Air Force PPS

TERMS

AF PPS Worksheet - refers to the template spreadsheet used as artifact in the accreditation/authorization (DIACAP/RMF) process to identify and document PPS for information systems; this spreadsheet also supports compliance determinations, approval, and registration in the DoD PPSM Registry (aka DoD PPS Database); each version of the spreadsheet contains an expiration date due to recurring changes with DoD PPS standards; see the "Worksheet, Process, & Registration" page for guidance

Change Requests - check out this page and the other, more specific, wiki pages on change request processes and specific types of requests to change the rules or configuration of devices on the network to allow communications interfaces or traffic flow

Cloud Services - check out this page for PPS guidance on Cloud Services

DoD DMZ Whitelist - check out the "DMZ Whitelist" page for guidance and procedures for Internet Facing Applications

DoD PPSM Category Assurance List (CAL) - check out this page for guidance on the use of PPS across DoD information networks based upon published DoD PPS Vulnerability Assessment Reports listed in the DoD PPSM CAL

Enclaves - circuit-enclaves and other hosting environments address PPS according to the components within their own accreditation/authorization package; check out the "Enclaves" page for guidance

Firewall Changes - check out the "Firewall Exceptions" page for guidance on requesting changes to firewalls to allow the use of PPS across enclave and DoD network boundaries.

Internet Access Point (IAP) - check out the "Firewall Exceptions" page for guidance on non-standard use of PPS across the IAP

Lessons Learned - would you like to know how to address AFSEN, VoIP, OpenFox, PEX, DoD KMI or other common issues? Check out the "Lessons Learned" page for more information

Non-Compliant PPS - do you plan to use a PPS not listed on the DoD PPSM CAL? Or use PPS that does not follow the standards of a DoD PPS Vulnerability Assessment report? Check out the "Non-Compliant PPS" page for more information on submitting a new PPS for review or obtaining an exception to current DoD PPS standards

Registration - every information system connecting to or operating on DoD networks (NIPRNet and/or SIPRNet) must have an entry in the DoD PPSM Registry; these PPS records show compliance with DoD PPS registration policy, allow compliance checks, and enable validation of interconnections and firewall

rules; check out the "PPS Worksheet & Registration" page for the process and to find out if an information system has proper PPS registration with a PPSM Tracking ID

Website Blocks (HOT - Recent Changes) - check out the "Website Blocked" page for guidance on how to address website blocks by either the Air Force or USCYBERCOM.

DoD PPS Description, Purpose, and Overview

Objective: Cataloging, regulating, and controlling the use and management of protocols, data services, and their associated port numbers on DoD information networks including interconnected information systems and software/applications.

Goal: Preventing the use of unregulated PPS that has the potential to damage DoD operations and interests.

Methods: Implementation of positive technical controls at the:

- Network level via "Deny All, Permit by Exception (DAPE)" for network boundary devices
- System/software/application level via "Least Function" by disabling any unnecessary PPS

PPS Defined:

- Protocol: A set of rules used by both ends of a communication channel. Information system protocols using the TCP/IP communication model have specific data packet types that are different for each protocol. Examples of transport layer protocols include, but are not limited to, TCP and UDP.
- Service: The named standard, unique, or proprietary packet structure and associated communication configuration that is instantiated.
- Port Number: The logical connection point for the transmission of information packets.

Vulnerability: Open, undocumented, and unnecessary ports, protocols, and services

Risks:

- Unauthorized connection of devices
- Unauthorized transfer of information
- Unauthorized tunneling
- Increased risk of data compromise and system unavailability

General Security Measures:

- Limit component functionality to a single function per device
- Review functions and services provided by information systems or individual components of information systems
- Determine which functions and services are candidates for elimination
- Disable unused or unnecessary physical and logical ports/protocols

PPS Points of Contact and Responsibilities

Various organizations contribute to the PPS process. The following information provides key POCs and information on their role in the process.

