CEAS Secure Computing Discovery
& Inventory

University of Colorado **Boulder**

Action Plan Development Phases

Phase 1: Organizational Unit Inventory & Discovery

- Collect computer and server inventory data
- Assess computers: determine Secure Computing status or actions

Phase 2: OIT Observation & Summarization

- Validate workbook data summarization & roll up
- Provide Security observations, risk identification & recommendations

Phase 3: Unit Secure Computing Plan Development

- Unit level to define plans for computer replacements or rebuilding to enroll computers
- Review unit level impact to budgets and resourcing to meet Secure Computing adherence

Phase 4 On-going monitoring

- Consultation with units, health assessment
- OIT to Develop and then monitor dashboard
- Unit Leadership to attest Unit level alignment to Secure Computing Campus standards

Secure Computing Action Plan Timeline

Fall 2024	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	June	July	Aug	Spet	Oct

Phase 1

Inventory and Discovery

Use Unit data list for Computer and Server on the Teams

OIT will support with taking servers offline

Phase 2

Data Review

Phase 3

Unit Secure Computing Plan Development

- New Computer
- Rebuild Computer
- Dispose old computer
- Server not yet Complaint

Phase 4

On-going Monitoring

OIT Unit Consultation

Be confident. Be inspired. Be a leader.
Be Boulder.

University of Colorado **Boulder**

Process: Secure Computing Action Plan Development

Phase 1: Inventory & Discovery

Fall 2024 Oct.-Jan

- Unit Leader identifies resources
- OIT Invites resources to Unit Teams
- OIT Hosts Action Plan training
- Unit starts Inventory & Discovery
- Review employee data
- Collect Computer Inventory data
- Assess Computers SC capable
- Collect Server Inventory data
- Notify Team Completion

OIT: Supports Units with Training, Office Hours & Support model intake form

Phase 2: Data Review

25 Feb-Mar

- OIT Validates Workbooks
- Review Summary Statistics
- Identify Recommendation

Phase 3: Unit Secure Computing Plan Development

25 March- Aug

Build Computers & Servers Secure Computer Action Plan

- New Computer Needed
  - Identify # New Computers Needed
  - Review budget impact with Budget person
  - Set quarterly targets for repurchase
- Rebuild computer
  - Identify # Computer Rebuilds needed
  - Set schedule with IT support for rebuilds & enrollment
- Dispose of Old Computer
  - Submit computers to Property Services for Disposal
- Servers not yet compliant
  - Ensure departmental servers are aligned to Server Standards

OIT and Unit Consultation

Phase 4: On-going Monitoring

Aug – Oct

- OIT: Building Secure Computing Dashboard
- OIT: Provide on-going progress updates
- Unit Leadership: Ownership for Computers & Servers Secure Computing Action Plan
- Unit Leadership: Attestation