Department of Defense

INSTRUCTION

NUMBER 8551.1

August 13, 2004

ASD(NII)/DoD CIO

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

References: (a) DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002
(b) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(c) Assistant Secretary of Defense for Command, Control, Communications, and Intelligence/DoD Chief Information Officer Memorandum, Subject: "DoD Ports, Protocols, and Services Security Techincal Guidance," November 5, 2002 (hereby canceled)
(d) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
(e) Committee on National Security Systems (CNSS) Instruction No. 4009, "National Information Assurance (IA) Glossary," May 2003[1]
(f) through (j), see enclosure 1

1. PURPOSE

Under the authority of reference (a) and consistent with reference (b) this Instruction:

1.1. Implements policy on using ports, protocols, and services in DoD information systems in a manner that supports the evolution to net-centric operations.

1.2. Supersedes reference (c).

[1] Available at http://www.nstissc.gov/Assets/pdf/4009.pdf

2. APPLICABILITY AND SCOPE

This Instruction applies to:

2.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

2.2. All existing, new, and planned DoD information systems with ports, protocols, and services that are visible to Department of Defense (DoD) managed network components.

2.3. This Instruction does not alter or supersede the existing authorities and policies of the Director of Central Intelligence regarding the protection of Sensitive Compartmented Information and special access programs for intelligence as directed by Executive Order 12333 (reference (d)) and other laws and regulations.

3. DEFINITIONS

Terms used in this Instruction are defined in references (a), (b), Committee on National Security Systems (CNSS) Instruction No. 4009 (reference (e)), or enclosure 2.

4. POLICY

4.1. Ports, protocols, and services (PPS) that are visible to DoD-managed network components shall undergo a vulnerability assessment; be assigned to an assurance category; be appropriately registered; be regulated based on their potential to cause damage to DoD operations and interests if used maliciously; and be limited to only the PPS required to conduct official business or required to address Quality of Life issues authorized by competent authority.

4.2. Assurance category assignments for PPS that are visible to DoD-managed network components shall be documented in a PPS Assurance Category Assignments List [2] that will be regularly updated to add new PPS and reassign others, as required.

---

[2] Available at http://pnp.cert.smil.mil/portsandprotocols

4.3. DoD information systems visible to DoD-managed network components shall use PPS according to the most current PPS Assurance Category Assignments List and implement them as described in the most current version of the Defense Information Systems Agency (DISA) issued Security Technical Implementation Guide (STIG) on Enclave Security,[3] Network Infrastructure STIG,[4] and the National Security Agency (NSA) issued Security Recommendation Guide (SRG) on Router Security Configuration.[5]

4.4. Use and configuration of PPS within enclave boundaries (i.e., not visible to DoD-managed components) are responsibilities of the enclave owner. However, use of PPS according to the PPS Assurance Category Assignments List and supporting security technical implementation guidance within enclave boundaries to the extent possible is advisable and encouraged.

4.5. All DoD information systems shall specifically document PPS that are visible to DoD-managed network components as part of the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) according to DoD Instruction 5200.40 (reference (f)).

4.6. All DoD information systems with PPS that are visible to DoD-managed network components shall be maintained on a central PPS registry that will be available to all the DoD Components.[6]

4.7. The PPS implementation in newly developed, newly acquired or modified DoD information systems that are visible to DoD-managed network components shall be assessed for operational risk by the PPS Configuration Control Board (CCB). System developers shall design or acquire information systems according to the PPS Assurance Category Assignments List and configure them according to the PPS STIGs and SRGs.

4.8. DoD information systems with PPS according to the most current PPS Assurance Category Assignments List, configured according to the PPS STIGs and SRGs, and as approved by the Defense Information Systems Network (DISN) Designated Approving Authorities (DAAs) shall be guaranteed the ability to communicate through all DoD enclave boundary protection mechanisms when required to conduct official business.

