Ports, Protocols, and Services Management (PPSM)

PPSM, Project Manager
29 July 2010
Develop and implement DoD policy and procedures that govern the use and management of applications, protocols, and services (with their associated ports) in DoD Information Systems; in a manner that promotes network security, interoperability, and the evolution of net-centric operations across the Enterprise Networks.

“Committed to Protecting Data End-to-End”
What is PPSM?

Created to ensure that applications, protocols, and services (with their associated ports) used in DoD Information Systems are registered, controlled, and regulated.

PPSM provides support to:

- Acquisition and Development
- Certification and Accreditation
- Enterprise, Organization, and System DAAs
- NetOps
- Perimeter and boundary defense
- Connection approval processes (UCAO/CCAO/DSAWG/DISN PAA)
- Firewall Administrators

Best known use - to configure network security devices (e.g. routers, firewalls, and IDS/IPS)
Why is PPSM Important?

To identify the vulnerabilities and risks associated with the use of certain protocols or services:

- Registered in the DoD PPSM Registry
- Undergo a vulnerability assessment
- Assigned an assurance category
- Regulated based on their potential to cause damage to DoD operations.

Adhering to PPSM guidance minimizes the inherent risk associated with the use of an application’s protocols and services.
What if I Do Not Comply?

Failure to comply with DoD Ports, Protocols, and Services Management (PPSM) requirements can result in:

- Compromise of the enclave boundary protections
- Impair functionality of the protocols and services
- DoD Information System exposed to unnecessary risk

DCPP-1: DoD information systems do not comply with DoD PPSM guidance, are not identified, or are not registered
What Else Should I Know?

**Negative Impacts:**

- Certification & Accreditation (C&A)
- Hosting/Fielding Systems in the Defense Enterprise Computing Centers (DECCs)
- May not be allowed to connect to GIG
- Traffic being Blocked by Destination Firewalls

Open, undocumented, and unnecessary ports, protocols, and services increase the risk of data compromise and system unavailability.
When to Comply w/PPSM

DIACAP Activities

1. Initiate and Plan
   IA C&A
   - Register System with DoD Component IA Program
   - Assign IA Controls
   - Assemble DIACAP Team
   - Initiate DIACAP Implementation Plan

2. Implement and Validate
   Assigned IA Controls
   - Execute DIACAP Implementation Plan
   - Conduct Validation Activities
   - Prepare POA&M
   - Compile Validation Results in DIACAP Scorecard

3. Make Certification Determination
   & Accreditation Decision
   - Make Certification Determination
   - Issue Accreditation Decision

4. Maintain Authorization to
   Operate and Conduct Reviews
   - Maintain Situational Awareness
   - Maintain IA Posture
   - Conduct Reviews (Review of IA Controls must occur at least annually)
   - Initiate Re-accreditation

5. Decommission
   - Retire System

DoD Information Systems
- AIS Applications
- Enclaves
- Platform IT Interconnections
- Outsourced IT-Based Processes

Decommission System

DCPP-1

DCPP-1
PPSM Process

• Register DoD IS – PPSM URL:  https://pnp.cert.smil.mil
• VA team researches associated protocols and services
• Technical Advisory Group (TAG)
• PPSM CCB Votes on Category Assurance Levels (CAL)
• Products published on IASE and DKO websites (high/low)

Information Assurance Support Environment – IASE

Army Knowledge Online/Defense Knowledge Online - AKO/DKO
NIPRNet - https://www.us.army.mil/suite/page/396114

UNCLASSIFIED
Assurance Levels

- Red – Banned
- Yellow – Acceptable
- Green – Best Practice

- Orange – Controlled (DSAWG Approved)
  - Operational Need
  - System by System basis
2009 Accomplishments

- Provided greater clarity of PPSM policy and technical guidance
- Redesigned the analysis criteria
- Developed and published the Exception Management Process
- PPSM training module -- DISN Data Services Training Manual.
- Introduced a new Assurance Category & Exception Process
- Awarded DISA Non-Technical Program/Project of the Year
Future Outlook

- Link the PPSM (Registry) database with other repositories
- Incorporating Air Force PPSM database
- Compliance validation and configuration management toolsets
- Differentiating between Classified and Unclassified environments
- Ability to access the PPSM Registry on the low side (NIPRNet)
PPSM

"Committed to Protecting Data End-to-End"

Questions?

UNCLASSIFIED
Back ups
Stakeholders

Who depends on PPSM?

- DoD
- Non-DoD Agencies
- PAAs (Principal Accrediting Authorities)
- DAAs (Designated Accrediting Authorities)
- DSAWG
- JTF-GNO -- Network Operations/Enforcement
- FSO – STIGS and Audits
- DISA CIO -- Certification & Accreditation authority
- Development Program Managers
- Acquisition Program Managers
- Firewall Administrators
- Commercial Vendors
What is a DoD Information System?

DoD Information System

Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections.
What does a DOD IS Look Like?

PPSM
Maintains DoD Registry of DoD IS ports, protocols and services usage

Hardware

Software

Application

Protocol

Service

Security Technical Implementation Guide (STIG)

Category Assurance Level (CAL)

Vulnerability Assessment (VA)
Assurance Level Changes

Old

• **Green** (High assurance)
  – Considered best security practices and recommended for use when implemented with the required mitigation strategy and approved for a specific DoD information system.

• **Yellow** (Medium assurance)
  – Acceptable for routine use only when implemented with the required mitigation strategy and approved for a specific DoD information system.

• **Red** (Low assurance)
  – Unacceptable vulnerability for routine use.
  – Only be allowed when approved by for a specific DoD information system under defined conditions and restrictions and if no suitable alternative exists.

NEW !!!

• **Green** (Best Practice)
  – Recommended as best security practices
  – Technical vulnerability acceptable with minimal mitigations
  – Advocated for use in new systems

• **Yellow** (Acceptable)
  – Technical vulnerability can be acceptably mitigated

• **Orange** (Controlled)
  – Technical vulnerability cannot be mitigated to an acceptable level
  – Legacy usage only - based on operational need
  – Not for use in the Acquisition and Development of new systems

• **Red** (Banned)
  – Prohibited – No Exceptions!
  – Technical vulnerability cannot be mitigated
  – Malware
  – Protocols and Services with no Life Cycle Support
  Or, 3rd Party Maintenance Support
Exception Package

- Operational Need
- Ports, Protocols, Services, and IP Addresses
  - Includes hosts, IP address ranges, and subnets
- Executive DIACAP package includes:
  - System Identification Profile (SIP)
  - DIACAP Implementation Plan (DIP)
  - System Accreditation Decision
- POA&M