Department of Defense
INSTRUCTION

NUMBER 8551.01
May 28, 2014

DoD CIO

SUBJECT: Ports, Protocols, and Services Management (PPSM)

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (a)) and pursuant to DoD Instruction (DoDI) 8500.01 (Reference (b)), this instruction reissues DoDI 8551.1 (Reference (c)).

a. Updates policy and standardizes procedures to catalog, regulate, and control the use and management of protocols in the Internet protocol suite, and associated ports (also known as “protocols, data services, and associated ports” or “ports, protocols, and services”); referred to in this instruction as PPS on DoD information networks (DODIN) including the connected information systems, platform information technology (IT) systems, platform IT (PIT), and products based on the potential that unregulated PPSM can damage DoD operations and interests.

b. Establishes PPSM support requirements for configuration management and continuous monitoring to include discovery and analysis of PPS to support near real time command and control (C2), of the DODIN and Joint Information Environment (JIE).

c. Establishes on the unclassified Risk Management Framework (RMF) Knowledge Service (KS), at https://diacap.iaportal.navy.mil/login.htm, a presence for current PPSM policies and procedures and provides a mechanism for the DoD cybersecurity community to post and share PPSM practical solutions and documents with other DoD community and mission partners.

d. Incorporates and cancels Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer memorandums regarding PPS (References (d) and (e)).

2. APPLICABILITY. This instruction:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector

General of the DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

b. Does not alter or supersede existing authorities and policies of the Director of National Intelligence regarding the protection of Sensitive Compartmented Information and special access programs for intelligence as directed by Executive Order 12333 (Reference (f)), and for national security information systems as directed by Executive Order 13231 (Reference (g)), and other applicable laws and regulations.

3. POLICY. It is DoD policy that:

a. All PPS used throughout planned, newly developed, acquired, and existing DODIN (whether used internal or external to the enclave), which include DoD Information Technology (IT), must be:

(1) Limited to only PPS required to conduct official business or required to address quality of life issues authorized by competent authority.

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

(3) Assigned an assurance category and documented in the Category Assurance List (CAL).

(4) Declared, including their underlying PPS, in the PPSM Registry currently located at https://pnp.cert.smil.mil/pnp.

(5) Implemented in accordance with established PPSM Configuration Control Board (CCB) policy, procedures, and standards; and DoD policy.

(6) Regulated by DoD based on the potential to cause damage to DoD operations if used maliciously.

b. DoD boundary protection devices such as routers, firewalls, and intrusion detection or prevention devices must be configured to allow only approved PPS.

c. PPS will be implemented by DoD IT to assure the ability to securely communicate across DODIN.

d. PPS not implemented in accordance with the DoD PPSM process will be blocked using boundary protection devices.

e. PPS RMF guidance and procedures, including those addressed by the PPSM Exception Management Process (Reference (h)), will be managed and maintained in the RMF KS at https://diacap.iaportal.navy.mil/login.htm.

f. PPS used in DODIN connections with mission partners will be documented in international agreements in accordance with DoDD 5530.3 (Reference (i)) or interagency memorandums of agreements or understandings, service level agreements, or contracts.

g. PPS implementation will support secure configuration management, continuous monitoring (including discovery and analysis), vulnerability management, baseline configuration compliance verification and risk scoring for PPS and coordination of PPSM in support of the near real time C2 of the DODIN and JIE.

4. RESPONSIBILITIES. See Enclosure 2.

5. RELEASABILITY. **Unlimited**. This instruction is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

6. EFFECTIVE DATE. This instruction:

a. Is effective May 28, 2014.

b. Must be reissued, cancelled, or certified current within 5 years of its publication to be considered current in accordance with DoDI 5025.01 (Reference (j)).

c. Will expire effective May 28, 2024 and be removed from the DoD Issuances Website if it hasn't been reissued or cancelled in accordance with Reference (j).

