

USFK REGULATION 25-70

INFORMATION MANAGEMENT (25)

# **Firewall- Configuration and Deployment Guidance for Boundary Firewall, Ports, Protocols and Services (PPS)**

11 August 2003

UNCLASSIFIED

HEADQUARTERS  
UNITED STATES FORCES, KOREA  
UNIT #15237  
APO AP 96205-5237

USFK Regulation  
No. 25-70

11 August 2003

(Effective: 11 August 2003)  
Information Management

FIREWALL - CONFIGURATION AND DEPLOYMENT GUIDANCE FOR BOUNDARY  
FIREWALL PORTS, PROTOCOLS, AND SERVICES (PPS)

**SUPPLEMENTATION.** Supplementation of this regulation and issuance of command and local forms by subordinate commands is prohibited unless prior approval is obtained from HQ USFK (FKJ6-CIA), Unit #15237, APO AP 96205-5237.

**INTERNAL CONTROLS.** This regulation does not contain management control provisions.

**1. PURPOSE.**

a. To delineate United States Forces, Korea (USFK) policy for the implementation of firewall devices for the Non-classified Internet Protocol Router Network (NIPRNET), to provide detailed configuration settings for ports, protocols, and services (PPS), and to specify security countermeasures associated with certain PPS settings, in accordance with (IAW) references 3(a), 3(b), 3(e), and 3(g).

b. To establish the requirement for boundary protection firewall type devices at termination of Defense Intelligence Service Agency (DISA) controlled Defense Intelligence Service Network (DISN) services within the USFK area of responsibility (AOR).

**2. APPLICABILITY.**

a. This policy is directive in nature and will remain in effect until otherwise superseded or rescinded by regulation or other appropriate media.

b. This policy applies to all firewalls at DISN interfaces, including all Department of Defense (DOD) CINC/Service/Agency (C/S/A) firewalls serving as network boundaries to the DISN, to include in-garrison and deployed networks.

c. This policy does not extend to Service or DOD agency internal network boundaries, where the use of ports and protocols services will be governed by internal organizational policy.

d. This policy is limited to those protocols that correspond to the Internet Protocol (IP) suite, specifically Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

## **USFK Reg 25-70**

### **3. REFERENCES.** The following are related publications:

a. Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (3CI) Policy Memorandum, "Increasing the Security Posture of the Unclassified by Sensitive Internet Protocol Router Network (SIPRNET), August 22, 1999.

b. Chairman of the Joint Chiefs Staff Instruction (CJCSI) 6510.01C, "Final Draft, Information Assurance (IA) and Computer Network Defense (CND)".

c. Chairman of the Joint Chiefs Staff Manual (CJCSM) 6510.01C Information Assurance -- Defense-In-Depth, 30 March 2001.

d. Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510, "Department of Defense Global Information Grid Information Assurance".

e. DOD Firewall Guidance, Version 1.2, 9 March 2001.

f. The Internet Assigned Numbers Authority, Protocol Numbers and Assignment Services, <http://www.iana.org/>.

g. USCINCPAC Configuration Guidance for Enclave Boundary Firewall Ports, Protocols, and Services (PPS), "Draft 22 Oct 01".

**4. EXPLANATION OF ABBREVIATIONS AND TERMS.** Abbreviations and terms used in this regulation are explained in the glossary.

**5. FIREWALL CHANGE NOTIFICATION (FCN).** Appendix A.

**6. FIREWALL CHANGE REQUEST (FCR).** Appendix B.

**7. FIREWALL POLICY STATEMENTS AND CONFIGURATIONS.** Appendix C.

**8. PORTS, PROTOCOL, AND SERVICES (PPS) CONFIGURATION.** Appendix D.

### **9. GENERAL.**

a. The common understanding of acceptable risk provides for maximum interoperability with an emphasis on security.

b. USFK organizations shall comply with theater firewall PPS configurations to mitigate common risk across the DISN and ensure interoperability across DOD C/S/A.

(1) Boundary firewalls and standardized configurations are required for all Metropolitan Area Network (MAN) entry points. The MAN boundary is essentially the physical, or logical location where the 1<sup>st</sup> Signal Brigade provides a connection to the DISN.

(2) Common types of firewalls include packet filters, circuit-level or proxy-based application gateways, and "stateful packet inspection" firewall. Detailed descriptions of each are contained in the glossary.

## 10. GUIDELINES.

a. Goals. The goal of this policy is to balance three equities for the DISN--

(1) Security - a policy with acceptable community risk and interoperability characteristics.

(2) Systems integration - a policy providing components with the ability to maintain operations and provide services to the USFK/CFC Commander and respective components.

(3) Inter-service Interoperability - a guarantee that applications will be capable of communicating through all DOD boundary firewalls using the ports, protocols and services required by the Commander, USFK/CFC and components.

b. Security. To ensure an acceptable DOD community risk is maintained, adherence to the technical guidance in Appendices A and B and the following applies:

(1) Deny-by-default. Any PPS not specified in Appendix D shall be designated as "Deny".

(2) PPS too susceptible to exploitation or attack shall never be used between C/S/As - designated as "Deny", hereafter referred to as **Black** (see Glossary, for a detailed description).

(3) PPS that have associated risk, but are operationally necessary will be used conditionally, provided specific security countermeasures are invoked to minimize associated risk - designated as "Conditional", hereafter referred to as **White** (see Glossary, for a detailed description).

(4) PPS with desirable security characteristics and advocated for future application development, hereafter referred to as **Green** (see Glossary, for a detailed description).

