# Ports, Protocols, and Services Management Process for the Department of Defense

David R. Basel
*Defense Information Systems Agency*

Dana Foat
*Defense-Wide Information Assurance Program Office*

Cragin Shelton
*The MITRE Corporation*


**Tuesday, 19 April 2005**
Track 1: 4:50 – 5:35 p.m.
Ballroom A

*All automated information systems (AIS) used on Department of Defense (DoD) data networks must register the data communication modes identifying the ports, protocols, and application services (PPS) used, and the network boundaries crossed. Compliance with the PPS requirements will reduce development time and cost, increase security, speed certification and accreditation steps, enhance AIS interoperability across the department, and speed operational deployment of all new and updated AIS in DoD. This article introduces the PPS basic concepts, and demonstrates how developers and program managers can comply with the PPS requirements, leverage the security analysis provided by the management office, and obtain the benefits listed.*

The overall goal of the Ports, Protocols, and Services Management Process (PPSMP) [1] is to improve both the interoperability of joint applications and the security of the overall Department of Defense (DoD) information infrastructure. The process supports many people in many roles: program managers, systems engineers, software developers, network operators, network security managers, router and firewall administrators, etc.

The authors hope this article reaches many of those people, and helps them understand both the value of participating in the PPSMP and the services it can provide.

For reader clarification, we begin this article with a discussion of the basic terms and concepts of computer network traffic on the Internet: protocol, Internet protocol (IP), IP protocol, service/application protocol/data service, and port.

## Protocol

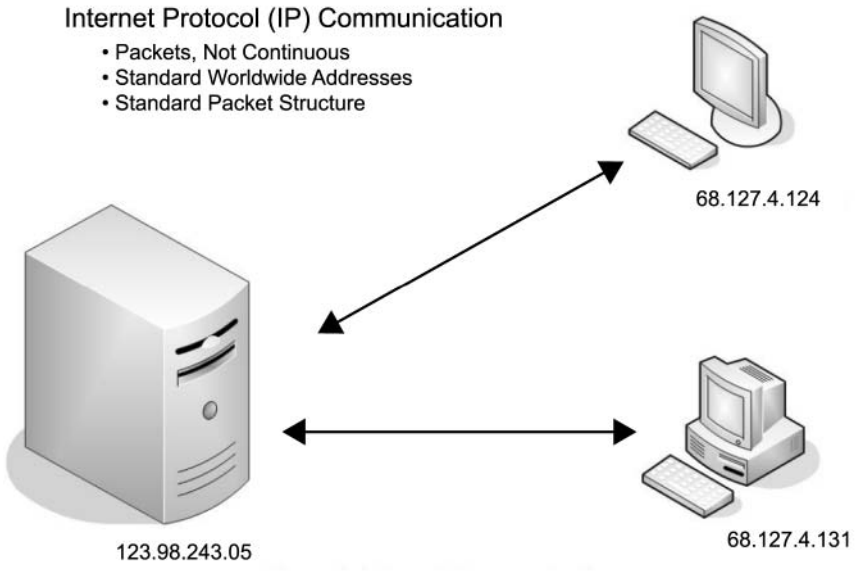
A protocol is simply an agreed upon way to communicate or interact. This word can have multiple meanings in different contexts. The meaning and context will become apparent below.

## Internet Protocol

The most fundamental protocol is the IP. The international group Internet Engineering Task Force (IETF) [2] sets the standards for the IP. The IETF's many standards documents – both draft and approved – called "Requests for Comment (RFC)," are at <www.ietf. org>.

The core principal of the IP is that all information travels between computers in data bundles called packets rather than in a continuous stream. Any information, for example a computer file, can be divided into packets by the sending computer and the packets reassembled into the complete file by the receiving computer. The IP defines several structures so this can happen. The two most important are an addressing scheme and a defined packet structure. Figure 1 illustrates the IP communications concept.

Figure 1: *IP Communication*




An IP address is like a computer's telephone number. You may have seen these four groupings of numbers separated by periods (or dots). Those are IP addresses as defined under Version 4 of the IP standard currently in use internationally.

