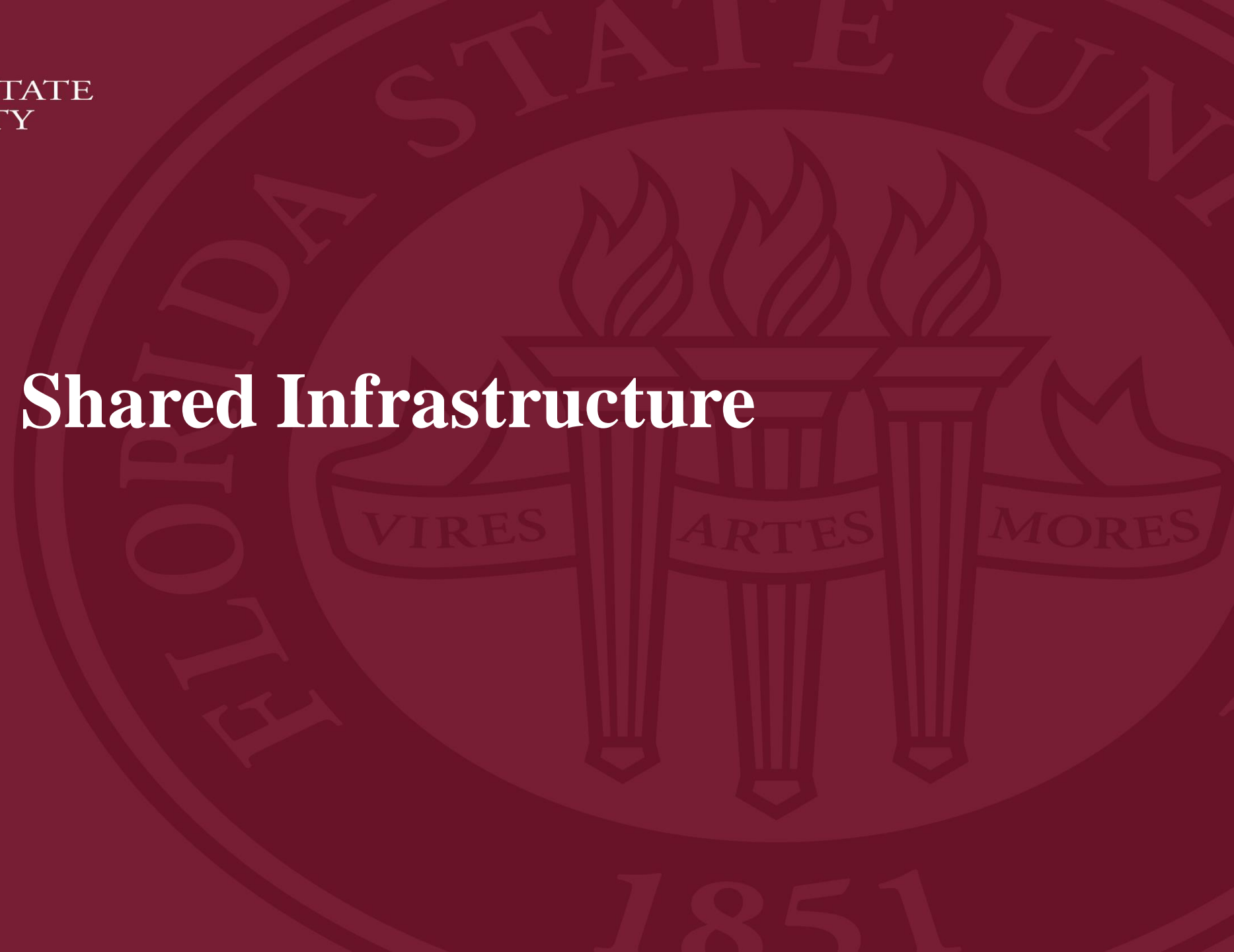




FLORIDA STATE  
UNIVERSITY

# Shared Infrastructure





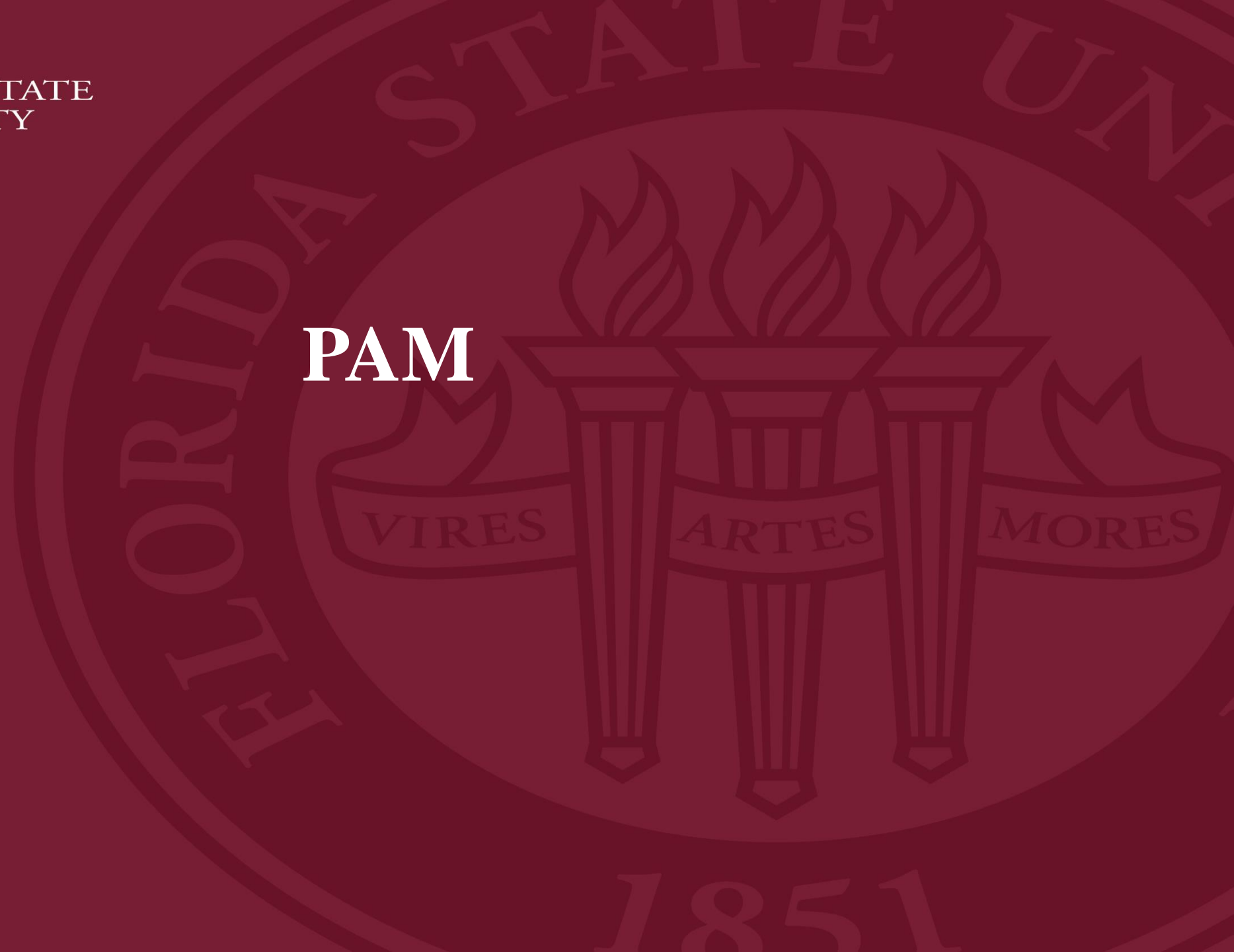
# Agenda

- PAM
- AWS
- IAM
- Network Update
- Cohesity



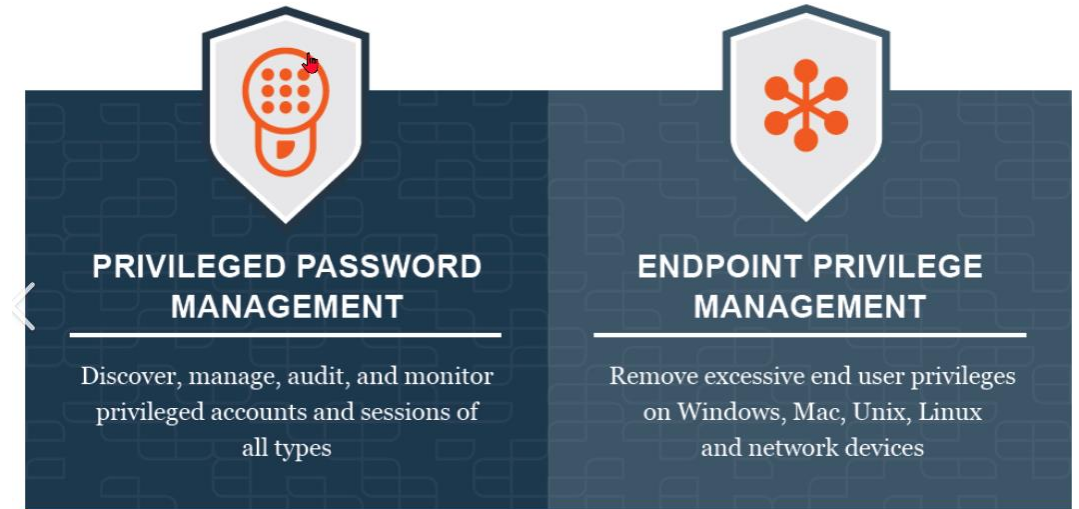
FLORIDA STATE  
UNIVERSITY

**PAM**



# PRIVILEGED ACCESS MANAGEMENT

- Beyond Trust cloud implementation
- PM CLOUD (Endpoint Privilege Management)
  - Implementation is in progress (CTS, IAM, CSIM)
  - Desktop Administration
- Password Safe (traditional PAM)
  - Implementation is in progress (IAM, CSIM, LEAS)
  - Manages privileged accounts
    - elevated permissions or access rights within FSU's systems or network
  - Linux, Windows, Network Devices, Databases, Applications Systems "managed" by ITS are being imported with active scanning
  - Associated Accounts management in planning
  - Departmental onboarding business processes in planning



- User Impacts
  - Desktop Administration
  - Password Vault
  - Modified Access Methods
  - More Secure Systems