David L DeVries

David L. De Vries
Acting Department of Defense
Chief Information Officer

Enclosures
1. References
2. Responsibilities
3. PPSM Overview
Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," April 22, 2013
(b) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(c) DoD Instruction 8551.1, "Ports, Protocols, and Services Management (PPSM)" August 13, 2004 (hereby cancelled)
(d) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum, "DoD Ports, Protocols, and Services (PPS) Management Processes," June 6, 2005 (hereby cancelled)
(e) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum, "SIPRNet Ports, Protocols, and Services (PPS) Management Processes," March 19, 2007 (hereby cancelled)
(f) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
(g) Executive Order 13231, "Critical Infrastructure Protection in the Information Age," October 16, 2001
(h) Defense Information Systems Agency, "Department of Defense Ports Protocols, and Services Management (PPSM), PPSM Exception Management Process," Version 2.2, November 13, 2013, as amended[1]
(i) DoD Directive 5530.3, "International Agreements," June 11 1987, as amended
(j) DoD Instruction 5025.01, "DoD Directives Program," September 26, 2012, as amended
(k) 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 [2]
(l) Chairman of the Joint Chiefs of Staff Instruction, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011
(m) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014
(n) DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," May 21, 2014
(o) Unified Command Plan, April 6, 2011, as amended
(p) DoD Directive O-8530.1, "Computer Network Defense (CND)," January 8, 2001
(q) Committee on National Security Systems (CNSS) Instruction No. 4009, "National Information Assurance (IA) Glossary," April 26, 2010
(r) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current edition
(s) Appendix III to Office of Management and Budget Circular A-130, "Management of Federal Information Resources," as amended
(t) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009

[1] PPSM Exception Process is available at: https://powhatan.iiie.disa.mil/ppsm/exception.html
[2] PPSM CCB Charter: https://powhatan.iiie.disa.mil/ppsm/meetings/pps-ccb-charter-signed-20041208.pdf

(u) National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Recommended Security Controls for Federal Information Systems and Organizations" April 2013, as amended

ENCLOSURE 2

RESPONSIBILITIES

1. DOD CHIEF INFORMATION OFFICER (DoD CIO). The DoD CIO:

a. Oversees and monitors the implementation of this instruction.

b. Assigns responsibility to review and approve the PPSM CCB charter (Reference (k)).

2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). Under the authority, direction, and control of the DoD CIO and in addition to the responsibilities in section 4 of this enclosure, the Director, DISA:

a. Manages the implementation of this instruction.

b. Establishes and manages a PPSM CCB with membership from the DoD Components to develop, maintain, approve, and publish CAL and PPSM standards in accordance with Reference (k).

c. Appoints an O-6 or equivalent civilian PPSM CCB chairperson with a Top Secret/sensitive compartmented information security clearance to lead the PPSM CCB and represent the PPSM CCB at the Defense Information Assurance Security Accreditation Working Group (DSAWG) as necessary. Provides a copy of the PPSM CCB appointment letter to the DoD CIO.

d. Establishes and maintains a presence in the RMF KS unclassified website at https://diacap.iaportal.navy.mil/login.htm to provide a mechanism for the DoD cybersecurity community to post and share PPSM practical solutions and documents with other DoD community and mission partners.

e. Establishes and maintains a PPSM Registry capability that is used to declare all PPS for DoD Components; and is made available to DoD mission partners connected to DODIN for their discretionary use.

f. Conducts (external) vulnerability assessments of declared PPS and documents them in a vulnerability assessment report.

g. Documents the assurance category for all PPS in the CAL.

h. Provides input and supports updates to Security Configuration Guides (SCGs), Security Requirements Guides (SRGs), and Security Technical Implementation Guides (STIGs) that apply to applications and PPS.

i. Participates in mission partner forums related to PPSM, sharing PPSM standards.

j. Designates the Secretariat for the PPSM CCB. The PPSM CCB Secretariat can be contacted at DoD.ppsm@mail.mil.

