

# Security Requirements

MayMarch 2000

Prepared for:

Department of the Navy  
Space and Naval Warfare Systems Command  
Naval Information Systems Security Office, PMW 161  
San Diego, CA

## **1.1 SECURITY REQUIREMENTS**

This document outlines and defines Security Requirements associated with procurement of the Navy Marine Corps Intranet (NMCI).

### **1.1.1 General**

Security services shall provide for the confidentiality, integrity, availability, authenticity, identification, access control, survivability and non-repudiation of information being transported over the NMCI. These security services shall also be applicable to all information during all phases of the NMCI contract. These security services shall be provided to protect both non-classified and classified information (at rest, in-use and in-transit) in accordance with the requirements defined in this document and the policy delineated in the NMCI Security policy. The requirements to protect both non-classified and classified are distinctly different as defined in this document and the NMCI Security policy.

Mechanisms implemented, as part of NMCI shall provide all NMCI users with the capability to protect, detect, react, and revise and recover from intrusions.

The design of the NMCI shall be robust enough to accommodate varying levels of services as dictated by changes in operational conditions (.i.e.- change in INFOCON levels during cyber attacks). The vendor shall identify potential architecture solutions that would accommodate these changes in service requirements.

The design of the NMCI shall provide adequate protection measures to increase its resistance to attacks that might partially or totally incapacitate it, and to prevent disclosure of sensitive (and classified) information that might make it vulnerable.. Protection of the network encompasses three aspects: operations, signaling (and routing), and physical protection. Mechanisms shall be implemented within the NMCI to adequately protect these three aspects of the ~~network.~~network. The contractor shall employ the appropriate mechanisms to ensure that Distributed Denial of Service Attacks and other risks to availability are properly mitigated.

The NMCI shall incorporate Defense in Depth mechanisms throughout each aspect of the infrastructure in accordance with section 2.1 and Chapter 3 of the DoN CIO Information Technology Standards Guidance (ITSG) and Appendix E of the DON CIO Information Technology Infrastructure Architecture (ITIA).

Specified IA guidelines of DoN Chief Information Officer (CIO) Information Technology Standards Guidance (ITSG) shall also be implemented within NMCI, as will compliance with the USMC CIO IA policy for all USMC NMCI users.

#### **1.1.1.1 Computer Network Defense (CND)**

Security services provided for/within the NMCI shall implement CND initiatives such as Information Operations Conditions (INFOCON) directives, and Information Assurance Vulnerability Alert (IAVA) notices, and shall be integrated within the existing DoD and DoN CND infrastructure.

### **1.1.2 Specific Requirements**

#### **1.1.2.1 Separation of Classification Levels**

The NMCI shall incorporate required boundary protection mechanisms to properly segregate systems operating at different classification levels. As required by national policy (DODD C-5200.5), all U.S. classified information must be protected with National Security Agency (NSA) approved high-grade cryptography. In addition to separating data at different classification levels,

the system must be designed so that the reliability and availability of a classified system cannot be effected by non-classified systems.

### **1.1.2.2 Certification & Accreditation (C&A)**

As specified in DoDD 5200.28 (Orange Book), DoDI 5200.40 (DoD Information Technology Security Certification and Accreditation Process - DITSCAP), and DoD 5200.2-R, all automated systems shall meet fundamental security requirements and must be accredited by the Designated Approving Authority (DAA) prior to processing classified or sensitive non-classified data. The NMCI shall be implemented with proper products, policies, and procedures to ensure required system C&A in accordance with this policy. Also, the specific IA guidelines specified in CNO ALCOM 081949Z SEP 99, DoN CIO ITIA, and DoN ITSG shall be implemented within the NMCI, as will compliance with the USMC CIO IA policy for all USMC NMCI users.

The Government will provide the NMCI vendor with the most current information regarding the C&A status of the existing DON networks that comprise the “as is” configuration of the NMCI. The NMCI vendor shall be responsible for developing a transition plan to support the migration from the “as is” NMCI at contract award to the vendor implemented NMCI. The NMCI vendor shall be responsible for delivering a system that can be certified and accredited in accordance with the DITSCAP. With this support, the NMCI vendor shall support the government in the following phases of C&A as defined in the DITSCAP:

- Definition,
- Verification
- Validation
- Post-Accreditation.

This accreditation is an essential part of the connection approval process (CAP) for NIPRnet and SIPRnet. The vendor shall be responsible for supporting the government in satisfying the requirements specified in DISA MSG DTG 021730ZNOV99 subject: DISN NON-CLASSIFIED BUT SENSITIVE INTERNET PROTOCOL ROUTER NETWORK (NIPRnet) CONNECTION APPROVAL PROCESS. Similarly, the vendor shall be responsible for supporting the government in satisfying the DISA requirements for connection to the SIPRnet, dated 20 August 1998. In providing C&A support, the NMCI vendor shall be responsible for delivering a security concept of operations document, sufficient architecture documentation, a system security authorization agreement (SSAA), risk assessments, risk mitigation plans, and other supporting documents required to support DITSCAP accreditation. The NMCI vendor shall support the DoN in the role as certification agent. The NMCI vendor shall not assume that existing Interim Authority to Operate (IATOs) will be extended for NMCI since the system architecture/functionality for NMCI may be very different than what exists today. Appendix 2 provides an outline of proposed C&A roles for NMCI.

### **1.1.2.3 COMSEC/TEMPEST Requirements.**

#### **1.1.2.3.1 Physical Security and COMSEC**

The equipment being installed or reconfigured under this contract will be used to process classified information. SECNAVINST 5510.30A, “Department of the Navy Personnel Security Program” of 10 Mar 99 and SECNAVINST 5510.36 ~~Department~~Department of the Navy Information Security Program Regulation” of 17 Mar 99, provide regulations and guidance for classifying and safeguarding information. Communications Security (COMSEC) information is handled and controlled in accordance with national and departmental directives. It is the responsibility of the contractor to ensure compliance with all pertinent Navy regulations, including

the National Industrial Security Program Manual (NISPO) and COMSEC supplements 5220.22S.

#### 1.1.2.3.2 TEMPEST

Equipment used to process RED classified information will be installed in a physically secure area. The equipment, installation design, and the interconnection/cabling layout (cable raceways, etc.) shall be installed in accordance with the RED/BLACK installation criteria of NSTISSAM TEMPEST/2-95, "RED/BLACK Installation Guidance" of 12Dec95 and NAVSO P-5239-22, "Protected Distribution Systems (PDS) Guidebook" of Oct 97. COMSEC equipment installations will follow appropriate documents.