# AWS

## Extending Production to the Cloud

Jose Rodriguez



FLORIDA STATE UNIVERSITY  
INFORMATION TECHNOLOGY SERVICES

# OVERVIEW

Goals

Network Design

Organizational Units and  
Account Structures

Engagement with Presidio



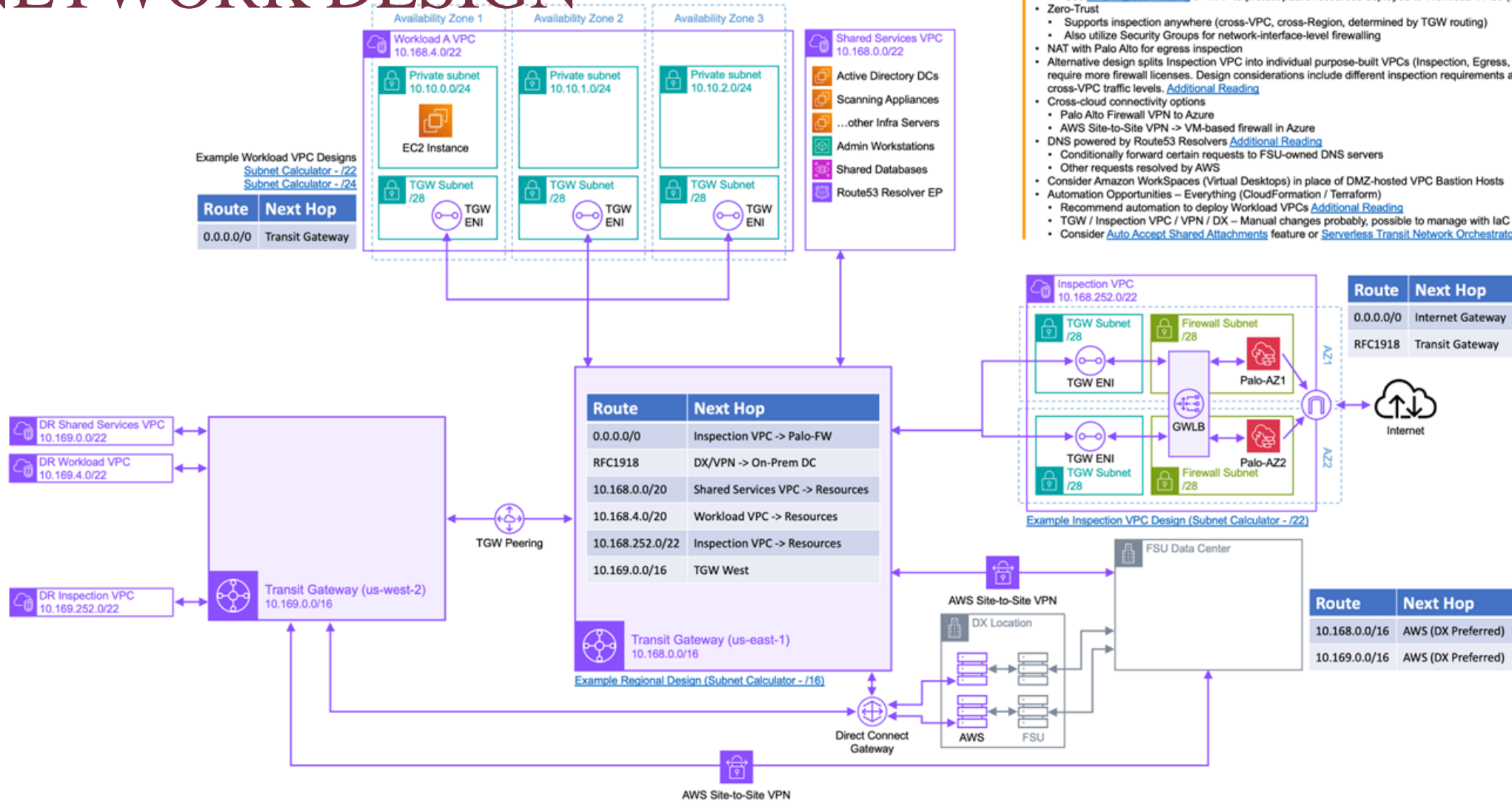
# GOALS

- Establish a foundation for extending our enterprise production systems to the AWS
- Facilitate Secure Research
- Set Standards for Cloud Deployments





