Combat Effectiveness Testing of System of Systems in the Face of Cyber Threat

Presented at
National Defense Industrial Association Conference

March 3, 2010

Jon Payne
USJFCOM IO Range
256.842.0156
Jonathon.payne@jfcom.mil

Overview

What – Combat Effective vs Regulatory Compliant

When – Early and Often

Why – Risk Assessment

Where – Closed Environment

How – Operationally Realistic, Distributed LVC

What: Combat Effective vs Regulatory Compliant

- Compliance is necessary
  - Fiduciary and ethical obligation
  - Framework for Configuration Management
  - Supports enterprise management

but insufficient . . .

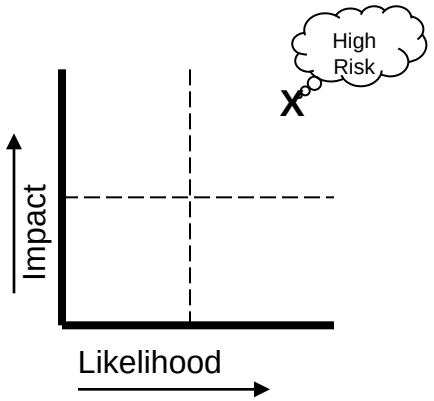
- Combat Effectiveness is essential
  - Survivable in the face of attack
  - Able to complete mission
  - Adds value to arsenal

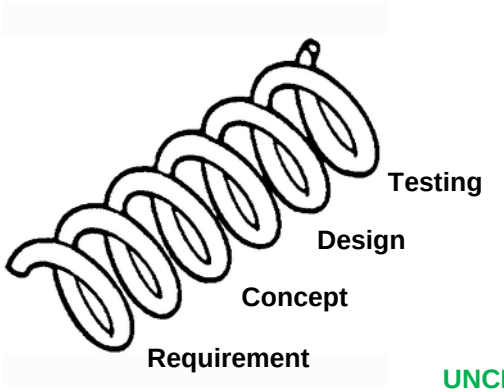
When: Early and Often

- Cost of failure is too high if the system is already built – find and fix early
- Survivability of a system against a cyber threat must be considered during:
  - Requirement generation
  - Concept development
  - System design and engineering
  - Developmental Testing
  - Operational Testing

Why: Risk Assessment

- Cost/benefit of cyber defense is a risk assessment
  - (A) What is the likelihood of failure?
  - (B) What is the impact of failure?
  - What are the costs to mitigate (A) or (B)?
- Risk analysis must be completed iteratively on modules, components, system, and system of systems



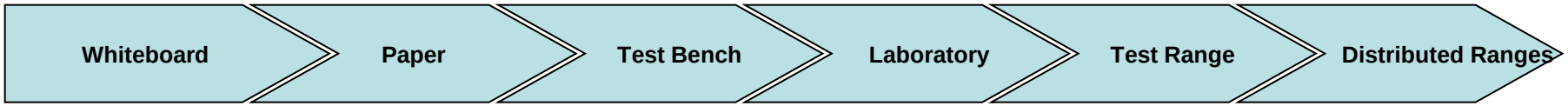


Where: Closed Environment

- Early assessment is whiteboard and paper process
- Testing begins in a controlled environment where variables are understood
- Testing environment must evolve early into operationally realistic “sandbox”
- Threat must be employed throughout the development and testing lifecycle
- Threat must be employed in a closed loop environment

How: Operationally Realistic Distributed LVC

- Use existing test ranges and assets
- Network capabilities at appropriate level of classification
- Use mission thread and operational TTPs
- Employ threat with likely capabilities, intent, and TTPs



IO Range Provides

- The only sustained capability to operate a distributed environment at multiple independent levels of security
- Standing infrastructure capable of supporting CNO, cyber testing, training and exercise
- Operationally realistic and technically representative environment
  - **Traffic Generation Systems** – provide realistic network activity
  - **CNO Labs** – CNO tool development, testing, and operations (servers, routers, firewalls)
  - **Large Computing Environments** – computers, switches, hubs, routers, and firewalls
  - **Telecom Environments** – Public Switched Telephone Network (PSTN), Public Land Mobile Network (PLMN), Global System for Mobile Communications (GSM)
  - **EW platforms**
  - **Threat systems and Red Teams**
  - **Communications** – Tactical C2, GPS, 802.11, LAN, WAN systems
  - **Supervisory Control and Data Acquisition (SCADA)/Critical Infrastructure Control Systems** – Using major vendors' hardware
  - **Models and Simulations**