Each of the four number groups can be any number from 0 to 255. Many countries, as well as the DoD, are upgrading to IP Version 6 (IPv6), which uses a very different address scheme. To save space, this article does not discuss IPv6 addressing. Many resources on IPv6 are available for the readers[1].

Once two computers find each other, they need to agree on how to communicate. The defined packet structure assists in this process. Very simply, each packet has two major parts: the header, with information about the packet, and the payload, with the actual data. Figure 2 illustrates this concept.

More than 100 standard rule sets, each with a different purpose, are available for the computer-to-computer communication. Here are examples of a few of the IP protocols most often seen on networks:

- **Protocol 1: ICMP - Internet Control Message Protocol.** ICMP packets allow two operating systems to trade status messages. A ping is a single packet sent from one computer to another that means simply, "Are you there?" If the receiving computer is listening for the ping and chooses to admit it is available for further contact,

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **MAY 2005** | | **00-05-2005 to 00-05-2005** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Ports, Protocols, and Services Management Process for the Department of Defense** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **MITRE Corporation,202 Burlington Road,Bedford,MA,01730-1420** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | | **6** | |

it replies with a one-packet ping reply, which tells the first computer, "Yes, I'm here and listening."

Why is it named *ping*? The name is borrowed from the world of submarines and sonar. Think back to every submarine movie you have seen. The sound sent out by the sonar is called a ping, because of the way it sounds on the speakers when reflected back to the submarine by the enemy ship lurking in the distance.

- **Protocol 6: TCP - Transmission Control Protocol.** TCP packets support positive confirmation that each chunk of data (packet) arrived intact and unchanged. This confirmation is essential when sending data that must not be lost or corrupted, such as a database record.
- **Protocol 17: UDP - User Datagram Protocol.** UDP packets can carry any content data, but they do not provide a feedback mechanism to confirm receipt of intact data. UDP is used to push large amounts of data (packets) out from the computer, and it is not critical if some of them get lost or broken, such as streaming audio or streaming video.
- **Protocol 50: ESP - Encapsulating Security Payload.** ESP packets have the primary data encrypted; only the sender and receiver, who have the right encryption keys, can read the data. This protection of confidentiality is part of the IP security set of standards, and is the basis for many virtual private networks.

Here is jargon watch No. 1: *Protocol* is the first word in this discussion with multiple meanings. The IP defines the overall structure of packets and IP addresses. The IP protocol defines the major type and function of packets. (Yes, spelling out *IP protocol* as *Internet protocol protocol* does sound redundant, but it is accurate. That is why you never see it spelled out.) The next term to be discussed, *service*, is also called the application protocol. In the context of the PPSM, protocol most often refers to the IP protocol.

## Service

Once two computers are communicating with the proper hardware system addresses (IP address), and computer-to-computer packet type (IP protocol), the individual programs on each computer still need to communicate properly. The programs must exchange data in the right format and packet structure for the programs themselves to understand. The rule for the agreed format at this level is called variously the *application protocol*, *data service*, or simply *service*. All three terms refer to the same aspect of the packet.

