High Assurance Security Architecture for Embedded Systems Program

Multiple Independent Levels of Security/Safety (MILS) Technology for High Confidence Systems

27 Apr 06

Mr Jahn A. Luke
Program Manager
Information Directorate
Jahn.Luke@wpafb.af.mil

Air Force Research Laboratory
Information Directorate
Embedded Information Systems Branch (AFRL/IFTA)

MISSION

***Research, develop, demonstrate, and transition real-time embedded information system technologies* to enable global information dominance and air and space superiority**

AFRL/IFTA
Wright Research Site (WRS)
Wright-Patterson AFB OH

CORE TECHNOLOGIES

Legacy System Modernization

Weapon System Security/ Information Assurance

Adaptive/Reconfigurable Embedded Systems

Prospective and Cognitive Architectures

System-of-Systems Interoperability

Real-Time Quality-of-Service

Embedded Systems Technologies for Unmanned and Autonomous Systems

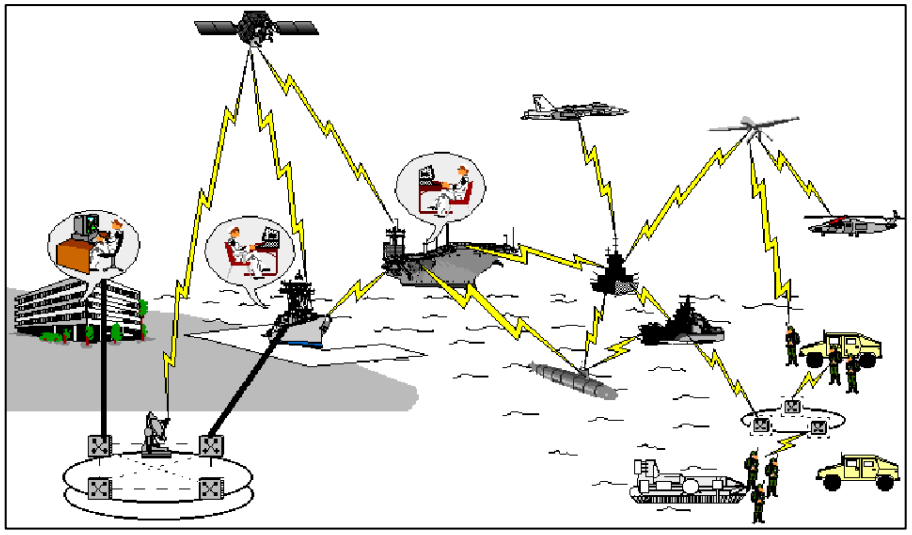
VISION

Affordable, Innovative, Secure, Net-Enabled embedded information systems to the Warfighter

Within the Global Information Grid (GIG)

Introduction

- **Net-Centric Operations (NCO) is characterized by the *sharing of information at all levels (TS/SCI through Unclassified)* between new and legacy systems within the Global Information Grid (GIG)**
- **The architecture of exiting legacy systems must be modernized to interoperate with new systems such as Unmanned Air Vehicles (UAVs) in order to achieve the NCO vision *(Net-Enabled)***
- **Information that is passed between and within these systems must be *shared securely* and to protect the warfighter and not compromise the mission**
- **Information needs to be shared between U.S. & Coalition Partners involving -**
  - **Multiple levels (MLS/MSLS)**
  - **Smart Push / Smart Pull**
  - **Web Services**
- **New capabilities and information sharing mean the ever increasing need for *Safe/Secure* components & support tools for system development and certification**



What is MLS/MSLS/MILS?

- **What is Multi-Level Security (MLS) / Multi-Single Level Security (MSLS)?**
  - **MLS: *Processes data of differing classifications securely*, e.g., guards, downgraders, firewalls, data fusion, data bases**
  - **MSLS: *Separates data of differing classifications securely*, one level at a time, e.g., communications platforms, infrastructures**
  - **MLS/MSLS requires in many cases separate, redundant hardware for each classification of data; meaning more space, weight, & power**
- **Current MLS/MSLS capabilities**
  - **Difficult to implement and expensive to certify**
  - **Costly to maintain and reconfigure**
  - **A problem to extend and to interconnect**
- **Multiple Independent Levels of Security/Safety (MILS)**
  - **A system that *supports multiple, separated entities*, each operating at a different classification level (security)**
  - **An software architecture that supports MILS, MLS, and MSLS; employs time/space partitioning; and enforces information flow, data isolation, periods processing, and damage limitation (safety/security)**

Our Challenge

How can the USAF, other DoD services and agencies *affordably* certify and field MLS/MSLS solutions on their systems and/or platforms?