---

[3] Available at http://iase.disa.mil/techguid/stig.html

[4] Available at http://iase.disa.mil/techguid/stig.html

[5] Available at http://www.nsa.gov/snac/index.cfm

[6] Available at http://pnp.cert.smil.mil/portsandprotocols

4.9. Legacy DoD information systems (i.e., those operational when this Instruction becomes effective) using PPS that are visible to DoD-managed network components, but not in compliance with the current PPS Assurance Category Assignments List and not approved by DISN DAAs shall be registered and allowed to continue in operation while the PPS undergoes a vulnerability assessment by the PPS CCB, is assigned to an assurance category, and approved by the DISN DAAs.

4.10. After a reasonable grace period, as determined by the DISN DAAs to allow for compliance with paragraph 4.9., above, unregistered PPS that are visible to DoD-managed network components that are not in compliance with the most current PPS Assurance Category Assignments List and not approved by the DISN DAAs shall be blocked at appropriate DoD enclave boundaries.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer shall:

5.1.1. Monitor the implementation of this Instruction.

5.1.2. Oversee the development and maintenance of the PPS Assurance Category Assignments List.

5.1.3. Establish a PPS CCB that shall:

5.1.3.1. Perform vulnerability assessments of PPS and provide the DISN DAAs recommendations on their assignment to assurance categories.

5.1.3.2. Maintain and update, as required, the PPS Assurance Category Assignments List and forward updated lists through the DISN DAAs to the DoD Chief Information Officer (DoD CIO).

5.1.3.3. Provide input and support to updates of STIGs and SRGs that apply to PPS.

5.1.3.4. Perform risk assessments of the PPS implementation in newly developed, newly acquired or recently modified DoD information systems when they are registered and provide the DISN DAAs recommendation for their use on DoD-managed networks.

5.1.3.5. Refer unresolved PPS issues to the DoD CIO through the DISN DAAs, as necessary.

5.2. The Chairman of the Joint Chiefs of Staff shall develop, coordinate, and promulgate PPS policies, doctrine, and procedures for Joint and combined operations consistent with this Instruction.

5.3. The Commander, U.S. Strategic Command, shall coordinate employment of PPS Network Management capabilities in support of Computer Network Defense (CND) operations as described in DoD Directive O-8530.1 (reference (g)) and the PPS Assurance Category Assignments List, as issued.

5.4. The Director, Defense Information Systems Agency, shall:

5.4.1. Manage the implementation of this Instruction.

5.4.2. Develop and publish PPS STIGs, including configuration guidelines and developer's guidance, in coordination with the PPS CCB.

5.4.3. Provide technical assistance to the DoD Components in the selection or configuration of PPS of their DoD information systems, as requested.

5.4.4. Develop and maintain a central PPS registry of all DoD information systems with PPS that are visible to DoD-managed network components.

5.5. The Director, National Security Agency, shall develop and publish SRGs, as required, and support the Director, DISA, in the development of other security implementation guidance for PPS.

5.6. The Heads of the DoD Components shall:

5.6.1. Select PPS for DoD information systems that are visible to DoD-managed network components according to the PPS Assurance Category Assignment List and configure them according to the PPS STIGs and SRGs, as appropriate.

5.6.2. Document the actual or planned use of PPS that are visible to DoD-managed network components for all DoD information systems as part of the DITSCAP (reference (f)).

5.6.3. Designate a point of contact to register the use of all DoD information systems with PPS that are visible to DoD-managed network components with the DISA.

5.6.4. Provide appropriate representatives to serve as members of the DoD PPS CCB and its working or advisory groups.

5.6.5. Ensure that all DoD information systems with PPS that are visible to DoD-managed network components are submitted to a central PPS registry.

5.6.6. Ensure that any DoD information system with PPS according to the most current PPS Assurance Category Assignments List, configured according to the PPS STIGs and SRGs, as appropriate, and approved by the DISN DAAs are guaranteed the ability to communicate through all DoD Component enclave boundary protection mechanisms when required to conduct official business.

5.6.7. Ensure that any unregistered PPS that are visible to DoD-managed network components and are not in compliance with the most current PPS Assurance Category Assignments List and not approved by the DISN DAAs are blocked at appropriate DoD enclave boundaries.

