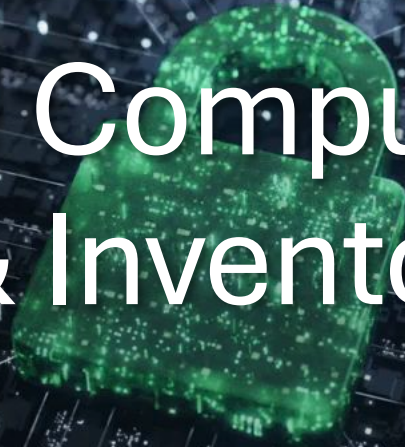


# CEAS Secure Computing Discovery & Inventory



# 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

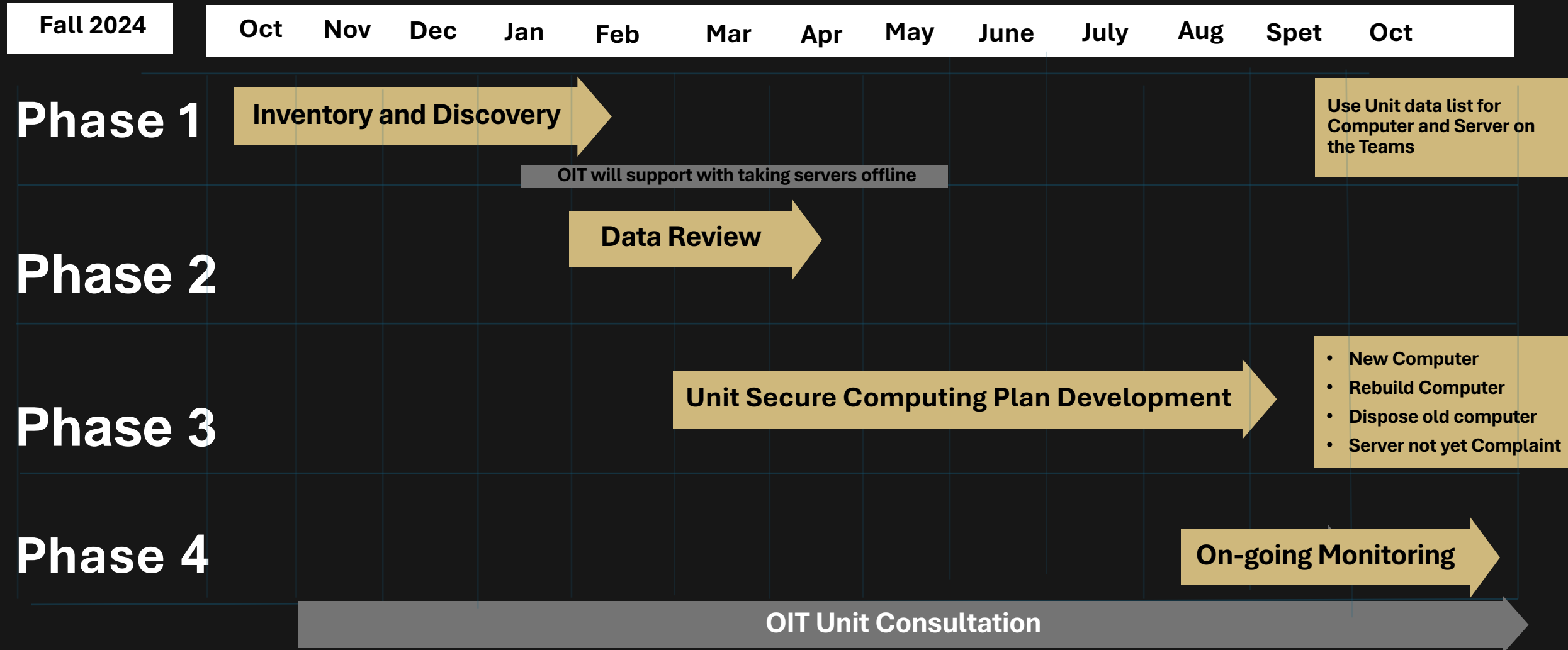
- Unit level to define plans for computer replacements or rebuilding to enroll computers
- Review unit level impact to budgets and resourcing to meet Secure Computing adherence



## 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



# Process: Secure Computing Action Plan Development