High Assurance Security Architecture for Embedded Systems

MILS Activity

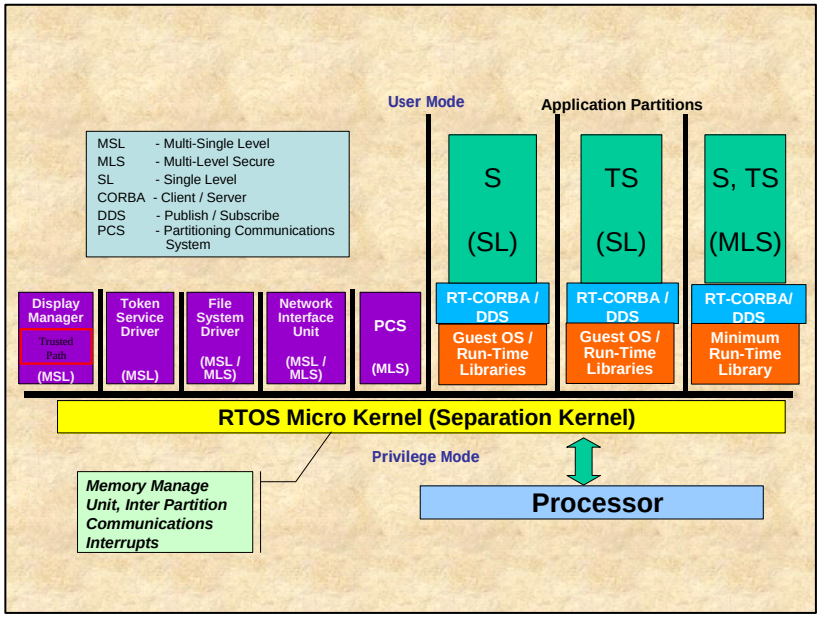
- AFRL/IFTA led *cost share* effort to provide *affordable* and near term *obtainable* solutions to achieve a *high assurance* architecture for use in DoD mission-critical embedded systems and workstations, comprising of RTOS and middleware products and support tools to aid in development, test, and evaluation
- Teamed with NSA, Open Systems Joint Task Force (OSD-ATL), DoD program offices, system integrators, commercial vendors, and academia
- Initiated under an earlier Air Force RDT&E task to meet the security challenges of embedded platforms such as the F-22A and F-35

MILS Architecture

Enabling technology providing a foundational infrastructure for Cross Domain Solutions (CDS) and mixed criticality (Safety/Security), supporting *MLS* & *MSLS* and applicable to:

- *Weapon Systems*
- *Communication Systems / Facilities*
- *Command and Control (C2) Platforms*

Enabling secure, dependable GIG Information Assurance (IA)



Industry Standards for Safety / Security

Safety

- **RTCA DO-178B, *Software Considerations in Airborne Systems and Equipment Certification***
- **ARINC-653, *Avionics Application Software Standard Interface (time and space partitioning)***

Security

- **ISO-15408, *Common Criteria for Information Technology Security Evaluation***
- **DCID 6/3, *Protecting Sensitive Compartmented Information Within Information Systems***

High Confidence Certification Goals

Common Criteria (Evaluation Assurance Level)*	***MSLS / MLS Separation Accreditation***
• **Basic Robustness (EAL3)**	**System High *(Closed Environment)***
• **Medium Robustness (EAL4+)**	**System High *(Open Environment)***
✓**High Robustness (EAL6+)****	**Multi Level Separation**
✓***DCID 6/3 Protection Level 5***	***Multi Nation Separation Accreditation***
✓***RTCA DO-178B Level A***	***Failure is Catastrophic***

* **Performed by a National Information Assurance Partnership (NIAP) Lab**

** **Requires formal methods artifacts for evaluation**

MILS Architecture

MILS Architecture (John Rushby, PhD) - concept targeted at enabling the composition of system properties from trusted components *(layered functionality & assurance)* consisting of:

Separation Kernel (SK)*

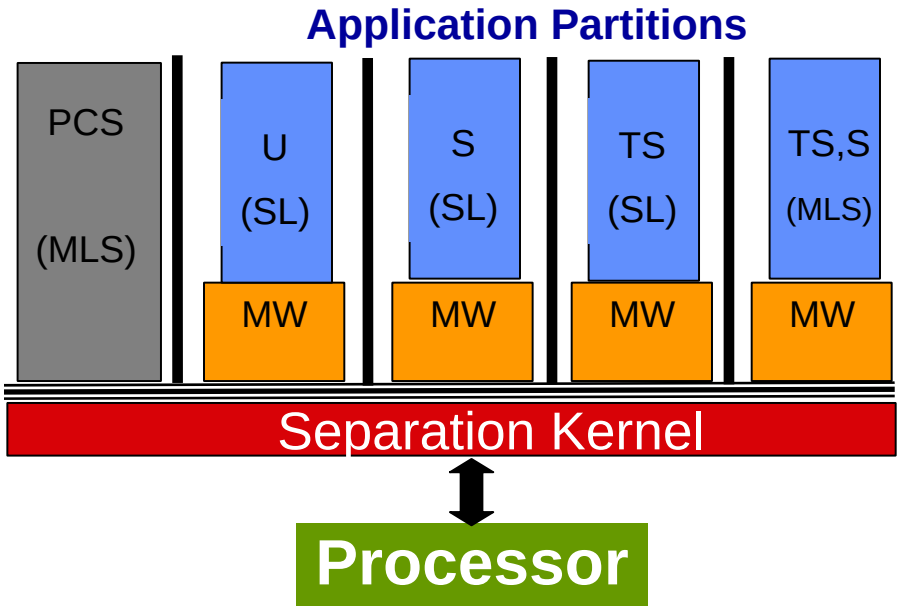
- **Provides data isolation and control of information flow**
- **Provides resource sanitization and damage limitation**
- **Really small: 4-5K lines of code for high robustness (EAL 6+) evaluation**