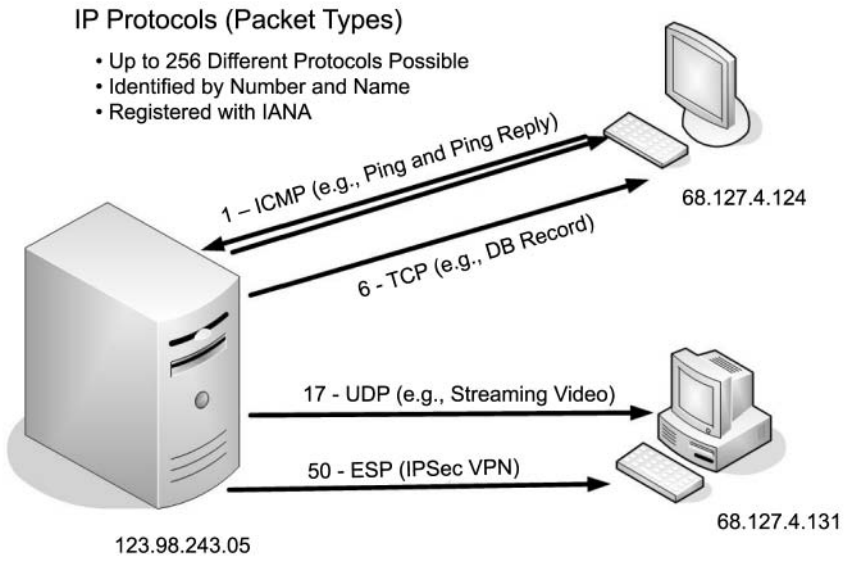



Figure 2: IP *Protocols*

While the IP has provisions for up to only 256 different protocols, it has set no limit on the number of possible services. Every application programmer could devise unique services for the programs to use to communicate over a network. In the interests of both interoperability and ease of programming, most do not. However, new programs introduce new services every year. Some are proprietary, while others become widely used standards.

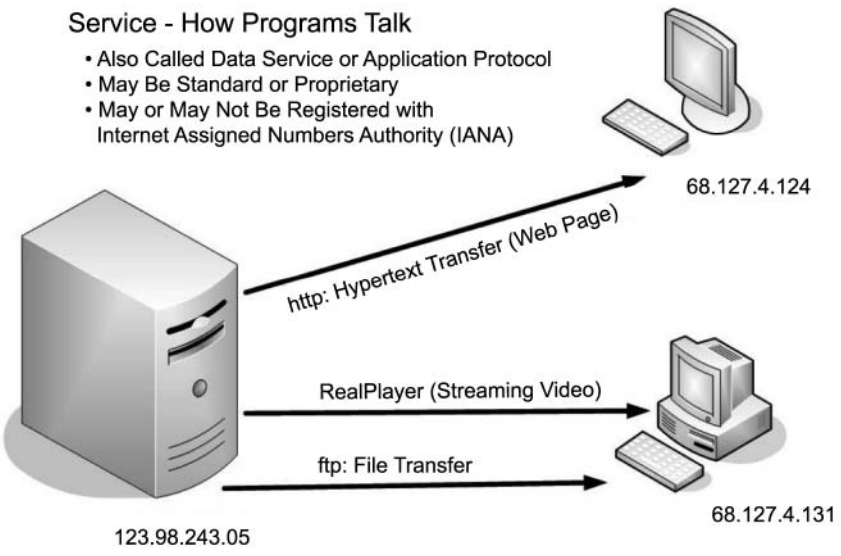
There are thousands of these services or application protocols because different types of programs need different types and orders and formatting for their data. Programmers who hope to see an application protocol become a standard may publish the specification as a RFC with the IETF, but they are not required to do so. Figure 3 illustrates the use of these services.

Examples of well-known and commonly used services include hypertext transfer protocol (http), used for sending Web pages; file transfer protocol (ftp), used for moving entire data files between computers; and telnet, used for remote computer terminal connections.

Within the packet-structure logic described so far, generally only two protocols carry packets that contain a defined service at the next level: TCP and UDP. In fact, many services can travel in either. Program architects decide which protocol to use depending on whether the priority is higher speed or packet-count throughput (UDP), or 100 percent intact packet arrival (TCP).

Here is jargon watch No. 2: Within the PPSM, *service* refers to the data service or

Figure 3: *Service*



application protocol as just described. However, in the world of network engineering, *service* can refer to a level or quality of service of the network (actual data transport speed limit and network availability). Service can also refer to a category of application running on a computer such as a Web service, a file service, a time reference service, a chat service, and so forth. A computer running one or more services is called a *server* (Web server, file server, time server, or chat server, for example).

## Port

The IP address sends each packet to the right computer. The IP protocol tells the receiving computer the packet type. The service indicated in the packet tells the receiving program the data structure. However, each computer may have many different programs running at the same time. And each program may be having conversations with more than one other computer at the same time.

For instance, a file server may be receiving thousands of requests to send out files to individual remote computers in the same minute. If the server agrees to support all of those requests, it needs some way to sort the incoming traffic to keep track of each two-way conversation, or session, separately.

The concept of the port provides the tool for managing multiple simultaneous sessions. For TCP and UDP packets with defined services, each packet also specifies a port number. The standard packet structure reserves enough room for the port number so it could be any number from 0 to 65,535.

