# Open Standard, “Type Certified”, Virtual, Real-time, Cross Domain Services

Chris Gunderson (cgunders@nps.edu)
David Minton (David.Minton@macefusion.com )

# Bottom Line Up Front

Information Assurance (IA) Certification and Accreditation (C&A) policies clash with mandates for interoperability:

- Policy says balance "need-to-protect" with "need-to-share," but only enforces need-to-protect.
- Traditional "guards" allow only selective sharing via archaic, expensive, physical separation.


Modern open standards (e.g. TCP/IP HTTPP XML) have moved applications up several layers of abstraction. Modern logical assurance argument allows C&A of a "type" of architecture, vice specific implementation of code:

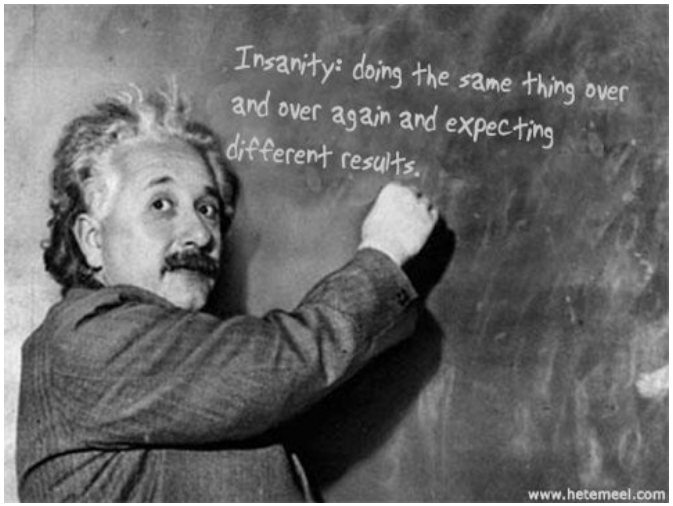
- Change in application layer s/w does not necessitate renewed C&A
- Open standard IA components + C&A paperwork are sharable across projects
- Cloud Cross Domain Services provision highly assured (PL4/5) virtual machines

Various MACE storefronts are implementing this paradigm. Recommend establishing government Enterprise Information System "Certification Engineer" at MACE to support UCDMO's and others' C&A modernization efforts.

# Are we Crazy?

*"…IC ITE, paves the way for a fundamental ship to operation as a IC-level IT Enterprise. We are being asked to change our historical agency IT models to a new common architecture – one that, through shared services, will become our future, single strategic IT platform for the IC. Our new IX IT architecture will enable better integration of the IC and build trust in information sharing. Missions will benefit from improved agility, scalability, and security while realizing lower operating costs. We will employ cloud technologies, wide-spread virtualization, thin-client desktops, application stores and improved security as we evolve to a modern, data-centric IC IT Enterprise."*

Al Tarasiuk, IC CIO, Assistant Director of National Intelligence

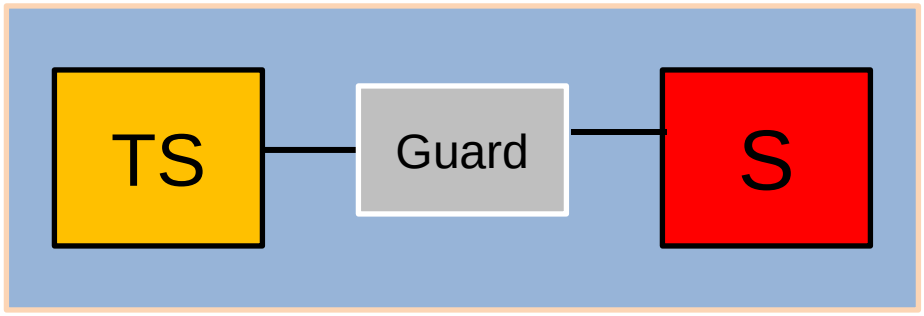



**Is it possible to achieve the profound improvements envisioned by IC ITE with an Information Assurance model based on the last century's technology? If not, what are the fundamental changes to the old IA technology and C&A paradigms we'll need to implement?**

# Assuring Balanced Need-to-Share and Need-to-Protect, at Scale, in the Cloud

- Cyber security concerns are valid and critical
- Need-to-share data and resources across domains is valid, critical and time sensitive
- Current IA/CDS technology and C&A paradigms are inadequate for all the above
- Defense Enterprise intended exploitation of Cloud efficiencies exacerbates issue.