Middleware (MW)*

- **Traditional RTOS Services *(device drivers, file systems, network stacks)***
- **Traditional Middleware Services *(RT-CORBA, DDS, Web Services)***
- **Partitioning Communications System (PCS) *– global enclave partition comm over TCP, etc.***

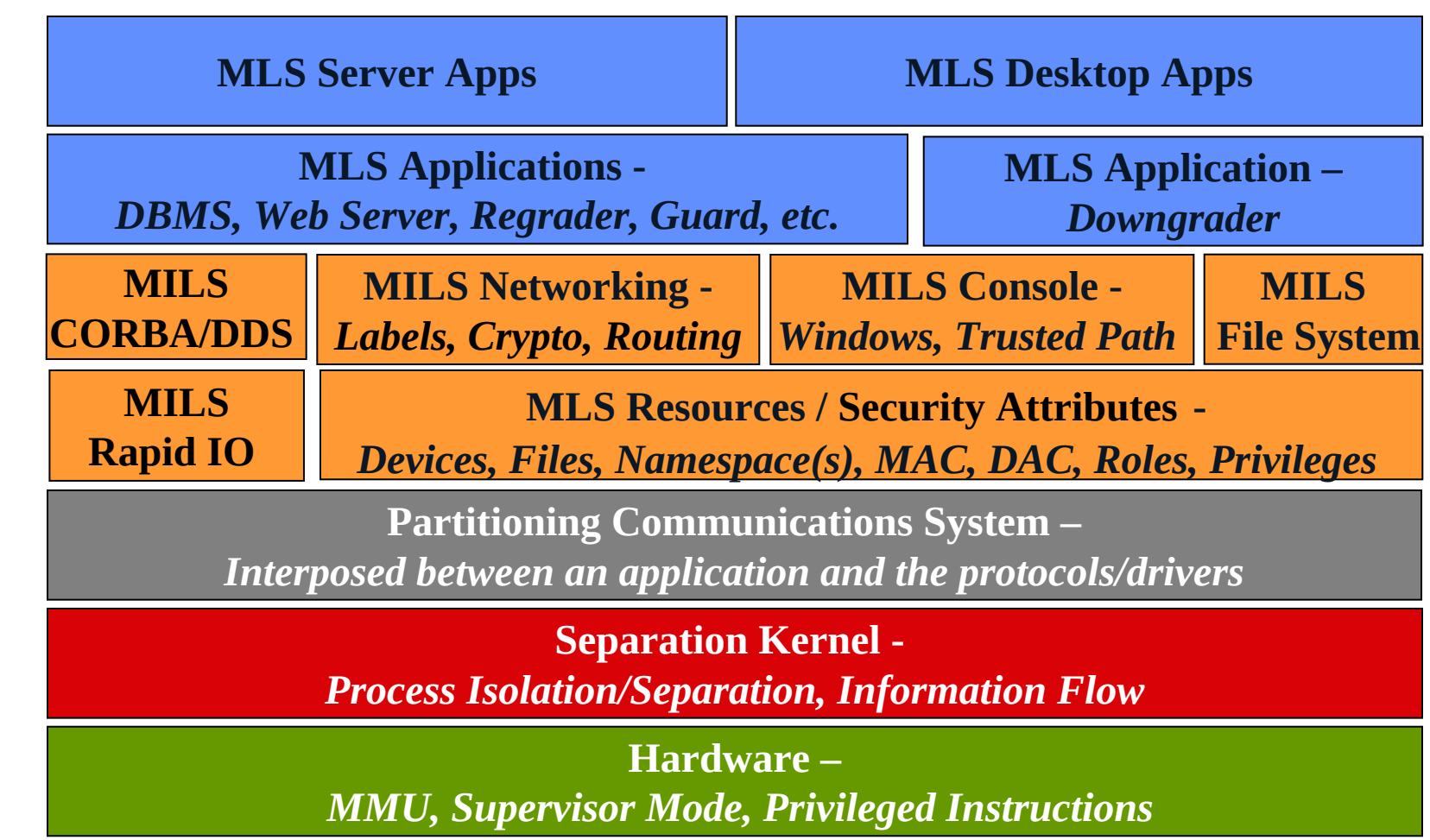
Applications

- **Implements *application-specific* security functions**
  - **Firewalls, guards, CDS, downgraders, etc.**