5.7. The DISN Designated Approving Authorities shall:

5.7.1. Review and approve proposed updates to the PPS Assurance Category Assignments List.

5.7.2. Review and approve DoD information systems that are visible to DoD-managed network components.

5.7.3. Establish grace periods for non-compliant legacy DoD information systems.

6. PROCEDURES

Implementation procedures are in enclosure 3.

7. EFFECTIVE DATE

This Instruction is effective immediately.

for Cheryl J. Roby
Linton Wells, II
Acting ASD NII

Enclosures - 3

E1. References, continued
E2. Definitions
E3. Implementation Procedures

E1. ENCLOSURE 1

REFERENCES, continued

(f) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997
(g) DoD Directive O-8530.1, "Computer Network Defense (CND)," January 8, 2001
(h) DoD Directive 5000.1, "The Defense Acquisition System," May 12, 2003
(i) OMB Circular A-130, "Management of Federal Information Resources, Transmittal 4," November 28, 2000
(j) DoD Memorandum, "DoD Ports, Protocols, and Services - Increasing Security at the Internet/DISN Boundary" January 28, 2003

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Application. A software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges. Examples include office automation, electronic mail, web services, and major functional or mission software programs (reference (a)).

E2.1.2. Assurance. A measure of confidence that the security features, practices, procedures and architecture of an Information Technology (IT) system accurately mediates and enforces the security (reference (f)).

E2.1.3. Automated Information System (AIS) Application. For DoD information assurance purposes, an AIS application is the product or deliverable of an acquisition program, such as those described in DoD Directive 5000.1 (reference (h)). An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System, Defense Messaging System). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note: An AIS application is analogous to a "major application" as defined in OMB Circular A-130 (reference (i)); however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System (reference (a)).

E2.1.4. Defense Information Systems Network (DISN). The DoD consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations (reference (a)).

E2.1.5. DISN Designated Approving Authority (DISN DAA). One of four DAAs responsible for operating the DISN at an acceptable level of risk. The four DISN DAAs are the Directors of DISA, DIA, NSA, and the Director of the Joint Staff (delegated to the Joint Staff Director for Command, Control, Communications, and Computer Systems (J-6)) (reference (a)).

E2.1.6. DoD Information System. A 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 (reference (a)).

E2.1.7. DoD-managed Network Components. Hardware and transport components owned or controlled by the Department of Defense to include routers, gateways, and firewalls distributed among multiple locations between DoD enclave boundaries and the Internet, supporting encrypted and unencrypted data, voice, and video transport.

E2.1.8. Enclave. A collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard information assurance capabilities, such as boundary defense, incident detection and response, and key management, and also deliver common applications, such as office automation and electronic mail. Enclaves are analogous to general support systems, as defined in reference (i). Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers (reference (a)).

E2.1.9. Enclave Boundary. The point at which an enclave's internal network service layer connects to an external network's service layer (reference (b)).

E2.1.10. Least Privilege. The principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error or unauthorized use of an information system (reference (e)).

E2.1.11. Outsourced IT-based Process. For DoD information assurance purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations (reference (a)).

E2.1.12. Platform IT Interconnection. For DoD information assurance purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems, such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems, such as water and electric. Examples of platform IT interconnections that impose security considerations include remote administration and remote upgrade or reconfiguration (reference (a)).

E2.1.13. Port. The logical connection point for the transmission of information packets.

E2.1.14. Protocols. The rules used by both ends of a communication channel. Information system protocols using the Transmission Control Protocol/Internet Protocol (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 User Datagram Protocol (UDP).

E2.1.15. Risk. A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact (reference (f)).

E2.1.16. Risk Assessment. A process of analyzing threats to, and vulnerabilities of, an IT system, and the potential impact that the loss of information or capabilities of a system would have on national security. The resulting analysis is used as a basis for identifying appropriate and effective measures (reference (f)).

