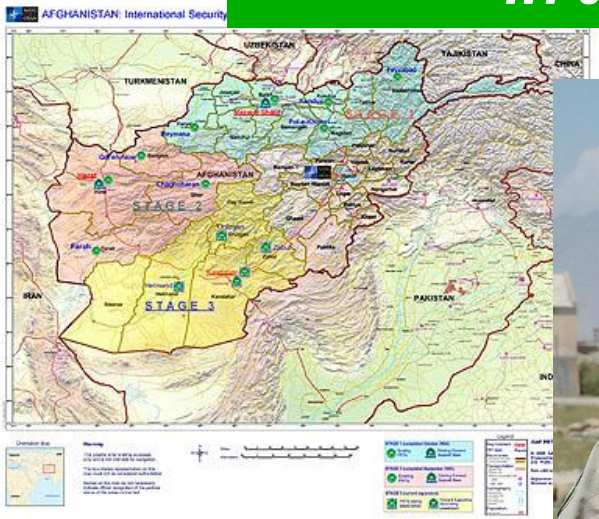
A Robustness Strategy

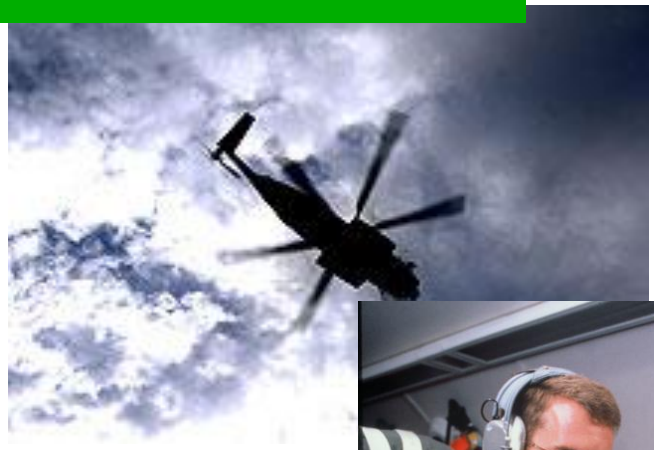
"High Assurance Challenges"
United States Central Command