Air Force:

- AF PPS Office - provides guidance on PPS policy and process; provides field support to information system PMs, ISSMs, ISSOs, Change Sponsors, Change Managers, and network operations squadrons under 24th AF; registers PPS for all information system accredited/authorized by Air Force AOs/DAAs; processes exceptions; serves as AF Representative for DoD PPS Technical Advisory Group (Ref AFI 17-130, *Air Force Cybersecurity Program Management* [formerly numbered as 33-200])

- SAF/CIO A6 - serves as AF voting representative on DoD PPSM CCB (Ref AFI 17-130)

- 24th Air Force - regulates use of PPS across AFIN/AFNet (Ref T.O. 00-33A-1001, *General Cyberspace Support Activities Management Procedures and Practice Requirements*); for specific information systems, the 24th AF also serves as the Cybersecurity Service Provider (CSSP) (formerly Computer Network Defense - Service Provider [CND-SP]) in accordance with DoDI 8530.01, *Cybersecurity Activities Support for DoD Information Network Operations*
    - CSSP First Name: 24 AF
    - CSSP Last Name: A3/6M
    - CSSP Phone Number: DSN 969-0326
    - CSSP Email: 24af.a3x.cndsp@us.af.mil
- AO/DAA - approves use of PPS through accreditation/authorization process - Ref DoDI 8551.01 and AFI 17-101, (formerly AFI 33-210), *Risk Management Framework (RMF) for Air Force Information Technology (IT)*
- Program Manager - ensures proper implementation of security controls and processes related to PPS to include POA&M actions and annual reviews (Ref AFI 17-101)
- Information System ISSM and ISSO - completes, verifies, and maintains PPS documentation as part of accreditation/authorization process which includes ensuring the associated PPS registration remains current; conducts POA&M actions for PPS (exceptions, etc.); conducts annual reviews of security controls related to PPS; submits updated PPS documentation through accreditation/authorization process to keep associated PPS registration current (Ref AFI 17-101)
- Change Sponsor - verifies change requests concerning PPS contain proper authorization and references (C&A, PPSM Registration ID, etc.) (Ref MPTO 00-33A-1100)
- Change Requester/Change Initiator - coordinates with information system ISSM/ISSO and/or PMO on any change request impacting PPS (firewall exception request, etc.); coordinates with the Enterprise Change Sponsor, when applicable (Ref MPTO 00-33A-1100)

DoD PPS Category Assurance List (CAL)

The **DoD PPS CAL** (use email certificates) provides a quick-reference list of PPS authorized by DoD. Common facts regarding the DoD PPS CAL:

- Contains separate sections for Unclassified, Classified network environments, and Exceptions
- Each entry corresponds to a DoD PPS VA Report
- The assurance levels (GREEN, YELLOW, etc.) remain valid ONLY when configured/implemented in accordance with the corresponding DoD PPS VA Report
- Published every month based upon PPS authorized or changed through the DoD PPS TAG and CCB process
- Each version of the DoD PPS CAL prescribes an expiration date to ensure use of the most recent version
- Two versions of the DoD PPS CAL exist - one sorted by port number and the other sorted by service name - both contain the same PPS
    - DoD also publishes a version of the **DoD PPS CAL in Excel** format - please note this version also includes the "CAL by Variation" and "CAL by Service with Variation" which provide aliases and variations for data service names
- Low and High Port field contains port numbers commonly associated with the specified data service and/or protocol - there may be other authorized port numbers specified in the DoD PPS VA Report; use of alternate port numbers requires approval via Non-Standard Use (NSU) Request
- Service Name field contains the common service name for each PPS - the DoD PPS VA Report for the PPS may specify other service names
- Title field refers to the full name for the PPS
    - DoD also publishes a list of aliases and variations to data service names for every PPS - please see the "DoD PPS CAL in Excel" format for that listing
- The Network Boundaries field (shows 1 through 16) shows authorized network boundaries for the PPS as specified within the DoD PPS VA Report; use across boundaries not specified in the DoD PPS CAL/VA report result in Non-Compliance during the DIACAP or RMF process (DIACAP IA Control DCPP-1 or RMF Control CM-7(1)) with a requirement to submit a NSU request
- The color-codes show the assurance category assigned to the PPS according to the DoD PPS VA Report
- Comments field contains miscellaneous remarks

- The Non-Standard Use section shows specific deviations for the use of PPS across DoD network boundaries - these represent NSU requests approved by the respective AO and DoD PPS CCB
- The Component Local Service Assessment (CLSA) section shows PPS that is approved for usage by certain components and only on those components network.
- The Exceptions section shows specific exceptions granted by the Defense IA/Security Accreditation Working Group (DSAWG) for the use of BANNED PPS.