3. DIRECTOR, NATIONAL SECURITY AGENCY (NSA). Under the authority, direction, and control of the Under Secretary of Defense for Intelligence, and in addition to the responsibilities in section 4 of this enclosure, the Director, NSA, develops and publishes SCGs as required, and supports the Director, DISA, in the development of PPSM standards.

4. DoD COMPONENT HEADS. The DoD Component heads:

a. Designate in writing a primary and one or more alternate voting representatives to the PPSM CCB chairperson and ensure representation at all PPSM CCB meetings. The representative must be a DoD military or DoD civilian at the O-6 or civilian equivalent level and possess a minimum Secret security clearance. Voting authority may be delegated downward one level.

b. Provide guidance and oversee Component DoD IT implementations including information systems, PIT systems, PIT, and products to ensure PPS are:

(1) Used only as required to conduct official business or address quality of life issues authorized by competent authority.

(2) Assessed for vulnerabilities and documented in an (internal) assessment report for internal PPS by the DoD IT owner in accordance with DoD and DoD Component guidance.

(3) Declared in the PPSM Registry at https://pnp.cert.smil.mil/pnp. For general information about the PPSM program, go to the Information Assurance Support Environment (IASE) webpages at: http://iase.disa.mil/ppsm or http://iase.disa.smil.mil/ppsm.

(4) Implemented in accordance with PPSM standards established by the PPSM CCB and in compliance with Reference (b), CJCSI 6510.01F (Reference (l)), and other applicable existing DoD guidance.

(5) Regulated based on the potential to cause damage to DoD operations if used maliciously.

(6) Verified prior to authorization, incorporation, or connection to DoD information systems or PIT systems for DoD IT in accordance with DoDI 8510.01 (Reference (m)).

(7) Documented and approved as part of the RMF for DoD IT in accordance with Reference (m).

c. Assure the interoperability of DoD IT in accordance with DoDI 8330.01 (Reference (n)) and DoD PPSM process so that:

(1) DoD IT can communicate securely across DODIN when implementing PPS.

(2) PPS not implemented in accordance with the DoD PPSM process are blocked using appropriate boundary protection devices.

d. Submit exception requests in accordance with the PPSM Exception Management Process in section 6 of Enclosure 3 of this instruction.

e. Contact the PPSM CCB Secretariat to initiate approval process for use of PPS not yet listed on the CAL, that are required for time-sensitive operational interoperability in support of operations with limited duration provided they are declared in the PPSM Registry at https://pnp.cert.smil.mil/pnp. The request to the PPSM CCB must include a plan for managing risk of the PPS until the associated vulnerability assessment reports can the PPSM CCB.

(1) The PPSM CCB will handle the time-sensitive operational needs with 72 hours of receipt.

(2) PPSM CCB may consult the DSAWG to address risk concerns when necessary.

f. Oversee DoD Component use of PPS not yet listed on the CAL for DoD Component IT connected to research, test, and evaluation (RT&E) information networks, such as the Defense Research and Engineering Network (DREN) and the Secret DREN provided:

(1) The PPS are used solely within the RT&E information network.

(2) The RT&E information network authorizing official provides the PPSM CCB a DSAWG-approved process for managing the risk of the PPS.

5. CJCS. In addition to the responsibilities in section 4 of this enclosure, the CJCS develops, coordinates, and distributes PPSM policies, doctrine, and procedures for joint and combined operations consistent with this instruction.