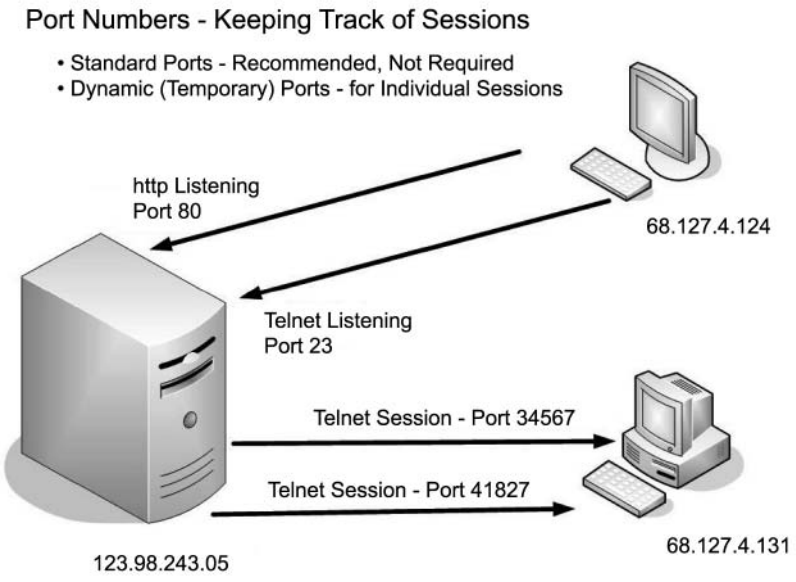
Think of each computer as an office building with one street address (the IP address), but many mailboxes for the separate offices. Think of the port number as the number on each of those internal mailboxes. Some offices (programs) by agreement use a standard local mailbox (port) number. For example, bulk mail delivery goes to port 25, requests for Web pages go to port 80, and requests for terminal sessions (telnet) go to port 23. Figure 4 illustrates the use of ports.

To help keep multiple conversations separate once a contact is started the host may say, "Send everything else for this session to one of my high number boxes. This is temporary, just for this exchange." These are dynamic or transient (or ethereal) ports.

By convention and as defined by both the IETF and the Internet Assigned Numbers Authority (IANA) [3], port numbers from 0 to 1,023 should be used only for the standard services as registered with IANA. Other services should use port numbers above 1,024. Developers may, if they wish, register with IANA any proprietary or non-standard service's use of particular ports above 1,024. This does not really reserve those ports for only that use, but it does notify all network users and engineers of the planned use.

Here is jargon watch No. 3: In the context of the PPSM and IP packet headers, *port* refers to the number that helps manage communication sessions. This information is important to network engineers and administrators who manage routers and firewalls, as described in the next section. However, those same router and firewall administrators also use port to refer to the physical connection on hardware where they plug in a network cable.

Figure 4: *Ports*




### *Boundary Filtering - Routers and Firewalls*

So, why does the PPSM care about all of those standards? Because network administrators can use them to enforce rules on network traffic via routers and firewalls. Figure 5 illustrates the use of firewalls. These rules can help limit traffic, block problem traffic, and allow favored traffic. Many network management and security devices can use the information in packet headers to decide how to handle the packets. Remember, each packet begins with a header, which is like an envelope, containing the following information: IP address from, IP address to, IP protocol (packet type), service type (if needed), port number (if needed).

Administrators can devise and apply rules based on header items, as follows:

- Deny any traffic that comes from a particular IP address or range of addresses.
- Deny any traffic that uses a service for a program that only insiders should be using.
- Allow any traffic using the standard port for a standard service (application protocol).
- Deny any traffic using a nonstandard port for a service declared.

## Policy and Process

The purpose of the ports and protocols policy is to provide the DoD with a framework for managing the use of PPS implemented within DoD information systems. This allows network administrators to know what data types are expected on their networks. At the same time it provides information on what types of traffic to block to protect the network.

The PPS policy, DoD Instruction 8551.1 [1], states that 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 its potential to cause damage to DoD operations and interests if used maliciously, and be limited to only the PPS required to conduct official business. In this section, we will discuss the processes of vulnerability assessments and assurance category assignments, the regulation of use or elimination of PPS within the DoD space, and the registration of information systems.