E2.1.17. Risk Management. A process concerned with the identification, measurement, control, and minimization of security risks in IT systems to a level commensurate with the value of the assets protected (reference (f)).

E2.1.18. Service. The named standard, unique, or proprietary packet structure and associated communication configuration that is instantiated on a port or range of ports. Common examples of services are: DNS, FTP and HTTP. For details see the Ports, Protocols, and Services Assurance Categories Assignments List.

E2.1.19. Security Technical Implementation Guide (STIG). A compendium of security configuration settings and best practices from many sources that apply to IT products (e.g., Windows 2000), logical configurations (e.g., enclaves) or technologies (e.g., PPS and mobile code). The NSA uses the synonymous term Security Recommendation Guide. The primary purpose is to provide security configuration guidance for:

E2.1.19.1. Improved confidentiality or integrity.

E2.1.19.2. Intrusion avoidance.

E2.1.19.3. Intrusion detection.

E2.1.19.4. Response and recovery.

E2.1.20. Threat. Any circumstance or event with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service (reference (f)).

E2.1.21. Virtual Private Network. An encrypted tunnel that can transport Internet protocols between enclaves, thus masking their exposure.

E2.1.22. Visible. Network traffic is "visible" when it can be analyzed to identify a specific port and protocol or data service.

E2.1.23. Vulnerability. A weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited (reference (f)).

E2.1.24. Vulnerability Assessment. The systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation (reference (f)).

E3. ENCLOSURE 3

IMPLEMENTATION PROCEDURES

E3.1. INTRODUCTION

The Department of Defense is committed to interoperability and mitigating shared risk in the community having DoD information systems with PPS that are visible to DoD-managed network components. Implementation of this policy identifies the activities of vulnerability assessment, registration, risk assessment, and enclave boundary implementation to support these goals. A vulnerability assessment measures the relative strength of the security features of a PPS. Registration of DoD information systems allows standardization of port and protocol mappings leading to interoperability and assists in the management of network resources. A risk assessment of a DoD information system provides a mechanism to reduce the threat to DoD networks and information while meeting operational requirements. Enclave boundary implementation allows the DoD Component to follow the principle of "least privilege," by employing only those ports and protocols required to conduct official business.

E3.2. SCOPE

This policy addresses protocols that correspond to the Internet Protocol Suite as described by the Internet Assigned Numbers Authority, Protocol Number Assignment Services,[7] and focuses on the three most widely used and needed protocols: Internet Control Messaging Protocol (protocol 1), Transmission Control Protocol (TCP) (protocol 6) and User Datagram Protocol (UDP) (protocol 17). This policy does not address PPS within Virtual Private Networks (VPNs). However, implementation of these procedures by the DoD Components in their VPNs is advisable and encouraged.

E3.3. VULNERABILITY ASSESSMENTS

Vulnerability assessments of PPS identify their security limitations and may provide countermeasures to limit their exposures. All PPS have vulnerabilities, but they vary in degree. The PPS vulnerability assessments process separates PPS by relative security into the three assurance categories described below:

---

[7] Available at http://www.iana.org

E3.3.1. RED. PPS designated as RED have a low level of assurance. These PPS implemented in DoD information systems expose DoD networks to an unacceptable level of risk for routine use. A RED PPS shall only be allowed when approved by the DISN DAAs for a specific DoD information system under defined conditions and restrictions and if no suitable alternative exists.

E3.3.2. YELLOW. PPS designated as YELLOW have a medium level of assurance. These PPS expose DoD networks to an acceptable level of risk for routine use only when implemented with the required mitigation strategy and approved by the DISN DAAs for a specific DoD information system.

E3.3.3. GREEN. PPS designated as GREEN have a high level of assurance. These PPS are considered best security practices and are recommended for use when implemented with the required mitigation strategy and approved by the DISN DAAs for a specific DoD information system.