6. COMMANDER, U.S. STRATEGIC COMMAND (USSTRATCOM). In addition to those responsibilities in section 4 of this enclosure, the Commander, USSTRATCOM:

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

b. Coordinates the use of PPS for DODIN monitoring and management capabilities in support of DoD information network operations and defensive cyberspace operations as part of the responsibility for operations and defense of DODIN established in the Unified Command

Plan (Reference (o)).

c. Directs implementation of PPSM operational policies and procedures consistent with this instruction in coordination with the Director, DISA.

d. Ensures operational security priorities regarding PPS are promptly addressed in coordination with the PPSM CCB and the DSAWG.

e. Blocks all externally visible PPS that are not implemented in accordance with the DoD PPSM process and terminates circuit connections to DODIN that pose an immediate unacceptable risk. Coordinates with the affected DoD Components to assess mission impact, conducts a threat assessment and assesses operational risk, implements appropriate mitigations, and determines an alternate means of communication before instituting a persistent disconnection.

f. Ensures DoD Components include processes for sharing enterprise situational awareness in accordance with DoDD O-8530.1 (Reference (p)).

ENCLOSURE 3

PPSM OVERVIEW

1. INTRODUCTION. The DoD is committed to implementing PPSM policies and procedures for enterprise-wide management and control of PPS used within DoD IT to:

a. Enhance baseline cybersecurity standards in accordance with Reference (b).

b. Standardize PPS usage and mappings leading to 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 that will aid the DoD Components with situational awareness and defense of their information networks.

2. PPS. The Department is committed to interoperability and mitigating shared risk in having all PPS and how they are used within planned, newly developed, acquired, and existing DODIN regulated based on their inherent vulnerabilities and potential to cause damage. PPSM does not conduct vulnerability assessments on port numbers. PPSM conducts vulnerability assessments on protocol(s) or data service(s) with their associated ports. Underlying protocols, data services, and port usage must be linked to the software.

3. DECLARATION. The PPSM program will implement an automated declaration process to capture relevant information early in the information system's RMF life cycle. Automated declaration allows federation of relevant information from appropriate DoD Component RMF repositories, thus maintaining authoritative PPSM information.

4. DISCOVERY AND ANALYSIS

a. The PPSM program will implement a discovery and analysis methodology that will support information security configurations, vulnerability management, and the interoperability of PPS used within DoD IT through machine-to-machine interfaces. This methodology will reduce operator burden and enhance DODIN defense capabilities.

b. Discovery will support the detection, capture, and monitoring of relevant data about PPS used within DoD IT.

c. Analysis will be supported by automated assessments and compliance verifications enabled by PPSM standards that are based on previously assessed and PPSM CCB-authorized PPS.

5. VULNERABILITY ASSESSMENTS. Vulnerability assessment and resulting reports (defined in the Glossary) are conducted because there are inherent vulnerabilities associated with the use of specific protocols in the Internet protocol suite that must be regulated based on their potential to cause damage to DoD operations.

6. PPSM EXCEPTION MANAGEMENT PROCESS

a. The PPSM Exception Management Process allows the DoD Components to request 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 non-standard usage (NSU).

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

c. The PPSM CCB evaluates NSU implementation requests that are required for interoperability in support of operational needs.

d. DoD Components may appeal PPSM CCB and DSAWG decisions to the DoD Information Security Risk Management Committee.

e. Procedures for preparation and processing of requests under the exception management process are found on the RMF KS at https://diacap.iaportal.navy.mil/login.htm.

7. RMF KS PPSM SUPPORT. The RMF KS at https://diacap.iaportal.navy.mil/login.htm will provide:

a. An unclassified on-line, web-based, and machine-to-machine interfaced authoritative source for current PPSM policies and procedures to uniformly apply PPSM standards and implementation strategies developed and distributed by the PPSM CCB for PPS used within DoD IT.

b. A data storage and retrieval, federation of relevant information from appropriate DoD Component RMF repositories, automated assessments and compliance verifications, summary reporting, and similar capabilities which support the discovery and analysis methodology described in section 4 of this enclosure.

