DISA

Defense Information Systems Agency

A Combat Support Agency

Forecast to Industry Program Executive Office – Mission Assurance/NetOps

**Mark Orndorff
Director,
PEO – MA/NetOps
29 July 2010**

What We Do

- We develop, acquire, and implement enterprise wide Computer Network Defense (CND) and IA security products and solutions that identify threats to the GIG, sense network and host-based attacks, develop/disseminate countermeasures.
- Provide situational awareness supporting GIG NetOps personnel.
- We provide secure and reliable identity management services for DoD applications and systems.
- We provide cross-domain information sharing solutions for users anywhere on the GIG.

Mission Assurance - Approach

- **Reduce Attack Surface**
  - **Configure securely, automatically**
  - **Enhance perimeter defenses – defense in depth**
  - **Drive out anonymity**

- **Improve Network C2**
  - **Improved situational awareness**
  - **Cyber attack detection, diagnosis, and reaction at network speed**

- **Improve Safe Sharing**
  - **Cross domain flows as enterprise service**
  - **Evolve directory, identity, and access control to support net-centricity**

![DISA - A Combat Support Agency logo]

Mission Assurance

Partnerships

- **Whitelist at NIPRNET boundary**
  - Reduced our attack surface by over 95%
- **Host Based Security System**
  - Reduce attack surface
  - Global situational awareness
- **Public Key Infrastructure (PKI)**
  - Removing anonymity
  - Identity Management
- **Command Cyber Readiness Inspections (CCRI)**
  - Decrease window of vulnerability exposure
  - Improve readiness

Opportunities

- **NIPRNET Hardening**
  - Web Content filter, e-mail security gateway, DNS proxy, virtual desktop
- **DMZ for internet facing applications**
- **Host Based Security System**
  - Multi-phased lockdown
  - Machine-to-machine enterprise architecture
- **Hardware token for SIPRNET PKI**
- **Network mapping**
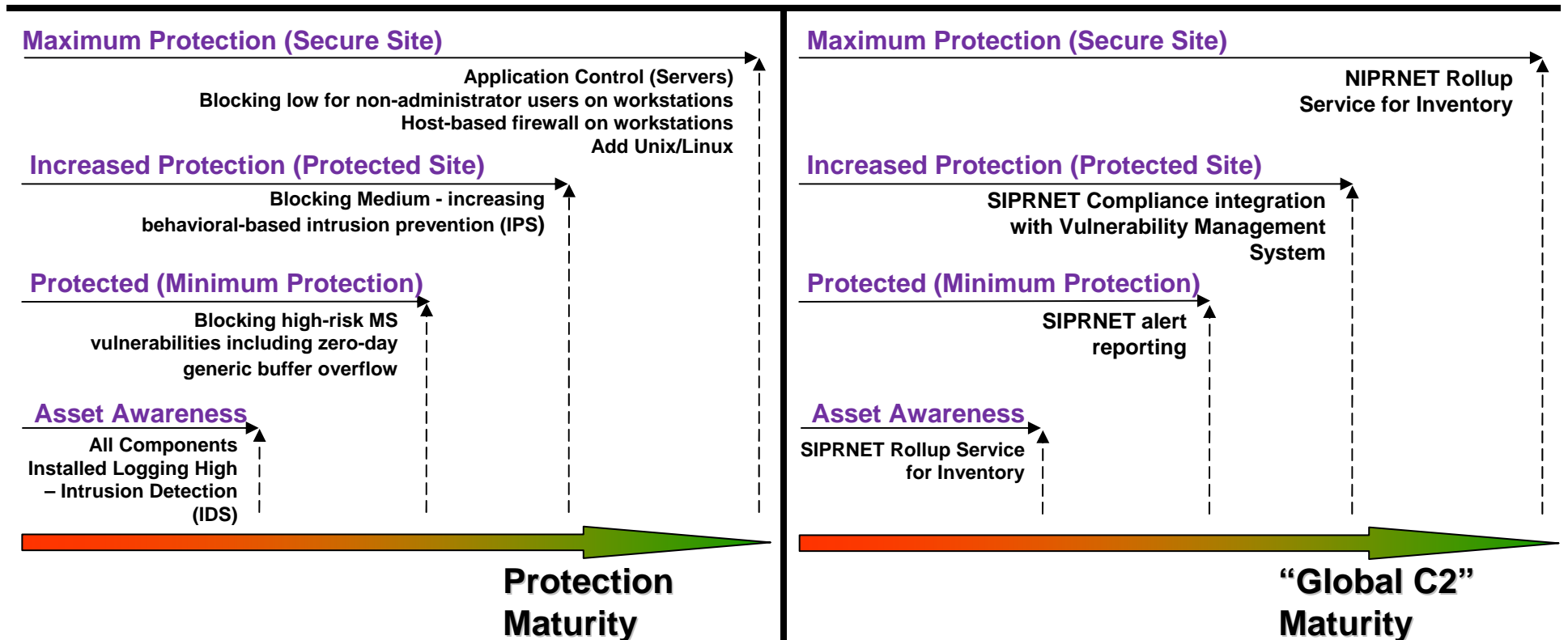- **Integrated cyber training**