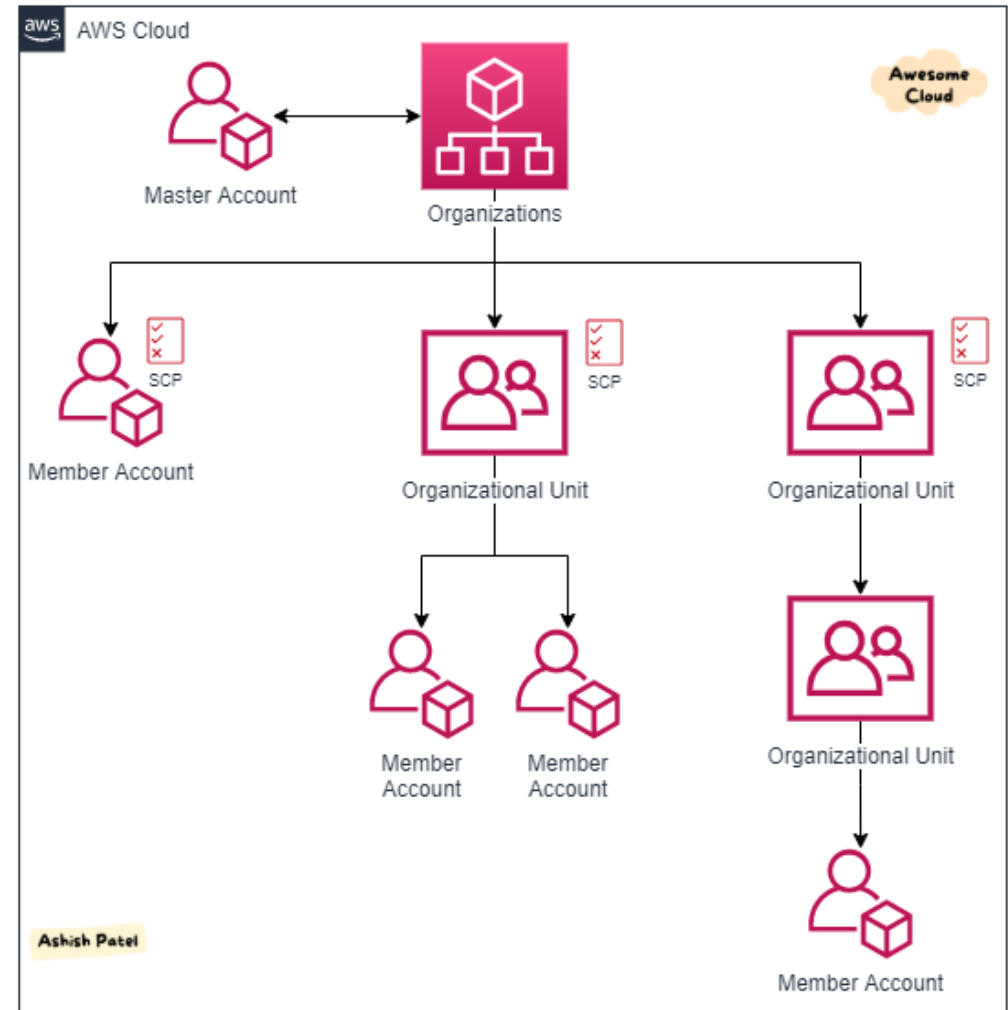
# NETWORK DESIGN





# ORGANIZATIONAL UNITS AND ACCOUNT STRUCTURES

- Organizational Units (OU) help you apply policies
- We set the framework for how to provision and manage accounts
  - Minimize account sprawl
  - Group related workloads to the same account
  - Organize by security and operational needs
    - Non-production vs production
    - HIPAA vs PCIDSS
  - Apply security at the OU rather than accounts
- Account Tiers
  - Sandbox
  - Non-production
  - Production



# ENGAGEMENT WITH AWS/PRESIDIO

- AWS Landing Zone Accelerator
  - Uses Cloud Formation or Terraform scripts to allow account deployment with different compliance requirements
- Facilitate fast deployment of secure accounts
  - Deployment templates for the following compliance:
    - HIPAA Research
    - NIST
    - PCIDSS



PRESIDIO®



# WHERE ARE WE NOW?

- Statement of work has been signed
- We anticipate starting end of April.
- Design Phase (2-3 weeks)
  - Infrastructure
  - Identity
  - Backup and Disaster Recovery
  - Operations
- Implementation (3-4 weeks)
- Pilot Migration (1-2 weeks)
  - HealthMPowerment Project







**IDENTITY ACCESS AND  
MANAGEMENT [IAM]  
MODERNIZATION PROJECT**

**Jose Rodriguez**  
**Shared Infrastructure Day**  
**Information Technology Services**

**March 5, 2024**

# AGENDA

PROJECT OVERVIEW

CHALLENGES AND  
OPPORTUNITIES

PROPOSED TIMELINE

PROJECT TEAM AND  
STAKEHOLDERS





ACCORDING TO THE 2023 CROWDSTRIKE GLOBAL THREAT REPORT, 80% OF ALL ATTACKS INVOLVE COMPROMISED IDENTITIES





# PROJECT OVERVIEW



The Identity and Access Management (IAM) project is focused on performing a comprehensive assessment and analysis of existing university and ITS IAM systems, policies, and associated business processes with the objective of developing a roadmap for implementing a more modern and scalable IAM solution at FSU.



The goal is to implement a solution and develop a program that is centered on operational improvement, efficiency and excellence, and a transformed and consistent student, faculty, and staff experience.



This effort aligns with our goal to advance FSU's cloud strategy and to establish identity-first security.



# CHALLENGES



Reduced security posture for the whole university due to shortcuts, decentralized identity management, uneven adoption of compliance procedures, and lack of rapid, accurate deprovisioning when necessary



Inflexibility in adding different kinds of users, including outside users



Delays in users' ability to access resources often result when manual workflows and approvals cannot be streamlined or easily orchestrated and overly complex systems are not easily understood