## 11. ASSUMPTIONS.

a. Component, Sub-unified, and Joint Task Force, and other USFK theater elements/agencies are assumed to adhere to standard Internet Assigned Numbers Authority (IANA) ports (ref (B)), unless otherwise stated. Organizations submitting for a deviation will identify the ports and protocols being used.

b. The requirements in this instruction will not conflict with the Intelligence Community's (IC) Open Source Information System (OSIS) firewall requirements. In cases where a conflict is noted, organizations will follow the deviation process described in paragraph 9.

c. Mobile code technologies will comply with ref 3e.

## **USFK Reg 25-70**

d. PPS needed within the MAN will be IAW ref 3e. Services will have separate approval authority for Service internal PPS. The Service Designated Approving Authority (DAA) will have sole approval authority for internal PPS use.

e. Virtual Private Networks (VPN) will be decrypted at or before entering the firewall. The USFK VPN Policy will be published in 2003.

## **12. RESPONSIBILITIES.**

### **a. HQ USFK CIO.**

(1) Review all FCNs and FCRs submitted IAW Appendices A and B.

(2) Direct the amendment of any FCN or FCR that contravenes appropriate levels of information assurance or interoperability.

### **b. HQ USFK J6.**

(1) Approve Joint Task Force (JTF)/Joint Mission Force (JMF) FCR submitted IAW Appendix B.

(2) Receive all FCN submitted IAW Appendix A.

### **c. HQ USFK J6O/CJCCC.**

(1) In conjunction with JTF-CNO, provide the USFK Theater Information Grid (TIG) status, ensuring that it is incorporated into the Global Information Grid (GIG) Information Assurance (IA) Common Operational Picture (COP).

(2) Share the TIG IA COP with USFK Components.

### **d. HQ USFK J6 IA.**

(1) Track all theater FCN by C/S/A and approved JTF/JMF FCR by Standardized Tactical Entry Points (STEP) site.

(2) Receive and validate all FCN and FCR submitted IAW Appendices A and B.

(3) Exercise planned or unannounced vulnerability and CND operational assessments.

(a) CND assessments are intended to provide USFK Components with specific technical assistance that ensure compliance with this policy and other best security practices, while providing HQ USFK the assurance that all assumed risks and known and validating the USFK TIG IA status.

(b) Vulnerability and CND assessments may consist of staff assistance visits and/or coordinated network scans.

e. 1st Signal Brigade.

(1) Operate and maintain firewalls at DISN entry points located at Camp Walker, CP TANGO and Yongsan-Garrison, with configuration settings contained in appendix D.

(2) Ensure protection for MAN as well as the Defense Information Infrastructure (DII) backbone Point of Presence (POP) from security threats by configuring boundary firewalls IAW appendix D.

(3) Provide justification for deviations from the USFK Firewall Policy by submitting FCN configuration IAW paragraph 9 and appendix A.

(4) Audit firewall and system log files.

(5) Ensure there are no unprotected connections into USFK MAN.

(a) No modems connected to systems that are also connected to the MAN.

(b) No wireless communications connected to the MAN. Note: Waiting on DOD policy.

(c) All traffic must pass through the firewall and security stack before entering the MAN.

(d) Disconnect FAX machines from the MAN.

### **13. DEVIATIONS.**

a. USFK component and sub-unified command deviations to this policy require HQ USFK IA validation and USFK CIO notification through the submission of a FCN found in Appendix A.

b. USFK JTF/JMF deviations to this policy, whether more or less restrictive, require HQ USFK J6O (C/JCCC) validation and USFK J6 approval through the submission of a FCR Appendix B.

c. MAN DAA will, at a minimum, document the specific deviation(s), including the expected duration, operational requirement, and any associated risk mitigation measures.

d. DAA approved documentation will be submitted to HQ USFK J6O (C/JCCC) for validation with a minimum lead-time of two weeks, using the FCN or FCR format in Appendices A and B.

e. Immediate requests (i.e., implementation timeline less than two weeks) must contain an operational justification statement for expedited processing.

## USFK Reg 25-70

**Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander, USFK (FKJ6-CIA), Unit #15237, APO AP 96205-5237. This publication is available electronically at: <https://www-eusa.korea.army.mil>**

FOR THE COMMANDER:

OFFICIAL:  
CHARLES C. CAMPBELL  
Lieutenant General, USA  
Chief of Staff

F. W. MORRIS  
Assistant Adjutant General

### **4 Appendixes**

- A. Firewall Change Notification (FCN)
- B. Firewall Change Request (FCR)
- C. Firewall Policy Statements and Configurations
- D. Ports, Protocol, and Services (PPS) Configurations

### **Glossary**

DISTRIBUTION:  
Electronic Media Only

**APPENDIX A**

**FIREWALL CHANGE NOTIFICATION (FCN)**

FROM: \_\_\_\_\_

TO: \_\_\_\_\_

CLASSIFICATION: \_\_\_\_\_

TYPE OF SERVICE REQUIRED: \_\_\_\_\_

DIRECTION OF SERVICE: Incoming, Outgoing, Both

IP(s) REQUIRING PORT, PROTOCOL OR SERVICE CHANGE: Class "C" or X.X.X.X

ACCESS PERIOD(s): Indefinite or Start / Stop times (Local Time)

LOCAL DAA APPROVAL: Name, Rank, and Position Title

OPERATIONAL IMPACT STATEMENT: If firewall change is not implemented, what is the operational impact to your network and systems? FCNs are deviations from the DOD and USFK Firewall Configuration Policy. This statement will be referenced for INFOCON changes. Generic statements may result in denial or service or a lower priority due to insufficient justification.

OTHER: Justification statement for notifications with an implementation timeline less than two weeks.