DoD PPSM Registry (aka DoD PPS Database)

1. Description and Purpose:

- Located on SIPRNet and NIPRNet
    - Systems operating on classified networks will appear in DoD PPSM-C Registry on SIPRNet
    - Systems operating on unclassified networks will appear in DoD PPSM-U Registry on NIPRNet
- Maintained by DISA
- Available to all DoD Components and mission partners for their use
- Used to declare all PPS, both internal and external, for each DoD information system connecting to, tunneling through, or operating on DoD information networks
- Each information system identified by unique 9-character ID called the DoD PPSM Tracking ID, aka PPSM Registry Number, with a prefix to identify the PPS program of record with DoD
    - "U" prefix identifies information systems in the DoD PPSM-U Registry
    - "C" prefix identifies information systems in the DoD PPSM-C Registry
- Serves as single, authoritative source for PPS authorized and approved for use by specific information systems
- Provides evidence of risk acceptance by AO or DAA (via DIACAP or RMF) for use of PPS by specific information systems
- Enables validation of changes to network boundaries, firewall rules, domain name records, and other devices on DoD information networks
- Enables Cybersecurity Reciprocity, authorizations to connect (AtC) within and among DoD Components, permissions to connect, interconnection agreements, service level agreements, and other documentation in support of connectivity between information systems, hosting enclaves, and DoD information networks
- Contains information on each information system to include system details, POCs, PPS used, network boundaries crossed, and source and destination details
-

2. Registering an Information System for PPS

-
- 1. Determine or identify the authorization package that covers the applicable software and/or hardware and coordinate with the ISSM.
- 2. Create or update the PPS documentation for that information system.

- 3. Integrate the PPS documentation into the authorization package under NIST Security Control CM-7 (DIACAP IA Control DCPP-1). Ensure adherence to configuration management procedures (impact assessment, CCB, etc.).
- 4. Request PPS registration using the AF PPS Registration Request tool and set an alert on your submission.
- 5. Receive confirmation of PPS registration from the AF PPS Registration Request tool alert, to include the DoD PPSM Tracking ID, if not already assigned.

Change Requests

The "Change Management" process provides a level of integrity and accountability on changes to rules and network devices monitoring, controlling, and regulating network operations and defense.

"Change Requests" reflect specific requests to change rules and/or network devices. As part of the review and approval process, various organizations check for authorizations on these requested changes to include evidence of the following:

- Information system approval through RMF by an AO
- Authorization to connect to the Air Force network (if applicable)
- DoD PPS registration
- Multi-factor authentication (if applicable)

If your Change Request receives a REJECTION from "AF PPS" during the review and/or approval processes, please follow the below steps for resolution:

- Coordinate with the applicable ISSM for the information system
- Obtain the "DoD PPSM Registration Confirmation Details" information for the applicable information system
    - The "PPSM Registration Confirmation Details" is an exported spreadsheet from the DoD PPSM Registry citing what the ISSM has formally declared for the PPS of the information system to include source and destination information
    - DO NOT use the AF-DoD PPS Worksheet - these are "working" documents for the RMF process and DO NOT reflect what the ISSM formally declared for the information system
    - As a reminder, the DoD PPSM Registry serves as the ONLY authoritative source for PPS in use by all DoD information systems to include their communication interfaces (source and destination)
- Compare the Change Request details to the PPSM Registration Confirmation Details
    - Ensure they match exactly according to the specified PPS and source/destination information which also indicates authorized/approved data flow
    - If the Change Request details do not match the PPSM Registration Confirmation Details, coordinate with the ISSM for changes to the Change Request or to the RMF documentation of the information system to include the AF-DoD PPS Worksheet
    - Depending upon the requirements, the ISSM may need to submit an update to the PPS registration for the associated information system

Guest Information Systems and Cybersecurity Reciprocity

1. The AF PPSM office only performs PPS registration for information systems accredited or authorized by an Air Force Authorizing Official (AO) as designated by the AF-CIO.

2. Information systems accredited by non-Air Force AOs or Air Force AOs designated by another DoD Component will follow their respective DoD Component guidance for PPS registration. Please see the DoD PPSM website for the PPS points of contact for other DoD organizations. This includes organizations such as:

- Defense Health Agency (DHA) - Almost all medical systems now receive accreditation/authorization from DHA, including information systems under Air Force Medical Operations Agency (AFMOA); POCs for these information systems must follow DHA PPS procedures
- Defense Information Systems Agency
- Defense Logistics Agency (DLA)
- Joint Strike Fighter
- US Navy
- USSOCOM

3. DoD organizations wishing to deploy their information systems to the Air Force must follow cybersecurity reciprocity guidance from DoDI 8510.01. Reference the Air Force AO Website for more guidance.