#### 1.1.2.3.3 NMCI TEMPEST Sites

The service provider will be required to abide by the TEMPEST requirements listed above. The countries/states involved with this procurement, outside of CONUS, include:

- Hawaii
- Iceland
- Puerto Rico
- Cuba

Note that the guidelines for each country and state will differ from typical CONUS implementations. The contractor must submit a completed TEMPEST requirements questionnaire (TRQ) for each site listed above which will be evaluated by a certified TEMPEST Technical Authority (CTTA) to determine site specific TEMPEST countermeasure requirements.

#### 1.1.2.4 Public Key Infrastructure (PKI)

As specified in DEPSECDEF Memo dtd 09 Apr 1999, DoD PKI Implementation, any PKI employed within DoD Services and Agencies shall be the DoD PKI. Thus, the NMCI shall incorporate DoD PKI in accordance with the following guidelines. Specifically, the high assurance PKI based in FORTEZZA and the medium assurance PKI based on X.509 Version 3 certificates shall be used within NMCI as appropriate. The Government will provide the Contractor with the DoD PKI user profile as GFE to be implemented within NMCI. Also, in accordance with DoD policy, all DoD PKI enabled applications will be required to use NSA authorized cryptography hardware tokens by 31 December 2002. In accordance with this policy, all PKI enabled applications for the NMCI must be compatible with the DoD PKI, and authorized DoD certificate authorities must issue all certificates. The Contractor will be responsible for PKI management functions, including user registration and key management in accordance with Attachment 5. Based on this policy, the NMCI shall be able to support the following mandated timelines:

- a. The contractor shall use only DoD Public Key Infrastructure (PKI)-enabled servers.
- b. The contractor shall, by October 2001, provide digital signature capability for all electronic mail.
- c. The contractor shall ensure the registration of all users by October 2001. This shall include registration, facilitation of the issuance of identity and e-mail certificates (signature and confidentiality) (as required) [LRA functions] and escrow of DoD PKI e-mail confidentiality keys. This shall also include management of user PKI certificates: including certificate revocation, tracking and implementation. The registration functions shall be performed to the extent necessary to augment the DEERS/RAPIDS-LRA capability to provide all required PKI LRA and management functions for users (personnel, servers, objects, devices, etc.).
- d. The contractor shall provide user training for DoD PKI certificate use.
- e. The contractor shall register servers and install DoD PKI server certificates for PKI

enabled applications by October 2001. By October 2001, DoD PKI certificates will be used for client-server identification and authentication for all private DoD and DoD-interest web servers on both classified and unclassified networks.

#### **1.1.2.5 Electronic Key Management System (EKMS)**

Existing EKMS infrastructure shall be used where required within NMCI for handling, distribution, processing, etc., of all COMSEC material.

#### **1.1.2.6 Network Time**

The NMCI will provide a method for providing consistent universal time across the enterprise for devices to be synchronized. This requirement is based on fusion of IDS, audit and security data.

#### **1.1.2.7 Multi-Level Security (MLS)**

Any implementation within NMCI of an MLS device interconnecting networks of different classifications shall be in accordance with government guidelines. For secret and below efforts, the Secret and Below Interoperability (SABI) requirements as defined in ASD/C3I memorandum on SABI dated 20 March 1997 shall be followed. The NMCI shall use Defense Intelligence Communication Accreditation Support Team (DICAST) requirements for interconnection to Joint Worldwide Intelligence Communications System (JWICS).

Any product/architecture deployed by the contractor, as part of NMCI to separate classification levels shall be government approved.

#### **1.1.2.8 External Network Interfaces**

Any external network interface to the NMCI shall be considered to originate from an untrusted source and shall comply with the NMCI Security Policy to gain connectivity. External network connectivity to the NMCI shall be dependent upon the external network's compliance with NMCI security policies. The NMCI Security policy paragraph SP-DC-9 (including sub-cases) defines the boundaries and layers within the NMCI. Any external network shall connect at the appropriate boundary in accordance with the policy defined for that layer of the NMCI.

##### **1.1.2.8.1 DISN Connectivity**

To provide connectivity to other Department of Defense (DoD) and government agency networks, the NMCI shall utilize and interface with the Defense Information System Network (DISN) which is administered by the Defense Information Systems Agency (DISA). Specifically, interfaces between NMCI and DISN shall allow for the transport of voice, video, and data on the Non-classified (but sensitive) Internet Protocol Router ~~Net~~Network (NIPRnet) and the Secret Internet Protocol Router ~~NET~~workNetwork (SIPRnet). The DISN Security Accreditation Working Group (DSAWG) evaluates security standards for the components of the DISN. DISA's Office of DISN Data Services promulgates and integrates these standards. For access to the DISN, the NMCI shall follow DSAWG approved security standards and comply with the DISN (NIPRnet, SIPRnet) Connection Approval Process (CAP).

- **NIPRnet Connection:** The NMCI shall connect, at boundary 1, with the NIPRnet to pass controlled non-classified information (formally known as sensitive but non-classified). In order to establish this connection, the NMCI shall comply with requirements set by the Chief, DISN Data Services. These requirements include .MIL domain registration, individual router registration, and compliance with the NIPRnet CAP as defined in DISA MSG DTG 021730ZNOV99 subject: DISN NON-CLASSIFIED BUT SENSITIVE INTERNET PROTOCOL ROUTER NETWORK (NIPRnet) CONNECTION APPROVAL PROCESS. The Network Information Center (NIC) provides detailed guidance for connecting to the NIPRnet

at www.nic.mil.

- **SIPRnet Connection:** The NMCI shall connect, at boundary 1, with the SIPRnet to pass controlled classified information outside its network. The DISA process for connection to the SIPRnet is described in detail in the SIPRnet Customer Connection Plan dated 20 August 1998. The NMCI shall comply with the SIPRnet Customer Connection Plan security standards and continue to comply with the updated security requirements that the DSAWG imposes on the SIPRnet.

#### 1.1.2.8.2 Marine Corps Enterprise Network (MCEN)

The Marine Corps Enterprise Network (MCEN) is an operational network and has its own security requirements and policies. These policies run in parallel with those of the NMCI, however there are some discrepancies. These differences are significant enough to require different connection interfaces. As the NMCI matures and the MCEN is incorporated, this will become less of a boundary layer concern and thus traffic will flow seamlessly between the two networks without need for enhanced security measures.

- **MCEN Network Operations Center (NOC):** The NMCI shall connect, at boundary 2, with the MCEN NOC to pass controlled information outside its network.
- **MCEN Tactical Data Network (TDN):** The NMCI shall connect, at boundary 2, with the MCEN TDN to pass tactical data outside its network.