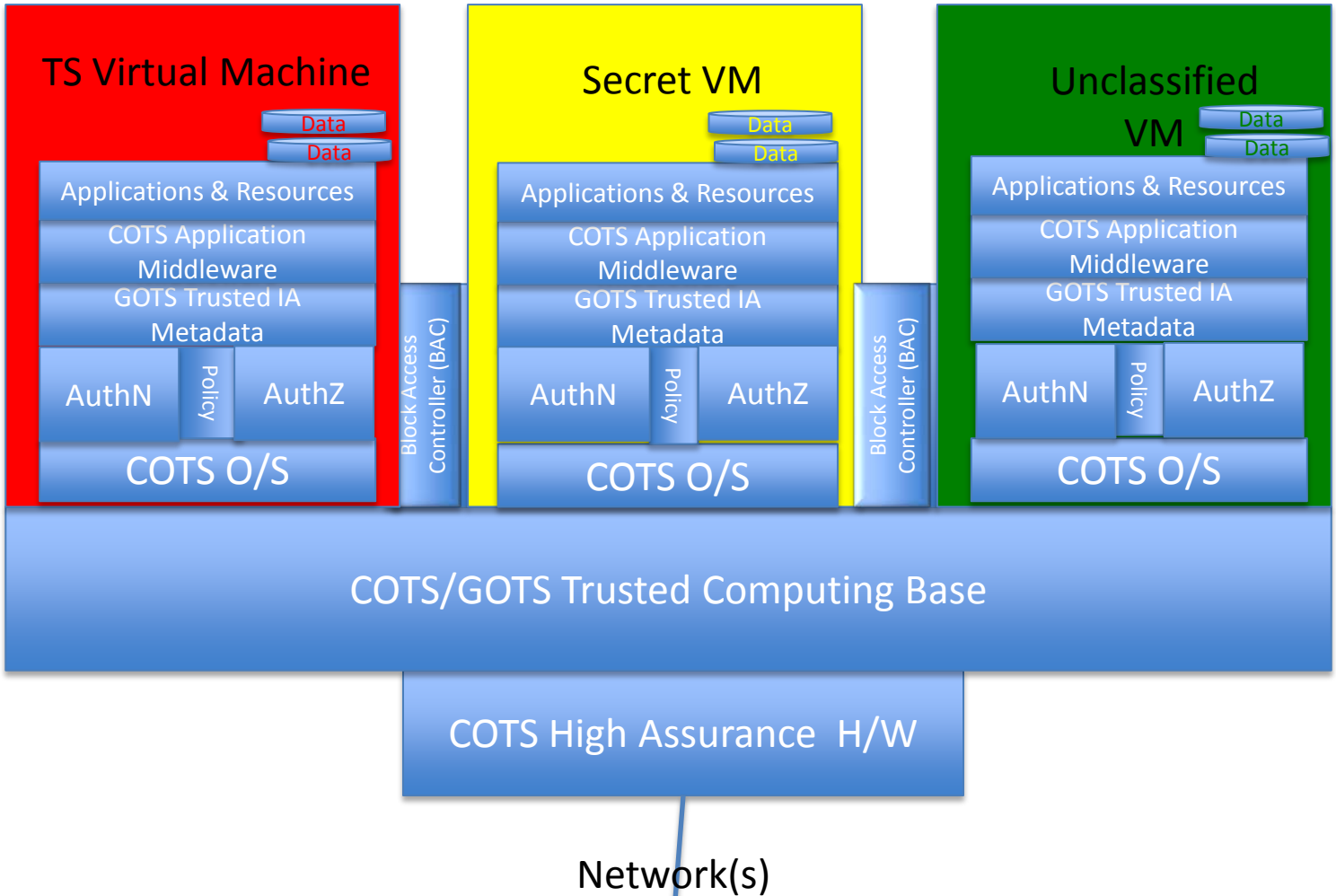
# Traditional Guard



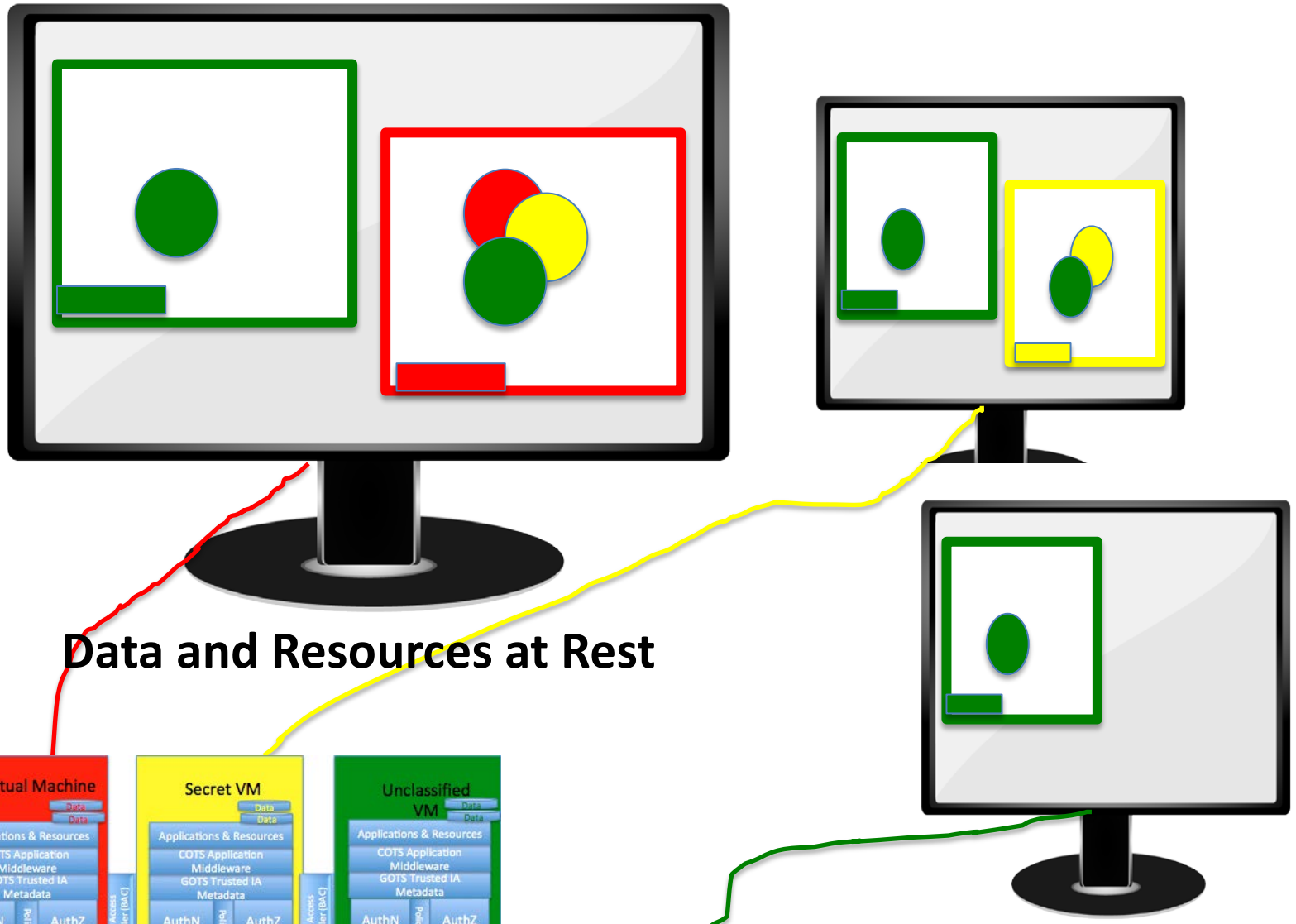

- Complex
- Proprietary
- Rigid, Brittle, doesn't scale
- Expensive
- Bottleneck
- High SWaP
- Slow

**Basically, a 100M LoC sanctioned security violation that makes everyone cringe…**

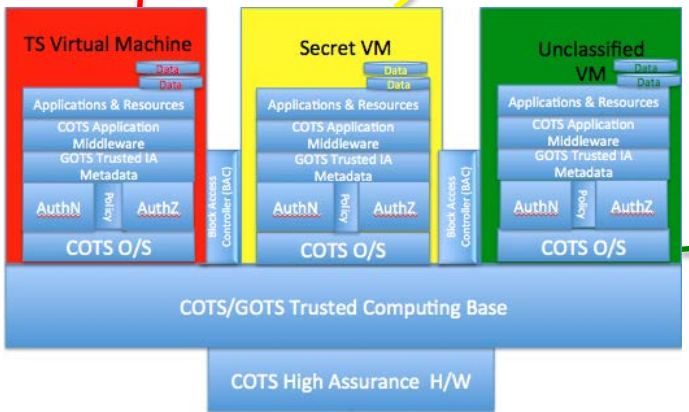
# New Paradigm: Virtual, Real-time, Cross Domain Services