**APPENDIX B**

**FIREWALL CHANGE REQUEST (FCR)**

FROM: \_\_\_\_\_

TO: \_\_\_\_\_

STEP SITE REQUIRING CHANGE: \_\_\_\_\_

CLASSIFICATION: \_\_\_\_\_

TYPE OF SERVICE REQUIRED: \_\_\_\_\_

DIRECTION OF SERVICE: Incoming, Outgoing, Both

IP(s) REQUIRING PORT, PROTOCOL OR SERVICE CHANGE: Class "C" or X.X.X.X

ACCESS PERIOD(s): Indefinite or Start / Stop times (Local Time)

LOCAL DAA APPROVAL: Name, Rank, and Position Title

OPERATIONAL IMPACT STATEMENT IF NOT SATISFIED: This section is used to determine allocation. Generic statements may result in denial of service or a lower priority due to insufficient justification. Specific operational statements are needed to prioritize decisions.

OTHER: Justification statement for notifications with an implementation timeline less than two weeks.

## APPENDIX C

## FIREWALL POLICY STATEMENTS AND CONFIGURATIONS

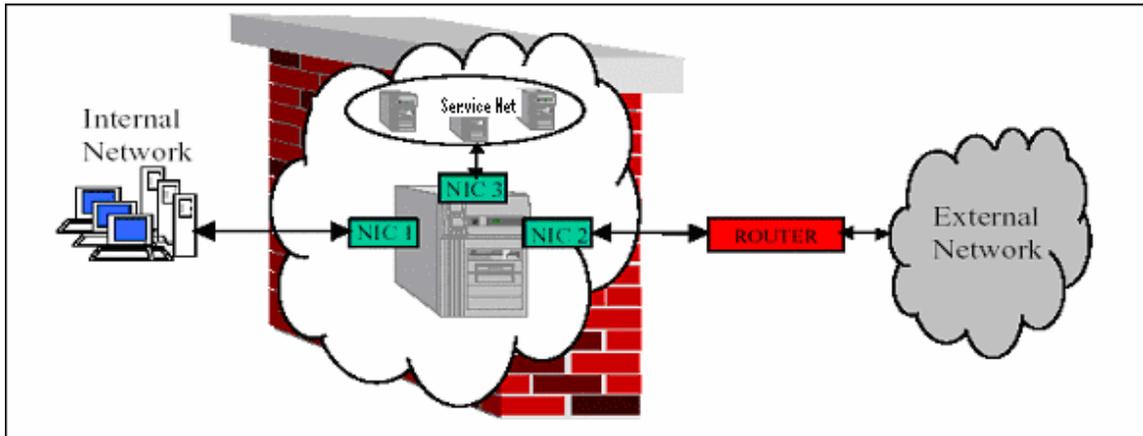
The following is a list of the firewall policies used to describe the security countermeasures to be used with PPS. It is assumed that network address translation (NAT) is enabled unless otherwise specified by the policies. Each network service that has a standard requirement will have one or more policy statements identifying the recommended security solutions.

Table 1: Firewall Policy Statements

Policy Statements
1. Deny
2. Demilitarized Zone (DMZ)
3. Allow
4. Relay
5. Restrict by Source IP
6. Restrict by Destination IP
7. Restrict by Source Domain
8. Restrict by Destination Domain
9. Allow inbound to only authorized servers
10. Strong Authentication
11. Encrypt over WAN
12. NAT OFF
13. Requires Transition – Time limited

a. Recommended Demilitarized Zone (DMZ) architecture. The DMZ is defined as the area in front of the firewall that is not fully protected. The DMZ should contain a combination of a security router, Intrusion Detection System (IDS), WEB Caching engine, other Proxies, etc. The firewalls external interface is the beginning of the DMZ. The DMZ ends at the beginning of the DISN, or the internal interface of a security router.

b. Dual-Homed with Screened Subnet. In the dual-homed with screened subnet firewall architecture (figure 1), a host is set up as a gateway with three Network Interface Cards (NICs): one connected to the external network through a router, one to the internal network, and one to the Service Network. Packet forwarding is disabled on the gateway, and information is passed at the application level or the network layer depending on the type of firewall used. The gateway can be reached from all sides, but traffic cannot directly flow across it unless that particular traffic is allowed to pass to the destination it is requesting.



**Figure 1. Dual-Homed with Screened Subnet (Service Network)**

(1) The router should be set up with Access Control Lists (ACL) or IP filtering so that connections are allowed between the router and the firewall only. This configuration has some of the same disadvantages of the regular Dual Home architecture. However, the screened subnet provides external, untrusted networks restricted access to the Service Net for services such as World Wide Web (WWW) or File Transfer Protocol (FTP).

(2) This allows the enclave to place its public servers in a secure network that requires external sources to traverse the firewall and its security policy to access the public servers, but will not compromise the operating environment of the internal networks if hackers attack one of the networks.

(3) Both the Dual-Homed and Dual-Homed with Screened Subnet configurations are acceptable.