### *Vulnerability Assessments*

Vulnerability assessments identify the security limitations of PPS. Any known countermeasures to limit the exposure of the vulnerability are identified in this

process. This research is performed by the Technical Advisory Group (TAG), which consists of subject matter experts from all of the DoD components, supported by technical expertise from the companies EDS and NetSec under the Defense Information Systems Agency (DISA) Information Assurance [4] contract.

Because of the complexity of some proprietary protocols, it may be necessary to invite service providers to explain the operation of their protocols. The vulnerability assessment reports are available at <http://iase.disa.mil/ports/index.html>.

### *Assurance Category Assignments*

Assurance category assignments identify the relative strength of PPS. The guidance discourages the use of low assurance PPS lacking adequate security countermeasures (category Red); accepts the use of medium assurance PPS, provided documented countermeasures are implemented (category Yellow); and encourages using high assurance PPS, which is considered a best practice when documented countermeasures are implemented (category Green).

Although this research is performed by the TAG, it is verified by the Configuration Control Board (CCB) to ensure that proposed countermeasures may be implemented in an operational network environment. The results of this process are documented in the PPS assurance Category Assignments List (CAL) [5].

### *Regulation*

The regulation of the PPS in DoD network space is a Defense Information System Network Security Accreditation Working Group (DSAWG) decision based on the recommendation of the CCB and the vulnerability assessment reports. The goal is to allow only those PPS that are required to conduct official business to cross enclave boundaries. In general, any PPS labeled as Red must not cross any enclave boundary into the DoD network space.

After issuance of the DSAWG decision, users of information systems implemented with Red PPS will be notified and the DoD PPS program manager (PM) will assist them with compliance. Within the two-year compliance timeframe, the information system may be redesigned with a more secure PPS (Yellow or Green), modified to alter the communications path, or implemented within a Virtual Private Network (VPN) solution.

Although a PPS may be labeled as Red, that category assignment does not necessarily mean that its use will be immediately eliminated from the DoD network space. With the assistance of the DoD PPS program manager, a DoD component may request an appeal for the implementation of the PPS within the information system to the DoD chief information officer. For some PPS designated as Red, there may be no more secure alternatives.

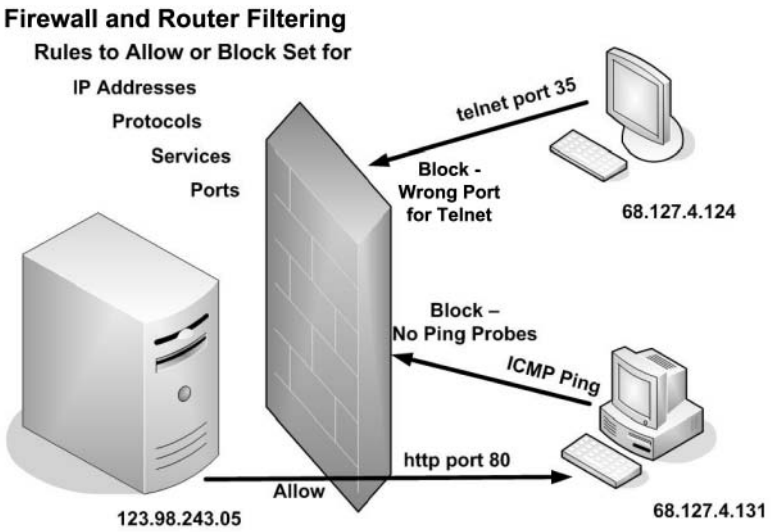



Figure 5: *Firewall and Router Filtering*

The TAG will review these PPS periodically to determine if new countermeasures provide adequate protections or if more secure alternative solutions become available. The DSAWG decision dates for the PPS are published in the CAL.

### *Registration*

DoD Instruction 8551.1 requires that all existing, new, and planned DoD information systems visible to DoD-managed network components must be registered in a PPS registry maintained by DISA. This process ensures that all necessary ports remain open as long as a DoD information system has PPS that cross enclave boundaries into the DoD network space.

Each DoD component has a point of contact (POC) who is authorized to register information systems. A list of the POCs is available at NetDefense Joint Task Force-Global Network Operations [6]. Once registration is completed, the process will automatically notify DoD network administrators to open ports and protocols as required on appropriate DoD routers and firewalls.

