Secure Research Computing

August 2022

University of Colorado **Boulder**

Secure Research Computing Introduction

1. Boulder campus Secure Research Computing - journey to CMMC – how we are getting there
2. Lessons learned on our journey so far

Secure Research Computing Mission

Provide secure research storage, networking, computing and consulting services that address researchers’ needs for compliance with federal regulations while also enabling secure collaboration.

Background - Research-driven demand

Historical demands – ***self-attesting***:

- NIST 800-171
- DFARS 7012
- Executive Order 13556 "Controlled Unclassified Information”
- HIPAA
- FERPA

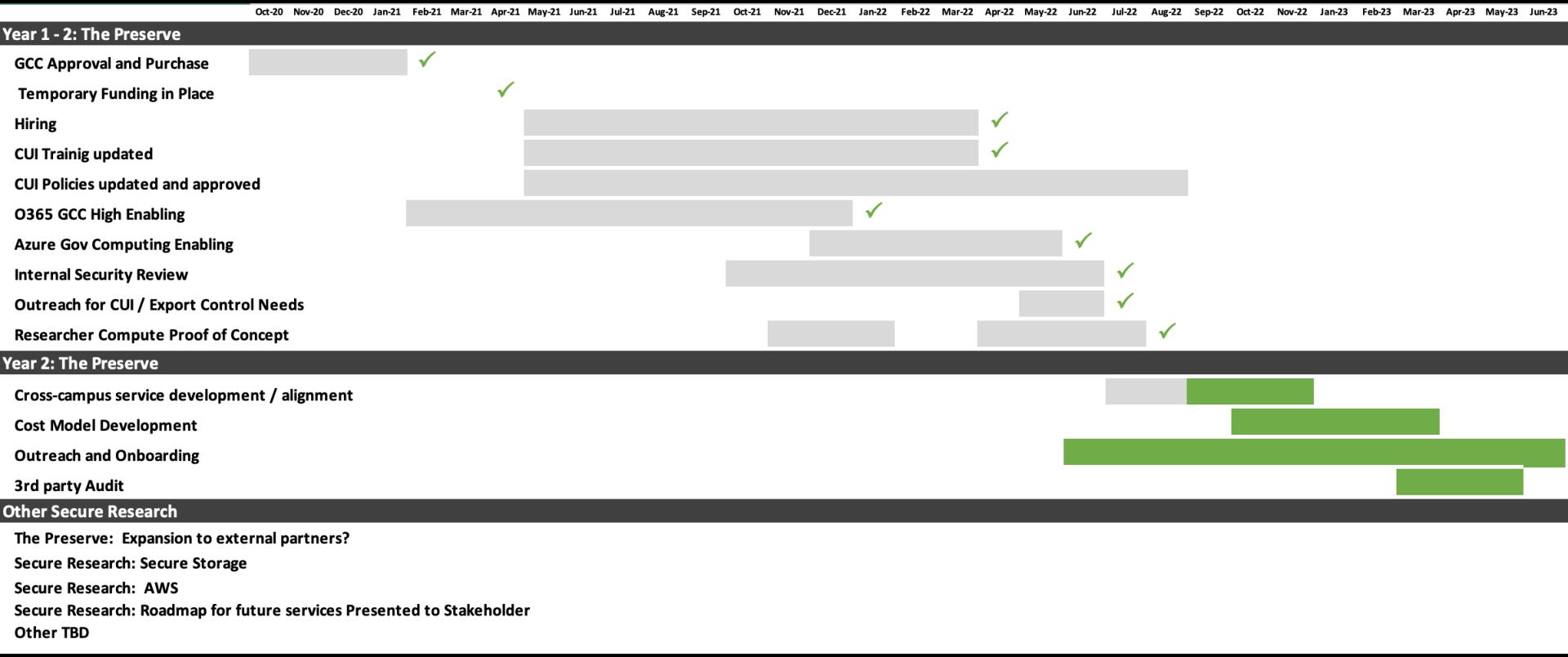
New emerging requirements – ***external certification***:

- Cybersecurity Maturity Model Certification

Boulder Campus response to CMMC – The Preserve

Use Case	Solution (Preserve components)	Who benefits
Send secure (encrypted) highly confidential messages to external partners	Office 365 GCC High - Outlook 	✓ Principal Investigators ✓ Other Researchers ✓ Sponsors ✓ Collaborators ✓ Compliance teams ✓ Research supporting staff
Collaborate on highly confidential research work products (status reports, findings, budgets)	Office 365 GCC High applications 	
Build and run researcher infrastructure (e.g. servers, databases) and applications (3rd part, custom) that handle highly confidential data	Azure Government CU Boulder Landing Zone	