#### 1.1.2.8.3 IT-21

IT-21 interfaces include two primary categories: 1) NOC/Mini-NOC, and 2) Secure transport services from piers to NOCs or Mini-NOCs. IT-21 has its own set of security standards and practices, and is based on the Defense in Depth framework, however it still must be considered as an external interface. IT-21 networks incorporate boundary protection mechanisms to properly segregate systems operating at different classification levels. In addition to separating data at different classification levels, the system shall be designed so that the reliability and availability of a classified system cannot be effected by non-classified systems as both types of network traffic exist within the IT-21 framework.

- **IT-21 NOC/Mini-NOC interface:** The NMCI shall connect, at Boundary 2, with the IT-21 NOC/Mini-NOC interfaces, to pass both classified and non-classified information.
- **Secure Transport Services:** The NMCI shall provide secure connectivity between piers and NOCs and Mini-NOCs. Secure connectivity is defined as ensuring the confidentiality, integrity, availability, authenticity, identification, access control, survivability, and non-repudiation of information (both non-classified and classified) in accordance with the NMCI Security policy.
- **Note: IT-21 Embarkables:** Once IT-21 embarkables, consisting of computing and NMCI resources have been embarked upon a ship, they shall use ship's resources and thus come under IT-21 security procedures and specifications to pass information.

#### 1.1.2.8.4 Networks Supporting Legacy Systems

Networks supporting legacy systems shall be considered to originate from an untrusted source and shall comply with the NMCI Security Policy to gain connectivity. Legacy network connectivity

within the NMCI shall be dependent upon that network's compliance with NMCI security policies. The NMCI Security policy paragraph SP-DC-9 (including sub-cases) defines the boundaries and layers within the NMCI. At a minimum, legacy networks shall connect to the NMCI at Boundary 1.

#### **1.1.2.8.5 Legacy Applications Servers**

Legacy application servers shall be considered untrusted and shall comply with the NMCI Security Policy to gain connectivity. Legacy server connectivity within the NMCI shall be dependent upon that server's compliance with NMCI security policies. The NMCI Security policy paragraph SP-DC-9 (including sub-cases) defines the boundaries and layers within the NMCI. At a minimum, legacy servers shall connect to the NMCI at Layer 0 (Demilitarized Zone-DMZ).

#### **1.1.2.8.6 DoN Extranets**

DoN Extranets shall be considered to originate from an untrusted source and shall comply with the NMCI Security Policy to gain connectivity. DoN Extranet connectivity within the NMCI shall be dependent upon that network's compliance with NMCI security policies. The NMCI Security policy paragraph SP-DC-9 (including sub-cases) defines the boundaries and layers within the NMCI. At a minimum, DoN Extranets shall connect to the NMCI at Boundary 1.

#### **1.1.2.8.7 Non-DoN Extranets**

Non-DoN Extranets shall be considered to originate from an untrusted source. Non-DoN Extranet connectivity within the NMCI shall be dependent upon that network's compliance with NMCI security policies. The NMCI Security policy paragraph SP-DC-9 (including sub-cases) defines the boundaries and layers within the NMCI. Non-DoN Extranets shall connect to the NMCI at Boundary 1. Some examples of Non-DoN Extranets are contractor networks, Federal/State/Local government networks.

#### **1.1.2.8.8 Commercial Internet Service Provider (ISP)**

Commercial ISPs shall be considered to originate from an untrusted source. Connectivity from commercial ISPs to the NMCI shall be at Boundary 1. Security measures in accordance with NIPRnet Security Policy shall be implemented within the NMCI to ensure separation between NIPRnet and commercial ISPs.

#### **1.1.2.8.9 Secure Provisional Transport**

The NMCI shall provide secure transport services for co-located Non-NMCI enclaves to Boundary 1. Services other than Secure transport across the NMCI shall not be provided. Some mechanisms that can provide secure transport are Virtual Private Networks (VPNs), Switched Virtual Circuits (SVCs), and Permanent Virtual Circuits (PVCs).

#### **1.1.2.8.10 Joint, Allied and Coalition Networks**

For coalition interoperability, the solution proposed shall be in accordance with the most stringent policies involved for the connected networks. The proposed solutions also must be certified and

accredited in accordance with DoD policy. For solutions that involve connection to the SIPRnet, the DISN Security and Accreditation Working Group (DSAWG) guidelines shall be followed. If the network is foreign operated, and a U.S.-only classified community is required on that network, then NSA-approved Type-1 encryption is mandated in accordance with DoD Directive C-5200.5, which requires that all U.S. classified information be protected with NSA-approved cryptography.

#### **1.1.2.8.11 Top Secret/Sensitive Compartmented Information (SCI)**

DON customers shall have the option of ordering Top Secret or Sensitive Compartmented Information (SCI) connectivity (e.g.-Joint ~~WorldWideWorldwide~~ Intelligence Communications System (JWICS)). The NMCI shall provide transport services in accordance with the applicable connection requirements for that TS/SCI network.

For example, the NMCI shall adhere to DIA security standards for JWICS in accordance with the Defense Intelligence Communication Accreditation Support Team (DICAST) for the JWICS/NMCI connection points. In order for the NMCI to provide JWICS data to its customers, the requirement shall be validated through the Unified Command and the JWICS program manager. The NMCI shall comply with all standards for security that have been established by the DICAST for connectivity to JWICS.

#### **1.1.2.9 Secure Voice Interface**

The NMCI shall provide for interfaces to existing secure voice systems, specifically for interoperability with Type 1 Secure Voice products. Specifically, the NMCI shall support interfaces to STU-II/IIIs and STEs to support Joint and Allied interoperability.

The NMCI shall provide secure wireless connectivity to the NMCI.

The NMCI shall be capable of bridging to existing infrastructure to ensure ship to shore secure voice interoperability.

#### **~~1.1.2.9~~1.1.2.10 Disaster Recovery Plan**

Any of the threats defined in section 4 of the NMCI Security Functions

Concept of Operations, as well as future and unknown threats, have the

potential to cause substantial loss of network availability, applications, data, and specific NMCI services. The contractor must develop and maintain Disaster Recovery Plans that will mitigate these risks. These plans shall be made available to the Government via the appropriate governance organization for annual review. The contractor shall identify the appropriate risks and trade-offs considered as part of their Disaster Recovery Plans. The contractor shall also identify the variations from their baseline system architecture that would be implemented as part of a disaster recovery scenario.