APPENDIX D

PORTS, PROTOCOL, AND SERVICES (PPS) CONFIGURATIONS

ICMP MESSAGES

ICMP Message Number	ICMP Message Name	Condition
0	Echo Reply	Allow Outbound Only
3	Destination Unreachable	Allow Outbound Only
4	Source Quench	Allow Both Directions
8	Echo Request	Allow Outbound Only
11	Time Exceeded	Allow Inbound Only
12	Parameter Problem	Allow Both Directions

TCP/UDP

Alphabetical by Service

Services	Ports	Prot.	Desig.	Policy		Conditions		Comments
				In	Out	In	Out	
AHIPC	3002	TCP	White	N/A	Cond	N/A (Client)	- Restrict by Destination IP - Requires Transition	DEERS/RAPIDS ID (Client) - USMC (added 30 March 2001)
AHIPC	4009	TCP	White	Cond	Cond	Allow inbound to only authorized servers	- Restrict by Destination Domain - Requires Transition	DEERS/RAPIDS ID (Server) - USMC (added 30 March 2001)
Audio streaming	1025-65536	UDP	Black	Deny	Deny			
Audit	5402	TCP	White	Cond	Cond	Allow inbound to only authorized servers	- Restrict by Destination IP	CAC Common Access Cards - USMC (added 30 March 2001)
Auth	113	TCP	Black	Deny	Deny			See DOD CERT Bulletin 95-43
Bootp	67	UDP	Black	Deny	Deny			
Bootpc	68	UDP	Black	Deny	Deny			
Calendar	5730	TCP	Black	Deny	Deny			
Chargen	19	TCP; UDP	Black	Deny	Deny			See CERT/CC 96-01 Denial of Service (UDP)
Daytime	13	TCP; UDP	Black	Deny	Deny			See CERT/CC 96-01 Denial of Service
Discard	9	TCP; UDP	Black	Deny	Deny			
DMS X.500	17003	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	
DNS	53	TCP; UDP	White	Deny	Cond	- Deny	- Relay	
DNSSEC	53	TCP; UDP	Green	Deny	Cond	- Deny	- Relay	
DPAS	5000	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	

Services	Ports	Prot.	Desig.	Policy		Conditions		Comments
				In	Out	In	Out	
DPAS	5557	TCP	White	Cond	Cond	-Allow inbound to only authorized servers	- Restrict by Destination IP	
Echo	7	TCP; UDP	Black	Deny	Deny			See CERT/CC 96-01 Denial of Service
Finger	79	TCP	Black	Deny	Deny			See CERT/CC Advisory 93-04 and DOD CERT Bulletin 93-06.
FTP-active	20,21	TCP; UDP	White	Deny	Allow	- Deny	- Allow	
FTP-passive	20,21	TCP	White	Deny	Deny	- Deny	- Deny	
Gopher	70	TCP	White	Deny	Cond	- Deny	- Restrict to destination domain	Used to access the Congressional Gopher Server
Hostname	101	TCP	Black	Deny	Deny			
HTTP	80	TCP	Green	Deny	Cond	- Deny	- Relay	
ICA	1494	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	
ICI (CMOS Interactive Communications Interface)	251	TCP	White	Cond	Cond	- Restrict by Destination IP	- Restrict by Destination IP	CMOS Interactive Communications Interface.
IMAP(SSL)	993	TCP	Green	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by destination domain - Relay	
IMAP2	143	TCP	Black	Deny	Deny			See CERT/CC 98-11, 98-07.
IMAP3	220	TCP	Black	Deny	Deny			See CERT/CC Advisory 98-11, 98-07, 97-09.
InfoConnect	256	TCP	White	Cond	Cond		- Restrict by Destination IP	
Interpid (Oracle)	1521	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	CAC Common Access Cards - USMC (added 30 March 2001)
IRC	194	TCP	Black	Deny	Deny			See CERT/CC Advisory 94-14 and DOD CERT Bulletin 93-33.
IRC	6665-6669	TCP	Black	Deny	Deny			
IRC	6667	TCP	Black	Deny	Deny			See CERT/CC Advisory 94-14 and DOD CERT Bulletin 94-33.
JCALs	UDP	2223	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP	JCALs is permitted through the firewall on an as-needed basis through the use of a NAVSEA proxy.
LDAP	389	TCP	White	Deny	Allow	- Allow inbound to only authorized servers	- Allow	
LDAP	390	TCP	White	Deny	Allow	- Allow inbound to only authorized servers	- Allow	
LDAPS	636	TCP; UDP	Green	Deny	Cond	- Deny	- Allow	LDAP protocol over TLS/SSL (was sldap).
LDAPS	637	TCP; UDP	Green	Deny	Cond	- Deny	- Allow	LDAP protocol over TLS/SSL (was sldap).
LINK	87	TCP	Black	Deny	Deny			
Listen	2766	TCP	Black	Deny	Deny			
Listener	1025	TCP	Black	Deny	Deny			

Services	Ports	Prot.	Desig.	Policy		Conditions		Comments
				In	Out	In	Out	
LPD (Printing)	515	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Encrypted over the WAN - Transition	Line printer spooler. See CERT/CC Advisories 97-19, 95-15. Defense Integrated Management Engineering System (DIMES)
MS CHAT	6665	TCP	Black	Deny	Deny			
MS CHAT listen	7000	TCP	Black	Deny	Deny			
MS NetMtg	1503	TCP	White	Cond	Allow	- Allow inbound to only authorized servers	- Allow	
MSP, v2	18	TCP	Black	Deny	Deny			
MS-RPC	135	TCP; UDP	Black	Deny	Deny			
MTA	102		White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP - NAT off	
NetBIOS	137-139	TCP; UDP	Black	Deny	Deny			
NETRJS	71-74	TCP; UDP	Black	Deny	Deny			
Netstat	15	TCP	Black	Deny	Deny			
NFS	2049	TCP; UDP	Black	Deny	Deny			See CERT/CC Advisories 98-12, 96-09, 94-15, 94-02, 93-15, 92-15, 91-21, and DOD CERT Bulletin 1999-A-6, 1999-01, 94-41.
NIS			Black	Deny	Deny			
NNTP	119	TCP	White	Cond	Cond	- Allow inbound to only authorized servers - DMZ	- Restrict by destination domain - Relay	
NNTP(SSL)	563	TCP	Green	Deny	Cond	- Allow inbound to only authorized servers - DMZ	- Restrict by destination domain - Relay	
Ntalk	518	UDP	Black	Deny	Deny			
Oracle	1521	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination Domain - Requires Transition	DEERS/RAPIDS ID - USMC (added 30 March 2001)
Oracle 8.x or >			Green					
POP-2	109	TCP	Black	Deny	Deny			See CERT/CC Advisory 98-11, 98-07, 97-09.
POP3 (SSL)	995	TCP	Green	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by destination domain - Relay	
PPTP	1723	TCP; UDP	White	Cond	Cond	Allow inbound to only authorized servers	- Requires Transition	DEERS/RAPIDS ID – USMC (added 30 March 2001)
PPTP	1723	TCP; UDP	Black	Deny	Deny			
RE-Mail-CK	50	TCP; UDP	Black	Deny	Deny			
Remote Job Entry	5	TCP, UDP	Black	Deny	Deny			
Rexec	512	TCP	Black	Deny	Deny			
Rlogin	513	TCP	Black	Deny	Deny			See CERT/CC Advisories 97-06, 95-15, 94-09.

