-funding. This service will ensure researchers know and have access to the many robust security resources at Texas A&M and ensure all researcher security related needs are being met.
 - Create and manage a professional exception process that ensures the proper balance is held between required security controls/processes and the vital ongoing needs of researchers.
 - Focusing on reducing the cost for researchers when it comes to cybersecurity needs so that grant proposals can be more competitive.

2. This Research Information Security team will be small but have a deep understanding of both researcher needs as well as the cybersecurity arena. This team will utilize existing resources across campus and the system, in accomplishing it's mission.
3. It is also recommended that this team manage a Research Information Security Working Group or Task Force placed under the current IT Governance structure, aimed at continuously gathering feedback from researchers, keeping a finger on the pulse of research and researcher security needs, and pipelining that information towards the creation of new useful and improved tools, processes, and resources for researchers.

Logistical Issues Addressed

The anticipated challenges to these recommendations are minimal, as this will be a new service initially offered to researchers who choose to take advantage of it. The goal is to expand the usage of this service across the university by providing a tangibly effective service, garnering trust, continuous feedback, listening to the needs of researchers when it comes to cybersecurity, and translating all of that into resources, tools, advisory, and processes that benefit all researchers at Texas A&M. The feedback mechanism is indeed built into the recommendations.

Proper communication and marketing of the resulting services and resources to all researchers will play a major role in its adoption.

Major Challenges Encountered and Resolution

The resources needed for year one of this program will consist of two full-time employees who are well versed in cybersecurity as well as having a solid understanding of research across the university. These resources currently do not exist and will need to be hired.

The total annual cost for this program is estimated at \$350,000 which includes the two senior security resources and all anticipated software, hardware, and cloud licensing.

This program will remain lean and utilize existing teams and resources across security and IT in accomplishing its goals.

These two resources will also be organizing and managing a taskforce composed of researchers from across different colleges to ensure a continuous feedback loop that keeps this program and resulting services effective for all its intended stakeholders.

Key Logistical Issues and Proposed Timeline

Performance metrics will focus on:

- Rate of adoption
- VOC (voice of the customer) surveys and results
- Number of new resources provided to researchers and their effectiveness

- Reduction of required grant budgets by utilizing this program amongst researchers on an annual basis

Proposed Timeline

- Program design begins: June 1, 2022
- Resources onboarded and active by: August 1, 2022
- Program Beta Kickoff by: September 1, 2022
- Program in full swing and feedback loop active via task force by: October 1, 2022
- Program Review and revision: March 1, 2023

Working Group 37: Subgroup 4: Application Security

Recommendation Overview

Recommendation #3: Prioritize cybersecurity to ensure campus services are not compromised.

Strategic Considerations

Whether inhouse built applications or vendor purchased software, these applications and software in the thousands at Texas A&M are installed on our servers and devices, storing and transmitting research personal, regulated, health, and other types of data every day. Many of these applications on the TAMU network also connect externally to the internet and other institutions.

Application and software vulnerabilities are the second largest vectors of successful cyber-attacks. Just in the last few years we have seen some of the largest, infamous, and most costly compromises happen due to weaknesses found in software and product code.

Secure SDLC (Software Development Lifecycle) is now just as basic to security as Antivirus or Firewalls, and for good reason. At Texas A&M University, we have over 150 developers in IT and many more across the university in the form of students, graduate students, research assistants, etc. The hundreds of applications developed at Texas A&M and the thousands of software and products purchased from vendors of all sorts need to be vetted before going into production use and housing data.

1. Create a Secure SDLC program consisting of the following elements:
 - Identify and **procure Secure-SDLC enterprise level tools**. Without these tools it is not possible to ensure Secure development or assess the state of security of applications and software, at scale. Such tools are not cost prohibitive but are vital to this program.
 - **Employ Product Security or Application Security experts** who will not only run the program but also work collaboratively with university Application Developers to ensure the program is successful.
 - Create and maintain a **comprehensive secure-development training program**. This training program will be co-developed by Application Security experts and Senior Application Developers to ensure it adequately addresses all aspects of the secure-SDLC.
 - This program will **include a well-defined process and pipeline** for enterprise application and software assessment and secure-development.