#### **1.1.2.11 Computer Network Defense (CND)**

NMCI shall incorporate all appropriate INFOCON and IAVA directives in accordance with the following policies/directives:

1. CNO R181840Z May 99 Navy Information Operations Condition (INFOCON) Implementation.
2. CJCS Memo CM-510-99, dated 10 Mar 99, DoD INFOCON Guidance.
3. Draft NCTF-CND Concept of Operations (CONOPS) dated 29 Jan 99.
4. MARFOR-CND CONOPS
5. CNO R211417Z Oct 98, Information Assurance Vulnerability Alert (IAVA) process.

6. MARFOR-CND IAVA Process
7. CNO R071310A Jul 99, Change of IAVA Reporting Agent.
8. MARFOR-CND Security Policy & Guidelines

Implementation of NMCI shall be consistent with current DoN Computer Incident Reporting guidelines such as OPNAVINST 2201.2, dated 3 Mar 98, Navy and Marine Corps Computer Network Incident Response.

Network availability and security sensor information from the entire NMCI shall be made available to DoN CND components (FIWC, NCTF-CND MARCIRT and MARFOR-CND).

DoN components (NCTF-CND and MARFOR-CND) of JTF-CND shall work with other elements of JTF-CND to coordinate NMCI network defense across DoD and the U.S. Government as a whole.

### **1.1.2.124 Information Assurance Training**

The contractor shall provide IA training in accordance with OPNAVINST 5239.1B for all users and system administrators. Upon completion of this training, the contractor shall provide the user, system administrator, or local Commanding Officer or Officer-in-Charge proof of completion of training.

### **1.1.3 Critical Government Roles with Respect to IA/CND**

Although the DoN expects the Contractor to pursue an aggressive strategy for design, deployment, and operation of the NMCI, authorized DoN personnel must perform a number of critical security roles. These roles fall into two categories: insuring that the security of the NMCI satisfies DoN, DoD, and Federal requirements and exercising essential command authority over DoN defensive Information Warfare (IW) activities. The NMCI shall provide DoN IA/CND personnel with information required to support Information Operations (IO) operational missions.

In concert with the requirements for Certification and Accreditation (C&A) of all DoD computer networks (classified and non-classified), authorized DoN personnel shall be the approving authority for the following components of the NMCI:

1. Security Architecture
2. Security critical product selections
3. Network connectivity plan
4. Security procedures
5. Other security critical factors as required

In the above role, DoN personnel will seek to use the most expeditious procedures without compromising the integrity of the security evaluation process.

DoN will utilize security assessment teams (Red and Green Teams) to conduct authorized simulated attacks against operational NMCI networks to ensure the NMCI satisfies the security related SLAs and that Navy, Marine Corps, DoN, DoD, and national security requirements are adhered to. As part of this approach, Red/Green Teams will also conduct design, product, and configuration reviews. Focus of Green Teams will be on contract related security requirements, while Red Teams will be less constrained and will focus on identifying vulnerabilities and risk associated with operation of the NMCI. DoN will ensure that Navy, Marine Corps, DoN, DoD, and national policies and procedures are followed in conducting Green/Red Team operations. While

DoN intends to use government contractor support personnel to supplement government personnel in conducting security assessment operations, leadership of these teams shall be government based.

As part of the contractor's efforts in providing support to the Government's Red and Green Teams, there is a requirement for the contractor to have some personnel with Top Secret/Sensitive Compartmented Information (SCI) clearances. The contractor shall have at least five personnel with Top Secret/SCI clearances to be able to support these efforts and to be able to receive proper threat/risk information.

With respect to CND, responses to network threats and attacks constitute Information Warfare (IW) defense command decisions that, as a minimum, shall be authorized by designated, uniformed DoN personnel. Along this line, the DoN command structure shall retain directive authority over all NMCI threat responses. These DoN personnel shall also be the conduits for authorized responses to directives received from JTF-CND or Joint Service regional CINCs, for coordinated Joint Service response to threats. In particular, as the INFOCON (information condition) level is raised during time of conflict, DoN personnel shall retain command decision authority. During these periods, SLA compliance may be relaxed at the discretion of the PCO.

DoN shall be the approving authority for the security architecture since government personnel will be responsible for security critical roles and will have to use the infrastructure for critical operations. The security architecture is the primary mechanism that underlies the criticality of the NMCI. The overall performance of the network will still be the responsibility of the contractor given this ~~constraint.~~DoN constraint. DoN personnel will retain only essential command authority and approval authority of security significant changes. With the constraints outlined above, the contractor is still responsible for the overall performance of the NMCI in accordance with the SLAs.

#### **1.1.4 Contractor Specific Internal Information Guidelines**

##### **1.1.4.1 Classified (DoD) Information Support**

The highest classification level of information required in connection with this procurement is TOP SECRET.

In accordance with the National Industrial Security Program Operating Manual, DoD 5220.M, the contractor shall possess or be able to possess a Facility Security Clearance equal to the highest level of classified information necessary to perform the tasks or services required on this contract.

Contractor personnel, whose duties require access to systems processing classified information, shall possess a security clearance at least equal to the highest degree of classification involved and shall have a validated need-to-know prior to beginning work on the classified system.

The sponsoring agency security requirements for classified systems shall be met by all contractor personnel accessing classified information, or contractor systems processing classified information.

The contractor shall perform internal assessments to determine position sensitivity and management controls necessary to prevent individuals from bypassing controls and processes, such as individual accountability requirements, separation of duties, access controls, and limitations on processing privileges at contractor facilities. These position sensitivity assessments will be forwarded to the Government for a determination of personnel suitability and requirements for individuals assigned to these positions in accordance with DRD3. Periodic re-evaluations of positions and suitability requirements will be necessary during the life of the contract as positions and assignments change.

The contractor shall conduct risk assessments, document the results, develop and maintain internal security plans. These plans shall describe how the contractor ensures the integrity, availability, and confidentiality of the information that it is operationally responsible to protect

within the vendor's facilities.

#### **1.1.4.2 Sensitive Information Support (Non-classified)**

Under current Federal guidelines, all officially held information is considered sensitive to some degree, and shall be appropriately protected by the contractor as specified in applicable IT Security Plans.

Types of sensitive information that will be found on DoN systems that the contractor shall have access to include, but are not limited to: Privacy Act information; proprietary information of other companies or contractors; resources protected by International Traffic in Arms Regulation (ITAR); technology restricted from foreign dissemination for competitive reasons; DoN administrative communications, including those of senior government officials; procurement or budget data; information on pending Equal Employment Opportunity (EEO) cases; labor relations; legal actions; disciplinary actions; complaints; IT security pending cases; civil and criminal investigations; information not releasable under the Freedom of Information Act (FOIA) (e.g. payroll, personnel, and medical data).