Services	Ports	Prot.	Desig.	Policy		Conditions		Comments
				In	Out	In	Out	
RPC	530	TCP; UDP	Black	Deny	Deny			
Rsh	514	TCP	Black	Deny	Deny			
RTELNET	107	TCP; UDP	Black	Deny	Deny			
Rwho	513	UDP	Black	Deny	Deny			
SARA	10005	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	Marine: Squadron Assistant Risk Assessment
SFTP	115	TCP	Black	Deny	Deny			
S-HTTP	443	TCP; UDP	White	Cond	Allow	- Allow inbound to only authorized servers	- Allow	
SMTP	25	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Relay	
SMTP (S/MIME)	25	TCP	Green	Cond	Cond	- Allow inbound to only authorized servers	- Relay	
SQL Server	1433	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP - Relay	
SQL*Net	1521	TCP	White	Cond	Cond	Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP - Relay	
SQL*Net	1522	TCP	White	Cond	Cond	Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	
SQL*Net	1525	TCP	White	Cond	Cond	Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	
SQL*Net	1601	TCP	White	Cond	Cond	Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	
SQL*Net	1748	TCP	White	Cond	Cond	Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	
SQL*Net v.2	1526	TCP	White	Cond	Cond	Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	
SSH	22	TCP	White	Cond	Allow	- Allow inbound to only authorized servers	- Allow	
SSL	443	TCP	Green	Cond	Cond	- Allow inbound to only authorized servers	- Relay	
Ssyslog	514	UDP	Green			- Allow inbound to only authorized servers	- Restrict by Destination IP	
Statsrv	133	TCP	Black	Deny	Deny			See CERT/CC Advisory 97-26 and DOD CERT Bulletin 96-12.
Supdup	95	TCP	Black	Deny	Deny			
SWA	9023	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	
SWA	9024	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	

Services	Ports	Prot.	Desig.	Policy		Conditions		Comments
				In	Out	In	Out	
SWA	9025	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	
SWA	9026	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	
Systat	11	TCP	Black	Deny	Deny			
Talk	517	UDP	Black	Deny	Deny			See CERT/CC Advisory 97-04 and DOD CERT Bulletin 97-07.
TCPMux	1	TCP	Black	Deny	Deny			
Telnet	23	TCP	White	Cond	Allow	- Allow inbound to only authorized servers - Allow outbound from only authorized servers - Strong Authentication - Relay	- Allow	
Time	37	TCP; UDP	Black	Deny	Deny			See CERT/CC 96-01 Denial of Service (UDP).
TOPS			White	Cond	Cond	- Allow inbound to only authorized servers	- DMZ - Transition	
UUCP	540	TCP	Black	Deny	Deny			See CERT/CC Advisory 92-06.
UUCP	541	TCP; UDP	Black	Deny	Deny			
UUCP-path	117	TCP	Black	Deny	Deny			See CERT/CC Advisory 92-06.
Video streaming	1025-65536	UDP	Black	Deny	Deny			
WASP	5403	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	CAC Common Access Cards - USMC (added 30 March 2001)
WASP	5404	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	CAC Common Access Cards - USMC (added 30 March 2001)
X.400	104	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP - NAT off	
X.500	102	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP - NAT off	
XDMCP	177	UDP	Black	Deny	Deny			

