# DoD INSTRUCTION 8551.01

# PORTS, PROTOCOLS, AND SERVICES MANAGEMENT

| | |
|---|---|
| **Originating Component:** | Office of the DoD Chief Information Officer |
| **Effective:** | May 31, 2023 |
| **Releasability:** | Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/. |
| **Reissues and Cancels:** | DoD Instruction 8551.01, "Ports, Protocols, and Services Management (PPSM)," May 28, 2014 |
| **Approved by:** | John B. Sherman, DoD Chief Information Officer |

**Purpose:** In accordance with the authority in DoD Directive 5144.02 and the guidance in DoD Instruction (DoDI) 8500.01, this issuance:

- Establishes policy and standardizes procedures for cataloging, governing, and managing the use and management of protocols in the internet protocol suite, related protocols, and data services referred to as Department of Defense information network (DODIN) ports, protocols, and services (PPS).
- Prescribes PPS management (PPSM) support requirements for configuration management, continuous monitoring, and automated discovery and analysis of PPS to support near-real-time DODIN joint information environment (JIE) command and control (C2).
- Establishes the website on the risk management framework (RMF) knowledge service (KS) for existing PPSM policies and procedures and provides a platform for the DoD cybersecurity community to post and exchange PPSM solutions and documents with mission partners.

# TABLE OF CONTENTS

# SECTION 1: GENERAL ISSUANCE INFORMATION

## 1.1. APPLICABILITY.

a. This issuance:

(1) Applies to OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense (OIG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components.")

(2) Does not alter or override existing Director of National Intelligence authorities and policies regarding the protection of sensitive compartmented information and special access programs for intelligence in accordance with Executive Order 12333 and for national security systems in accordance with Executive Order 13231, and other applicable laws and regulations.

b. Nothing in this issuance will infringe on the OIG DoD's statutory independence and authority as articulated in the Inspector General Act of 1978, as amended, in the Appendix of Title 5, United States Code, referred to in this issuance as the "Inspector General Act." In the event of any conflict between this issuance and the OIG DoD's statutory independence and authority, the Inspector General Act takes precedence.

## 1.2. POLICY.

All PPS used throughout planned, newly developed, acquired, and existing DODIN (whether used internal or external to the enclave); DoD information technology; organic cloud computing; and managed data services must:

a. Be limited to only PPS required to conduct official business or needed to address quality of life issues authorized by the competent authority.

b. Be declared, including their underlying PPS, in the PPSM Registry located at https://pnp.cert.smil.mil/pnp for classified and https://pnp.cert.mil/pnp for unclassified.

c. Be implemented in accordance with established PPSM Configuration Control Board (CCB) policy, procedures, and standards; and DoD policy.

d. Must meet the requirements in Paragraph 3.2.

# SECTION 2: RESPONSIBILITIES

## 2.1. DOD CHIEF INFORMATION SECURITY OFFICER (DOD CISO).

Under the authority, direction, and control, and acting on the behalf of the DoD Chief Information Officer, the DoD CISO:

a. Oversees and monitors the implementation of this issuance.

b. Provides oversight and guidance to the Director, Defense Information Systems Agency (DISA), in the development, review, and approval of the PPSM CCB Charter in accordance with the responsibilities assigned to the Director, DISA, in Paragraph 2.2.b.

## 2.2. DIRECTOR, DISA.

Under the authority, direction, and control of the DoD Chief Information Officer, and in addition to the responsibilities in Paragraph 2.4., the Director, DISA:

a. Maintains all DoD information technology, cloud computing, and managed data services and ensures that they are:

(1) Assessed for vulnerabilities and documented in a vulnerability assessment report with recommendations to support the implementation of security measures to address vulnerabilities.

(2) Assigned an assurance category and documented in the category assurance list (CAL).

b. Develops, coordinates, reviews, and approves the PPSM CCB Charter.

c. Establishes and manages a PPSM CCB with membership from the DoD Components to develop, maintain, approve, and publish PPSM standards in accordance with the PPSM CCB Charter.

d. Appoints a DoD military officer in the grade of O-6, or civilian employee equivalent, possessing a Top Secret clearance with sensitive compartmented information access as the PPSM CCB chairperson to:

(1) Lead the PPSM CCB and represent the PPSM CCB at the Defense Security and Cybersecurity Authorization Working Group (DSAWG) established by CJCS Instruction (CJCSI) 6211.02D, as required.