Where We Are

A Combat Support Agency

- **Host Based Security Systems (HBSS)**
  - Pushing for complete deployment across DoD
- **Expanding the capabilities across the DMZ's**
  - Log Aggregation and management
  - Web Proxy
  - Web Filtering
- **Situational Awareness**
  - Integration of additional data sources
  - New designs to meet the Warfighter's emerging needs
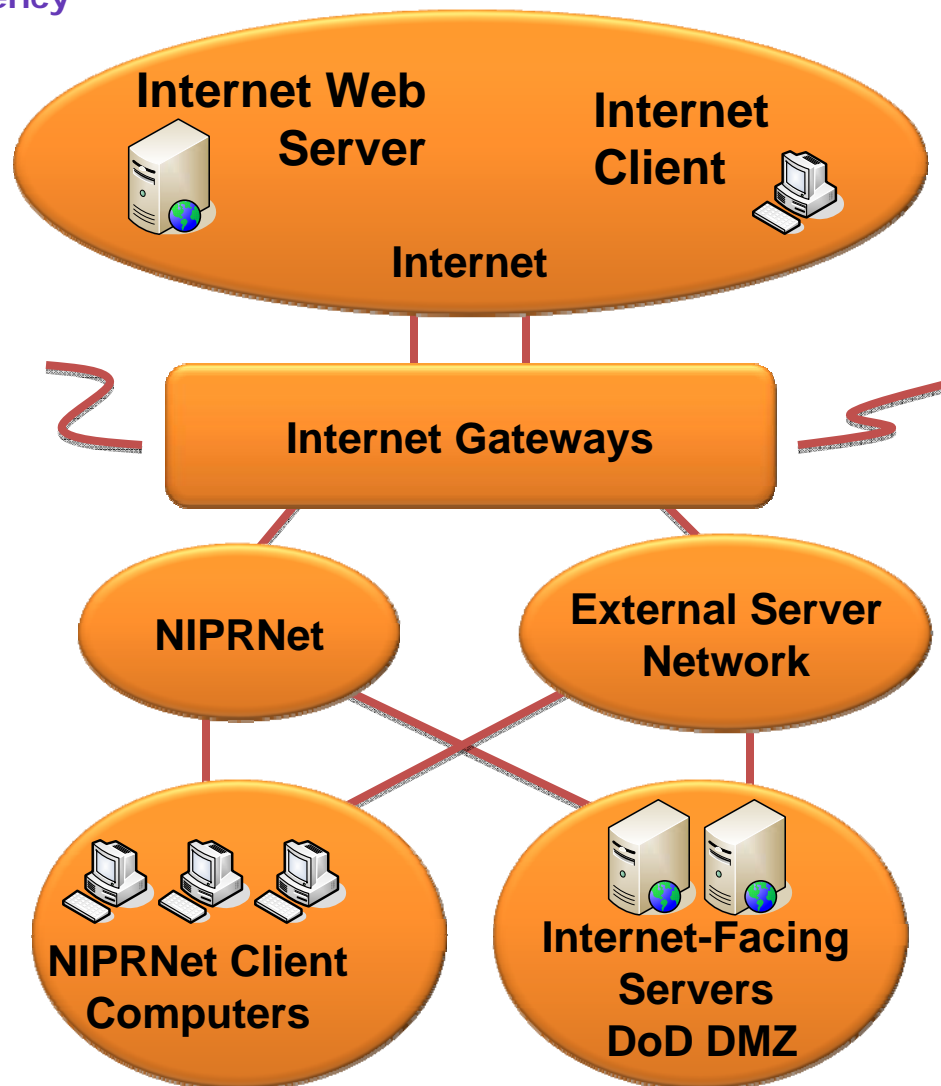- **Expansion of Enterprise Cross Domain**