## Ports, Protocol, and Services Configurations

### Numerical by Port

Services	Ports	Prot.	Desig.	Policy		Conditions		Comments
				In	Out	In	Out	
NIS			Black	Deny	Deny			
Oracle 8.x or >			Green					
TOPS			White	Cond	Cond	- Allow inbound to only authorized servers	- DMZ - Transition	
TCPMux	1	TCP	Black	Deny	Deny			
Remote Job Entry	5	TCP, UDP	Black	Deny	Deny			
Echo	7	TCP; UDP	Black	Deny	Deny			See CERT/CC 96-01 Denial of Service
Discard	9	TCP; UDP	Black	Deny	Deny			
Systat	11	TCP	Black	Deny	Deny			
Daytime	13	TCP; UDP	Black	Deny	Deny			See CERT/CC 96-01 Denial of Service
Netstat	15	TCP	Black	Deny	Deny			
MSP, v2	18	TCP	Black	Deny	Deny			
Chargen	19	TCP; UDP	Black	Deny	Deny			See CERT/CC 96-01 Denial of Service (UDP)
FTP-active	20,21	TCP; UDP	White	Deny	Allow	- Deny	- Allow	
FTP-passive	20,21	TCP	White	Deny	Deny	- Deny	- Deny	
SSH	22	TCP	White	Cond	Allow	- Allow inbound to only authorized servers	- Allow	
Telnet	23	TCP	White	Cond	Allow	- Allow inbound to only authorized servers - Allow outbound from only authorized servers - Strong Authentication - Relay	- Allow	
SMTP	25	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Relay	
SMTP (S/MIME)	25	TCP	Green	Cond	Cond	- Allow inbound to only authorized servers	- Relay	
Time	37	TCP; UDP	Black	Deny	Deny			See CERT/CC 96-01 Denial of Service (UDP).
RE-Mail-CK	50	TCP; UDP	Black	Deny	Deny			
DNS	53	TCP; UDP	White	Deny	Cond	- Deny	- Relay	
DNSSEC	53	TCP; UDP	Green	Deny	Cond	- Deny	- Relay	
Bootp	67	UDP	Black	Deny	Deny			
Bootpc	68	UDP	Black	Deny	Deny			
Gopher	70	TCP	White	Deny	Cond	- Deny	- Restrict to destination domain	Used to access the Congressional Gopher Server
NETRJS	71-74	TCP; UDP	Black	Deny	Deny			

Services	Ports	Prot.	Desig.	Policy		Conditions		Comments
				In	Out	In	Out	
Finger	79	TCP	Black	Deny	Deny			See CERT/CC Advisory 93-04 and DOD CERT Bulletin 93-06.
HTTP	80	TCP	Green	Deny	Cond	- Deny	- Relay	
LINK	87	TCP	Black	Deny	Deny			
Supdup	95	TCP	Black	Deny	Deny			
Hostname	101	TCP	Black	Deny	Deny			
MTA	102		White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP - NAT off	
X.500	102	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP - NAT off	
X.400	104	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP - NAT off	
RTELNET	107	TCP; UDP	Black	Deny	Deny			
POP-2	109	TCP	Black	Deny	Deny			See CERT/CC Advisory 98-11, 98-07, 97-09.
Auth	113	TCP	Black	Deny	Deny			See DOD CERT Bulletin 95-43
SFTP	115	TCP	Black	Deny	Deny			
UUCP-path	117	TCP	Black	Deny	Deny			See CERT/CC Advisory 92-06.
NNTP	119	TCP	White	Cond	Cond	- Allow inbound to only authorized servers - DMZ	- Restrict by destination domain - Relay	
Statsrv	133	TCP	Black	Deny	Deny			See CERT/CC Advisory 97-26 and DOD CERT Bulletin 96-12.
MS-RPC	135	TCP; UDP	Black	Deny	Deny			
NetBIOS	137- 139	TCP; UDP	Black	Deny	Deny			
IMAP2	143	TCP	Black	Deny	Deny			See CERT/CC 98-11, 98-07.
XDMCP	177	UDP	Black	Deny	Deny			
IRC	194	TCP	Black	Deny	Deny			See CERT/CC Advisory 94-14 and DOD CERT Bulletin 93-33.
IMAP3	220	TCP	Black	Deny	Deny			See CERT/CC Advisory 98-11, 98-07, 97-09.
ICI (CMOS Interactive Communications Interface)	251	TCP	White	Cond	Cond	- Restrict by Destination IP	- Restrict by Destination IP	CMOS Interactive Communications Interface.
InfoConnect	256	TCP	White	Cond	Cond		- Restrict by Destination IP	
LDAP	389	TCP	White	Deny	Allow	- Allow inbound to only authorized servers	- Allow	

Services	Ports	Prot.	Desig.	Policy		Conditions		Comments
				In	Out	In	Out	
LDAP	390	TCP	White	Deny	Allow	- Allow inbound to only authorized servers	- Allow	
S-HTTP	443	TCP; UDP	White	Cond	Allow	- Allow inbound to only authorized servers	- Allow	
SSL	443	TCP	Green	Cond	Cond	- Allow inbound to only authorized servers	- Relay	
Rexec	512	TCP	Black	Deny	Deny			
Rlogin	513	TCP	Black	Deny	Deny			See CERT/CC Advisories 97-06, 95-15, 94-09.
Rwho	513	UDP	Black	Deny	Deny			
Rsh	514	TCP	Black	Deny	Deny			
Ssyslog	514	UDP	Green			- Allow inbound to only authorized servers	Restrict by Destination IP	
LPD (Printing)	515	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Encrypted over the WAN - Transition	Line printer spooler. See CERT/CC Advisories 97-19, 95-15. Defense Integrated Management Engineering System (DIMES)
Talk	517	UDP	Black	Deny	Deny			See CERT/CC Advisory 97-04 and DOD CERT Bulletin 97-07.
Ntalk	518	UDP	Black	Deny	Deny			
RPC	530	TCP; UDP	Black	Deny	Deny			
UUCP	540	TCP	Black	Deny	Deny			See CERT/CC Advisory 92-06.
UUCP	541	TCP; UDP	Black	Deny	Deny			
NNTP (SSL)	563	TCP	Green	Deny	Cond	- Allow inbound to only authorized servers - DMZ	- Restrict by destination domain - Relay	
LDAPS	636	TCP; UDP	Green	Deny	Cond	- Deny	- Allow	LDAP protocol over TLS/SSL (was sldap).
LDAPS	637	TCP; UDP	Green	Deny	Cond	- Deny	- Allow	LDAP protocol over TLS/SSL (was sldap).
IMAP (SSL)	993	TCP	Green	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by destination domain - Relay	
POP3 (SSL)	995	TCP	Green	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by destination domain - Relay	
Listener	1025	TCP	Black	Deny	Deny			
SQL Server	1433	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP - Relay	
ICA	1494	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP	
MS NetMtg	1503	TCP	White	Cond	Allow	- Allow inbound to only authorized servers	- Allow	
Interpid (Oracle)	1521	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	Restrict by Destination IP	CAC Common Access Cards - USMC (added 30 March 2001)