# Virtual Real-time Cross Domain Services

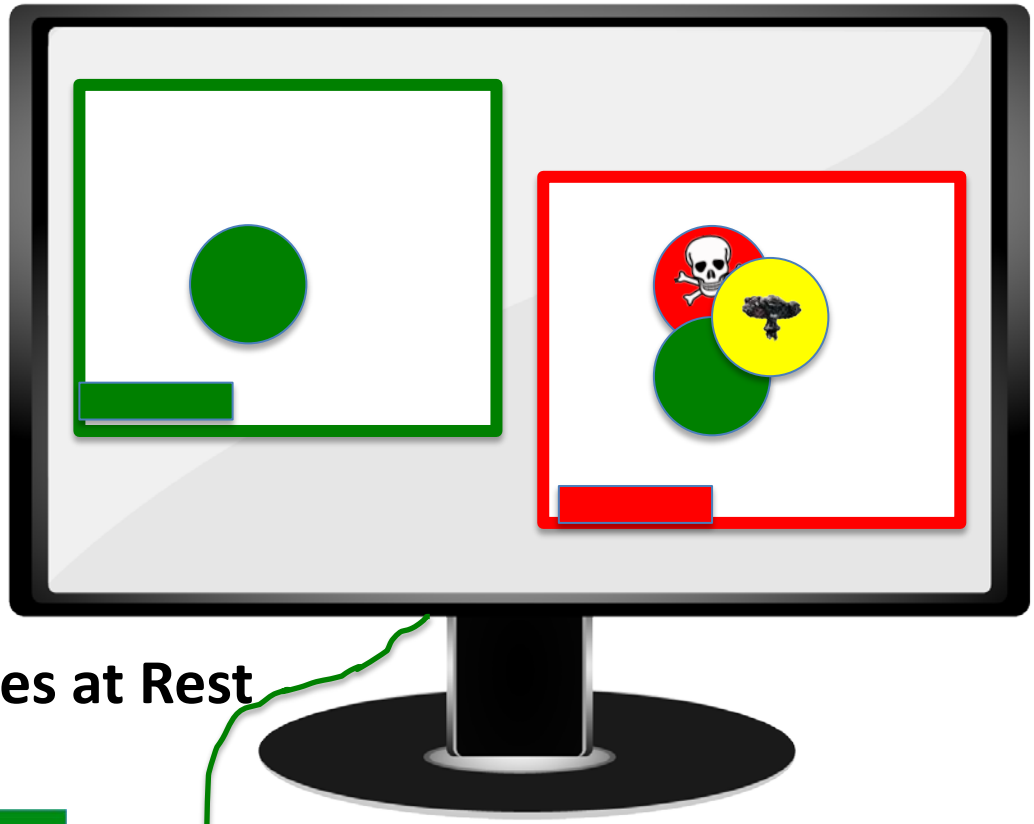


## Data and Resources at Rest

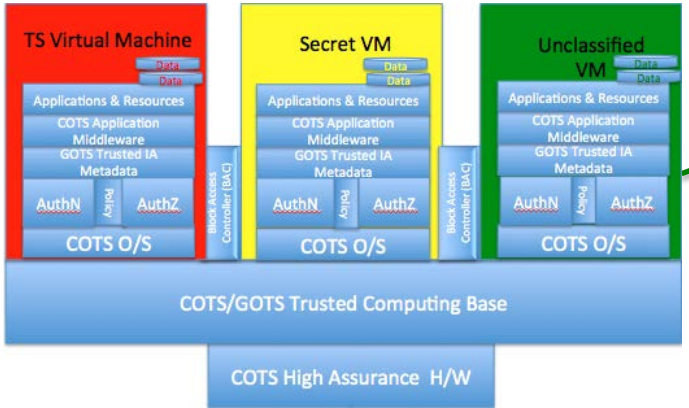



## Policy: e.g. Enforce Bell Lapadula

# Virtual Real-time Cross Domain Services

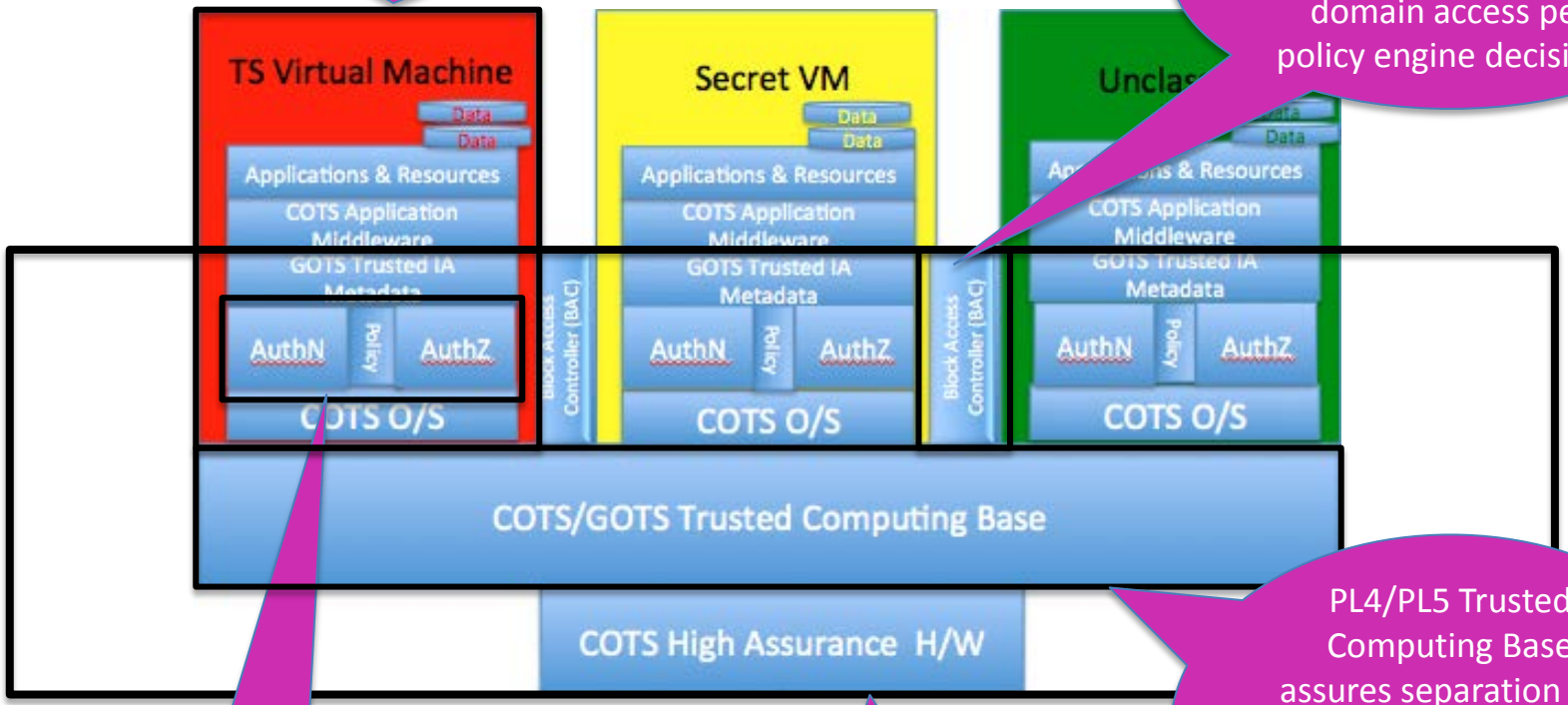


## Data and Resources at Rest




## Policy: e.g. Enforce Dynamic Emergency Need-to-Share Mandate

Virtual Machines support host O/S and COTS/GOTS stack of choice. These are abstracted away from security layers and so may be updated without refreshing C&A