The contractor shall perform internal assessments to determine position sensitivity and management controls necessary to prevent individuals from bypassing controls and processes, such as individual accountability requirements, separation of duties, access controls, and limitations on processing privileges at contractor facilities. These position sensitivity assessments will be forwarded to the Government for a determination of personnel suitability and requirements for individuals assigned to these positions.. Periodic re-evaluations of positions and suitability requirements will be necessary during the life of the contract as positions and assignments change.

The contractor shall conduct risk assessments, document the results, develop and maintain internal security plans. These plans shall describe how the contractor will ensure the integrity, availability, and confidentiality of the information that is operationally responsible to protect within the vendor's facilities and at government facilities. For example the contractor shall ensure that foreign nationals within their corporate staff will not have access to NMCI data that is not ~~releasable.~~ releasable. A decision to accept any residual risk will be the responsibility of the DoN system owner and the DoN information owners. The contractors risk assessments and IT Security Plans shall be updated at least every three years or upon significant change to the functionality of the assets, network connectivity, or mission of the system, whichever comes first. If new or unanticipated threats or hazards are discovered by the contractor, or if existing safeguards have ceased to function effectively, the contractor shall update the risk assessments and IT Security Plans (within 30 working days) and shall make appropriate risk reduction recommendations to the DoN system owner and the DoN information owners (within 5 working days).

#### **1.1.4.3 Privacy And Security Safeguards**

The contractor shall not publish or disclose in any manner, without written consent of the government, the details of any security safeguards designed, developed, or implemented by the contractor under this contract or existing at any DoN Center.

The contractor shall develop procedures and implementation plans to ensure that IT resources leaving the control of the assigned user (such as being reassigned, removed for repair, replaced, or upgraded) is cleared of all DoN data and sensitive application software by a technique approved by the government. For IT resources leaving DoN use, applications acquired with a "site license" or "server license" shall be removed. Damaged IT storage media will be degaussed and destroyed.

To the extent required to carry out a program of inspection and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of government data, the contractor shall afford DoN access to contractor facilities, installations, technical capabilities, operations,

documentation, records, databases, and personnel.

## 1.2 DEFENSE IN DEPTH STRATEGY

While perfect security in an information-sharing environment is impossible, there is much that can be done within the limits of the current state-of-the-practice to minimize system vulnerabilities and counter potential threats. To this end, the Department of the Navy (DoN) has defined a defense in depth strategy that uses currently available protection technology installed in a layered system of defenses, much the way a bank vault may be built with sequential doors and many alarm systems. Defense in Depth is designed to protect the confidentiality, integrity, authenticity, identification, access control, non-repudiation, survivability, and availability of the information and IT systems in a network centric warfare environment. Defense in Depth is defined by its architectural components and by the manner, or framework, in which these components are installed and operated. The information in this section describes the IA environment in which NMCI must operate continuously and successfully. Further specific security related requirements are specified in the NMCI Request For Proposal (RFP). NMCI shall implement Defense in Depth mechanisms throughout each aspect of the infrastructure (e.g.-hubs, switches, routers, servers, workstations, etc.) in accordance with this section and Chapter 3 of the DoN CIO ITSG and Appendix E of the DON CIO ITIA.

### 1.2.1 Defense in Depth Components

This section presents the components that will be used to implement Defense in Depth.

Protection Tool	Confidentiality	Integrity	Authenticity	Availability
Firewalls and Packet Filtering	Yes		Yes	Yes
Intrusion Detection	Yes		Yes	Yes
Content Filtering		Yes		Yes
Virtual Private Network (VPN)	Yes	Yes	Yes	
DoD PKI Enabled Applications	Yes	Yes	Yes	
Encryption	Yes	Yes	Yes	

**Table 14 Security Requirements Addressed by Available Protection Tools**

#### 1.2.1.1 Firewalls

A firewall is a collection of hardware and software components that is used to provide protection for a defined set of users in a specified enclave. There are different types of firewalls such as stateful monitoring firewalls, application layer proxy firewalls, and router-based firewalls. To date, the DoN has chosen to implement application layer proxy firewalls at the primary entry points (Boundary 1) to external networks such as the NIPRnet. Within the Navy, these firewalls have been implemented at the Fleet Network Operations Centers (NOCs), Fleet-CINC headquarters, Type Commanders, SYSCOMS, and other shore locations. Additionally, within the Navy and Marine Corps, application layer proxy firewalls have been fielded at the Base Area Network (BAN) level. Under the Defense in Depth approach, firewalls should be implemented at multiple layers (Regional, Metropolitan Area Network (MAN), Base Area Network (BAN), Local Area Network (LAN), etc.) to provide additional layers of protection. Thus, firewalls can be at Boundaries (1, 2, 3, and 4).

#### 1.2.1.2 Intrusion Detection Systems (IDS)

Network based IDSs provide a capability to monitor network traffic for anomalies based on known attack signatures. IDSs, however, cannot check for attack profiles it has not seen before. Thus, other mechanisms must be implemented to monitor unusual network activity when an intrusion occurs. According to DON policy, IDSs are to be centrally monitored. Within the Navy the activities are the Fleet Information Warfare Center (FIWC) and Navy Component Task for

Computer Network Defense (NCTF-CND), and within the Marine Corps IDSs are centrally monitored by the Marine Corps Computer Incident Response Team (MARCIRT). IDSs implemented within NMCI shall be interoperable with existing IDS infrastructure and applications at DON CND activities. NMCI vendors shall be responsible for providing any system upgrades (both hardware and software), training and installations required at DON CND activities (including FIWC, NCTF-CND, Marine Corps Information Technology Network Operations Center-MITNOC, etc.) to support their (NMCI vendors) proposed architecture. This would include providing any upgrades to support data analysis, inspection of application security updates, etc. at DON CND activities. Host based IDS is normally implemented for high value units, e.g. servers. At a minimum, NMCI shall implement host based IDSs for all critical servers. It is envisioned that a combination of the two methods will provide portions of the layered defense protection that the NMCI requires. NMCI shall incorporate both network and host-based IDSs (or devices that provide similar functionality) as part of a layered defense in depth strategy.

#### **1.2.1.3 Content Monitoring**

There are many COTS products available that will perform content monitoring. Content monitoring shall be used within the NMCI to ensure availability, proper usage of government assets and bandwidth and provide another layer of defense.