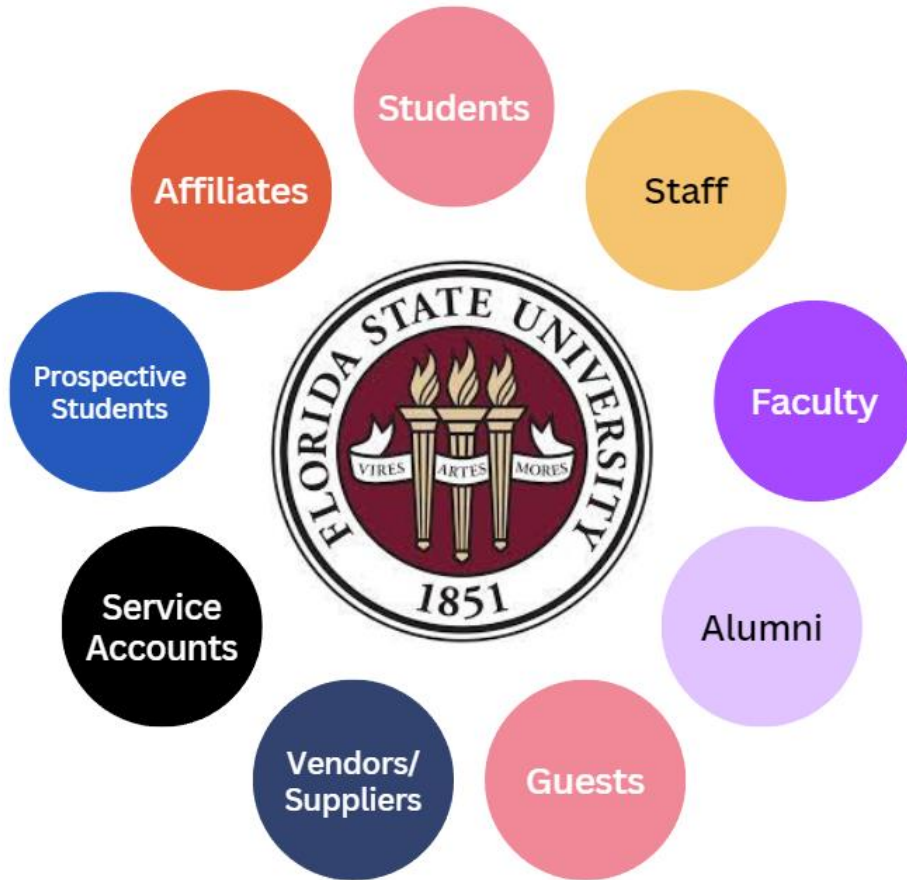
It is difficult to track and manage the lifecycle of a digital identity



Universities are the Most Complex Organizations



# VARYING TYPES OF USERS



FSU supports many different types of users with different levels of requirements

Varying user types for one person

Varying access levels

Varying life cycles

Varying software license needs

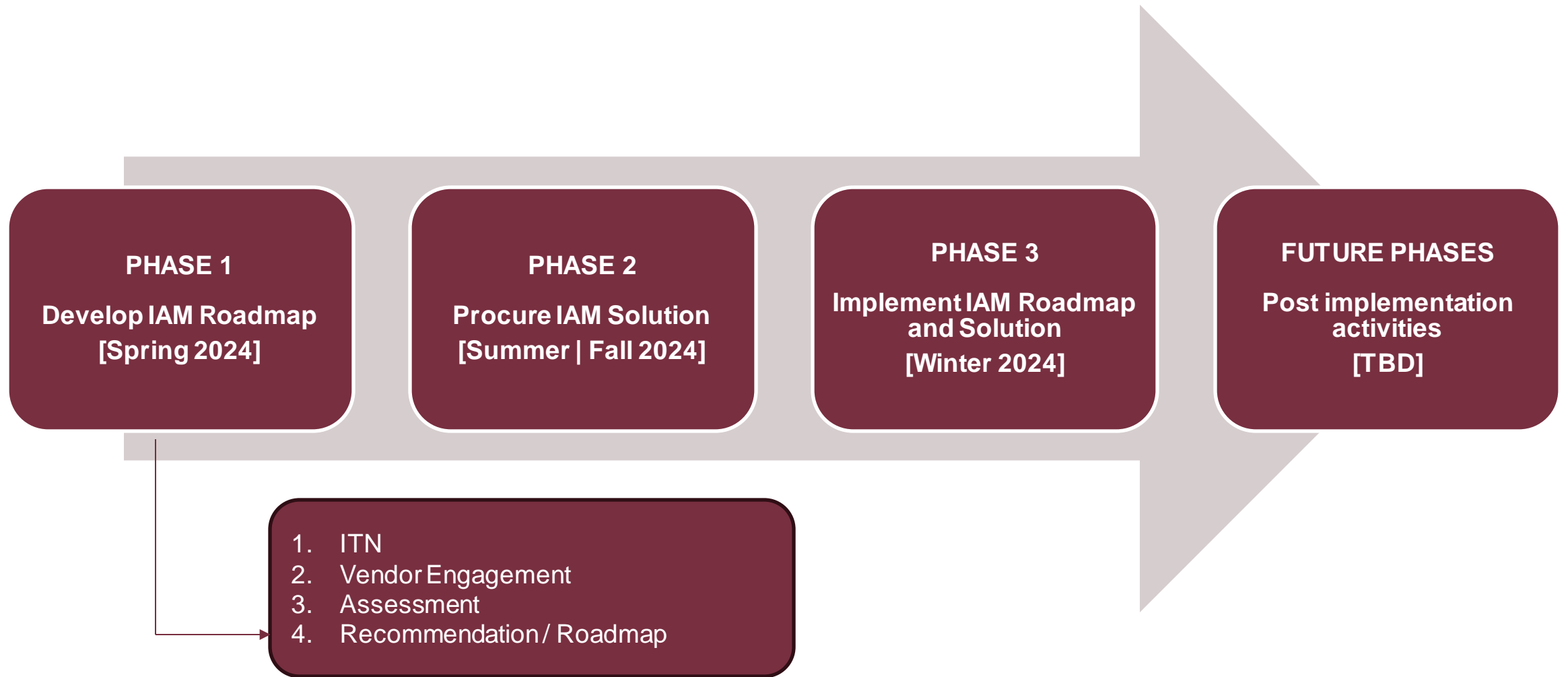


# BENEFITS / OPPORTUNITIES

- ✓ Align IAM efforts to business goals and outcomes
- 📅 Improved security and compliance (Identity-First Security)
- 👤 Streamlined tracking and management of user lifecycle
- 📈 Increased productivity and collaboration
- 😊 Improved user experience
- ☁️ Cloud capabilities and scalability