*** MILS Foundational Layers for High Assurance**

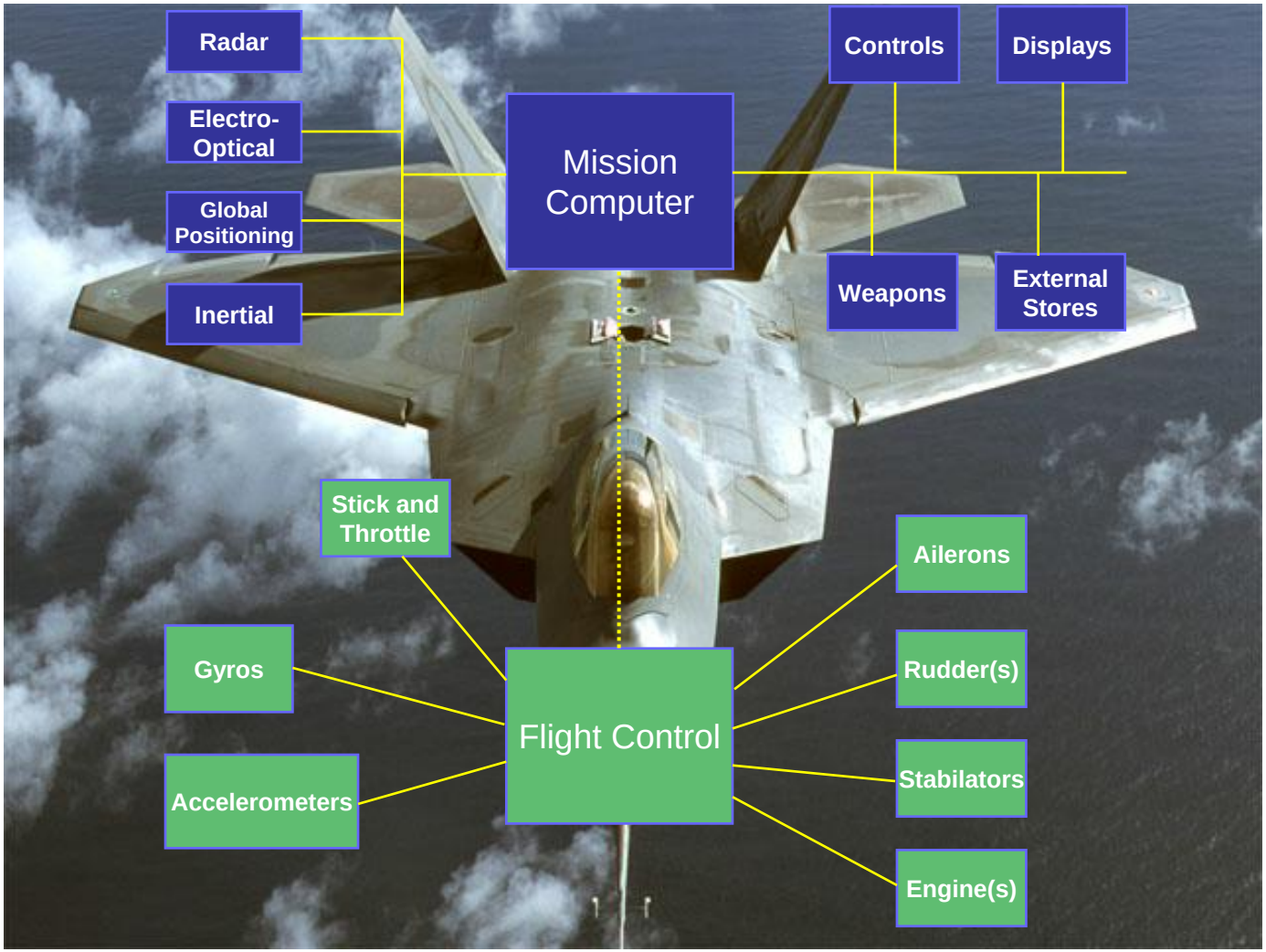
Notional MILS Architecture "Software Stack" Layering



High Assurance Security Architecture for Embedded Systems Approach

- ***MILS Architecture (Near Term)***
  - **Work with NSA, Industry, Academia, and the Standards Bodies (i.e., The Open Group) in supporting the development and review of *Protection Profiles* for MILS architecture components**
    - **RTOS (Separation Kernel) product**
    - **Middleware products (PCS, RT-CORBA, DDS, File System, Network Stack, etc.)**
  - **Support *US-based* RTOS and middleware vendors in achieving certified EAL 6+ (high robustness) products through the *NIAP Labs* and work the aggregating of these MILS components**
  - **Support the evaluation, demonstration, and transition of MILS technologies applied to *real-time embedded* (mission critical) systems hosted on weapon system platforms**
  - **Support the feasibility / concept demonstration of a *high assurance MLS Workstation /Server* using MILS Separation Kernel and Middleware components hosted on COTS processor technology within a desktop/laptop environment *(in conjunction with NSA)***
- ***Next Generation High Confidence Architecture (Near-Mid Term)***
  - **Collaborate with the *High Confidence Software and Systems (HCSS) Coordinating Group (CG)* under the National Coordination Office for Networking and Information Technology Research and Development (NITRD) to support the development and certification of the *next generation* high assurance architecture and associated components**
  - **Conduct research in developing consolidated processes / support tools that can be jointly used to address *safety* and *security* to aid in architecture development and reduce overall cost of formal testing, evaluation, and certification**