#### **1.2.1.4 Content Filtering**

The NMCI shall incorporate content filtering products and techniques, because many forms of electronic information can contain harmful content such as viruses, worms, and Trojan horses. This "malicious code" can be transmitted across a network in a number of ways including SMTP email attachments, FTP file downloads, and Java applets. Numerous COTS products exist that can check these routes to identify such potentially harmful content. If properly configured and frequently updated, these tools can identify harmful content before it has the chance to do any damage, and in many cases can repair already damaged files.

#### **1.2.1.5 Virtual Private Network (VPN)**

VPN devices used within NMCI shall be selected according to Appendix 1-Naval VPN Selection Criteria. VPNs shall only be implemented as part of the NMCI with a well-defined, acceptable usage policy and security CONOPS. VPNs can provide a secure remote access capability for users as well as a point-to-point encryption capability that can be utilized for application programs that implement risky protocols. The primary goal is for those programs utilizing risky protocols to migrate away from the protocols. However under certain conditions (policy and security CONOPS) as defined earlier, VPNs shall be implemented to transmit required operational data.

#### **1.2.1.6 DoD PKI Enabled Applications**

PKI enabled applications provide integrity of the data and managed user access to the application through the employment of digital certificates. Additionally, PKI provides confidentiality of the data while in storage or in transit. Applications must be DoD PKI aware, and be able to work in this environment, i.e. be X.509v3 compliant.

#### **1.2.1.7 Web Security**

The NMCI shall implement mechanisms to provide protection of web in accordance with the following DoD policies:

- DEPSECDEF Memo dtd 7 Dec 99, Web Site Administration, Policies & Procedures
- DEPSECDEF Memo dtd 24 Sept 98, Information Vulnerability and the World Wide Web
- OSD Memo dtd 9 Jan 98, Policy for establishing and maintaining a publicly accessible Department of Defense Web Information Service

- CNO Message DTG P 232300Z Oct 98, Navy World Wide Web Policy Execution
- CNO Message DTG R 140100Z Nov 98, Waiver Request to Navy World Wide Web
- IA Training and Certification joint memo dated 29 June 1998, from Under Secretary of Defense (Personnel and Readiness) and Assistant SECDEF for C3I
- SECNAVINST 5720.47 on DoN Policy for Content of Web Sites

### 1.2.1.8 Encryption

Encryption can be used to provide not only information confidentiality but also integrity and mutual authentication of the communicating parties. Appropriate use of encryption technology can provide cryptographic separation of information at different levels of classification, permitting such information to be communicated via a common infrastructure, and even “tunneled” across a non-secure public Internet. NSA evaluates the strength of cryptographic devices for securing classified data. NSA endorsed Type 1 devices are currently available to provide link layer, IP and ATM layer encryption. As stated in paragraph 1.1.2.1, U.S. classified information must be protected with National Security Agency (NSA) approved high-grade cryptography. For non-classified information, a variety of software and hardware products are available that have encryption and digital signature capabilities. For implementation within NMCI, products used to protect Sensitive but Non-classified/Non-classified information shall be FIPS 140-1 certified, unless otherwise approved by government. At a minimum, the vendor shall provide products with the following FIPS 140-1 certification levels:

- Cryptographic modules (hardware and software at least level 2) (excluding VPN clients)  
 Note: Target criteria for hardware-based VPNs is FIPS 140-1 Level 3 certification.  
 Hardware-based VPNs implemented within NMCI after 30 Jun 2002 shall be FIPS 140-1 Level 3 certified.
- Cryptographic modules (VPN clients) at least level 1

The most commonly used standards include the Data Encryption Standard (DES) and a variation called 3DES (triple DES) for providing confidentiality, and Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1) for providing data integrity and authentication. The NMCI shall comply with DoD wide encryption standardization as it is promulgated.

The Government will provide NMCI Type 1 encryption as government furnished equipment (GFE). The offeror shall provide COTS Type 2 cryptographic products (e.g., firewalls, VPNs, IDS, etc.) and other COTS products that utilize Type 3 and 4 algorithms, in accordance with the security ~~requirements~~requirements in the solicitation. The Government will also provide classified keying material (Government Security Policy and Requirements allow dynamic generation of some keys). Government will not retain custodial responsibility for Type 1 encryption products or keying material provided as GFE. The offeror shall be held accountable for encryption products and keying material turned over to contractor’s CMS custodians as GFE. Within the United States Pacific Command’s (USPACOMs) area of responsibility (AOR), the NMCI contractor shall implement bulk encryption for all transmission channels in accordance with USCINCPAC INSTRUCTION 5230.15. Unless otherwise directed by the Government, other non-contiguous NMCI sites (Cuba, Puerto Rico, Iceland) shall also be covered by this instruction for protection of transmission channels.

### 1.2.1.9 NMCI Communities.

A Community of Interest (COI) is a logical grouping of users who have a requirement to access information that should not be made available to the general NMCI user population. This requirement can be based on specific security requirements, geographical location, unique functional requirements, or unique command relationships. To meet this requirement, a logical perimeter is established around the COI, using Defense in Depth IA mechanisms. Some examples of COIs are personnel systems (for handling Privacy Act Data), geographically dispersed major claimants, and commands and shipyards handling nuclear propulsion data.

COIs will be established under the authority of the NMCI Governance and Operations Organization.

The NMCI contractor shall dynamically establish, maintain, and disestablish multiple communities whose membership is dependent upon the presentation of community (enclave) credentials (PKI/keys), as required by and in coordination with the Government. All of the communities above the non-classified level require Type 1 cryptographic separation. However, the DAA may authorize the use of PKI and VPN technology for COI implementation within classified enclaves, as long as PKI and VPNs are not the primary mechanisms used to provide security services. Communities within non-classified enclaves require the use of PKI and VPN technology for cryptographic separation. Coalition isolation requires the appropriate type of releasable cryptographic separation as determined by Government. Connection between DoN and coalition communities requires a Government approved gateway or guard appliance.

Some communities of interest (e.g., the USMC) will require the NMCI architecture to provide a separate enclave that rides the overarching NMCI. These community of interest enclaves will be established to allow security management and operational direction and will be separated from NMCI at large through boundary 2 firewall suites. These boundary 2 firewalls will enable implementation of a security domain, similar to establishing a service-wide community of interest, and will support implementation of unique security requirements. Boundary 2 firewall suites providing this function will mirror the NMCI solution for meeting boundary 1 security requirements.

NMCI shall be capable of supporting COIs for Secret and below networks. Figure 1 depicts general categories of COI mechanisms that shall be supported within NMCI.