Services	Ports	Prot.	Desig.	Policy		Conditions		Comments
				In	Out	In	Out	
Oracle	1521	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination Domain - Requires Transition	DEERS/RAPIDS ID - USMC (added 30 March 2001)
SQL*Net	1521	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP - Restrict by Destination IP - Relay	
SQL*Net	1522	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	
SQL*Net	1525	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	
SQL*Net v.2	1526	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	
SQL*Net	1601	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	
PPTP	1723	TCP; UDP	White	Cond	Cond	- Allow inbound to only authorized servers	- Requires Transition	DEERS/RAPIDS ID - USMC (added 30 March 2001)
PPTP	1723	TCP; UDP	Black	Deny	Deny			
SQL*Net	1748	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP - Relay	
NFS	2049	TCP; UDP	Black	Deny	Deny			See CERT/CC Advisories 98-12, 96-09, 94-15, 94-02, 93-15, 92-15, 91-21, and DOD CERT Bulletin 1999-A-6, 1999-01, 94-41.
JCALs	2223	UDP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Source IP	JCALs is permitted through the firewall on an as-needed basis through the use of a NAVSEA proxy.
Listen	2766	TCP	Black	Deny	Deny			
AHIPC	3002	TCP	White	N/A	Cond	N/A (Client)	- Restrict by Destination IP - Requires Transition	DEERS/RAPIDS ID (Client) - USMC (added 30 March 2001)
AHIPC	4009	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination Domain - Requires Transition	DEERS/RAPIDS ID (Server) - USMC (added 30 March 2001)
DPAS	5000	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	
Audit	5402	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	CAC Common Access Cards - USMC (added 30 March 2001)
WASP	5403	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	CAC Common Access Cards - USMC (added 30 March 2001)
WASP	5404	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	CAC Common Access Cards - USMC (added 30 March 2001)
DPAS	5557	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	
Calendar	5730	TCP	Black	Deny	Deny			
MS CHAT	6665	TCP	Black	Deny	Deny			

Services	Ports	Prot.	Desig.	Policy		Conditions		Comments
				In	Out	In	Out	
IRC	6665-6669	TCP	Black	Deny	Deny			
IRC	6667	TCP	Black	Deny	Deny			See CERT/CC Advisory 94-14 and DOD CERT Bulletin 94-33.
MS CHAT listen	7000	TCP	Black	Deny	Deny			
SWA	9023	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	
SWA	9024	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	
SWA	9025	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	
SWA	9026	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	
SARA	10005	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	Marine: Squadron Assistant Risk Assessment
DMS X.500	17003	TCP	White	Cond	Cond	- Allow inbound to only authorized servers	- Restrict by Destination IP	
Audio streaming	1025 65536	UDP	Black	Deny	Deny			
Video streaming	1025 65536	UDP	Black	Deny	Deny			

**GLOSSARY**

**Section I. Abbreviations**

ACL	Access Control List
AOR	Area of Responsibility
CFC	Combined Forces Command
COP	Common Operational Picture
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CND	Computer Network Defense
C/S/A	CINC/Service/Agency
DAA	Designated Approving Authority
DII	Defense Information Infrastructure
DISA	Defense Intelligence Service Agency
DISN	Defense Information System Network
DMZ	Demilitarized Zone
DOD	Department of Defense
FCN	Firewall Change Notification
FCR	Firewall Change Request
GIG	Global Information Grid
IA	Information Assurance
IANA	Internet Assigned Numbers Authority
IAW	in accordance with
IC	Intelligence Community

## **USFK Reg 25-70**

ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
HQ	Headquarters
JMF	Joint Mission Force
JTF	Joint Task Force
LAN	Local Area Network
MAN	Metropolitan Area Network
NAT	Network Address Translation
NIPRNET	Non-classified Internet Protocol Router Network
OSIS	Open Source Information System
POP	Point of Presence
PPS	Ports, Protocol and Services
STEP	Standardized Tactical Entry Points
TCP	Transmission Control Protocol
TIG	Theater Information Grid
UDP	User Datagram Protocol
USCINCPAC	United States Commander-in-Chief, Pacific
USFK	United States Forces Korea
VPN	Virtual Private Networks
WWW	World Wide Web
3CI	Command, Control, Communications and Intelligence

## Section II. Terms

**Access Control** - The process of limiting access to the resources of a system only to authorized programs, processes, or other systems (in a network). Synonymous with controlled access and limited access.

**Allow** - A firewall rule set that permits traffic to transit the network boundary, regardless of the protocol being used, to communicate from one host (source) to another (destination).

**Application** - An application is any data entry, update, query, report, email or other program that calls/invokes a protocol with a registered or unregistered port, for example Power Track, Automated Business Services System (ABSS), Global Combat Support System (GCSS), Global Command and Control System (GCCS), network control, etc.

**Approval** - The formal process of enrolling the desired use of a protocol and its associated port number(s) on DOD networks.

**Attack** - The act of trying to bypass security controls on a system. An attack may be active, resulting in the alteration of data; or passive, resulting in the release of data. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures. The intentional act of attempting to bypass security controls on an automated information system (AIS).

**Authentication** - The process of determining someone or something is what they say they are.

**Authorization** - The process of checking the rights (or permissions) to the server resource that are allowed for the subject; for example, a subject might be allowed read access but not write access to a server resource.