LtCol Diana L. Staneszewski
DSN: 651-6638/2319
stanesdl@centcom.mil

Coalition Information Sharing Challenge

We Need to Share and Protect Information in a Dynamic Environment





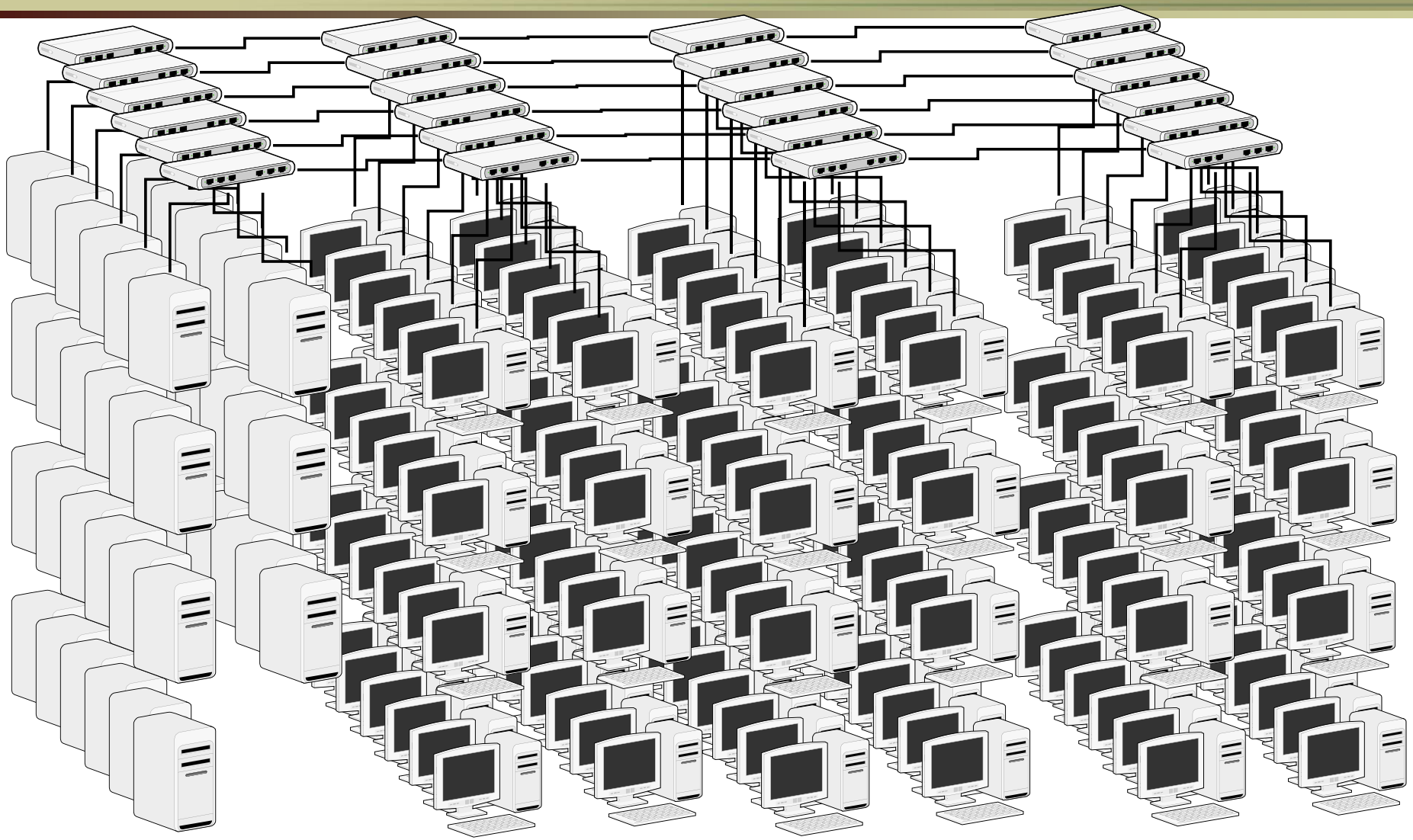
Coalition Information Sharing!

Coalition Information Sharing!