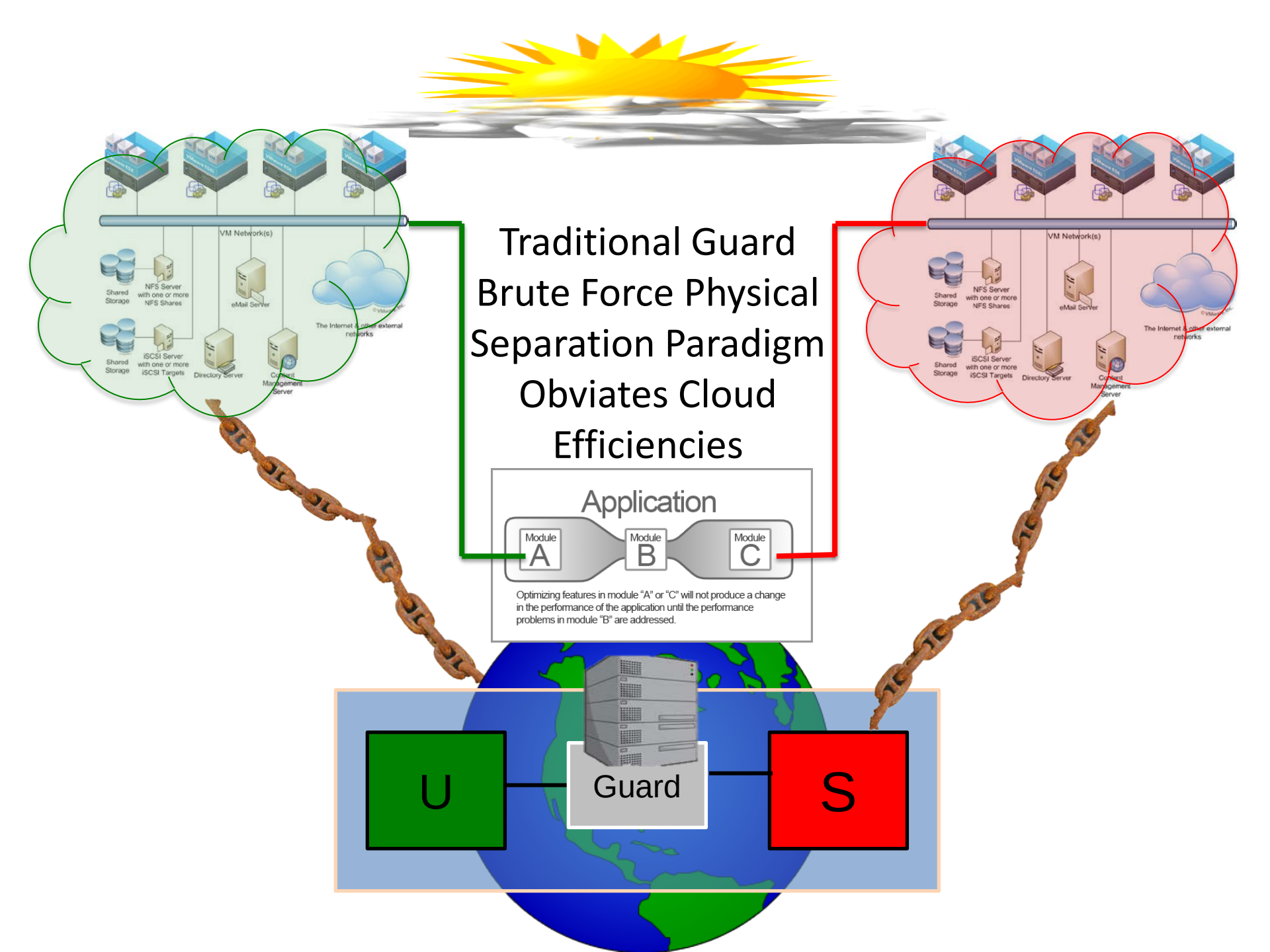


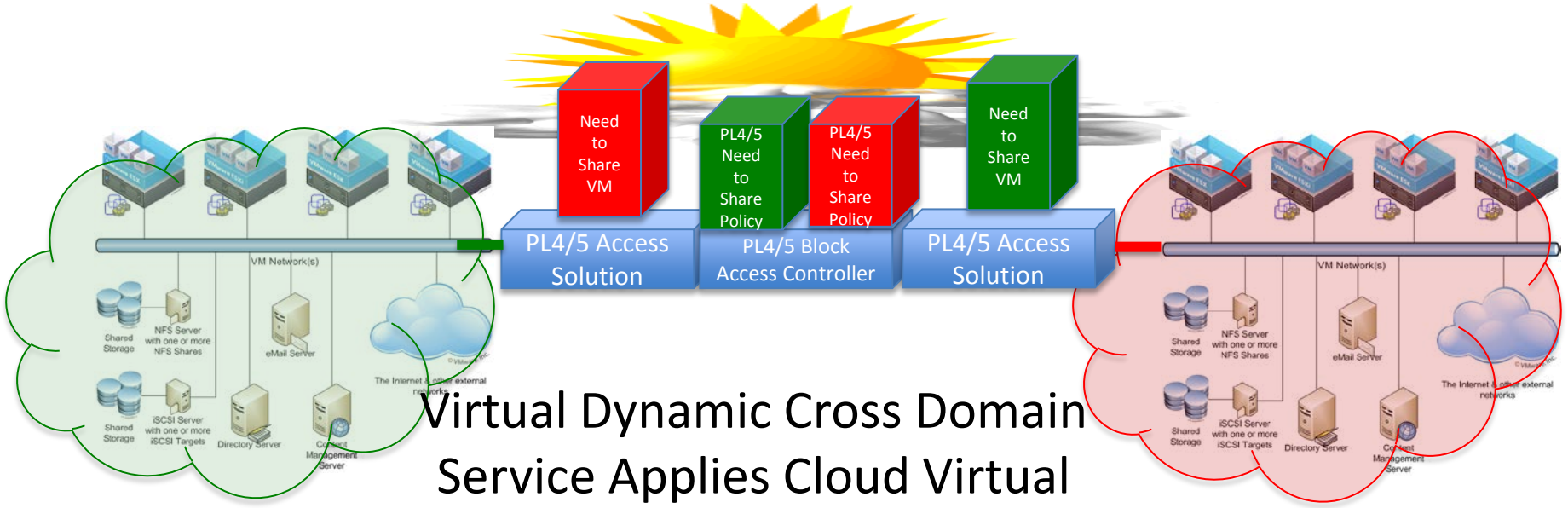

PL4/PL5 GOTS Block Access Controller allows dynamic cross domain access per policy engine decisions