(2) Send a copy of their PPSM CCB appointment letter to the DoD CISO.

(3) Establishes and manages the unclassified RMF KS website (https://rmfks.osd.mil/) to provide the DoD cybersecurity community with a forum to post and share practical solutions and documents with other DoD community and mission partners.

(4) Establishes and maintains the PPSM Registry capability used to declare all PPS for DoD Components, which is made available to DoD mission partners linked to DODIN for their desired use.

(5) Directs the PPSM Program Management Office (PMO) to conduct vulnerability assessments of declared PPS and document them in a vulnerability assessment report.

(6) Directs the PPSM PMO to document the assurance category for all PPS in the CAL.

(7) Maintains control correlation identifiers, security requirements guides, and security technical implementation guides (STIGs) developed by DISA consistent with security controls and assessment procedures used by the DoD.

(8) Directs the PPSM PMO to participate in mission partner forums related to PPSM to share PPSM standards.

e. Ensures the transfer of information to foreign mission partners is approved and undertaken in accordance with DoDI 2040.02.

## 2.3. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE.

Under the authority, direction, and control of the Under Secretary of Defense for Intelligence and Security; the authority, direction, and control exercised by the DoD CIO over the activities of the Cybersecurity Directorate, or any successor organization, of the National Security Agency, funded through the Information System Security Program; and in addition to the responsibilities in Paragraph 2.4., the Director, National Security Agency/Chief, Central Security Service:

a. Develops and publishes security configuration guides as required in coordination with the DoD CISO.

b. Supports the Director, DISA in developing PPSM standards.

## 2.4. DOD COMPONENT HEADS.

The DoD Component heads:

a. Designate in writing to the PPSM CCB chairperson, a primary and one or more alternative voting members to support PPSM CCB meetings.

(1) The representative must be a DoD military officer in the grade of O-6 or a DoD civilian employee in the grade of General Schedule (GS)-15 and have at least a Secret security clearance.

(2) If necessary, the representative can delegate to a DoD military officer in the grade of O-5 or a DoD civilian employee in the grade of GS-14 with at least a Secret security clearance.

(3) A representative from OIG DoD may attend in a non-voting role only.

b. Oversee their respective Component's PPSM program to:

(1) Assess it for vulnerabilities and document them in an internal vulnerability assessment report for internal PPS by the system owner in accordance with PPSM component local service assessment process.

(2) Track on the classified network in the Classified PPSM registry at https://pnp.cert.smil.mil/pnp and the unclassified system in the PPSM registry at https://pnp.cert.mil/pnp.

(3) Implement standards established by the PPSM CCB and in accordance with DoDI 8500.01, CJCSI 6510.01F, and CJCSI 6211.02D.

(4) Verify PPS before authorization, incorporation, or connection to systems or technology in accordance with DoDI 8510.01.

(5) Validate PPS for DoD systems in accordance with DoDI 8510.01.

(6) Maintain information technology interoperability in accordance with DoDI 8330.01.

(7) Communicate PPS securely across the DODIN.

(8) Block invalid PPS using appropriate boundary protection devices.

(9) Oversee usage of PPS not listed on the CAL for DoD Component systems operating on research, test, and evaluation (RT&E) information networks if:

(a) Using PPS remains solely in the RT&E information network and does not traverse the DODIN.

(b) The RT&E information network authorizing official provides the PPSM CCB a DSAWG-approved process to manage PPS risk.

## 2.5. CJCS.

In addition to the responsibilities in Paragraph 2.4., the CJCS develops, coordinates, and distributes PPSM policies, doctrine, and procedures for joint and combined operations in accordance with this issuance.