MILS Background
Challenges of the F-22A



Characteristics

- Large and complex
- Requires frequent software updates
- Mix of computation types
  - Logic/State Machine
  - Computational
  - Signal Processing
  - Feedback Control
- **MLS requirement**

Problems

- Legacy i960 and 1750A processors - DMS issue / inadequate to handle new capability
- Proprietary RTOS and middleware

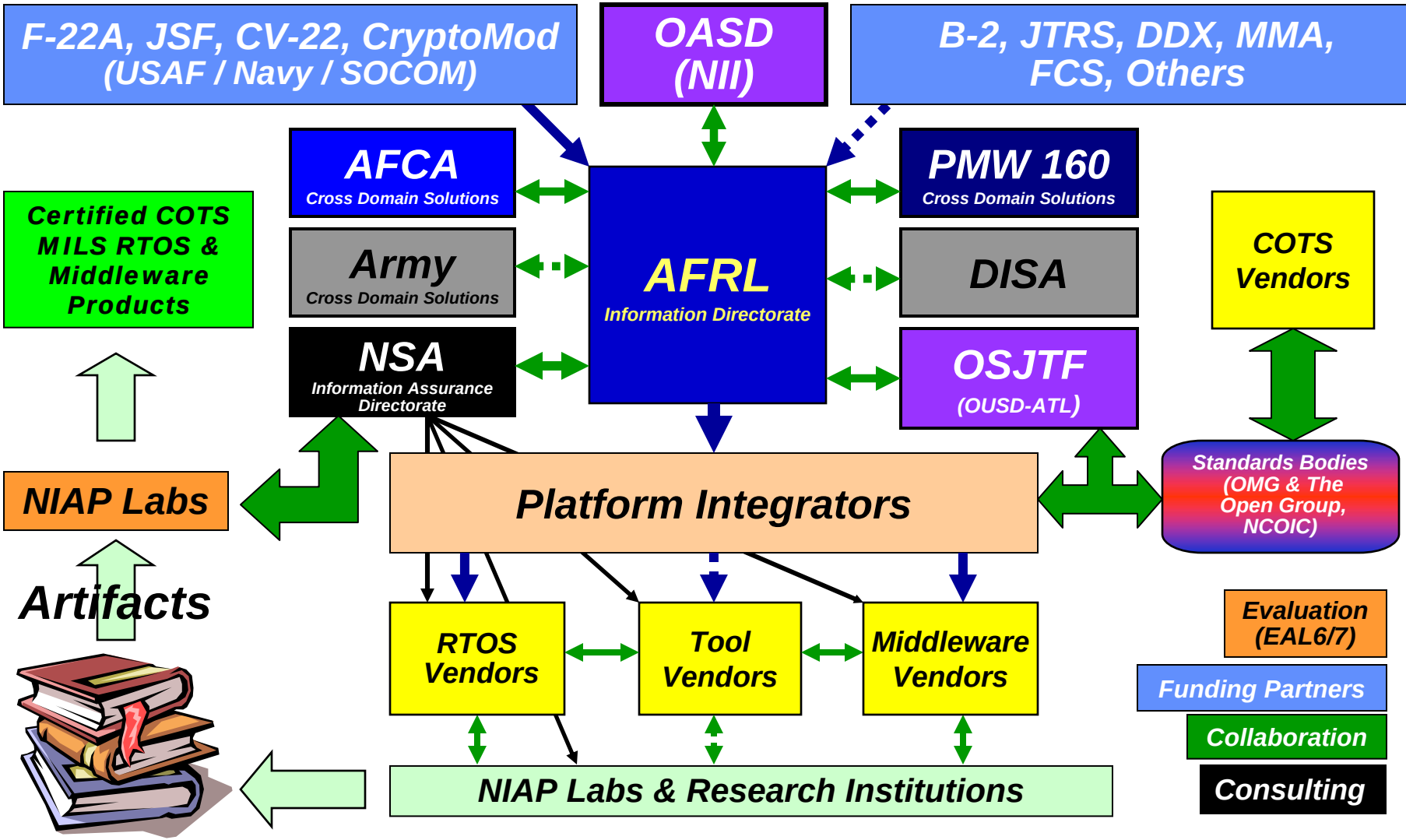
MILS Business Case: Cost Benefit to DoD Centrally Funded COTS Product Certification via NIAP with NSA Participation

- Today's contracts call out overall weapon system capabilities, not best "long term ownership" practices at component levels.
- Programs certify under the (DoD Information Technology Security Certification & Accreditation Process (DITSCAP) for the entire weapon system
  - Not suitable for COTS vendor ownership and reuse / sales.
  - Programs drive products toward point solutions, not a standards based, multi-program solution.[1]
  - Tracking component certification cost is difficult to acquire.
- *Example of a proprietary RTOS solution vs. COTS RTOS solution for a weapon system platform*

