Our Presentation

- Introduction of UMD team
- UMD’s Answer to Campus Call for CUI
- How Does CUIE Work
- Demonstration of Our Solution
- Lessons Learned
- What’s New
- Questions and Answers
Who Are We…

- Division of Information Technology Research Technology Services
- Provide consulting and support to our research community
- Closely collaborate with:
  - Division of Research
  - DIT Security and Compliance,
  - Libraries and Research Commons
  - Departmental IT support teams
UMD Research Technology Team

- Samuel Porter - Associate Director of Research Computing
- Sheila Zellner-Jenkins – Sr. Research Technology Analyst
- Eric Byrd - Research Technology Engineer
- April Patterson - Security Compliance Analyst
A UMD CUI SOLUTION…OUR JOURNEY

- 2017-2018: DFAR 252.204-7012 begins appearing, discussions begin with School of Engineering around solutions
- Spring - Fall of 2019: Strategic planning and decisions
- Winter of 2019: Implementation begins
- Spring of 2020: Forming a team, writing the SSP, and creating our processes
- Summer of 2020: Launch of the system
Critical factors in solution selection:

- Scalability
- Cost
- Purpose-built for security
- Manageable by a small team
- Knowledgeable and flexible vendor

*End-User Experience*
A UMD CUI SOLUTION...OUR JOURNEY

- Hyperconverged cluster in a secure section of our data center
- Tera Insights' tiCrypt software solution to provide secure virtual machines and encrypted file storage
What is Tera Insights tiCrypt…

- University of Florida and Tera Insights partnered to develop tiCrypt
- Purpose built for compliance with NIST 800-171, 171b, and 800-53
- Designed specifically to support university research
- Combines secure file sharing (Dropbox like) with secure processing (VMs) all in a web interface
How the User Access CUI

Access CUI Environment using a VPN, your passphrase, and a Private Key that encrypts your files.
User View
Inside Our CUI Environment

- Components of Secure CUI Environment
  - Vault
    - File uploading and downloading
    - File Sharing
  - Secure Virtual Machine
    - Create a project virtual machine
    - User Management for user cui environment
  - Home Drive
    - Create a secure virtual drive attached to virtual machine
    - Secure virtual drive for storing data during data analysis process
CUIE System Demo
End User Wants CUI

- Researcher Request
- Certification of CUI Data
- Secure Virtual Machine Image Created
- Secure Virtual Environment Created
Our CUIE “Backend” Management

- Microsoft Development Tool Server
- SPLUNK (SIEM)
- VEAMM/ISILON DATA BACKUP AND STORAGE
- NEXPOSE RAPID 7

Management System
CUI COMPLIANCE TRACKING

- Onboarding and Personnel Verification
- Training
- Inventory
- Vulnerability Scanning
- Logging
- tiCrypt Audit system
Auditing Our CUI Environment

- tiCrypt Audit System auditing tasks
  - User login and logouts
  - user storage usage
  - Privileged user activity (system administrators)
  - User upload, download and deletion of data
  - Overall monthly user activity summary
  - Security Breach Activity (critical alerts)
CUIE Audit Demo
OUR IMPLEMENTATION HURDLES

- System Security Plan Creation and Approval
- Manual creation and migration of virtual machine images to new environment
- Streamlining the image creation and migration to tiCrypt
- Software license
WHAT’S NEXT...

- Real-world SSP feedback
- New DFAR rule implications and action items (Self-Assessment)
- System Automation and Enhancements
- CMMC Level 3 certification
Q/A

Want to learn more?
Contact us at
it-research-consult@umd.edu