This Secure SDLC program is intended to implement a mostly-automated pipeline ensuring the many critical and large security gaps in the thousands of applications and software used by Texas A&M are closed and we move rapidly towards a continuously shrinking attack surface on the application front.

Logistical issues Addressed

The proposed recommendations will be part of a four-phase process that:

- Phase 1: initially sets up the tools and resources needed,
- Phase 2: designs and implements a mature, versatile, and mostly-automated pipeline and process,

- Phase 3: goes through a rapid implement-fail-learn-redo phase with a diverse sample set of developers and applications
- Phase 4: Markets the matured program University and system-wide and subsequently begins full production activity.

The largest anticipated challenge is to ensure bottlenecks are not unintentionally created where they should not exist.

- The phased approach is intended to find areas in the process that can turn into a bottleneck and resolve them before going full production with the program.

The second anticipated challenge is adoption into the program by faculty and researchers. The key to addressing this challenge is two-fold:

- First to ensure the appropriate University SAPs and Controls require any application or software that will be installed on TAMU network and store or transmit regulated or sensitive data to have gone through this program and process.
- Second is to involve, as much as possible, and as soon as possible, the staff and faculty most impacted by this effort. Giving them the opportunity to offer input into the process.

Major Challenges Encountered and Resolutions

The largest anticipated challenge is to ensure bottlenecks are not unintentionally created where they should not exist.

- The phased approach is intended to find areas in the process that can turn into a bottleneck and resolve them before going full production with the program.

The second anticipated challenge is adoption into the program by faculty and researchers. The key to addressing this challenge is two-fold:

- First to ensure the appropriate University SAPs and Controls require any application or software that will be installed on TAMU network and store or transmit regulated or sensitive data to have gone through this program and process.

Second is to involve, as much as possible, and as soon as possible, the staff and faculty most impacted by this effort. Giving them the opportunity to offer input into the process.

Another challenge to this recommendation is overcoming the natural resistance most IT staff have towards change.

Interdepartmental coordination between various stakeholders will be key in adopting the recommended frameworks to fit the unique and diversified needs of the university.

Additional challenges may arise from outside resources such as contractors or others who develop systems that do not follow the prescribed security requirements and checks, proposed in the SDLC companion guide.

This could be addressed within contract stipulations and the security review process at the onset.

Key Logistical Issues and Proposed Timeline

- Develop a new internal policy and procedures such as:
 - A Secure Development Life Cycle (SDLC) Control and accompanying best practice guide to address the types of applications that can be developed, the platforms they can be developed in, how often they must be reviewed, and the step necessary to move them into a production environment (change management).

Implementing these recommendations will take nine to twelve months, while full adoption is expected to take an additional twelve to fifteen months. Upon completion the universities overall cybersecurity risk footprint will be greatly reduced. There should also be some small to moderate financial gains as costs associated with shadow IT are reduced.

- Phase 1: July 1, 2022 - Set up the tools and resources needed –
- Phase 2: September 1, 2022 - designs and implements a mature, versatile, and mostly-automated pipeline and process
- Phase 3: December 1, 2022 - a rapid implement-fail-learn-redo phase with a diverse sample set of developers and applications
- Phase 4: May 1, 2023 - Market the matured program University and system-wide and subsequently begin full production activity.