If the registration is for a new PPS configuration in a newly developed or newly acquired DoD information system, or for a modification of an existing DoD information system, the PPS will be temporarily opened, as required, until the DSAWG has accepted the risk of the PPS within the DoD network space. The assessment and assignment of categories to PPS takes approximately three months. Therefore, it is important to register information systems as soon as possible in the development or acquisition process to ensure availability of the intended PPS.

## Benefits

Information system managers, architects, and developers in today's software development environment are rapidly being led to the realization that security is not an add-on feature but must be identified as a core requirement from the beginning. This concept is also referred to as *baked in security*. The PPSMP registration process enables DoD components to identify and eliminate poor business and security practices (e.g., unencrypted remote management of routers and firewalls from the Internet). This section identifies the benefits of the PPSMP to PMs, system engineers, software developers, designated approving authorities, and network operations staff.

Many protocols and network-based services were designed by people who were not concerned with malicious behavior. As a result, a computer that uses these protocols and services is exposed to attack. However, many of these risky protocols and services are useful, and a few are even necessary.

One way of dealing with the risky protocol problem is to limit the population that can interact using a particular protocol or service. In practice, this is often done by limiting the use of a risky protocol to the local workgroup, or local area network. A firewall or filtering router blocks the protocol at the group boundary, thereby shielding members of the

group from the people on the *outside* who might attack machines on the inside that have the protocol enabled. Although in this case a firewall is an enabler of a capability, it can also cause interoperability problems if people or applications on either side of the boundary must use that risky protocol for essential communication across the boundary.

The ports and protocols process is the method the DoD uses to determine the *riskiness* of particular protocols and services, and then balances that risk against the operational utility of the protocol with guidance on when and how to use the protocol and service.

### *Program Managers*

By providing PMs with the list of approved PPS, the DoD allows PMs to target the acquisition of systems and system components that must meet interoperability goals and information assurance goals. DoD PMs can request that the PPSMP process review considers using PPS prior to making costly implementation decisions. The DoD PPSMP was developed with the understanding that DoD PMs are continually focused upon multiple challenges, as follows:

- Provide and refine products and services in conjunction with the mission element needs statement, required operational capability, major automated information system review council, and defense information technology security certification and accreditation process processes.
- Meet the schedule.
- Execute fiscal responsibility.
- Minimize fielding costs.
- Minimize software maintenance costs.
- Reduce time to accredit and time to field.

PMs will no longer need to develop multiple system baselines to comply with different component firewall policies. The PPSMP (DoD Instruction 8551.1, paragraph 4.8) requires network security administrators to open enclave boundaries for properly registered AISs using recommended PPS. Early adopters of the PPSMP are Health Affairs and the High Performance Computing Office.

### *System Engineers*

The PPSMP provides the ability to choose compatible products early in the system development cycle and supports a standardized architecture, which reduces configuration management issues with network connections. The PPSMP also simplifies the accreditation process by encouraging standard implementation and consistent reporting methods. It reduces rework costs for system fielding due to PPS cross-component conflicts.

### *Software Developers*

Software developers will be able to use the standard implementation configurations provided in the CAL. The configurations identified in the CAL provide the target architectures that have been vetted by the DSAWG.

### *Designated Approving Authorities*

The PPSMP supports the designated approving authorities (DAAs) by identifying the technical risk of using specific PPS. This identification enables the DAAs to perform informed risk assumption evaluations and decisions. The PPSMP also reduces DAA staff evaluation time for registered AISs and PPS, which use standard configurations and are fielded in full compliance with DISA security technical implementation guides.

*"The PPSMP provides the ability to choose compatible products early in the system development cycle and supports a standardized architecture, which reduces configuration management issues with network connections."*

### *Network Operations Staff*

The Network Operations staff includes both network operators and system administrators. The PPSMP supports the Network Operations staff by providing standard implementation configurations, standardizing router configurations with predefined rule sets to be used as required to meet operational requirements, and reducing hostile/unintended traffic.