84% cost savings

Individual Program Costs	Proprietary Solution	COTS Solution
Development Costs (10 years)	$9 Million	$0
Runtime licenses (3000 units)	$0	$600,000
Annual Maintenance (10 year)	$???? Program borne through life cycle	$1 Million ($100,000 per year for 10 years)
Security Certification Costs	$5 Million[2] Unknown, estimate	$5 Million[3]
Total Program Costs over 10 years	~ $16+ Million	$6.6 Million
Cost for 5 DoD programs	~$80+ Million 5 x ($16M+)	$13 Million $6.6M + (4 X $1.6M)

MILS Activity
Where We Are Today



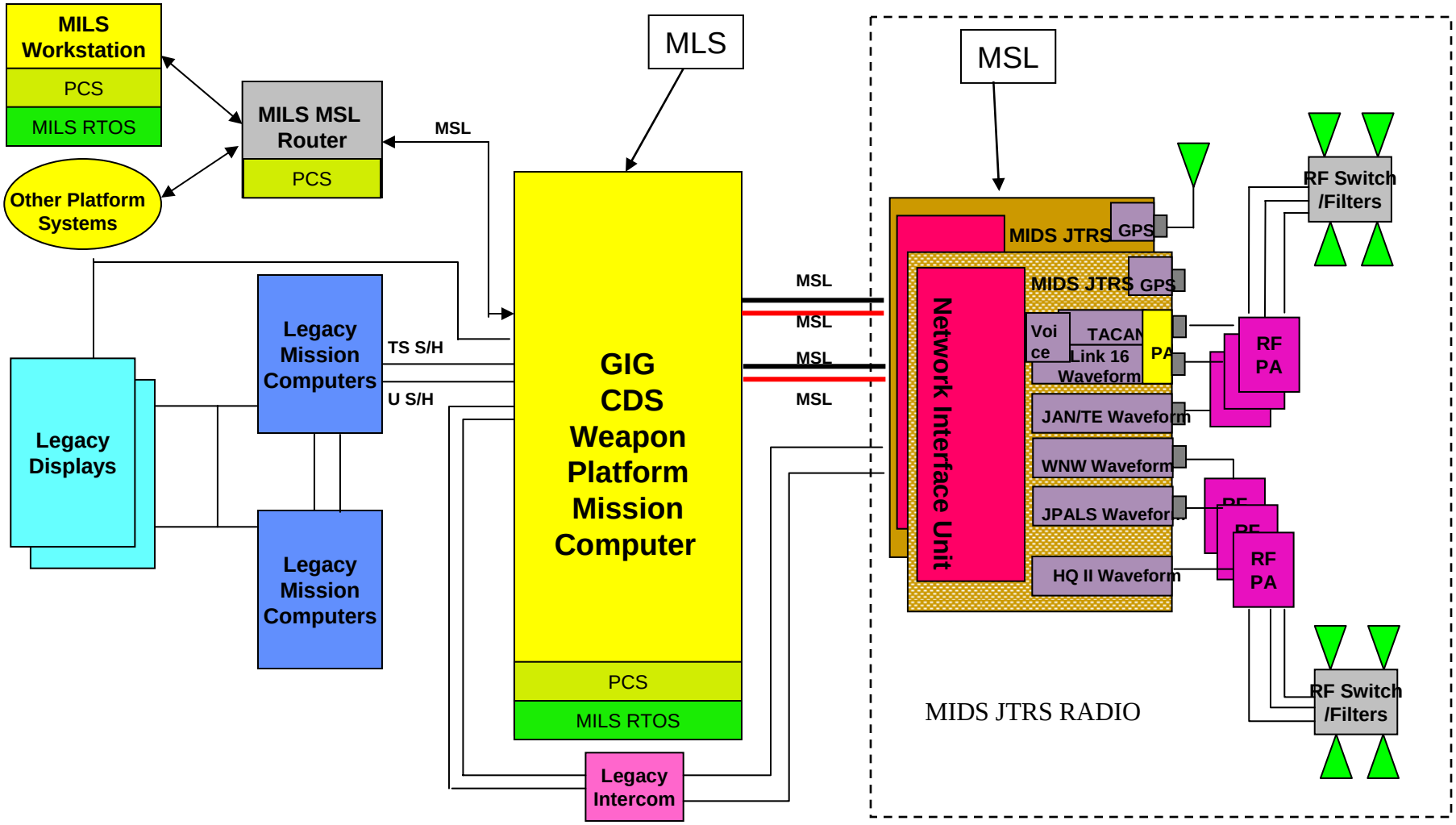
MILS Partners
Industry & Academia

- **Platform Integrators**
  - Lockheed Aero (ADP)
  - Boeing-St Louis
  - Raytheon-El Segundo
  - Northrop Grumman-El Segundo
- **MILS RTOS Vendors / Announced Products**
  - Green Hills Software — *INTEGRITY-178B, INTEGRITY Workstation w/ Padded Cell*
  - LynuxWorks — *LynxSecure*
  - Wind River Systems — *VxWorks MILS*
- **MILS Middleware Vendors / Announced Products**
  - Objective Interface — *PCSexpress, ORBexpress, DDSexpress*
  - RTI (in discussions) — *DDS*
  - Wind River/Interpeak — *IPSecure (Trusted Network Stack)*
- **MILS Test Beds, Research, & Related Activities**
  - LM Aero- Ft Worth
  - Boeing-St Louis & Seattle
  - General Dynamics C4 Systems-Scottsdale
  - Northrop Grumman (Space Technology)
  - Raytheon-El Segundo
  - Rockwell Collins
  - SRI International
  - University of Idaho