APPENDIX A: Supplemental Information
TAMU Identity of Tomorrow & Peer Comparison

Peer Institution Comparison

An Identity of Tomorrow Technology Whitepaper

*The Texas A&M Identity of Tomorrow initiative is centered around three pillars: **Unify, Fortify, and Modernize**. We are setting out to unify Active Directory services on campus, fortify identity management infrastructure using commercial-grade technologies, and modernize our single-sign-on (SSO) platform.*

Right-Sizing An Identity Team

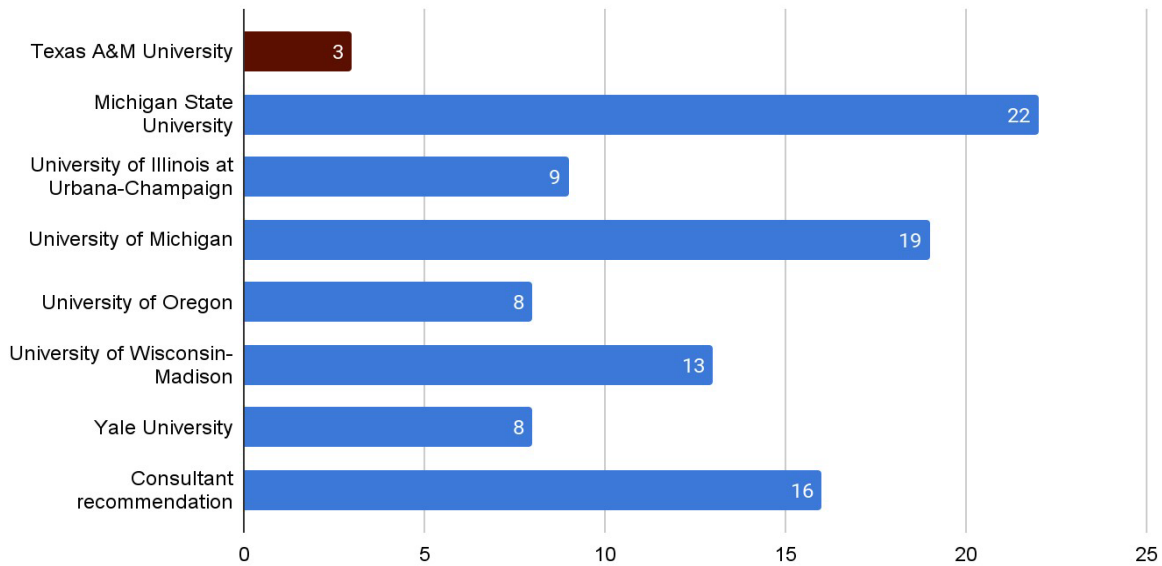
Understaffing a critical area like Identity and Access Management creates a significant security risk for the institution, and jeopardizes our ability to deliver effective technology services at scale. There is no perfect answer for how large a team should be, but we can leverage data from other university IAM teams to help us understand how IAM is managed in peer institutions. Furthermore, we have recommendations from expert consultants that indicate we are dramatically understaffed in key positions.

Roles & Responsibilities

Each university in the benchmark set had at least one:

- Senior engineer or team lead
- Developer
- Systems administrator (Active Directory)

FTE Count Comparison



Identity of Tomorrow Peer Institution Comparison

1

Data on peer institution staffing levels was gathered through an InCommon¹ community forum conversation. Each school except for Yale University included management of directory services (AD) as part of its Identity program and operated using a distributed or federated model of service management.

Consultant recommendations (Protiviti)

After a thorough current state analysis, our consultants noted that we were four FTE below an appropriate staffing level for current operations. Additionally, they recommended the addition of 10-11 *new* FTE in order to reach an appropriate staffing level for a steady state Identity program in the future. Of particular concern was the level of staff support available for Active Directory, particularly considering the recommendation to consolidate domains into a single, consolidated AD service for campus.

Conclusion

Based on this analysis, we have two primary recommendations:

- Increase FTE count to at least 9, meeting the median among our peer institutions

¹ InCommon is an Internet2 initiative.

- Move the primary responsibility for Active Directory and Azure AD to the IAM team

Although primary responsibility for Active Directory should be moved to the IAM team (*service ownership*), the overall management can still be shared with Systems Engineering, particularly with regard to the underlying infrastructure for the service. Considering how integrated M365 and Azure services are with AzureAD, a very close working relationship between the SYSE and IAM teams will be necessary to ensure success with those products.