4. As a part of cybersecurity reciprocity, the deploying organization **MUST** provide the DoD PPSM "Registration Confirmation" notice or e-mail from the DoD PPSM Registry as an artifact to the connection approval authority for the Air Force as part of the Authorization to Connect (AtC) process.

5. The receiving organization MUST update their own accreditation or authorization documentation to reflect the documented agreement. At a minimum, the receiving organization must update security control CA-3 to show interconnections with the deployed information system.

- Information system name - as identified within eMASS or the accreditation/authorization approval document
- Information system version - as identified within eMASS or the accreditation/authorization approval document
- Accreditation (DIACAP) or authorization (RMF) approval document/reference (eMASS, etc.)

- Accreditation/Authorization Termination Date (ATD) - expiration of the DIACAP or RMF approval
- Authorization to Connect (AtC) approval document/reference (from eMASS, etc.) if the information system falls under the conditions for Cybersecurity Reciprocity from DoDI 8510.01, Enclosure 5
- POCs at site and PMO
- DoD PPSM Tracking ID
- Associated PPS impacting the circuit-enclave to include relevant source and/or destination information
    - NOTE 1: Not all PPS used by the information system will impact the circuit-enclave
    - NOTE 2: At a minimum, you must identify the onsite IP addresses/range
- Associated Change Requests or Incident Tickets (if applicable)
- Agreement Document and Date (CCB decision, service level agreement, MOA/MOU, site deployment checklist, etc.)
- Review Date (annual reviews required)

Non-DoD Guest Information Systems (Mission Partner)

1. Non-DoD entities that fall under the US Government do not follow DoD guidance for PPS or C&A/A&A reciprocity; they must follow National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, and NIST 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, guidance for unclassified and sensitive information systems. For PPS issues, the sponsoring DoD activity must:

a. Ensure support agreements exist (DoDI 8010.01).

b. Ensure the mission partner's information system received approval according to NIST SP 800-37.

c. Provide the results of NIST Security Control CM-7(1) and (3) for PPS to include properly completed documentation identifying the PPS required for use. The AF-DoD PPS Worksheet will satisfy this requirement.

d. Ensure the use of PPS across the DoDIN adheres to PPS standards from published vulnerability assessments from DoD.

e. Ensure the proper declaration of the PPS through the PPS registration process. Submit a PPS registration request using the tool on this site (left pane of page).

f. Must coordinate with any hosting enclave(s) regarding the required use of those PPS (NIST/RMF Security Control CA-3).

g. Must use the AF Change Management process for any modifications to boundary control/defense machanisms (firewalls, proxy servers, e-mail gateways, etc.) on the AFNet.

2. Foreign Mission Partners must adhere to DoDI 4000.19 and DoDD 5530.3.

3. Depending upon the entire transactional path of the traffic, use of the PPS may require exceptions if the data flow transits the Internet Access Points (IAP) controlled by DISA (JFHQ-DoDIN/USCYBERCOM).

PPS and Domain Name Service (DNS)

1. Information systems with a requirement to establish DNS records, whether internal or external, directly imply a communications interface for the specified server(s)/host(s). That communications interface will require the use of a PPS.

- You must identify the PPS associated with that specific communications interface in your PPS worksheet
- Your PPS worksheet must document the IP address and fully qualified domain name (FQDN) for the specified for the specified server/host
    - FQDN = the hostname of the server and the domain name (DNS namespace)
    - Domain name = organization name/domain ("usaf" or "af") and domain suffix or top level domain (.mil)
    - For web services/servers, you may specify the uniform resource locator (URL) and/or FQDN depending upon what you intend to submit for DNS
- The PPS in question must have an association with an information system approved through the RMF assessment and authorization process
- The information system must have a current and valid DoD PPS registration with a DoD PPSM Tracking ID

2. Please contact the system administrator for the server/host to help identify the PPS requiring the use of DNS records.

3. Change Requests submitted for the creation of DNS records (A and/or PTR) will undergo review, validation, and approval.