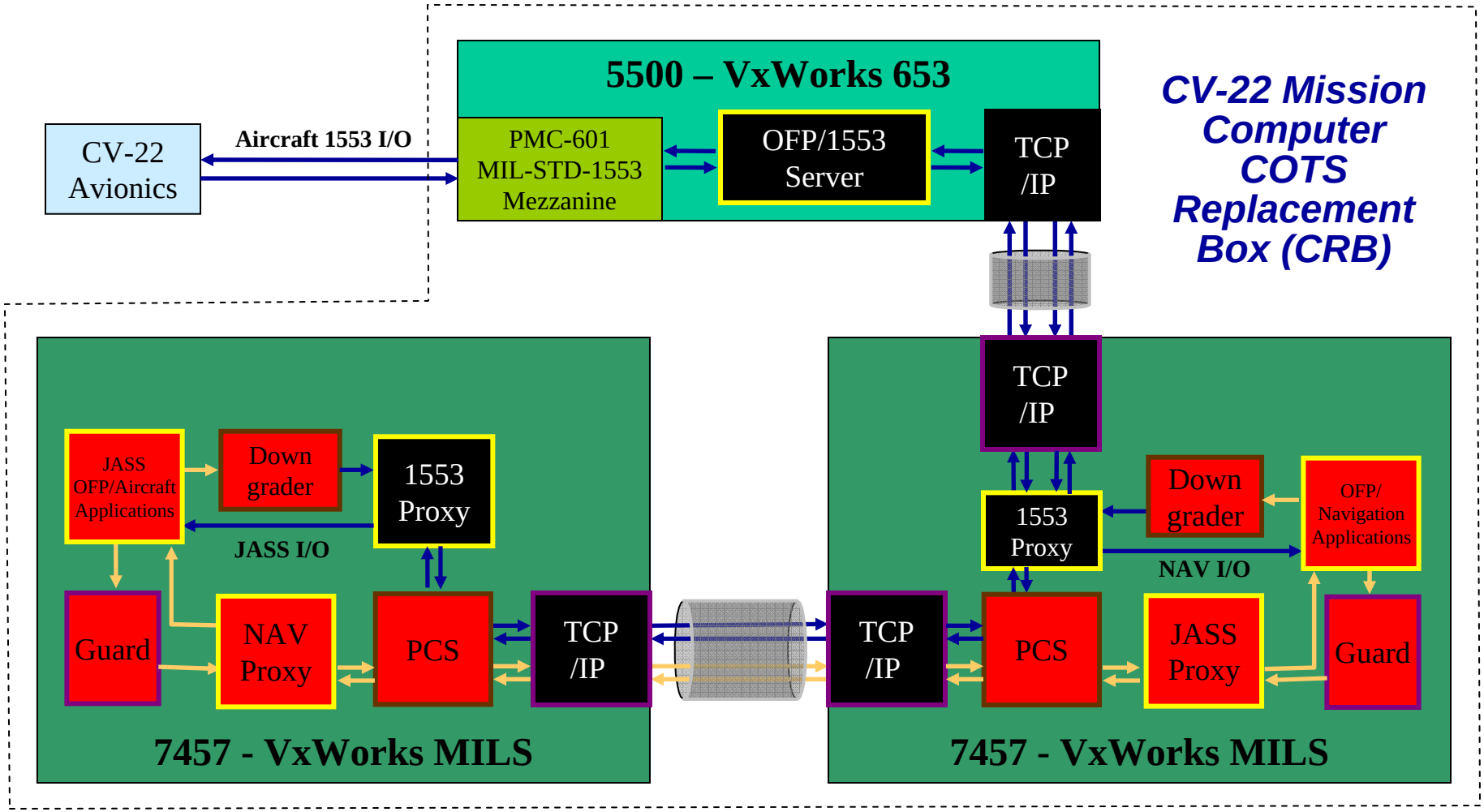
MILS Activities

- **Programmatic**
  - MILS activity endorsed by the CSNI Office at Air Force Communications Agency (AFCA)
    - AFCA stood up last year as new AF Cross Domain Solutions (CDS) office at Scott AFB
  - Working with CryptoMod program & Navy PMW 160 CDS to help move MILS effort forward
- **Technical**
  - **JTRS/MILS Integration Studies**
    - Two separate studies completed by Boeing and Lockheed Martin to look at issues regarding platform integration of JTRS and how MILS could be implemented
  - **Multi-Platform Security Requirements (MPSR) Study**
    - Study recently completed by Boeing to identify MLS/MSLS requirements across multiple Boeing platforms, looked at the MILS architecture, and evaluated two high assurance workstations approaches for NSA and JFCOM
  - **Protection Profile Activities (in conjunction with TOG)**
    - MILS SK PP - In final review at NSA
    - MILS PCS PP - In final work by Raytheon/OIS
    - MILS Console System PP - In final draft by LM/LynuxWorks
    - MILS Network System (Trusted Network Stack) PP – In initial draft by Interpeak/SRI Intl
  - **Formal Methods Artifacts Generation / RTOS Evaluation Support**
    - GHS INTEGRITY-178 RTOS product on its way to EAL 6+, going into F-22A and JSF
  - **MILS Architecture Study / Risk Reduction / Assessment**
    - CV-22 Open System Architecture (OSA) looking at MILS technology