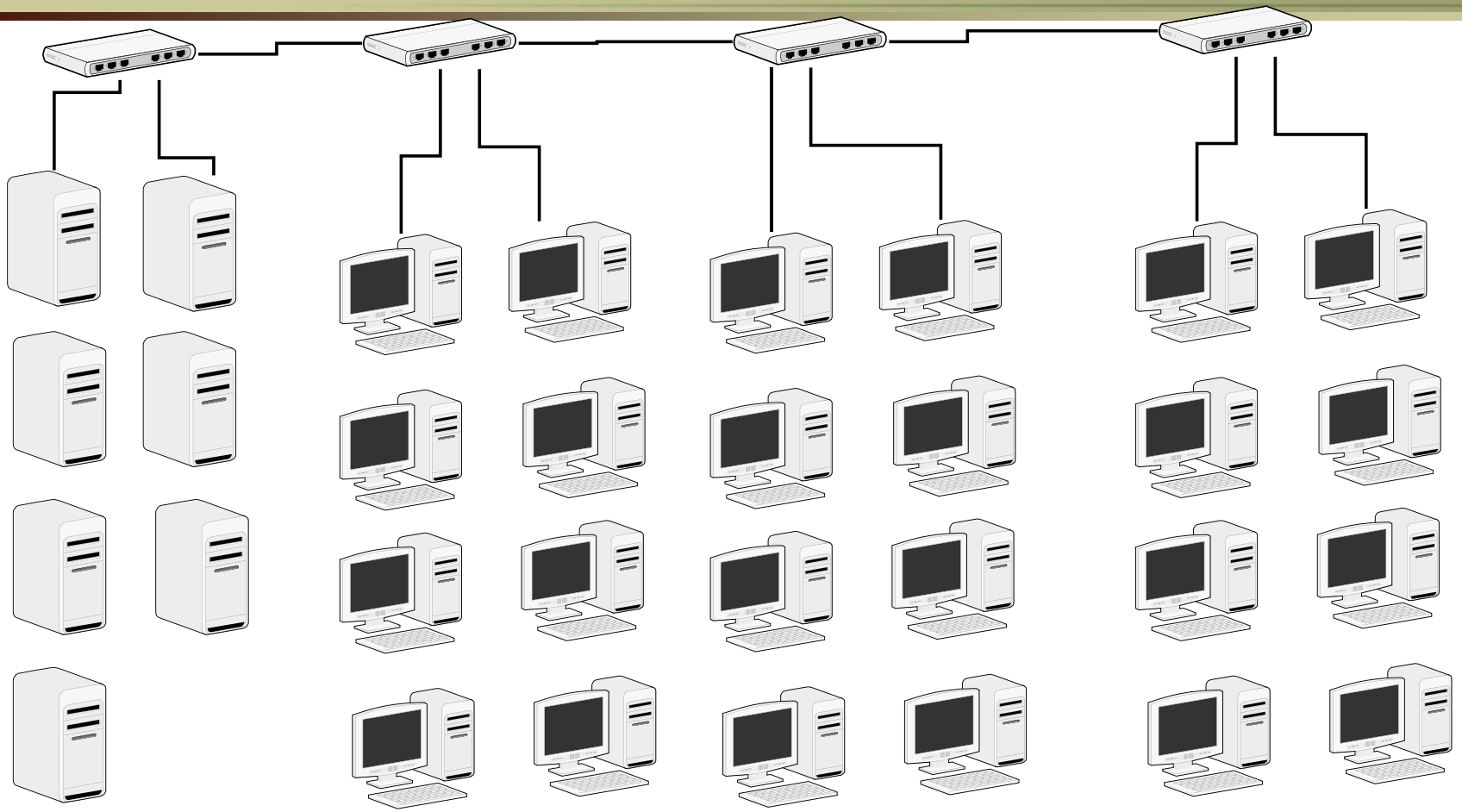
"The solidarity and collective will of the Coalition is our strength against the enemy that preys on weakness"

Admiral William Fallon, Commander
United States Central Command

Current CENTCOM Network Architecture



Desired CENTCOM Network Architecture



Today's Solution…not the answer!

- Separate physical networks
- Bloated front and back end equipment
- Each require US Type 1 Crypto
- Inefficient network monitoring

Desired Capabilities

- **Single infrastructure, i.e., workstations, switches, cables, etc.**
- **Reduce “air gap” transfer of info between networks**
- **Easier, faster network setup and administration**
  - Reduce sys admin, maintenance, manpower, Base Operating Services, etc.
- **Smaller IT logistics footprint and tail, less power consumption**
- **Ensure separation of domains in presence of consolidation**
- **Interoperate with deployed Coalition partner systems**
- **Ability to rapidly configure COIs without major physical change to the network**

Maximize use of existing IT investments

What we are doing

MISSION

Reduce workstation/network infrastructure to enable easier, faster network setup/administration. Create smaller logistics footprint with less power consumption and a capability to ensure robust separation of network classification domains.

END STATE

A capability to access separate networks (SIPRNET, NIPRNET, CENTRIXS, JWICS, and Bilateral Networks) on a single workstation, connected to a single wire, connecting to data centers for each networks.

Overview

- **System Security Engineering Process:**
  - Determining the recommended strength and degree of assurance for proposed services and mechanisms that become part of the solution
  - Strength and assurance features provide basis for selection of proposed mechanisms and a means of evaluating products that implement those mechanisms
- **Risk Factors:**
  - Degree of damage that would be suffered if the security policy were violated
  - Threat environment
  - Etc.
- **The value of the information to be protected and the perceived threat environment are used to determine the recommended**
  - Strength of mechanism level (SML)
  - Evaluation assurance level (EAL)