IO Range Mission Areas

Supports all life cycle activities in the following **mission areas**, as tasked by USD(I) and original stakeholders:

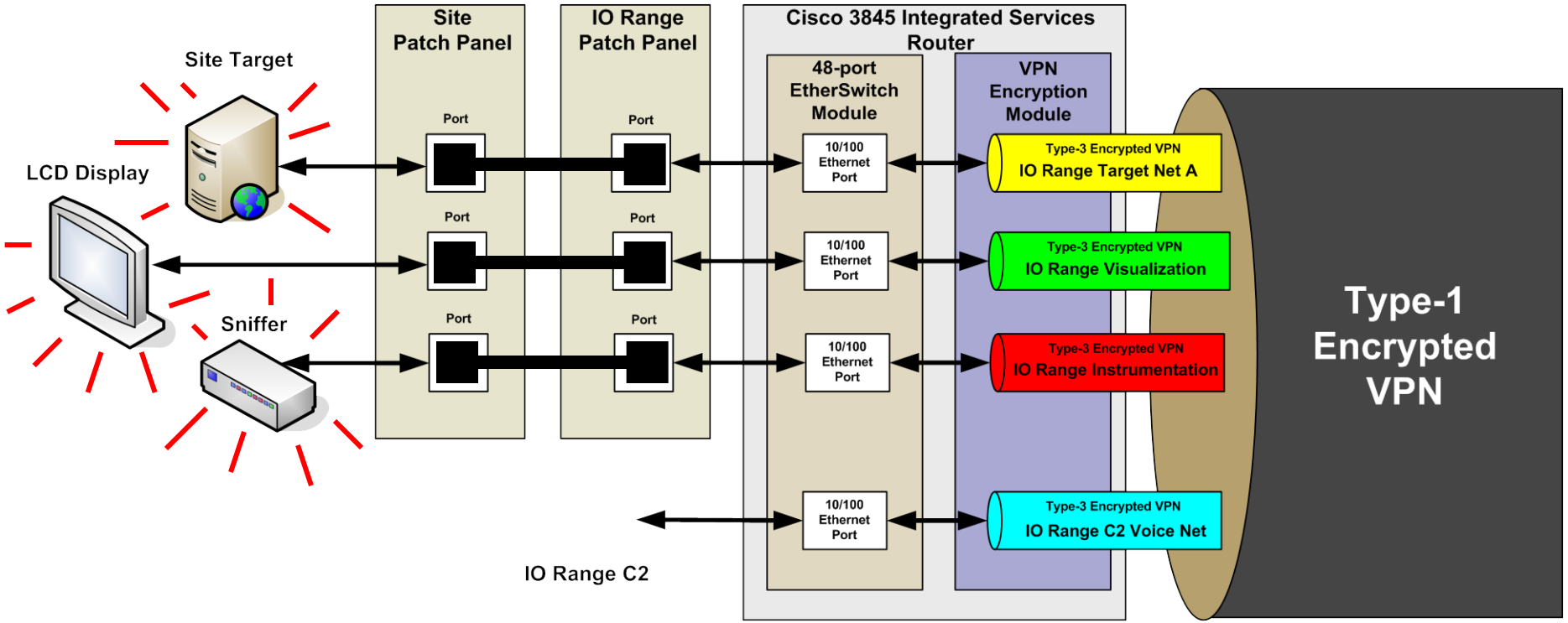
- Basic and advanced research and development (R&D)
- Experimentation
- Modeling and Simulation (M&S)
- Developmental test and evaluation (DT&E)
- Operational test and evaluation (OT&E)
- Exercises
- Training Certification
- Studies and Analyses
- Battle lab demonstrations, Advanced Concept Technology Demonstrations (ACTDs), Advanced Technology Demonstrations (ATDs), and other experiments
- Tactics, techniques, and procedures (TTP) development
- Rules of engagement (ROE) approvals and authorities
- Legal reviews and assessments
- Tool and weapon system operations
- Joint Munitions Effectiveness Manual (JMEM) validation
- Mission rehearsal
- Targeting and battle damage assessment (BDA) development

Key IO Range Concepts

- ***Standing infrastructure***
  - Supports execution of events at multiple independent levels of security
- ***Closed loop network***
  - Encrypted backbone to support secure tailored customer events
  - Multiple VPN tunnels within each circuit to segregate traffic
- ***Streamline event approval process***
  - Comprehensive Event Agreements
  - Short and long term Interconnection Security Agreements (ISA)
  - Leverage existing DoD policies and processes
- ***Centralized management, security and coordination***
  - IO Range Operations Center (IOROC) at JWFC provides single point for the distributed IO Range