## 2.6. COMMANDER, UNITED STATES CYBER COMMAND.

In addition to the responsibilities in Paragraph 2.4., the Commander, United States Cyber Command:

a. Develops, coordinates, and distributes PPSM operational policies, doctrine, and procedures to implement this issuance.

b. Directs the PPSM PMO to coordinate PPS use for the DODIN monitoring and management capabilities to support DoD information network operations and defensive cyberspace operations as part of the responsibility for DODIN operations and defense.

c. In cooperation with the Director, DISA, implements PPSM operational policies and standards in accordance with this issuance.

d. Directs and maintains operational security priorities regarding PPS as coordinated with the PPSM CCB and the DSAWG.

e. Blocks all externally visible PPS not correctly implemented or enabled in accordance with this issuance and disconnects connections to, on, or through the DODIN transport. When required:

(1) Coordinates with the affected DoD Component heads to assess mission impact.

(2) Monitors the DODIN for threats and operational risks.

(3) Directs appropriate mitigations to be completed as documented in the vulnerability assessment report identifying operational risk and proper implementation strategies. (See Paragraph 3.4. for more information about vulnerability assessments.)

(4) Determines an alternate means of communication before establishing a constant disconnect.

f. Requires DoD Component heads to provide processes for sharing enterprise situational awareness in accordance with DoDI 8530.01.

# SECTION 3: PPSM PROGRAM

## 3.1. PPSM.

The PPSM program conducts vulnerability assessments on ports, protocols, and their underlying data services. It standardizes their use in support of security and interoperability. PPSM does not conduct vulnerability assessments on port numbers. All underlying PPS must link with software and systems approved by an authorizing official.

## 3.2. DECLARATION.

a. The PPSM program implements an automated declaration process to capture relevant information early in the system's RMF life cycle. System owners must register their PPS in the appropriate registries, located at https://pnp.cert.smil.mil/pnp for classified and https://pnp.cert.mil/pnp for unclassified.

b. The PPSM CAL is the authoritative list of all approved PPS. The PPSM-unclassified and PPSM-classified registries are the systems of record for all declared uses of PPS.

c. Automated PPS discovery will support the detection, capture, and monitoring of relevant data about PPS used within DoD systems.

d. Automated validation checks in the PPSM registries will support the analysis and compliance verifications established by PPSM.

e. The DoD regulates the following functions based on the potential to cause damage to DoD operations if used maliciously:

(1) Physical or virtual boundary protection devices for the DoD (e.g., routers, firewalls, intrusion detection or prevention devices) must allow only approved PPS to pass data.

(2) Approved PPS implementation supports DoD systems to enable secure communications across the DODIN.

(3) Boundary protection devices will block PPS not implemented in accordance with DoD PPSM standards.

(4) PPS RMF guidance and procedures, including those addressed by the PPSM exception management process, will be documented in the RMF KS at https://rmfks.osd.mil/rmf/Pages/default.aspx.

(5) PPS used in DODIN connections with mission partners must adhere to applicable international agreements negotiated and concluded in accordance with DoDI 5530.03. Interagency memorandums of understanding, service-level agreements, or contracts must specify the approved use of PPS.

(6) PPS supports secure configuration management, continuous monitoring (e.g., discovery and analysis), vulnerability management, baseline configuration compliance verification, and risk scoring, with PPSM coordination to support near real-time C2 of the DODIN and JIE.

(7) PPSM standards will be implemented as directed by the authorizing official for the system for DoD-wide management and PPS control used in DoD systems to:

(a) Enhance baseline cybersecurity standards in accordance with DoDI 8500.01.

(b) Standardize PPS usage and mappings to support interoperability.

(c) Establish PPSM-related configuration management to support near real-time C2 of the DODIN and JIE, continuous monitoring, discovery, and analysis.

(d) Establish a PPSM presence in the RMF KS to aid the DoD Components with situational awareness and defense of their information networks.

## 3.3. DISCOVERY AND ANALYSIS.

a. The PPSM program implements a discovery and analysis methodology that supports information security configurations, vulnerability management, and PPS interoperability used in DoD systems across machine interfaces. This methodology will reduce operator burden and enhance the DODIN defense capabilities.

b. Discovery will support detecting, capturing, and monitoring relevant data and network traffic concerning the PPS being used in DoD systems.

c. Automated assessments will support the analysis and compliance verifications established by PPSM.