Boeing Study: Notional GIG Enabled Platform with JTRS Radio & MILS CDS on a C2 Platform



Proposed MILS Approach for CV-22 Operational Flight Program (OFP)



AFRL Collaboration with NSA, SPAWAR, & SOCOM

Enterprise impact R&D

Near to Mid Term

- Cross-domain gateway “services”
- XML appliances
- Pipelined event driven architecture

- High Assurance Platform WorkStation (NSA, SOCOM, General Dynamics)

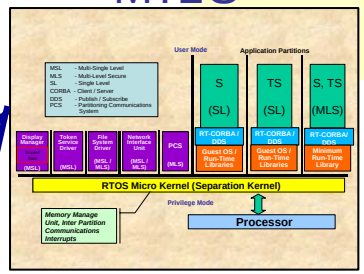
- Trusted Services Engine (SPAWAR, SOCOM, Galois)
- Oracle Data Vault

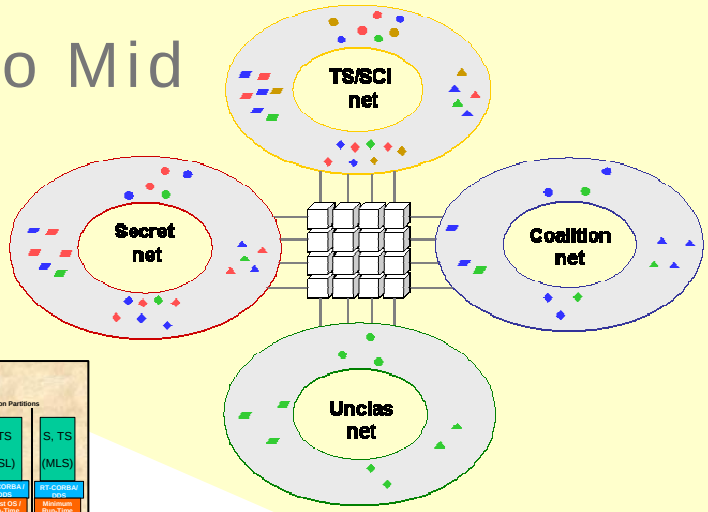
- MILS RTOS (AFRL, GHS)
- SE-Linux

MLS Gateway | MLS Desktop | MLS Repository

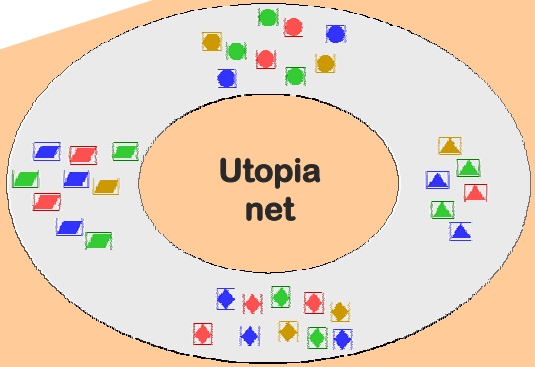
Trusted Platform

MILS





JV 2020



MILS Components: Applicable not only to DoD

- **High Confidence Systems are needed by the War-Fighter *and***
  - **Homeland Defense**
  - **Safety Critical World**
  - **Process Control World**
  - **Financial World**
  - **Bio-Medical World**
- **Interest shown by DHS for process control systems and supervisory control and data acquisition (SCADA) systems used in power plants, and the oil and gas industry**
- **The MILS Separation Kernel / middleware components can provide the lowest risk, quickest development time technology for high assurance systems**

Summary

- MILS protection profiles are currently being written and products are being developed by vendors to meet ***high assurance*** needs of DoD platforms/systems and interoperability of systems within the GIG
- COTS /standards based solution, reduces the dependency on proprietary solutions (i. e., operating systems, middleware)
- Anticipated benefits/cost savings to AF and the rest of DoD
  - Reduced Power/Weight/Space for platforms
  - Reduced Product/Artifact Development Cost
  - Reduced Certification & Accreditation (C&A) / Maintenance cost
- Without this effort, lead DoD program offices will only accomplish the work necessary to meet their certification requirements, leaving subsequent programs in DoD having to "re-invent the wheel" to accomplish theirs
- AFRL/IFTA is seeking core sponsorship within DoD and elsewhere to help continue to this effort and along with matching funds from other program offices, help to move MILS technology forward in the near term
- AFRL/IFTA is beginning to look at the near to mid term challenges ahead of mixed criticality and Non-Traditional ISR, where a next generation, high confidence architecture will likely be needed