Determining the Degree of Robustness

Information Value	Threat Levels						
	T1	T2	T3	T4	T5	T6	T7
V1	SML1 EAL1	SML1 EAL1	SML1 EAL1	SML1 EAL2	SML1 EAL2	SML1 EAL2	SML1 EAL2
V2	SML1 EAL1	SML1 EAL1	SML1 EAL1	SML2 EAL2	SML2 EAL2	SML2 EAL3	SML2 EAL3
V3	SML1 EAL1	SML1 EAL2	SML1 EAL2	SML2 EAL3	SML2 EAL3	SML2 EAL4	SML2 EAL4
V4	SML2 EAL1	SML2 EAL2	SML2 EAL3	SML3 EAL4	SML3 EAL5	SML3 EAL6	SML3 EAL6
V5	SML2 EAL2	SML2 EAL3	SML3 EAL4	SML3 EAL5	SML3 EAL6	SML3 EAL6	SML3 EAL7

SML: Strength of Mechanism Level

EAL: Evaluation Assurance Level

Information Value

Violation of the information protection policy would:

- **V1 - Have negligible adverse effects or consequences**
- **V2 - Adversely affect and/or cause minimal damage to the security, safety, financial posture, or infrastructure of the organization**
- **V3 - Cause some damage to the security, safety, financial posture, or infrastructure of the organization**
- **V4 - Cause serious damage to the security, safety, financial posture, or infrastructure of the organization**
- **V5 - Cause exceptionally grave damage to security, safety, financial posture, or infrastructure of organization**

Threat Levels

- **T1 - Inadvertent or accidental events (e.g., tripping over a power cord)**
- **T2 - Passive, casual adversary with minimal resources who is willing to take little risk (e.g., listening)**
- **T3 - Adversary with minimal resources who is willing to take significant risk (e.g., unsophisticated hackers)**
- **T4 - Sophisticated adversary with moderate resources who is willing to take little risk (e.g., organized crime, sophisticated hackers, international corporations)**
- **T5 - Sophisticated adversary with moderate resources who is willing to take significant risk (e.g., international terrorists)**
- **T6 - Extremely sophisticated adversary with abundant resources who is willing to take little risk (e.g., well-funded national laboratory, nation-state, international corporation)**
- **T7 - Extremely sophisticated adversary with abundant resources who is willing to take extreme risk (e.g., nation-states in time of crisis)**

USCENTCOM Example

Information Value	Threat Levels						
	T1	T2	T3	T4	T5	T6	T7
V1	SML1 EAL1	SML1 EAL1	SML1 EAL1	SML1 EAL2	SML1 EAL2	SML1 EAL2	SML1 EAL2
V2	SML1 EAL1	SML1 EAL1	SML1 EAL1	SML2 EAL2	SML2 EAL2	SML2 EAL3	SML2 EAL3
V3	SML1 EAL1	SML1 EAL2	SML1 EAL2	SML2 EAL3	SML2 EAL3	SML2 EAL4	SML2 EAL4
V4	SML2 EAL1	SML2 EAL2	SML2 EAL3	SML3 EAL4	SML3 EAL5	SML3 EAL6	SML3 EAL6
V5	SML2 EAL2	SML2 EAL3	SML3 EAL4	SML3 EAL5	SML3 EAL6	SML3 EAL6	SML3 EAL7

SML: Strength of Mechanism Level

EAL: Evaluation Assurance Level

Levels of Assurance

- **EAL 1 Functionally Tested**

  Applicable where some confidence in correct operation is required, but when threats to security are not viewed as serious. This EAL is of value where independent assurance is required to support contention that due care has been exercised with respect to protection. An example is the protection of personal information.

- **EAL 2 Structurally Tested**

  Requires cooperation of the developer in the delivery of design information and test results, but should not demand more effort (or substantially increased cost or time) than is consistent with good commercial practice. This EAL is applicable where a low to moderate level of independently assured security is required in absence of an available development record. An example is securing legacy systems, or cases in which access to the developer is limited.

- **EAL 3 Methodically**

  Tested and Checked. Permits conscientious developer to gain maximum assurance from positive security engineering at design stage without substantial alteration of existing sound development practices. It is applicable where moderate level of independently assured security is required.

Levels of Assurance (cont)

- **EAL 4 Methodically Designed, Tested, and Reviewed**

  Permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices, which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. This is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. It is applicable in those circumstances in which a moderate to high level of independently assured security in conventional products is required, and where developers or users are prepared to incur additional security-specific engineering costs.