## 3.4. VULNERABILITY ASSESSMENTS.

a. PPS vulnerability assessments will follow the DoD vulnerability management process, in accordance with DoDI 8531.01.

b. The PPSM program performs vulnerability assessments in accordance with the PPSM further action process. The vulnerability assessment report identifies operational risk and appropriate implementation strategies. These implementation strategies are derived from the applicable STIGs, security classification guides, and security requirements guides.

## 3.5. PPSM EXCEPTION MANAGEMENT PROCESS.

a. The PPSM exception management process allows the DoD Component Technical Advisory Group or CCB representative to request the use of non-compliant PPS based on an

operational need when no other suitable alternative exists. The two conditions for non-compliance are "banned" or "nonstandard usage."

b. The DSAWG, on behalf of the DoD principal authorizing the official, evaluates exception requests for banned PPS and determines whether to accept or deny the shared risk to the DODIN.

c. The PPSM CCB evaluates nonstandard usage implementation requests for availability and interoperability to support operational needs.

d. DoD Component Technical Advisory Group or PPSM CCB decisions that do not meet the required concurrence level will be elevated to the DSAWG and to the DoD Information Security Risk Management Committee in accordance with the DSAWG Charter.

e. Procedures for preparing and processing requests under the exception management process are located on the RMF KS.

## 3.6. RMF KS PPSM SUPPORT.

The RMF KS provides:

a. Unclassified electronic, web-based, and machine-to-machine authoritative sources for existing PPSM policies and procedures to systematically apply the principles and methods of implementation PPSM CCB developed and distributed for DoD systems.

b. Data storage and retrieval, pooling of relevant information from appropriate DoD Component RMF repositories, automated assessment and compliance verification, summary reporting, and similar capabilities that support the discovery and analysis methodology in accordance with Paragraph 3.3.

c. A resource for the DoD cybersecurity community to post and share practical solutions and documents with other DoD community and mission partners.

# GLOSSARY

## G.1. ACRONYMS.

| ACRONYM | MEANING |
|---|---|
| C2 | command and control |
| CAL | category assurance list |
| CCB | configuration control board |
| CJCS | Chairman of the Joint Chiefs of Staff |
| CJCSI | Chairman of the Joint Chiefs of Staff instruction |
| CNSSI | Committee on National Security Systems instruction |
| DoD CISO | DoD Chief Information Security Officer |
| DoDI | DoD instruction |
| DODIN | Department of Defense information network |
| DISA | Defense Information Systems Agency |
| DSAWG | Defense Security and Cybersecurity Authorization Working Group |
| GS | general schedule |
| JIE | joint information environment |
| KS | knowledge service |
| OIG DoD | Office of Inspector General of the Department of Defense |
| PMO | program management office |
| PPS | ports, protocols, and services |
| PPSM | ports, protocols, and services management |
| RMF | risk management framework |
| RT&E | research, test, and evaluation |
| STIG | security technical implementation guide |

## G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

| TERM | DEFINITION |
|---|---|
| **analysis** | An automated compliance verification process that evaluates declared or discovered data against established PPSM standards. |
| **assessment** | A manual process that establishes PPSM standards for the secure and effective configuration of applications and PPS. |
| **assurance category** | An information security designation assigned to control and regulate the use of protocols and data services based on functional capabilities, vulnerability assessments, and other PPSM standards and the potential to cause damage to DoD operations. |
| **authorizing official** | Defined in Committee on National Security Systems Instruction (CNSSI) No. 4009. |
| **banned** | A protocol or service that is prohibited by DoD policy and will not be allowed to cross the DODIN without an approved exception (see the definition of the PPSM exception management process). |
| **boundary protection device** | Defined in CNSSI No. 4009. |
| **CAL** | A summary reference used for implementing and promoting the standardization and management of PPS used on the DODIN. |
| **data service** | A named standard, unique, or proprietary packet structure that provides the software interface communication from one information network application to another. |
| **declaration** | A mechanism designed to capture relevant data about DoD information technology (i.e., applications and their underlying PPS). It includes the registration process and encompasses obtaining data from other federated sources or via electronic sensing. |
| **discovery** | The automated detection and capture of relevant data about information systems (i.e., applications and their underlying PPS) are used for assessment and analysis. |
| **DODIN** | Defined in the DoD Dictionary of Military and Associated Terms. |
| **enclave** | Defined in CNSSI No. 4009. |