Network operators are responsible for the operations and maintenance of major segments of managed networks. Network Operations customers include the United States Strategic Command Joint Task Force-Global Network Operations (JTF-GNO), DISA operations, JTF-GNO Global Network Center, Global Network Support Center, Theater Network Centers, NetDefense, and Computer Emergency Response Teams and Network Operations Centers of the DoD components.

System administrators are responsible for the installation and maintenance of information systems, providing effective information system utilization, and ensuring the use of adequate security parameters and sound implementation of established information assurance policy and procedures.

Benefits realized by the Network Operations staff include advance notice of specific vulnerabilities, potential attack vectors known before exploits exist (e.g., Blaster, Slammer), and aid in the immediate impact analysis of potential port closures during attack/protection decisions. Other benefits include the standardization of router configurations with predefined rule sets to be used as required and the reduction of hostile/unintended traffic.◆

## References


1. Department of Defense. "Ports, Protocols, and Services Management (PPSM)." DoD Instruction 8551.1. Washington: DoD, 13 Aug. 2004 <www.dtic.mil/whs/directives/corres/html/85511.htm>.
2. The Internet Engineering Task Force. Internet Society. 8 Feb. 2005 <www.ietf.org>.
3. Internet Assigned Numbers Authority. 12 July 2004. Internet Society. 8 Feb. 2005 <www.iana.org>.
4. Defense Information Systems Agency. Information Assurance Support Environment. DISA. 8 Feb. 2005 <http://iase.disa.mil>.
5. Defense Information Systems Agency. "PPS Assurance Category Assignments List" Release 2.0. Ports and Protocols. Feb. 2005 <http://iase.disa. mil/ports/index.html>.
6. Department of Defense. "Net Defense (DoD-CERT) Branch of JTF-GNO at JTF-GNO." DoD Ports and Protocols Program. 8 Feb. 2005 <www.cert.mil/portsandprotocols>.


## Note

1. See <http://ipv6.disa.mil>, <www.ipv6.org>, and <www.ipv6forum.com>.

## About the Authors

**David R. Basel** is the project manager for the Department of Defense (DoD) Ports and Protocol Management Project. He is a member of the Defense Information Systems Agency (DISA) Global Information Grid Combat Support Directorate's Center for Network Services. Basel has been with DISA for 13 years. He has held several first-line supervisory and chief engineer positions, including division chief for Communications Network Security, chief engineer for DoD Share Data Environment, and deputy program manager for the DoD Ada Program. Basel has a Bachelor of Science in computer science from Bowling Green State University.

**Center for Network Services**
**GIG Combat Support Directorate**
**DISA**
**P.O. Box 4502**
**Arlington, VA 22204-4502**
**Phone: (703) 882-1553**
**Fax: (703) 882-3336**
**E-mail: disapao@disa.mil**

**Dana Foat** is a computer systems analyst assigned to the Defense-Wide Information Assurance Program Office, Office of the Assistant Secretary of Defense for Networks and Information Integration. Prior to his current assignment, he held various network security positions with the Information Assurance Directorate at the National Security Agency. Foat is a Certified Information Systems Security Professional. He has a Bachelor of Science in mathematics from Valparaiso University, a Master of Science in computer science from Johns Hopkins University, and a Master of Business Administration from the University of Pittsburgh.

**Defense-Wide Information**
**Assurance Program Office**
**1215 S Clark ST**
**STE 1101**
**Arlington, VA 22202-4302**
**Phone: (703) 602-9974**
**Fax: (703) 602-7209**
**E-mail: dana.foat@osd.mil**

**Cragin Shelton** is a senior Information Security engineer with The MITRE Corporation. He has been involved with management of Department of Defense (DoD) information systems and networks since 1984. Since retiring from the U.S. Air Force in 1997, he has concentrated on information security and information assurance aspects of DoD systems and networks. Shelton is a Certified Information Systems Security Professional. He has a Bachelor of Science in chemistry from Centenary College of Louisiana and a Master of Science in Systems Management (information systems) from the University of Southern California.

**The MITRE Corporation**
**7515 Colshire DR**
**MS T320**
**McLean, VA 22102**
**Phone: (703) 883-5836**
**Fax: (703) 883-1245**
**E-mail: cshelton@mitre.org**