# SCOPE AND PROPOSED TIMELINE



# PROJECT TEAM



---

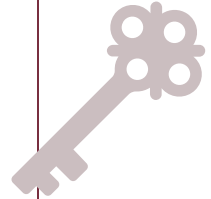
Bobby Sprinkle	ITS ELT
Andrea Dial	Project Manager
Jose Rodriguez	Enterprise Architect
Martin Schaefer	IAM Systems Manager
Diane Higgins	IAM Functional Lead
Corey Webster	CSIM
Leah Paul	ITS Student Central
Jonathan Banks	ITS Human Resources
Anna Piedrahita	PeopleSoft Security
Joe Brigham	ISPO
William Atkins	CTS
Jenn Specht	Data & Analytics

---





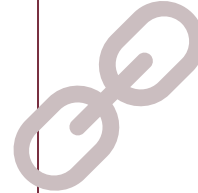
# STAKEHOLDERS



## KEY STAKEHOLDERS

Leadership, functional and technical project members

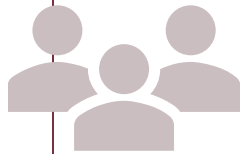
*Internal stakeholders of organization or project with direct role in project*



## STAKEHOLDERS

University offices, departments, and units

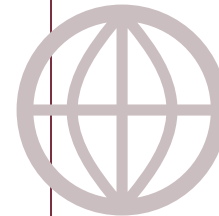
*Primary stakeholders directly impacted from project and may have direct or indirect role in project*



## CAMPUS PARTNERS

Departments, faculty, staff and students

*Stakeholders that will be impacted by project outcomes*



## EXTERNAL

Vendors

*Stakeholders outside organization with role in project*



# MORE INFORMATION

## Project web page

- <https://its.fsu.edu/iam>

## Project contact email

- [IAM-Project@fsu.edu](mailto:IAM-Project@fsu.edu)





THANK YOU!