| TERM | DEFINITION |
|---|---|
| **externally visible** | Traffic that traverses the DODIN when the ingress or egress communications at an enclave's external boundary can be monitored and analyzed to identify specific PPS. |
| **information technology** | Defined in CNSSI No. 4009. |
| **internal PPS** | Under the control of a single authorizing official and security policy. |
| **internet protocol suite** | Set of communications protocols used for the Internet and similar networks that provide rules and standards specifying how data should be formatted, addressed, transmitted, routed, and received. |
| **interoperability** | Defined in DoDI 8330.01. |
| **mission partners** | Defined in DoD Directive 8000.01. |
| **near real-time** | Denoting or relating to a data-processing system that is slightly slower than real-time. |
| **nonstandard usage** | Anything registered that is not compliant with the approved standard, as listed on the CAL. |
| **port** | The logical connection point used for transmitting information packets. |
| **PPSM exception management process** | A mechanism for requesting and tracking the use of banned and nonstandard usage PPS. |
| **PPSM standards** | Build-to implementation strategies (i.e., configuration guidelines), software developer guidance, vulnerability assessment reports, the CAL, and other PPSM artifacts established and approved by the PPSM CCB to catalog, regulate, and control the use and management of PPS on the DODIN. |
| **protocol** | Defined in CNSSI No. 4009. |
| **security requirements guide** | Defined in DoDI 8500.01. |
| **STIG** | Defined in DoDI 8500.01. |
| **system** | Defined in CNSSI No. 4009. |

| TERM | DEFINITION |
|---|---|
| **vulnerability assessment** | Defined in CNSSI No. 4009. |
| **vulnerability assessment report** | A report that documents the vulnerability assessment, operational risk assessment, and security implementation strategies of PPS based on its capability, functionality, and exploitability. The authoritative PPSM artifacts used to help reduce the DODIN and JIE risk while meeting operational requirements. |

# REFERENCES

Chairman of the Joint Chiefs of Staff Instruction 6211.02D, "Defense Information Systems Network (DISN) Responsibilities," January 24, 2012

Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011

Committee on National Security Systems Instruction No. 4009, "Committee on National Security Systems (CNSS) Glossary," March 2, 2022

Configuration Control Board Department of Defense Ports, Protocols, and Services Management Charter, "Configuration Control Board Department of Defense Ports, Protocols, and Services Management," December 8, 2004[1]

Department of Defense Ports Protocols, and Services Management (PPSM): PPSM Exception Management Process, Version 2.6, September 17, 2019, as amended[2]

Department of Defense Ports Protocols, and Services Management (PPSM): PPSM Further Action Process, Version 1, June 2, 2017

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," March 17, 2016, as amended

DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," March 27, 2014, as amended

DoD Instruction 5530.03, "International Agreements," December 4, 2019

DoD Instruction 8330.01, "Interoperability of Information Technology, Including National Security Systems," September 27, 2022

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022

DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, as amended

DoD Instruction 8531.01, "Vulnerability Management," September 15, 2020

Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended

Executive Order 13231, "Critical Infrastructure Protection in the Information Age," October 16, 2001, as amended

Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

United States Code, Title 5, Appendix, Inspector General Act of 1978, as amended

[1]Available to authorized CAC holders at: https://dl.cyber.mil/ppsm/pdf/pps-ccb-charter-signed-20041208.pdf

[2] Available to authorized CAC holders at: https://disa.deps.mil/org/RE4/RE42/PPSM/External/Knowledge_Service/Vulnerability_Assessment/Exception%20Management/exception_management_process_ver_2_6.pdf