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

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

C2	command and control
CAL	Category Assurance List
CCB	Configuration Control Board
CJCS	Chairman of the Joint Chiefs of Staff
DISA	Defense Information Systems Agency
DoD CIO	DoD Chief Information Officer
DoDD	DoD Directive
DoDI	DoD Instruction
DODIN	Department of Defense information networks
DREN	Defense Research and Engineering Network
DSAWG	Defense Information Assurance Security Accreditation Working Group
IASE	Information Assurance Support Environment
IT	information technology
JIE	Joint Information Environment
KS	Knowledge Service
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSU	non-standard usage
PIT	platform information technology
PPS	Internet protocol suite and associated ports
PPSM	ports, protocols, and services management
RMF	Risk Management Framework
RT&E	research, test, and evaluation
SCG	Security Configuration Guide
SRG	Security Requirements Guide
STIG	Security Technical Implementation Guide
USSTRATCOM	U.S. Strategic Command

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this instruction.

analysis. Automated compliance verification process that evaluates declared or discovered data against established PPSM standards.

authorizing official. Defined in Committee on National Security Systems Instruction No. 4009 (Reference (q)).

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.

banned. Protocol or Service, in its native form, is prohibited by DoD policy and will not be allowed to cross DODIN without an approved exception (see PPSM Exception Management Process definition).

boundary protection. Defined in Reference (q).

boundary protection device. Defined in Reference (q).

CAL. Summary reference used for implementing and promoting the standardization and management of PPS used on 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 (i.e., declared). A mechanism designed to capture relevant data about DoD IT (e.g., applications and their underlying PPS). Includes what was formerly known as the Registration process, but also encompasses obtaining data from other federated sources, whether or not those sources were populated by other registration activities or via electronic sensing.

discovery. The automated detection and capture of relevant data about information systems (e.g., applications and their underlying PPS) used for assessment and analysis.

DODIN. Defined in Joint Publication 1-02 (Reference (r)).

DoD information network operations. Defined in Reference (r).

enclave. Defined in Reference (q).

enclave boundary. Defined in Reference (q).

external PPS. Under the control of multiple authorizing officials and security policies

externally visible. Traffic that traverses DODIN when the ingress or egress communications at an enclave's external boundary can be monitored and analyzed to identify specific PPS.

information system. Defined in Reference (q).

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 provides rules and standards specifying how data should be formatted, addressed, transmitted, routed and received.

interoperability. Defined in Reference (n).

IT. Defined in Reference (q).

IT Service. Defined in Reference (b).

major application. An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application, as defined in Appendix III to Office of Management and Budget Circular A-130 (Reference (s)). All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

mission partners. Defined in DoDD 8000.01 (Reference (t)).

packet. A formatted unit of data.

PIT. Defined in Reference (b).

PIT system. Defined in Reference (b).

port. The logical connection point used for transmitting information packets.

protocol. Defined in Reference (q).

PPSM Exception Management Process. A mechanism for requesting and tracking the use of banned and NSU PPS.

PPSM standards. Build-to implementation strategies (i.e., configuration guidelines), software developer guidance, vulnerability assessment reports, the CAL, and other PPSM artifacts that are established and approved by the PPSM CCB to catalog, regulate, and control the use and management of PPS on the DODIN.

product. Defined in Reference (b).

SCG. NSA developed and distributed configuration guidance for a wide variety of software, both open source and proprietary.

SRG. A DISA developed compendium of security policies, technical requirements, and best practices derived from the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Reference (u)) information assurance controls and other sources decomposed into measurable control correlation identifiers that apply to classes of IT products and logical configurations.

STIG. A DISA developed, product specific compendium of security configuration settings and best practices, based on one or more SRGs and NIST standards that applies to specific IT products and logical configurations. The primary purpose of a STIG is to provide security configuration guidance for optimal confidentiality, integrity, and availability; intrusion avoidance and detection; and incident response and recovery.

visible. Network traffic that can be analyzed to identify specific PPS.

vulnerability assessment. Defined in Reference (q).

vulnerability assessment report. Documents the vulnerability assessment; operational risk assessment and security implementation strategies of PPS based on its capability, functionality, and exploitability; and are the authoritative PPSM artifacts used to help reduce the risk to the DODIN and JIE while meeting operational requirement.