- **EAL 5 Semi-formally Designed and Tested**

  Permits a developer to gain maximum assurance from security engineering based on rigorous commercial development practices supported by moderate application of specialized security engineering techniques. This EAL is applicable where a high level of independently assured security in a planned development is required along with rigorous development approach.

- **EAL 6 Semi-formally Verified Design and Tested**

  Permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment to protect high value assets against significant risks. It is applicable to the development of security products that will be used in high-risk situations.

- **EAL 7 Formally Verified Design and Tested**

  Applicable to the development of products to be used in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Realistically, it is limited to products with tightly focused functionality that is amenable to extensive formal analysis.

Strength of Mechanism

- **SML1 - basic strength or good commercial practice. It is resistant to unsophisticated threats (roughly comparable to T1 to T3 threat levels) and is used to protect low-value data. Examples of countered threats might be door rattlers, ankle biters, and inadvertent errors**

- **SML2 - medium strength. It is resistant to sophisticated threats (roughly comparable to T4 to T5 threat levels) and is used to protect medium-value data. It would typically counter a threat from an organized effort (e.g., an organized group of hackers)**

- **SML3 - high strength or high grade. It is resistant to the national laboratory or nation-state threat (roughly comparable to T6 to T7 threat levels) and is used to protect high-value data. Examples of the threats countered by this SML are an extremely sophisticated, well-funded technical laboratory and a nation-state adversary.**

Solution

- **Single workstation to host multiple networks in multiple COIs**
  - High robustness, secure software, expandable for future requirements
  - Ability to continue to use existing, unaltered Microsoft operating system, applications, device drivers
  - Capability to add new hardware devices and drivers
- **Single network infrastructure on a "single wire“**
  - Replace multiple network interface cards with a single NIC connecting to a single switch
  - Hardware information separation switch to accommodate legacy systems on the “single wire”
- **Low security accreditation risk**
- **Low cost**
- **Affordable tech refresh and affordable re-certification**
- **Minimize disruption to existing systems, software, and operations**

USCENTCOM J8

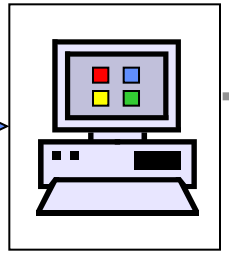
- **USCENTCOM J8 Science Advisor challenged his staff to find a way to eliminate the mass of wires and multiple computers on the Action Officers desk**
- **Called together the R&D community to seek a solution**
- **Briefed CENTCOM on a group working Multiple Independent Levels of Security (MILS)**
  - Primarily embedded software for aircraft; however provides separation of security domains
- **USCENTCOM challenged the community to solve our problem on networks**
- **Green Hills Software (GHS) and Objective Interface Systems (OIS) briefed USCENTCOM on a proposal for a JCTD that will provide for our requirements**
- **USCENTCOM is sponsoring the One Box – 1 Wire (OB1) Project as a Joint Capabilities Technology Demonstration (JCTD)**

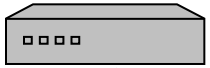
What we can achieve with OB1 (Operational View – OV1)

Legacy Non-Collapsed Environment:

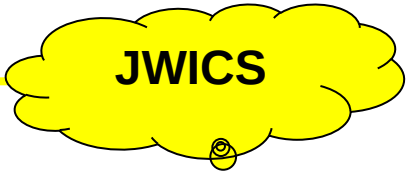
Enclave Data Center / External WAN

Collapse the desktop infrastructure to One box-1 Wire

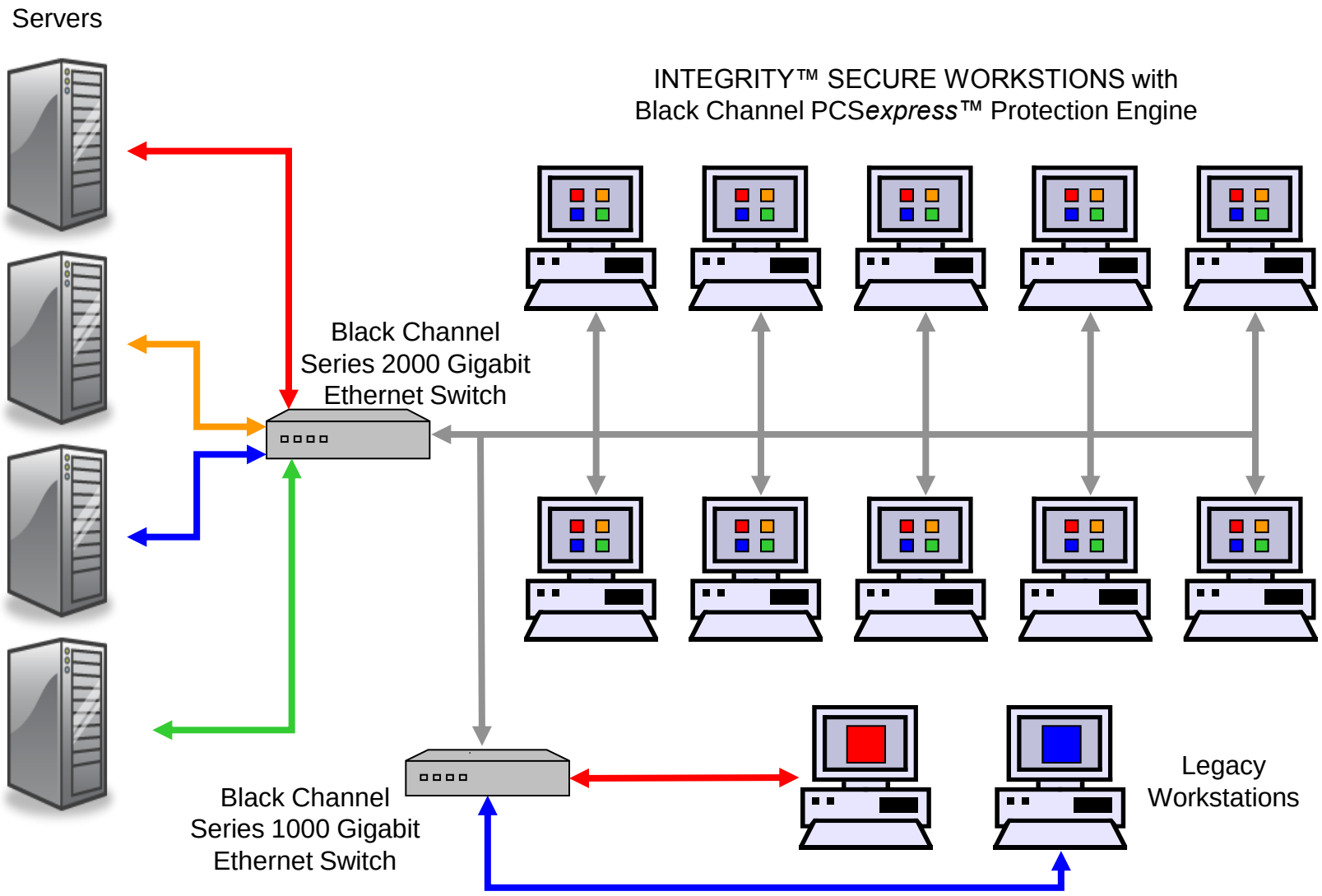




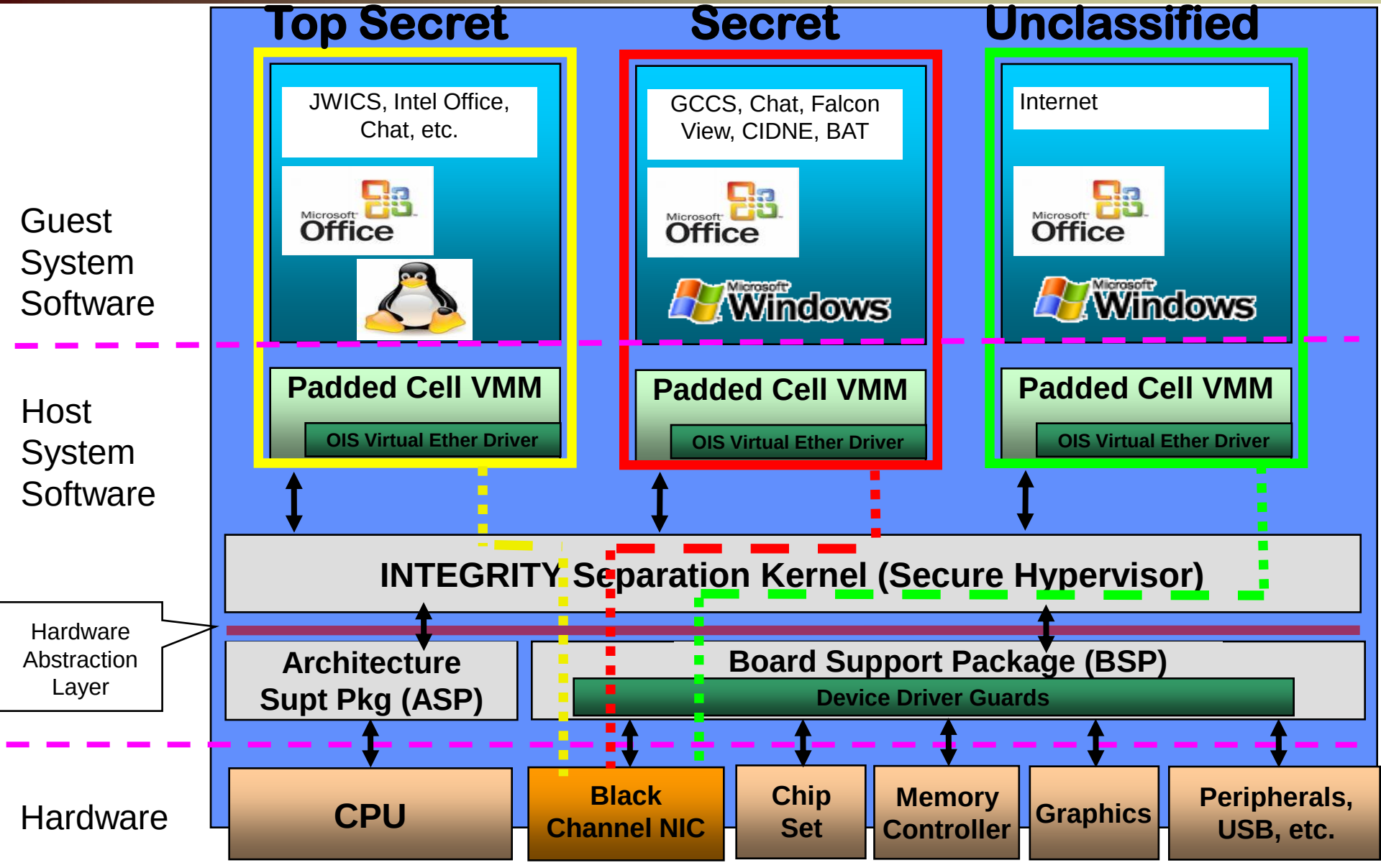
Secure Ethernet Switch



SV-1: System View 1



How OB1 keeps data separate while hosted on a common platform



Warfighter Pay-off

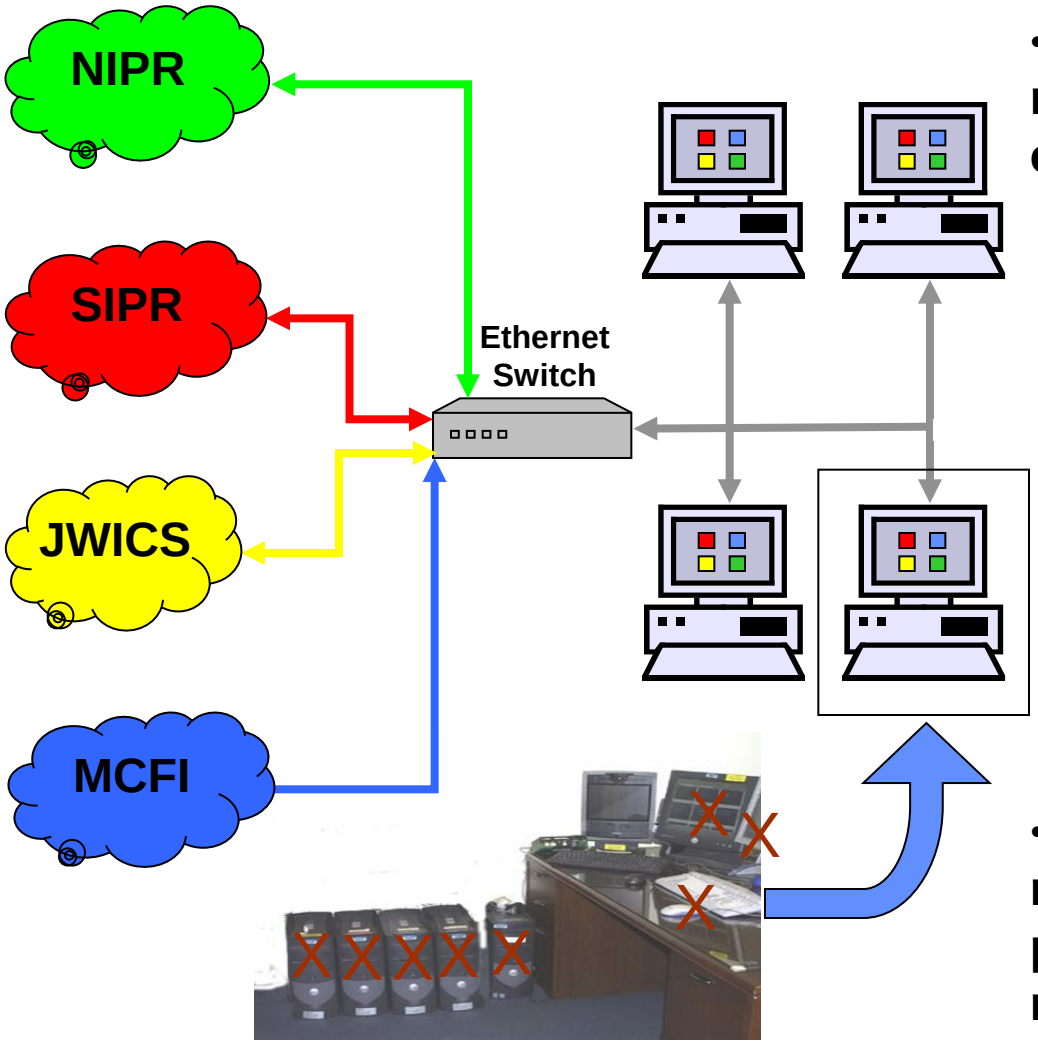
- **Delivery of information to Commanders and Warfighters much faster**
- **Reduction of redundant networks and hardware**
- **Reduce SWaP (Size, Weight, Power)**
- **Reduce cost**
- **Reduce complexity**
- **Reduced maintenance burden**
- **Allow Joint Task Force (JTF) to establish networks in the field much more rapidly**

Current Status of OB1

- **OSD (AT&L) designated One Box – 1 Wire (OB1) as an FY-09 "Rolling Start" JCTD**
- **The Technical Manager for this JCTD is Space and Naval Warfare Systems Center (SPAWAR) Atlantic and has established a test lab for the certification of OB1**
- **$4.3M???? has been applied to the JCTD so far**
- **The NIC and Switch encryption must be compliant to IPSEC, IKE V.2, and X.509 standards per NSA.**
- **Remaining efforts are aimed at final integration and Certification, Testing, and Evaluation, and user assessments**

What is the Bottomline?
"OB1 is a weapon that supports the way we fight"

"Designed for the environments where we fight"



- Only technology that meets the requirements of our high threat operational environment
  - Non U.S. controlled or "certified" physical spaces characteristic of tactical environment (tents/ad hoc construction etc.)
  - High number of mission partners with unknown backgrounds/levels of trust
  - Use of unclassified networks potentially exposes us to external risks (hackers)
- High "Robustness" – solution is mathematically proven and penetration tested to keep the networks separate and protected

Questions?

From this…

To this