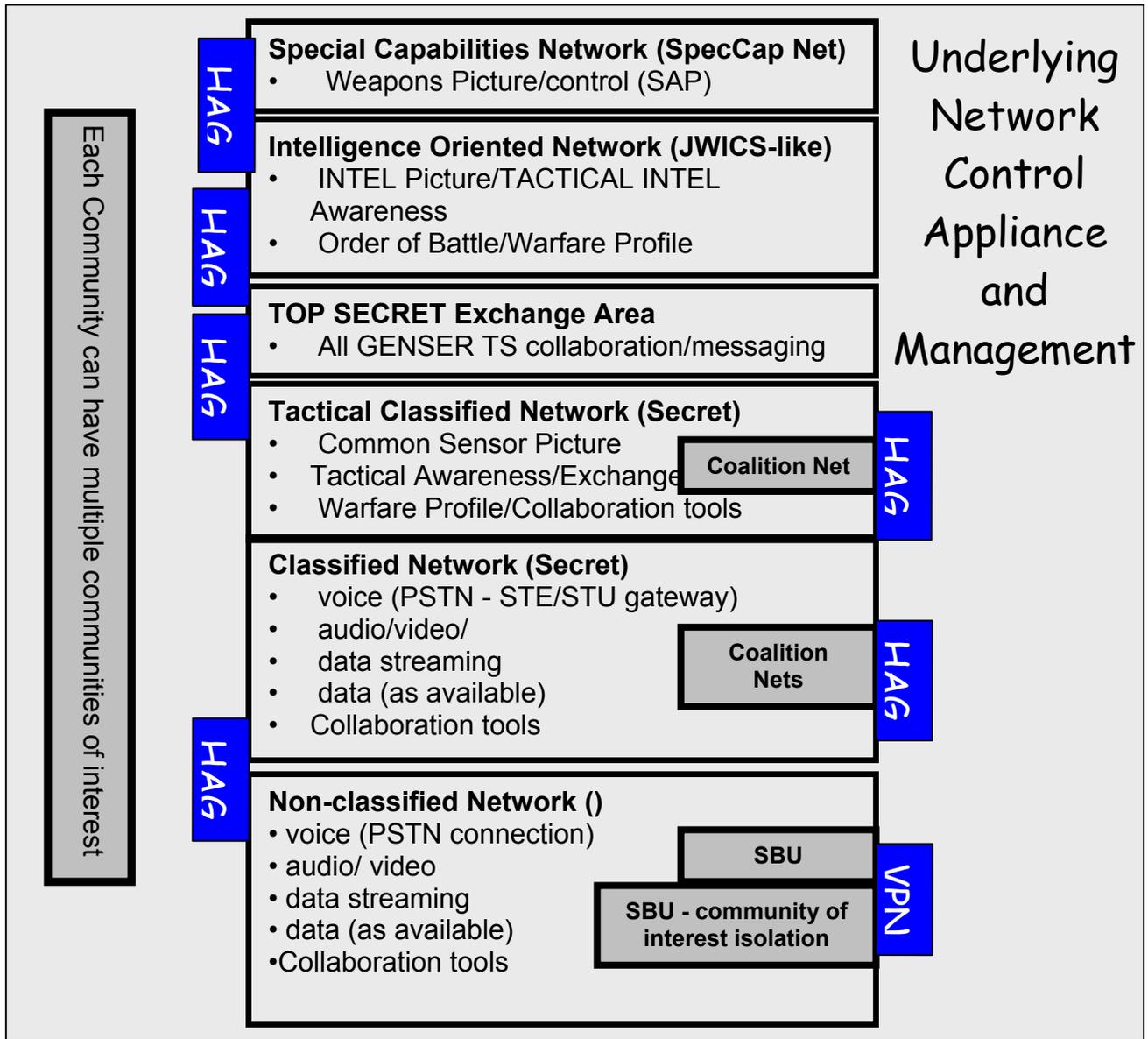


Figure 1: NMCI Communities

**1.2.1.10 Audit Data Ownership And Handling**

Components within the NMCI security infrastructure (Firewalls, Intrusion Detection Systems (IDSs), Virtual Private Networks (VPNs), Audit Agents on workstations/servers, etc.) will generate data that will be used to verify Service Level Agreements, investigate security incidents, and provide documented history of information system use that can be used in Uniformed Court of

Military Justice (UCMJ) and civil courts when necessary. Proper auditing of the NMCI and handling of the resultant data is critical to its use. The NMCI contractor shall propose a statistically relevant amount of security audit data to be collected in order to confirm service level agreement compliance, investigate security incidents, and provide a documented history of information system use. The government has the responsibility of reviewing and approving this security-auditing plan that shall be a part of the Security CONOPS deliverable. The security-auditing plan shall be reviewed and revised throughout the life of the NMCI contract as necessary as determined by the government. The government shall be the owner of all data hosted on the NMCI or generated by any part of the NMCI infrastructure at all levels. In order for the audit data to be valid in legal proceedings, the NMCI contractor shall ensure the integrity of the data is maintained, and shall implement necessary protection mechanisms to safeguard its transfer to the government. Custody through proper chain of custody implementation and compliance with the most current industry and judicial requirements for evidence shall be required for all handling of NMCI audit data.

#### **1.2.1.11 Sensor Grid Data Collection**

The contractor shall implement a Sensor Grid within the NMCI security infrastructure that collects intrusion/incident/audit data from a wide variety of sources including but not limited to Firewalls, IDSs, Content Monitoring products, Content Filtering products, servers, hosts, etc. The contractor shall implement automated tools to collect this data and to send it to the appropriate DoN CND organizations. At a minimum, this intrusion/incident/audit data shall be sent via the appropriate automated tools to the NCTF-CND, FIWC, Marine Forces Computer Network Defense (MARFOR CND), and MITNOC.

#### **1.2.2 Defense in Depth Framework**

This section describes the framework in which the Defense in Depth components will be installed to provide the layered boundary protections required by the network-centric architecture. Based on a risk management philosophy, security tools will be employed to enhance the security of the DoN information infrastructure without adversely impacting required system functionality. This is the goal of the DoN's Defense in Depth strategy.

In Defense in Depth, security protection mechanisms are employed in layers at multiple locations in the system architecture. The intent is to provide a combination of protection mechanisms that is broad enough to address all the security requirements, and deep enough to provide sufficient redundancy across multiple layers. Breadth means combining security mechanisms to provide assurance in all the primary security areas, such as confidentiality, integrity, authentication, and availability. For example, within encryption, depth may mean combining link encryption under network, or Internet Protocol (IP), layer encryption under email (application layer) encryption. Another example would be to use two different anti-viral packages (perhaps one at the firewall/mail server, and another on the end-user workstations) so that if a virus is not detected by one package, it may be caught by the other. This approach ensures that DoN systems maximize resistance to attacks and minimize the probability of a security breach due to a weakness in any single security mechanism.