- Approval will occur based upon the below records:

    - Associated RMF authorization package from eMASS or other repository (e.g., XACTA)

    - DoD PPS registration for the associated information system; the PPS registration must clearly show the fully qualified domain name (FQDN) or uniform resource locator (URL) as the destination for a specific PPS

- Approval authority and implementation depends upon the applicable DNS namespace:

    - ***.usaf.mil** - reflects the Internal DNS namespace using the **private domain name** for Active Directory in the Air Force; approval occurs locally (not by 24th AF) with implementation by CSCS Directory Services

    - ***.af.mil** - reflects the External DNS namespace using the **public domain name** for Active Directory in the Air Force; approval occurs at the Enterprise level by 24th AF with implementation by 26th NOS

4. Please note 24th Air Force may have additional review and approval standards for the establishment of External DNS records to include:

- Risk mitigation information
- Evidence of multi-factor authentication
- Information on cloud service provider, if applicable

- Software evaluation/assessment information, if applicable
- Cybersecurity Service Provider (CSSP)
- Use of DMZ services, if applicable

Non-Compliant PPS

Unknown PPS - using a PPS without a corresponding assessment report constitutes an unknown and unauthorized PPS without a risk assessment.

- Use of an unknown PPS across the network boundaries of two or more DoD Components will require a Risk Assessment (RA)
- Use of an unknown PPS within or across the network boundaries of a single DoD Component (e.g., only US Air Force) will require a Component Local Service Assessment (CLSA)

Exceptions to DoD PPS Standards - DoD PPSM also created the *PPSM Exception Management Process* to track, monitor, and control PPS with technical vulnerabilities and inadequate mitigations that are still required to support an approved operational need.

Service Disruptions - Connectivity Issues

If you experience a service disruption or loss of connectivity related to firewall or boundary defense rules, please contact your local Network Service provider, Change Sponsor, or Communications Focal Point (CFP) to open an Incident Ticket to determine the cause.

- As part of the troubleshooting process, the Incident Ticket process will review firewall rules at the base level (Tier 3), AF Gateways (Tier 2), and eventually DoD-level (Tier 1) to determine if any rules caused the loss of connectivity
- Remain in contact with your liaison for the status of the Incident Ticket

PPSM References and Further Reading

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems

NIST 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

CJCSI 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND)*

DoD 5200.2-R, *Personnel Security Program*, (paragraphs AP10.2 and C3.6.15 - Defines levels of Information System Users and appropriate level of investigation)

DoD 8570.01-M, *Information Assurance Workforce Improvement Program* (defines Information Technology levels according to role based access requirements)

DoDI 8500.01, *Cybersecurity*

DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*

DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM)*

DoDM 5200.02_AFMAN 16-1405, *Air Force Personnel Security Program*

AFI 17-101 (formerly AFI 33-210), *Risk Management Framework (RMF) for Air Force Information Technology (IT)*

AFI 17-130, *Air Force Cybersecurity Program Management (formerly numbered as 33-200)*

AFMAN 17-1301 (formerly 33-282), *Computer Security (COMPUSEC)*

AFSSI 8551, *Ports, Protocols and Services (PPS) Management*

MPTO 00-33A-1001, *General Cyberspace Support Activities Management Procedures and Practice Requirements* (ETIMS account required to access via the hyperlink)

MPTO 00-33A-1100, *AFNet Operational Change Management Process*

DISAC 300-110-3, DISN Security Classification Guide (*Use CAC email certificate and select the "300" series circulars*)

DISAC 300-115-3, DISN SIPRNet Security Classification Guide (*Use CAC email certificate and select the "300" series circulars*)

Note: The PPSM Security Classification Guide, DISAC 300-110-4 was cancelled with no replacement

DoD PPSM Exception Management Website - link to latest version of the DoD PPSM Exception Management Process guide and Exception Request form

DoD PPSM Website

DISA Mission Partner Training Program

DISA STIGs - link to DISA STIG site for implementation guidance on various network environment and operating systems

USCYBER Command (USCYBERCOM) Orders & Directives area for CTOs, CAMs and WARNORDs

DMZ Documents - CYBERCOM site for NIPRNet DMZ guidance- CYBERCOM site for NIPRNet DMZ guidance

PPS Lessons Learned - Link to latest Lessons Learned information

DoD PPSM Read Board - get the latest news and information about PPS from DoD.

DoD PPSM CLSA Process - Generate an assessment for Local Services in order for it to be it added to the CAL by the DoD PPSM office