HBSS Evolution

DISA

A Combat Support Agency

1. **Safe installation on all Windows systems**
2. **Global Situational Awareness on SIPRNET followed by NIPRNET**
3. **Deliberate process to improve security level and add capabilities (including DoD-unique components)**

Maximum Protection (Secure Site)

Application Control (Servers)
Blocking low for non-administrator users on workstations
Host-based firewall on workstations
Add Unix/Linux

Increased Protection (Protected Site)

Blocking Medium - increasing
behavioral-based intrusion prevention (IPS)

Protected (Minimum Protection)

Blocking high-risk MS
vulnerabilities including zero-day
generic buffer overflow

Asset Awareness

All Components
Installed Logging High
– Intrusion Detection
(IDS)

Protection Maturity

Maximum Protection (Secure Site)

NIPRNET Rollup
Service for Inventory

Increased Protection (Protected Site)

SIPRNET Compliance integration
with Vulnerability Management
System

Protected (Minimum Protection)

SIPRNET alert
reporting

Asset Awareness

SIPRNET Rollup Service
for Inventory

"Global C2" Maturity

6

NIPRNet Perimeter Defense

DISA
A Combat Support Agency

Internet Web Server

Internet Client

Internet

General Purpose NIPRNET Defenses

Internet Gateways

DoD DMZ

For Externally Visible Servers in a DoD DMZ

NIPRNet

External Server Network

NIPRNet Client Computers

Internet-Facing Servers DoD DMZ

The Next 60 Days

Contract/Task/Area of Support	Anticipated Award
FY10	
DISA NetOps Support	4QFY10
IA2 IA and Security Engineering Support	4QFY10

The First Half of FY 2011

Contract/Task/Area of Support	Anticipated Award
FY11	
Assured Compliance Assessment Solution (ACAS)	1QFY11
Email Security Gateway (EMSG)	1QFY11
eMASS	1QFY11
NetOps SA	1QFY11
Public Key Enabling (PKE)	1QFY11
Client Server Enterprise License	2QFY11

Where We Are Going

- **Host Based Security Systems (HBSS)**
  - Fully deployed across the network
  - Additional capabilities to address warfighter needs
  - Examine technology for future host based architecture
- **Expand the DMZ's**
  - Reduce/mitigate/eliminate Denial of Service risk
  - E-Mail security and filtering
  - Web vulnerability scanning
  - Log Aggregation and management
- **Vulnerability Scanning and Remediation**
- **Refine future requirements and identify technology refresh requirements for follow-on capabilities**

Contract/Task/Area of Support	Anticipated Award
FY11	
Privilege Management Solution	3QFY11
DoD Antivirus	4QFY11
Detection Denial of Service (DDOS)	4QFY11
Host Based Security System – Maintenance/Support Services	4QFY11
Host Based Security System - Open Architecture	4QFY11
Remediation Tool	4QFY11

How Do We Get There

- **Partnership with vendor community**
  - Better communication of our needs
  - Need your help to ensure that we are providing clear, obtainable, and realistic requirements
  - Assist in removing our blinders so we look for innovation and unique solutions to our problems
  - To market and implement solutions
  - To understand the market space and develop innovative ways to scope costs related to the actual usage
  - Streamline our process

- **We don't have all of the answers – but together we can solve the problem**

With your HELP

Our Next Steps

- **Increased vendor participation in Market Research and acquisitions (Vendor days and demonstrations)**

- **"Brainstorming" events to encourage both Government and industry innovation**

- **Emphasis on implementation of solutions – reduce the deployment time**

Partnership