Journey


Oct-20
Nov-20
Dec-20
Jan-21
Feb-21
Mar-21
Apr-21
May-21
Jun-21
Jul-21
Aug-21
Sep-21
Oct-21
Nov-21
Dec-21
Jan-22
Feb-22
Mar-22
Apr-22
May-22
Jun-22
Jul-22
Aug-22
Sep-22
Oct-22
Nov-22
Jan-23
Feb-23
Mar-23
Apr-23
May-23
Jun-23
Year 1 - 2: The Preserve
GCC Approval and Purchase
Temporary Funding in Place
Hiring
CUI Trainig updated
CUI Policies updated and approved
O365 GCC High Enabling
Azure Gov Computing Enabling
Internal Security Review
Outreach for CUI / Export Control Needs
Researcher Compute Proof of Concept
Year 2: The Preserve
Cross-campus service development / alignment
Cost Model Development
Outreach and Onboarding
3rd party Audit
Other Secure Research
The Preserve: Expansion to external partners?
Secure Research: Secure Storage
Secure Research: AWS
Secure Research: Roadmap for future services Presented to Stakeholder
Other TBD

The Preserve Computing Infrastructure

Shared Services:

- Identity and Access Management
  - Request for access form and process – tied to governing business processes
  - Separate credentials from everything else
- Managed virtual desktops
- Security monitoring
- Security Auditing (OIT-Information Security)

Research Project-Specific Services:

- Isolated subscriptions – each research project's compute infrastructure is isolated
- Managed Azure Virtual Desktops
- Security Information and Event Management

Researcher Responsibilities

Compliance - general:

- CUI training for self and staff / team
- Ensure team members, collaborators meet compliance requirements for projects and proposals
- Follow access review and removal procedures
- Follow required government CUI markings where relevant

Compliance – Computing Infrastructure:

- Follow software vetting guidelines
- Follow guidelines and standards for self-written software
- Plan and manage infrastructure costs (supported by OIT and Microsoft)
- Follow change management procedures
- Ensure 3rd party applications are patched and current
- Support incident investigations as needed

Lessons Learned

Staffing

- Hiring was difficult amidst pandemic and continues to be a challenge.
- Role clarification is ongoing as we stand up new services.
- “Swivel-chair” approach between environments presents workload, context-switching and responsiveness challenges.
- Mixed results using vendors to help with staffing capacity challenges during hiring delays.

O365

- Sensitivity labeling end-user experience
  - Explaining the role of the sensitivity labels to end-users is challenging
  - Request for Outlook plugin for CUI came in from one tester
- Access to only browser version of apps proved to not be sustainable -> implementation of virtual desktop infrastructure.
- Acceptance of Microsoft platform
  - Mac and Linux users not used to using Windows machines
  - Request for Linux as a desktop vm presents user acceptance challenges.

Lack of Azure Gov Feature Parity

- Several missing Sentinel connectors – e.g. storage accounts.
- Missing firewall/NSG FQDN tags.
- Still no support for Azure AD joined AVD hosts with FSLogix profiles. Prevents use of features like single-sign-on across MS apps.
- AVD auto-scaling not available.
- Fewer instance sizes available and lower compute limits.
- No "request files" feature in OneDrive – would be better if this could be made available via conditional access policy by domain for example.
- Mix of gov-specific and public endpoints that need to be allowed and managed. See US gov GCC endpoints.

Identified Need of Separate Ticketing System

- Per compliance guidelines, system information is to be treated as CUI which means we needed to find another ticketing tool:
  - User emails help system with specific system information
  - Technical teams need to share system information to implement change requests, share technical details on requests/incidents (assumes urls in environment are system information)
- Azure devops not available in Gov
  - Need to explore purchasing separate Fedramp ticketing system (MS Dynamics, ServiceNow Fedramp)
  - Maintaining separate products for change/incident and repository management

Challenges Building an "Offline" Environment

- Usability: Disabled clipboard between environments
- Application licenses management and costs (e.g. Acrobat Pro)
- Data ingress: experimented with multiple designs which have varying costs and risks.
- Development: most tools expect access to Github, even the Azure portal

Compliance is Complex

- Compliance includes Business Processes which makes serving multiple business entities (campuses, universities) challenging – but not impossible
- Avoid over-documenting – less can be more
- Self attesting on compliance is very different from preparing for an external audit
- Crawl-walk-run approach if you have time can help teams get better at interpreting controls and applying them over time
- Threat modeling and risk assessment framework and skills should be developed with training and matured
- Investing in technical security skills training recommended - to improve conceptual understanding and continue to establish a security mindset
- A highly secure environment comes with a higher cost and may not fit budgets for all confidential and highly confidential data classifications

Other - Miscellaneous

- Purchasing process took a long time
- Went through 2 unsuccessful attempts to get a .gov domain name
- Scaling question for AVD's
- Funding model and allocating costs could become complex
  - GCC High licenses – fund centrally from department budgets?

Vision for Years 2 - 3

A researcher …

- Understands the cost of building and running compute resources in the environment.
- Understands what costs should be built into their proposals vs which services are provided by the campus.
- Has more than one secure computing and storage option for different levels of compliance requirements.

Plan for Years 2 - 3

- ❑ Data ingress design and build
- ❑ Automate core infrastructure and MVP (Infrastructure as Code)
- ❑ Develop cost model for core infrastructure in Azure Gov.
- ❑ Provide training (via vendor or internal) for calculating and managing project-specific infrastructure costs.
- ❑ Develop at least one other option for secure storage based on researcher inputs and available funding.
- ❑ External audit.

Q&A