# FSU BACKBONE UPGRADE

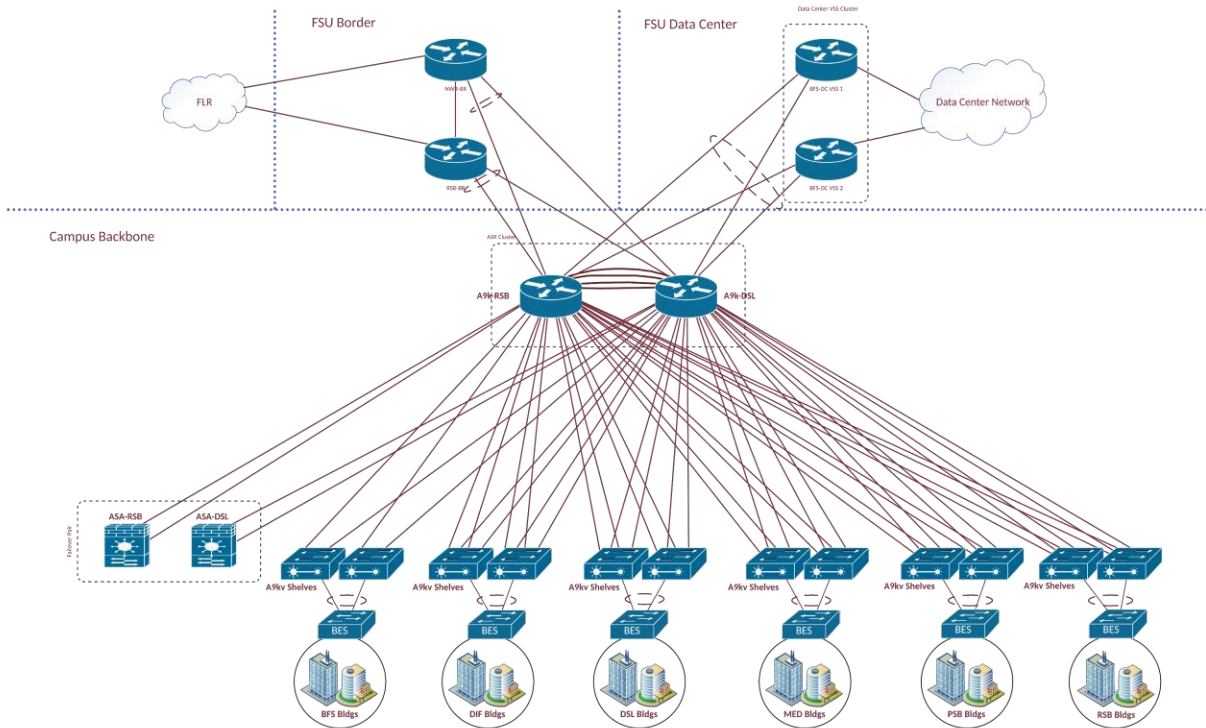


FLORIDA STATE UNIVERSITY  
INFORMATION TECHNOLOGY SERVICES

# OUT WITH THE OLD ... IN WITH THE NEW

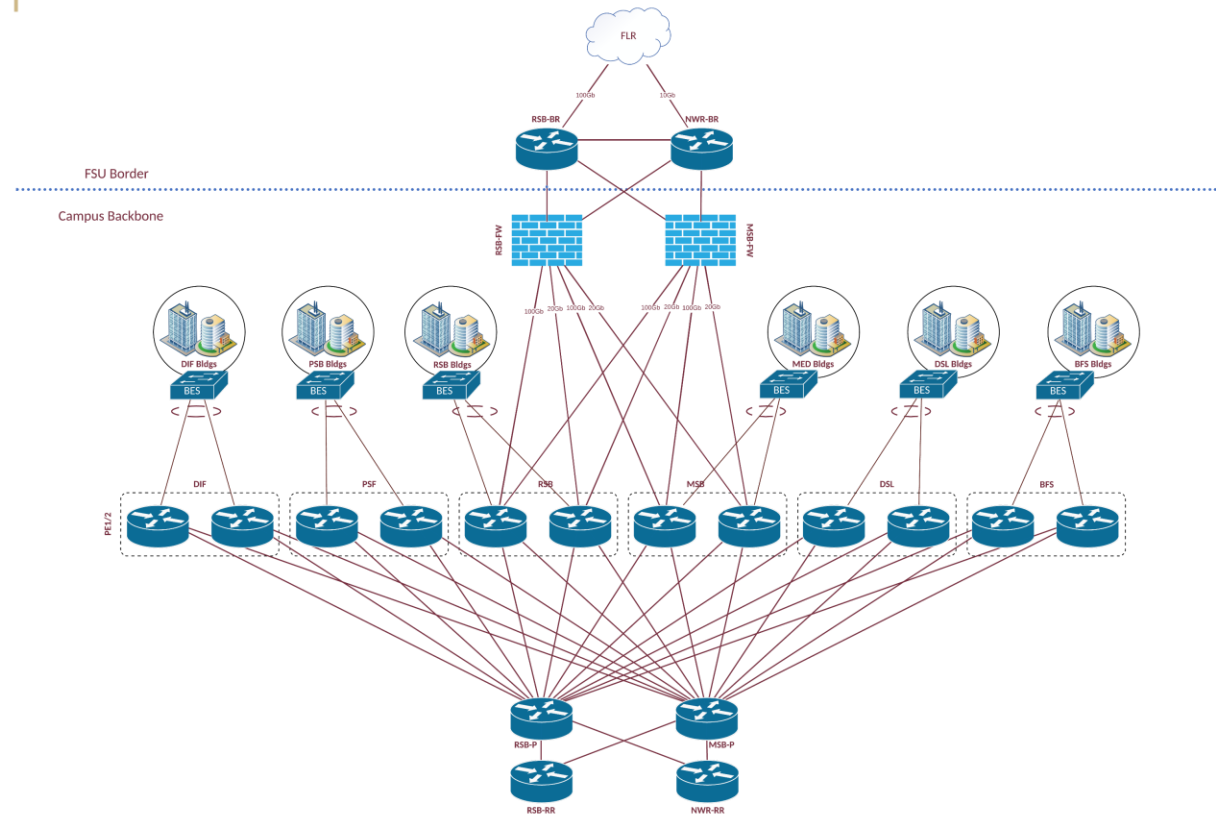
## 10Gb Backbone

TLH Campus: Backbone Router Physical Connections



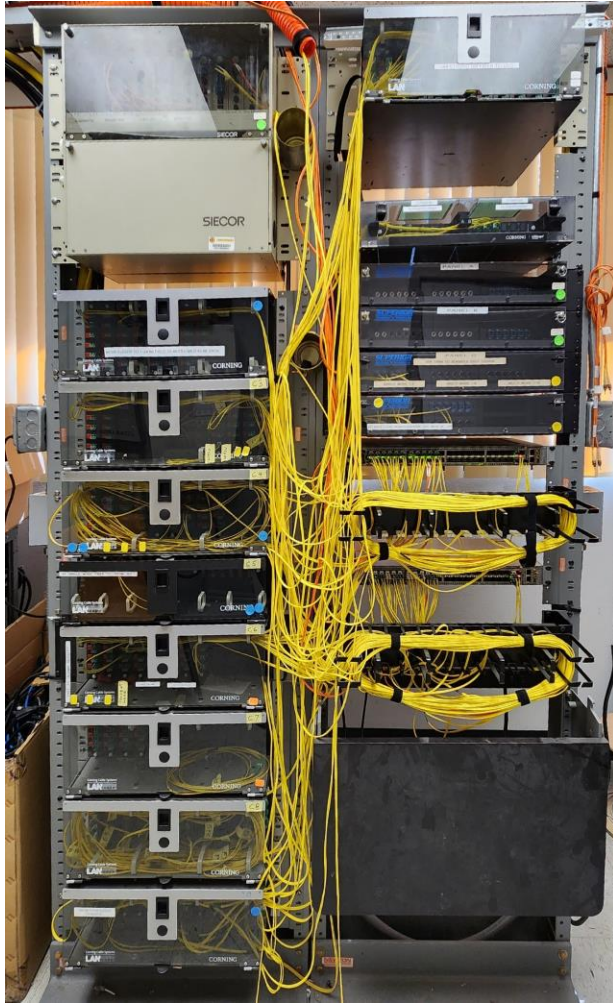
## 100Gb Backbone

TLH Campus: Backbone Router Physical Connections





# SLIGER NODE ROOM



No more of the Zeisler soup/olive cans?!?