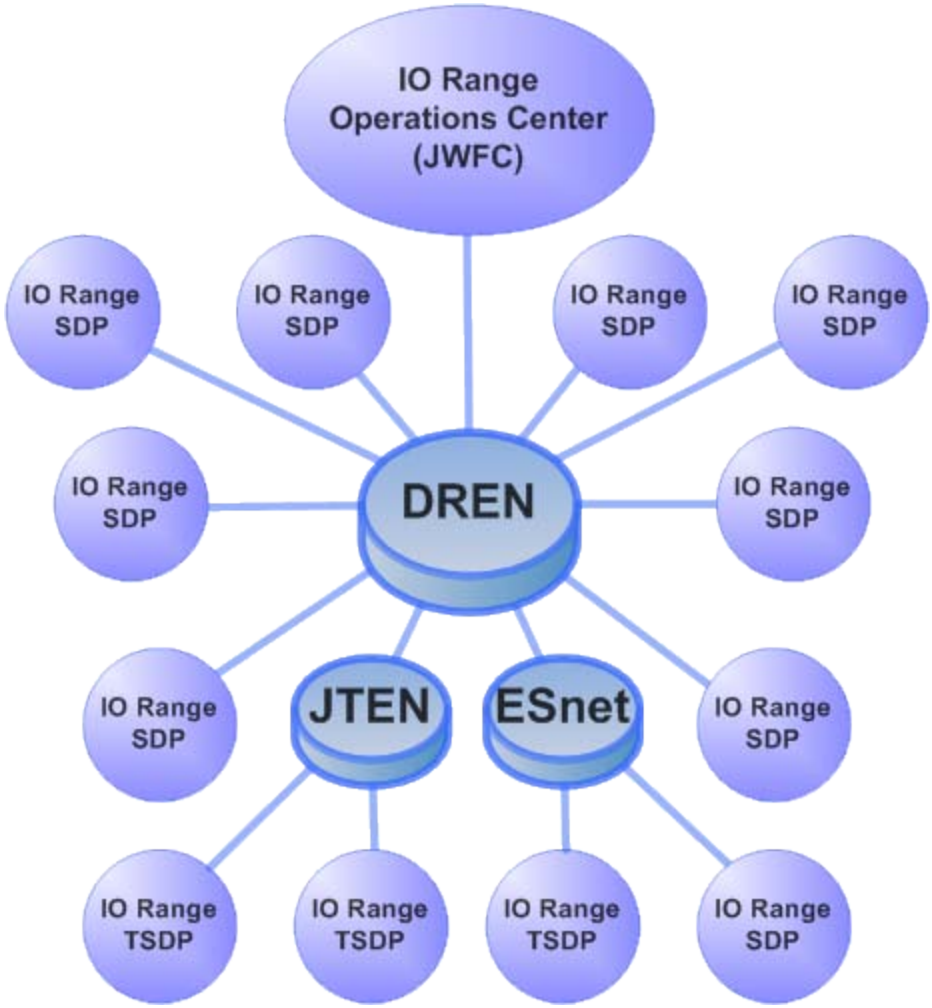
Segregation of IO Range Activities

- IO Range architecture supports multiple segregated activities at different classification levels
  - Patch panels enable sites to control connections to IO Range
  - One-for-one relationship between ports and VPNs