PL4/PL5 Policy Engine enforces local need-to-share policy

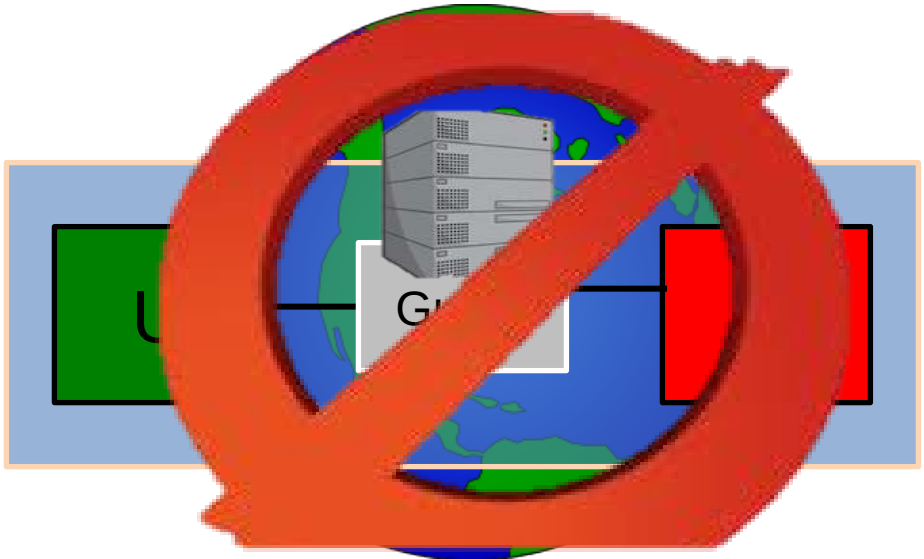
Open Standard, "Type Certified" security stack is ~80% pre-approved.