E3.4. CATEGORY ASSIGNMENTS

Category assignments assist the DoD Components in selecting PPS with the highest possible assurance while still meeting operational requirements. The PPS Assurance Category Assignments List identifies protocols or services with accepted well-known ports and provides detailed implementation procedures. It is the responsibility of the CCB and the DISA to update and maintain the PPS Assurance Category Assignments List. The most current list is available online.[8]

E3.5. REGISTRATION

E3.5.1. Registration Policy. All DoD information systems that have PPS that are visible to DoD-managed network components shall be registered. Registration of DoD information systems promotes interoperability and assists in the management of network resources. DoD information systems with PPS requiring registration include legacy as well as those in development or acquisition. Each DoD Component shall register all of the DoD information systems it uses with the DISA in order to ensure that necessary ports remain open as long as a DoD information system has PPS that are visible to DoD-managed network components.

---

[8] Available at http;//pnp.cert.smil.mil/portsandprotocols

E3.5.2. Registration Process

E3.5.2.1. Each DoD Component has a point of contact (POC) who is authorized to register information systems. A list of POCs is available at the PPS homepage.[9] Once registration is completed, the PPS registration process shall automatically notify DoD network administrators to open ports and protocols as required on appropriate DoD routers and firewalls.

3.5.2.2. If registration is for a newly developed or newly acquired DoD information system, or a modification (i.e., a new implementation of an existing DoD information system involving changes to configuration), the ports and protocols to support the DoD information system will be temporarily opened, as required, until the DISN DAAs have accepted or rejected the risk of the DoD information system under their risk management process. If the registration is for a legacy system (i.e., one that is operational when this Instruction becomes effective), supporting ports and protocols will be allowed to remain open pending a DISN DAA decision. If assistance is needed for registration contact the help desk as listed on the PPS homepage.[10]

E3.6. RISK MANAGEMENT

E3.6.1. Risk Assessment. Risk assessments analyze the threats to and vulnerabilities of the PPS implementation of a DoD information system. The goal of the assessment is to determine the likelihood of exploitation and the potential impact that the loss of information or capabilities of a system may have on national security. The risk assessment includes a resolution of any conflicts between a protocol and associated port number(s) to ensure interoperability. All PPS that are visible to DoD-managed network components require a risk assessment by the CCB and a risk management decision from the DISN DAAs. An appeals process to the DoD CIO is available to settle any disputes with the DISN DAAs' operational decisions.

---

[9] Available at http;//www.cert.mil/portsandprotocols and http://pnp.cert.smil.mil/portsandprotocols

[10] Available at http://www.cert.mil/portsandprotocol

E3.6.2. Risk Management Process. Once the registration process is completed, the CCB shall initiate the risk assessment of the DoD information system. After reviewing the operational requirements and determining the vulnerabilities and threats the DoD information system may impose on the DoD network, the CCB shall forward a recommendation to the DISN DAAs. The status of all ongoing risk assessments may be found on the PPS homepage.[11] The DISN DAAs' decision shall be based on the following:

E3.6.2.1. A clearly defined operational requirement for the specified PPS supporting the functionality of the DoD information system.

E3.6.2.2. Verification that network requirements have been addressed as part of the DITSCAP process.

E3.6.2.3. Determination by the CCB that no conflicts exist for the mapping of port numbers and protocols of previously registered DoD information systems and the new DoD information system.

E3.6.2.4. Evidence of compliance with mitigation techniques prescribed in the PPS Assurance Category Assignments List.

E3.6.2.5. Consideration of any known specific threats against the implementation of the DoD information system as reported by the CCB.

E3.7. APPEAL PROCESS

A DoD Component may appeal a decision by the DISN DAAs to the DoD CIO. The appeal shall be made by a date specified by the DISN DAAs or the DoD network administrators shall close affected ports and protocols on DoD routers and firewalls. Submission of an appeal shall guarantee that the ports and protocols remain open until the DoD CIO decision. Appeals may be initiated by contacting the PPS Help Desk.[12]

---

[11] Available at http://pnp.cert.smil.mil/portsandprotocols

[12] Available at http://www.cert.mil/portsandprotocol