IO Range Network Topology

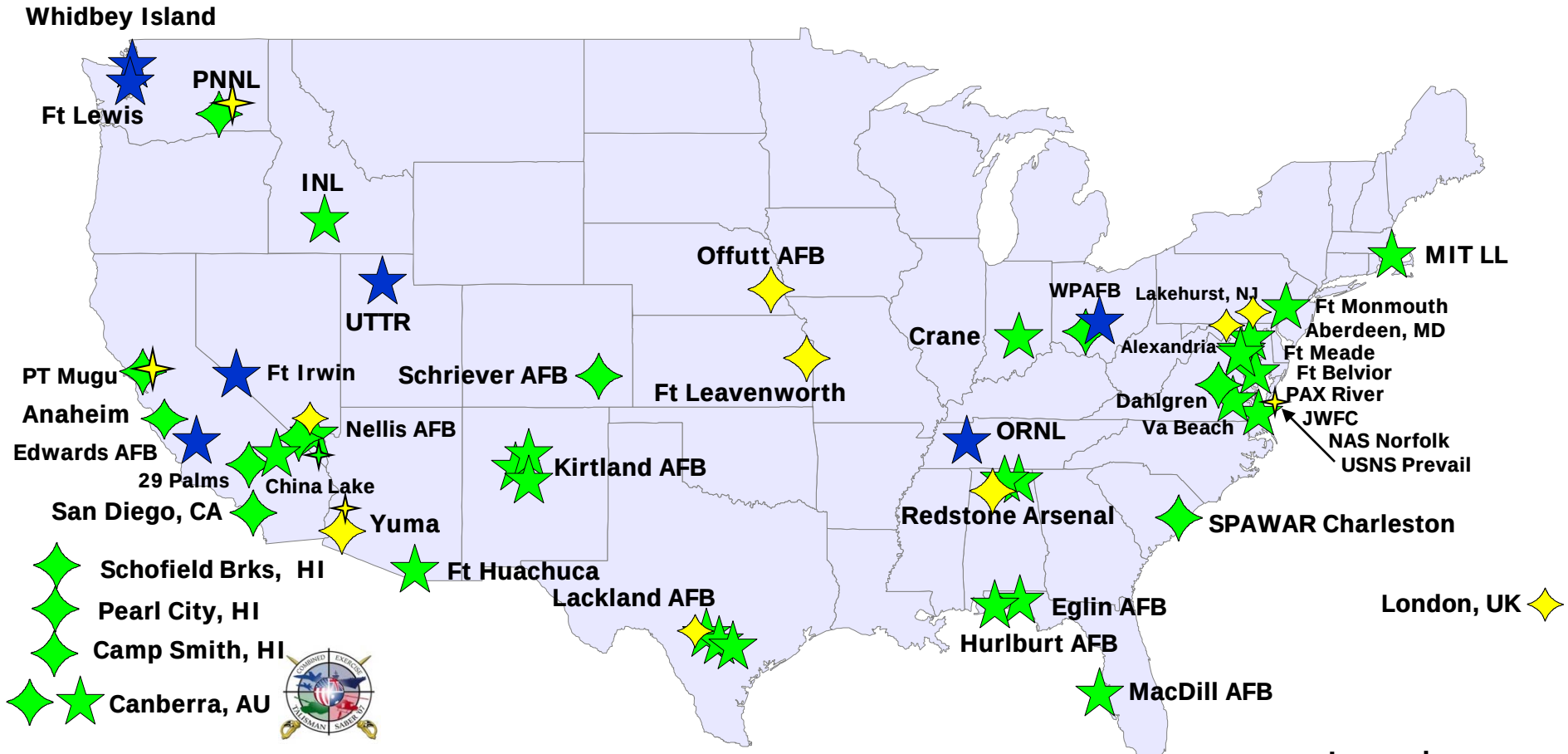
- **The IO Range utilizes a full-mesh VPN network topology**
- **DREN is primary provider of site to site connectivity**
- **Provides point to point encryption across a high-performance and low latency wide area network**
- **Utilize JTEN where DREN is not feasible**
- **Utilize ESnet to connect to DOE labs and facilities**



IO Range Service Delivery Points

- IO Range Service Delivery Points (SDP) are equipment suites located at each member site
  - Encrypts all site-to-site traffic using appropriate COMSEC
  - Provide persistent connectivity between all IO Range sites
  - Supports the rapid creation of logical ranges between the participating sites
  - Facilitates the participation of additional organizations co-located at or near the participating site
  - Segregates/Isolates user communities to mitigate the risks associated with co-mingling multiple classification levels
  - Support integration of the necessary technologies/services required by the IO Range

Information Operations Range



IO Range:

1. Increases COCOM awareness and confidence in IO capabilities
2. Increases integration of non-kinetic effects with kinetic warfare
3. Supports emerging IO technologies
4. Facilitates training against IO targets sets
5. Integrates IO capabilities into Joint training, testing, and experimentation