# WHAT ARE WE DOING?

Cisco ASR 9000 (14)



Cisco NCS 55A1 (14) & Cisco Virtual Router Reflectors (2)

Cisco ASA 5585 (2)



Palo Alto 5450 NGFW (2)

Single mgmt interface



Manage 14 individual routers

Cisco Security Manager



Panorama

62RU rack space



19 RU rack space

33,050 lines of router code



186,572 lines of router code

35,700+ lines Cisco ACLs  
(permit, deny, remarks)



3,500-4,000 unique Palo Alto policies!








MPLS backbone



EVPN



# WHAT DO WE GET?

10Gb backbone links		100Gb backbone links
Most bldgs: 2x1Gb		Most bldgs: 2x10Gb (some to 2x40Gb or 2x100Gb)
ExpressLane Expansion		Extending SDMZ VRF into backbone
VLAN flexibility		VLAN/prefix can exist in multiple locations
FW throughput		ASA: 40Gb/s; 20Gb/s w/ inspection PA: 200Gb/s; 189Gbps w/ inspection
FW sessions		ASA: 350K new/sec; 10M concurrent PA: 3.6M new/sec; 100M concurrent
NGFW		L7 firewall; recognize apps, can function as IPS



# WHAT'S NEXT?

- Automate all the things on the backbone!
- Test IP mobility throughout the EVPN backbone
  - Wired & wireless
- Push EVPN solution into buildings for RBAC at switch port?



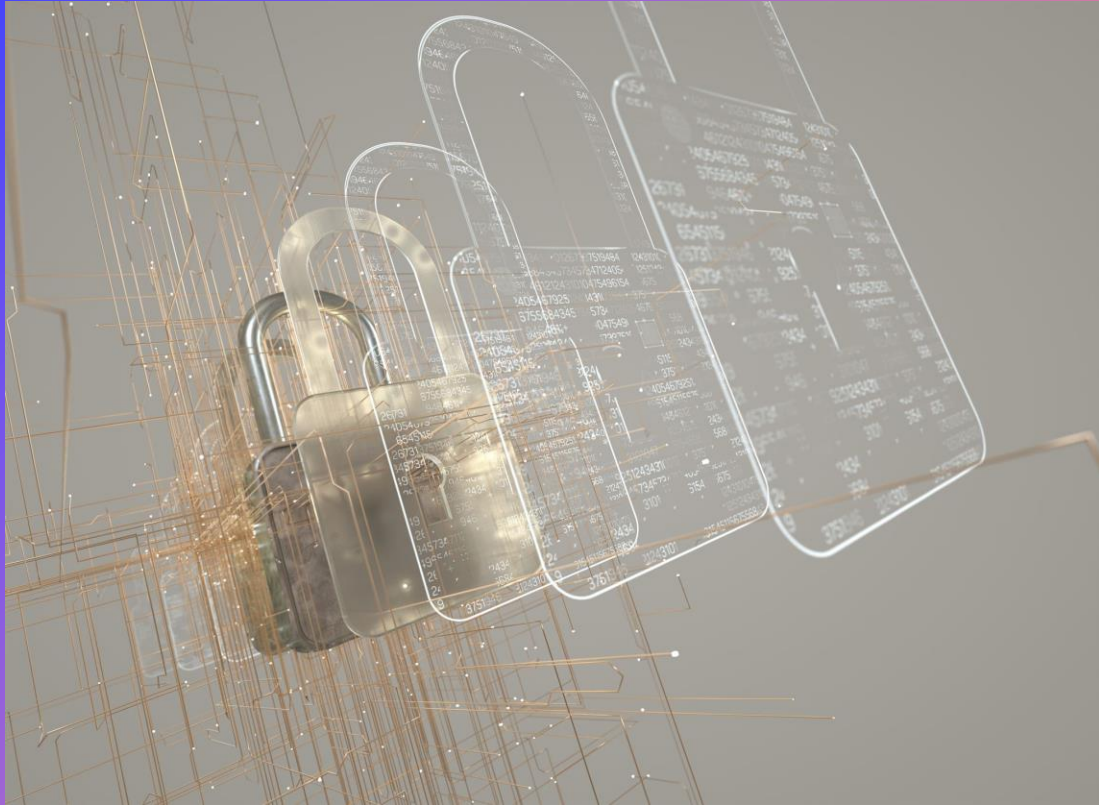
ANSIBLE



# COHESITY IMMUTABLE BACKUP



FLORIDA STATE UNIVERSITY  
INFORMATION TECHNOLOGY SERVICES



# Immutable Backups vs Mutable Backups

- Immutable backups are read-only copies of data that cannot be modified or deleted.
- Mutable backups are writable copies of data that can be modified or deleted.
- Mutable backups are targeted for deletion during a ransomware attack.
- Immutable backups provide an additional layer of protection against ransomware attacks.
- Immutable backups are less susceptible to accidental deletion or modification.



# Cohesity

- Immutable file system: backup is kept in an immutable state it is never accessed directly only a copy of the backup is ever made available.
- Datalock which uses a worm like technology, which means write once read many. This helps achieve a higher order of immutable backups.
- MFA integration to help mitigate phishing schemes and password hacks.





# Campus wide rollout

- New Cohesity service rolled out by end of April.
- Will be dedicated for use by our campus partners.
- Pricing options:

Immutable backup with only on prem storage - monthly charge of \$65.75/TB

Immutable backup with additional AWS offsite copy - monthly charge of \$124.50/TB





FLORIDA STATE  
UNIVERSITY

Questions?





FLORIDA STATE  
UNIVERSITY

# Thank You!