**Black** - PPS designated as not approved for cross-enclave use. These PPS have been determined to have exploitable vulnerabilities that may permit a remote attack, reveal information regarding the network architecture, or contain services that are no longer used because the functionality is provided by another, more secure service. Black PPS shall **not** be used in developing applications for use across the DII.

**Centralized Management** - The concept of using a single, designated management authority. It includes system management, program and project management, and product management.

**Certification** - The process of determining the effectiveness of all security mechanisms. The comprehensive evaluation of the technical and non-technical security features of an AIS and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

## **USFK Reg 25-70**

**Conditional** - This is a firewall rule set that is denied by default, but may be allowed when implemented under additional considerations. Such consideration may require specific architectural implementation or the use of additional software to help mitigate some risks inherent within those protocols and services.

**Configuration** - A collection of an item's descriptive and governing characteristics, which can be expressed in functional terms, i.e., what performance the item is expected to achieve; and in physical terms, i.e., what the item should look like and consist of when it is built.

**Deconfliction** - The process to identify and resolve the issues related to any conflicting use of a protocol and its associated port number(s) on DOD networks.

**Defense Information Infrastructure (DII)** - The shared or interconnected system of computers, communications, data applications, security, people, training and other support structures serving DOD local, national, and worldwide information needs. DII connects DOD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to the subscribers over the Defense Information Systems Network (DISN) and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DOD information.

**Deny** - A firewall rule set that does NOT permit traffic to transit a network boundary across a giving port. Protocols or services that commonly use these ports have been determined to pose a significant threat to the protected network. Therefore the protocol is not allowed to enter the protected enclave from an untrusted enclave.

**Demilitarized Zone (DMZ)** - The area in front of the firewall that is unprotected.

**Enclave** - A network under the operational control and authority of a single organization with the responsibility to define and implement security controls.

**Enforcement** - A collaborative process to monitor and control the use of a protocol and its associated port number(s) on DOD networks.

**Firewall** - A system or combination of systems that enforces a boundary between two or more networks. A gateway that limits access between networks IAW local security policy.

**Green** - PPS designated as representing the best security practices advocated for use in future applications. These PPS meet all enforceable existing and future DOD and service policies and have an acceptable risk. Migration to these PPS is desirable and will result in a lower risk.

**Inbound** - A TCP/UDP connection that originates from outside the enclave to inside the enclave.

**Information Assurance (IA)** - Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DODD S-3600.1 of 9 Dec 96)

**Legacy Systems** - Systems that are candidates for phase-out, upgrade, or replacement. Generally legacy systems are in this category because they do not comply with data standards or other standards. Legacy system workloads must be converted, transitioned, or phased out.

**Local Area Network (LAN)** - A local network of users, systems, wiring, switching, and ancillary devices which is established under a single administrative control to provide network services. A LAN is typically no larger than a single building. When several LANs are interconnected under a single broad administrative control they form a Campus Area Network (CAN) or a Metropolitan Area Network (MAN). A CAN or MAN is normally the largest increment of a network that does not require WAN connections to communicate between elements.

**Network Address Translation (NAT)** - A process that converts network addresses between two different networks. NAT is typically used to convert public network addresses (such as IP addresses) into private local network addresses that are not recognized on the Internet. NAT provides added security as computers connected through public networks cannot access local computers with private network addresses.

**Non-Classified Internet Protocol Router Network (NIPRNET)** - The data communications component of the DISN used for unclassified but sensitive data.

**Outbound** - A TCP/UDP connection that originates from inside the enclave to outside the enclave.

**Port** - A logical point of connection, most especially in the context of TCP (Transmission Control Protocol), which is part of the TCP/IP protocol suite developed for what we now know as the Internet.

**Port Number** - In Internet protocol networks (i.e., the Internet and DOD NIPRNET and SIPRNET), a port is an integer number assigned to a logical network service to differentiate and direct appropriate requests, contained in incoming traffic, to that specific service running on a host computer.

**Protocol** - Agreed-upon methods of communications used by computers. A specification that describes the rules and procedures those products should follow to perform activities on a network, such as transmitting data. If they use the same protocols, products from different vendors should be able to communicate on the same network.

**Protocol Services** - Any function performed by a protocol; for example send, receive, routing, etc.

## **USFK Reg 25-70**

**Relay** - Any device that does not provide a direct line of communications through the firewall (e.g., secure server).

**Risk Assessment** - The process of identifying program risks within risk areas and critical technical processes, analyzing them for their consequences and probabilities of occurrence, and prioritizing them for handling.

**Service** - A process or application that runs on a server and provides some benefit to a network user.

**System** - 1 The organization of hardware, software, material, facilities, personnel, data, and services needed to perform a designated function with specified results, such as the gathering of specified data, its processing, and delivery to users. 2. A combination of two or more interrelated pieces of equipment (sets) arranged in a functional package to perform an operational function or to satisfy a requirement.

**Threat** - The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security.

**Virtual Private Network (VPN)** - a physically disparate set of networks that share a common security perimeter and policy through secured internet work communication.

**Vulnerability** - A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

**Vulnerability Assessment** - Systematic examination of an AIS or product to determine the adequacy of security measures, identify security deficiencies, probe data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation in a network-centric environment.

**White** - PPS designated as required to ensure interoperability across the NIPRNET. These PPS shall be used whenever there is a current operational requirement between enclaves. Risk mitigation conditions levied against these PPS will include required firewall configuration. Specific security countermeasures shall be invoked as standard policy statements.

**Wide Area Network (WAN)** - A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks. The Internet and DOD NIPRNET are examples of a WAN.