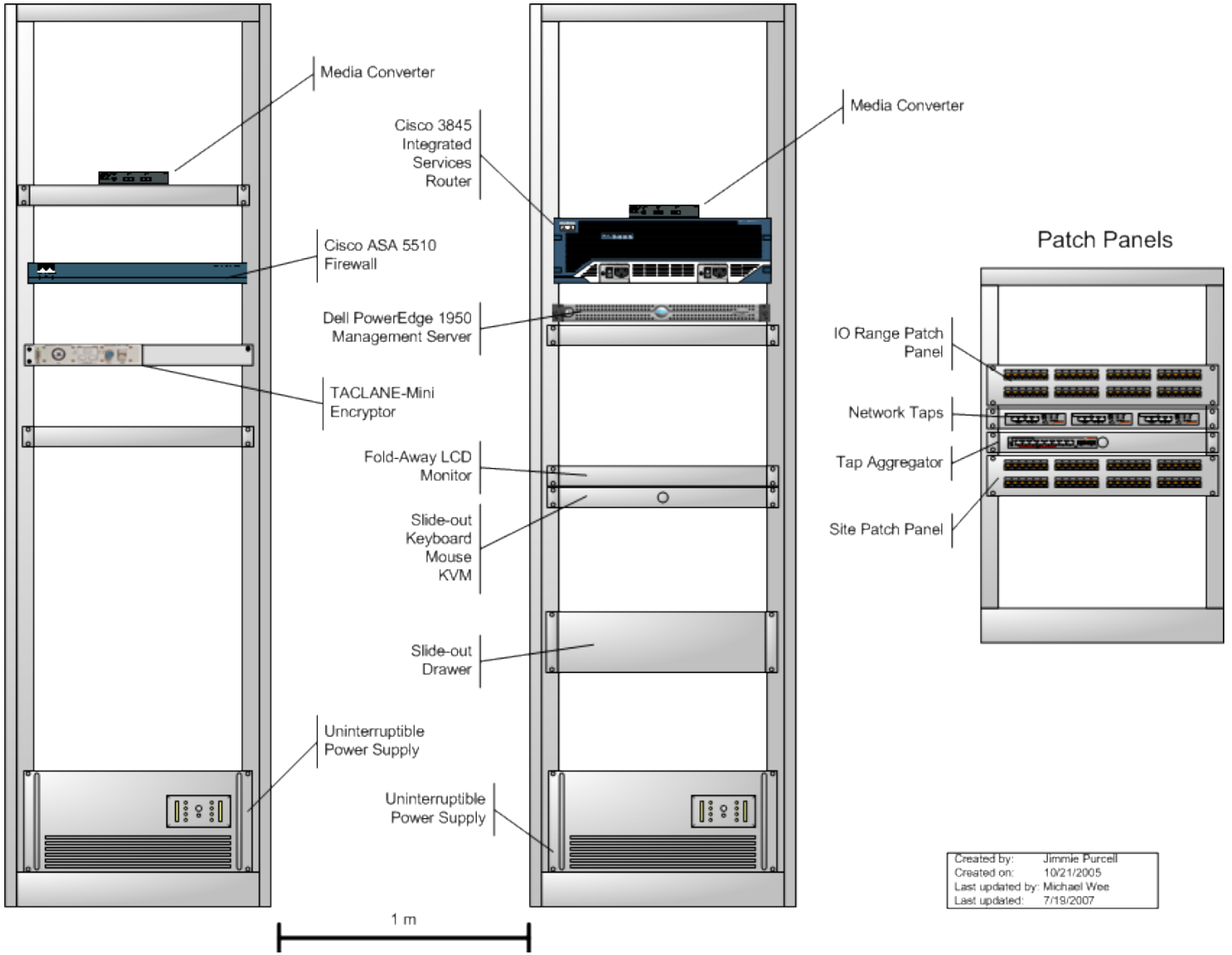
Legend

	Persistent	Transactional	Micro
Installed	★	✦	✦
In Progress	★	✦	✦
Planned	★	✦	✦

Current as of: 01 Dec 09

IO Range Service Delivery Point Design

- **Nominal configuration consists of two 19in full-height racks with separate external patch panels**
- **Full-height rack support growth and new requirements**



Summary

The IO Range:

- Increases COCOM awareness and confidence in IO capabilities
- Increases integration of non-kinetic effects with kinetic warfare
- Supports emerging IO technologies
- Facilitates training against IO targets sets
- Integrates IO capabilities into Joint training, testing, and experimentation

Points of Contact

Chief: LTC John Ballard
Comm 757-836-9785
DSN 836-9785

Email Contacts

Future Ops ior-reqs@jfcom.mil

Current Ops ior-ops@jfcom.mil

Security IOJMO-Sec@jfcom.mil

Technical ior-nosc@jfcom.mil

Questions?

Information Operations Range
“Dare to Know”