PL4/PL5 Trusted Computing Base assures separation per UCDMO CDS access solution arguments. I.e. UCDMO approved virtual solution = TCB.


Traditional Guard
Brute Force Physical
Separation Paradigm
Obviates Cloud
Efficiencies
VM Network(s)
Shared Storage
NFS Server with one or more NFS Shares
eMail Server
The Internet & other external networks
iSCSI Server with one or more iSCSI Targets
Directory Server
Content Management Server
Application
Module A
Module B
Module C
Optimizing features in module "A" or "C" will not produce a change in the performance of the application until the performance problems in module "B" are addressed.
U
Guard
S



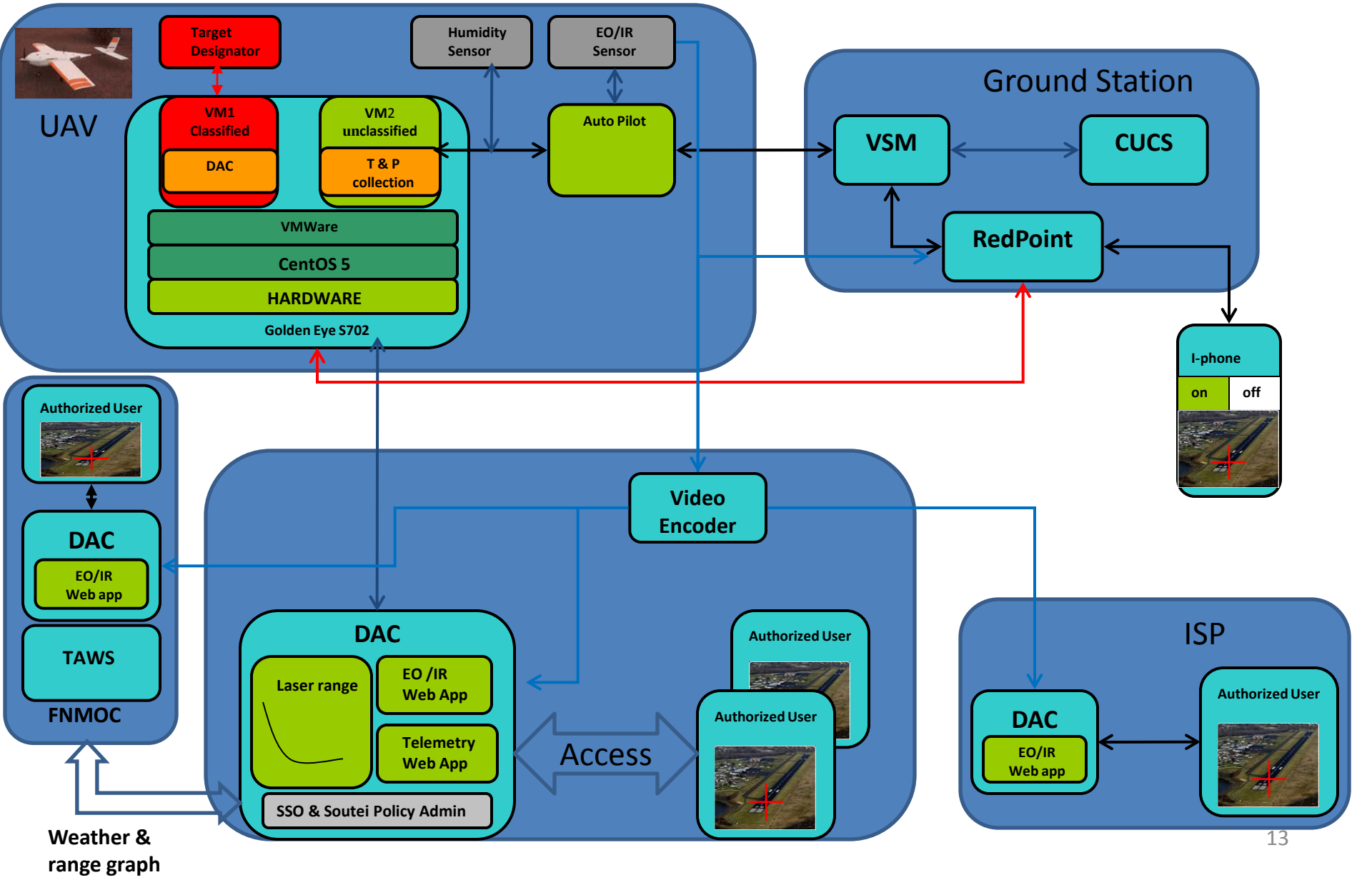

# Virtual Dynamic Cross Domain Service Applies Cloud Virtual Machine Paradigm to Enhance Security and Enable Economic and Operational Efficiencies



