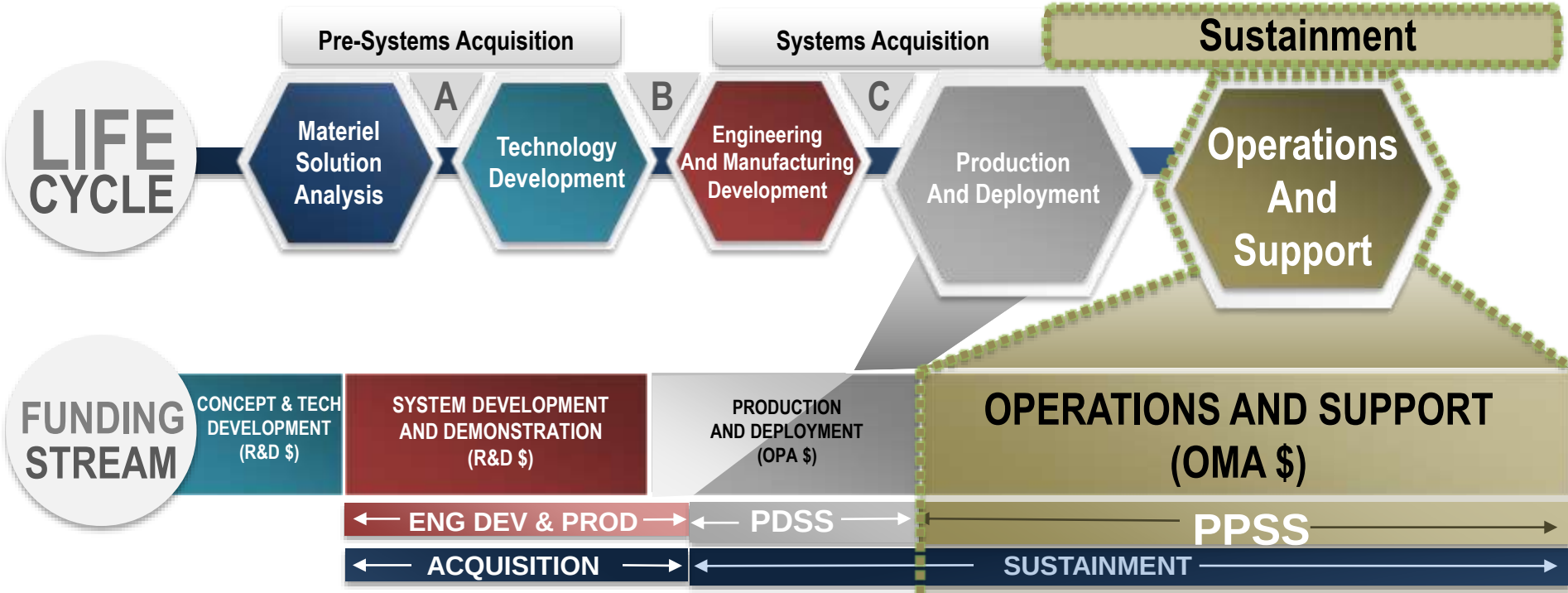
Cyber Security Requirements

From a Software Sustainment Perspective

February 25, 2015

Mr. Larry Muzzelo
Director, CECOM SEC

Our Role in the Acquisition Lifecycle



Software Acquisition Support – CECOM provides software engineering technical expertise as matrix employees to PMs. This support includes defining software requirement, overseeing software testing, performing configuration management and guiding acquisition decisions to reduce life-cycle support costs.

Post Deployment Software Support – From the point a system is provided to the First Unit Equipped (FUE) to the end of production (there are exceptions – this is the general rule). Funding is the responsibility of the PM and generally funded with OPA or OMA.

Post Production Software Support – Starts first year after production ends until item divested by the Army. Funded with OMA from Depot Maintenance (Army G4) accounts.

Post Production Software Support (PPSS)

Description:

The processes, procedures, people, materiel, equipment, facilities and information required to support, maintain and operate a system's software

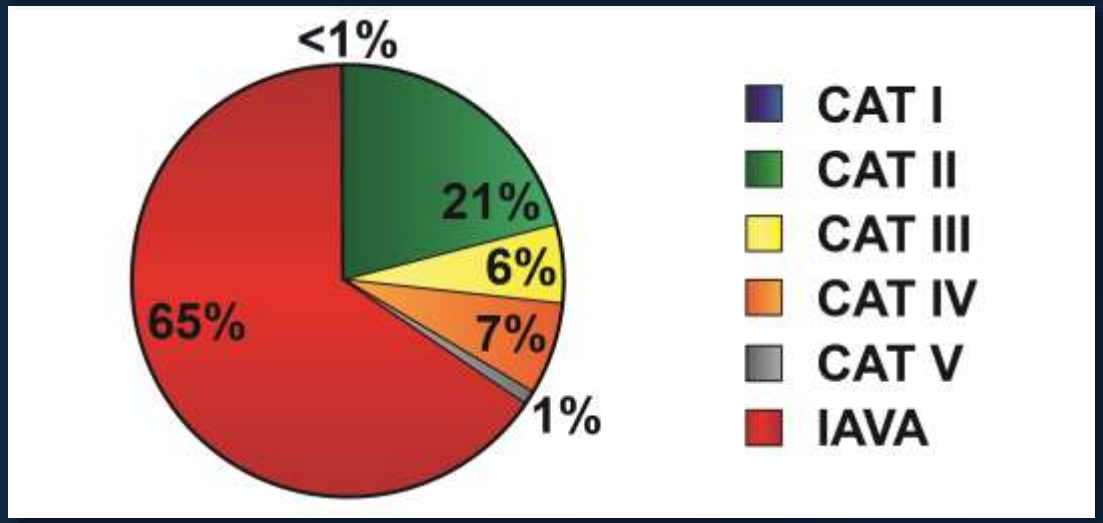
Activities:

- Fixes to address Information Assurance Vulnerability Alerts (IAVAs)
- Resolution of anomalies preventing mission accomplishment
- Changes to support operational needs or environment
  - Responding to new threats or requirements
  - Maintaining interoperability with other changing systems
  - Accommodating new weapons, systems or munitions
- Field Support
- Acquisition & management of COTS software licenses

Software Security Patching in PPSS

Fielded PORs receive IAVA updates through PPSS

FY14 PPSS Requirements



Vendors IAVAs

ORACLE
OpenSSL
Adobe
redhat. LINUX
Microsoft
vmware
solarwinds
hp
CISCO
mozilla FOUNDATION

Over 100 Vendors




Cyber Security Requirements Challenges

- No holistic requirements strategy; cyber defense is implemented on a system by system basis
- Army is increasing its reliance on COTS software for C4ISR Programs of Record (PORs)
  - We now share many of the same cyber security risks as industry
- Cyber defense sustainment for C4ISR PORs relies on IAVA patches
  - Most IAVA solutions provided by product vendor (usually commercial software/hardware vendor)
  - IAVA patches typically issued on quarterly basis
  - No current automated means to push to C4ISR tactical PORs
- Measuring cyber readiness of systems/units