# MACE Virtual Real-time Cross Domain Service (VR-CDS)

- Implements NSA Multiple Levels of Security (MILS) architecture.
- Successfully demonstrated in partnership with USMC, JFCOM, NPS and SOCOM aimed at maturing Multi-Level Security at the tactical edge.
- Reduces the current UCDMO approved solutions to one computer small enough for tactical UAV.
- No appreciable latencies introduced.
- Builds on COTS releases of the NSA High Assurance Platform and AFRL Type 1 Hypervisor
- Conforms to AT&L next-generation standard ground receive station IA design.
- C&A requires carefully socializing new paradigm with certification authorities. That said, SABI ticket for U-S issued.
- Under development in MACE Electronic Warfare Service Architecture (EWSA), and Counter Narcotics Information System storefronts
- Scheduled for SABI ATO in FY14

# Demonstrated Software Configuration



# Counter Narcotics Information System VR-CDS Variant

- Mission Application:
  - Global Discovery Airborne ISR Project: Share SBU information collected by DEA in Afghanistan with DoD via SIPRnet
  - CN Information System Pilot: Share multi-source JIATF South intelligence with the larger CN community while maintaining the inherent sources of the data at the appropriate classification levels
- Design
  - ….
  - …. (describe design)
- C&A:
  - Per CENTCOM Regulation 25-28, DoDI 8510, and DEA regulation XXXXXX…..
  - ATO scheduled for _____

# Marine Corps Electronic Warfare Service Architecture VR-CDS Variant

- Mission Application:
  - Global Discovery Airborne ISR Project: Share SBU information collected by DEA in Afghanistan with DoD via SIPRnet
  - CN Information System Pilot: Share multi-source JIATF South intelligence with the larger CN community while maintaining the inherent sources of the data at the appropriate classification levels
- Design
  - ….
  - …. (describe design)
- C&A:
  - Per MAGTF EW Strategy, USMC reg xyz, and DoDI 8510.
  - ATO scheduled for _____

# Required Departures from Current C&A Paradigms

The enterprise cloud must inherit the certifications and accreditations of the hosted Cross Domain Services.

- "Inherit" means that all DAAs agree that the assurance arguments that led to the original C&A are valid, and remain valid, in the new environment.
- Today, DAAs rarely agree to inherit assurance arguments across their domains.

To achieve cloud efficiencies regarding rapid evolution of capabilities, all concerned DAA must

- Accept the argument that changes to the upstream technology stack – that they do not control - do not change their C&A assurance arguments, or …
- Blindly accept the risk associated with uncontrolled changes.

Otherwise, Cross Domain Services must be recertified every time changes are made within the enterprise cloud. Today, DAAs do not accept either option.

# Information System Certifiers' vs. Builders' Perspective

Architects and engineers tend think in terms of functional layers, e.g., Multiple logical functional layers can exist in the same hardware.

Certifiers and accreditors are legally responsible for IA of well-defined physical systems, not s/w abstractions. They think in terms of security boundaries and managing vulnerabilities from that perspective.

- Vulnerabilities are weaknesses that adversaries can potentially exploit.
- Security boundaries tend to align with physical accountability, rather than functional, logical, process.
- DAAs do not C&A environments that introduce unknown (to them) vulnerabilities. DAAs only C&A software processes that fall clearly inside their well-defined, physically accountable, environments.
- Hence, C&A arguments are usually based on ownership and control of physical hardware devices.

Note: Virtual machine Cross Domain Services, by definition, would capture well-defined logical functionality and managed vulnerabilities, within an equally well-defined and guaranteed security boundary.

# VR-CDS C&A Strategy

- Describe the Cloud Multi-Level Cross Domain Services target architecture
  - Dynamically composable, assured virtual machines
  - PL4/5-equivalent MLS services
  - Includes assured dynamic need-to-share policy engines.
  - Include timeline that shows migration to the target environment.
- Identify specific pilot projects that will do the evolutionary work.
- Partner with operationally motivated, DAAs. Explain the C&A assurance argument, i.e. vulnerability management and security boundary delineation
  - Emphasize the need to establish logical separation as preferable to physical separation.
  - Explain how to immediately use currently UCDMO-approved separation solutions
  - Show clearly, how and why multiple independent DAAs will agree to a C&A inheritance strategy
  - Explain why they will not require C&A updates whenever tech refresh occurs upstream of their accredited cloud services.
- Address all traditional classes of CDS; i.e. transfer, MLS, and access solutions.
- Leverage success of transfer solution based MLS such as CENTAUR in the near term,

# Recommendation

- Establish Government Enterprise Information System Certification Engineer research initiative at MACE
- Recruit expert in legacy and modern IA/CDS and C&A technologies, policies, and methods.
- Appoint as IPA or NPS research associate.
- Assign tasks:
  - Collect dynamic, policy, based need-to-share requirements across MACE storefronts and beyond
  - Research best practices in and outside of government
  - Assist projects design virtual, open standard, enterprise security service layer(s).
  - Work with UCDMO and C&A authorities to:
    - Prepare modern enterprise arguments for assured virtual separation paradigms that allow inheritance of controls within and across clouds and similar architectures.
    - “Type certify” cloud-based, mulit-level, cross domain services
  - Develop position description to transition research project activities into permanent government billets