The Defense in Depth strategy is directly analogous to sea control concepts. Fleet air defense can serve as an example. An outer defense boundary is defended by intercept fighters such as F-14s and controlled by E-2Cs. A second boundary layer of defense is the missile zone defended by Aegis cruisers, which intercept attackers that have not been stopped by the outer layer. Inside the missile zone lie the point defense zones where the defensive weapons are chaff, close in warfare systems, and tactical electronic warfare systems. If the system is working properly, the number of attacks that penetrate to the inner zone is less than the capacity of the point defense weapons.

Four boundaries of defense are defined in this framework. Note that these boundaries may be

logical and are not necessarily physically separate. Note also that the selection, placement, and configuration of particular security mechanisms are implementation dependent, and are driven by the information protection requirements for the particular DoN information system that is being protected. Within each classification level a number of logical security boundaries, need to be established and defended. The NMCI shall support the implementation of security products at each of these boundaries in accordance with the following: Chapter 3 of the DoN CIO ITSG and Appendix E of the DON CIO ITIA . These boundaries are:

- Boundary 1: Logical Boundary between NMCI and External Networks.
- Boundary 2: Logical Boundary between NMCI and Communities of Interest (COIs). These COIs could be at Metropolitan Area Network (MAN)/Base Area Network (BAN)/Local Area Network (LAN) level, or between different organizations or functional groups.
- Boundary 3: Logical Boundary between COIs and Host level.
- Boundary 4: Final Layer of Defense: Application/Host Level.

Corresponding to the discussion of boundaries within the NMCI is a discussion of layers of defense implemented as part of a Defense in Depth strategy. The number of layers of defense protecting any given network node will depend on its physical placement within the NMCI architecture, criticality in support of warfighting capabilities, and restrictions on data or protocols at the node.

Corresponding to the discussion of boundaries within the NMCI is a discussion of layers of defense implemented as part of a Defense in Depth strategy. The number of layers of defense protecting any given network node will depend on its physical placement within the NMCI architecture, criticality in support of warfighting capabilities, required functionality, end-end performance requirements, interoperability, and restrictions on data or protocols at the node. Additional and more detailed information describing the Defense in Depth strategy, protection mechanisms, and current policy and standards can be found in the ITSG document. and the Network Defense Strategy document titled "NMCI Active Computer Network Defense Strategy: Cyber-Centric Maneuver Warfare" Additionally, SPAWAR PMW 161, the Navy's INFOSEC organization, maintains a web page (<http://infosec.navy.mil>) with comprehensive links to INFOSEC information, including information on available security products, links to anti-viral tools, INFOSEC news and articles, security policies and procedures, and the Naval Computer Incident Response Team (NAVCIRT).

Within the various boundaries and layers of defense within the NMCI, applicable security policies will be implemented. The NMCI Governance and Operations Organization shall be responsible for the implementation of these security policies. The above noted boundary 1 firewall policies are a subset of these security policies.

Layer 0: Demilitarized Zone (DMZ). This would affect communication between the NMCI and ~~public networks that is~~ public networks that are not afforded the same degree of protection provided by an integrated network security suite.

Layer 1: External boundary level protection. This would affect communication between the NMCI and external networks such as NIPRnet/INTERNET or SIPRnet/.

Layer 2: Communication internal to the NMCI.

Layer 3: Communication within COIs in the NMCI without the use of a VPN

Layer 4: Communication within COIs in the NMCI with the use of VPN

Layer 5: Application/Host Level.

### 1.2.3 NMCI NIPRnet Boundary 1 through 4 Firewall Policy

**The following paragraphs provide a proposed NMCI NIPRnet Boundary One Firewall Policy. For NIPRnet Boundaries Two, Three, and Four and other proposed protection layers, the Offeror shall propose a firewall policy, which will be subject to government approval as part of the certification and accreditation process.**

#### 1.2.3.1 NMCI NIPRnet Boundary 1 Firewall Policy

NMCI Boundary 1 NIPRnet Policy (Tables 2 through 9) display services that are to be permitted or denied for NMCI-NIPRnet boundary 1 firewalls. If a service is not listed, the service is denied. The tables categorize services as follows:

- Table 2 - Network Infrastructure/Management Services
- Table 3 - Electronic Messaging Services
- Table 4 - Remote Access Services
- Table 5 - Network Information Discovery and Retrieval Services
- Table 6 - File Transfer Services
- Table 7 - Collaborative Services
- Table 8 - Mobile Code Services
- Table 9 - Encrypted Services

For each service, the tables:

- indicate whether the service is allowed from the NMCI enterprise network out to the NIPRnet,
- indicate whether the service is allowed into the NMCI enterprise network from the NIPRnet, and
- provide additional discussion regarding the use of the service between the NMCI and the NIPRnet, if necessary.

SNMP	Allow Queries Out	No.
	Allow Replies In	No.
DNS	Allow Out	Restricted
	Allow In	Restricted
	Discussion	Permitted through firewall via a split DNS configuration that consists of an internal server and an external server. The external server is located on the bastion host of the firewall. The internal server resolves queries from host machines on the internal protected network(s) and forwards queries for external names to the bastion host that forwards the queries to other external DNS servers. The external server on the bastion host resolves queries from the internal server and presents a restricted DNS database to external systems.
NTP	Allow Out	No.
	Allow In	No.
Syslog	Allow Out	No.
	Allow In	No.
Finger	Allow Out	No.
	Allow In	No.
ICMP	Allow In	No.
	Allow Out	No.
NIS	Allow Out	No.
	Allow In	No.
Routing	Allow Out	No.
	Allow In	No.
Netbios	Allow Out	No.
	Allow In	No.

Vines IP	Allow Out	No.
	Allow In.	No.

**Table 2. Network Infrastructure/Management Services**

SMTP	Allow Out	Yes
	Allow In	No
	Discussion	All electronic smtp-based mail is proxied through a secure mail forwarder on the bastion host of the firewall.
X.400	Allow Out	Yes (As DMS sites come online)
	Allow In	Yes (As DMS sites come online)
	Discussion	
X.500	Allow Out	Yes (As DMS sites come online)
	Allow In	Yes (As DMS sites come online)
	Discussion	
POP3	Allow Out	Yes
	Allow In	No
	Discussion	Outgoing POP3 requests are proxied through the firewall to external servers. An authenticated POP3 proxy (APOP) can be used to allow inbound requests.
NNTP	Allow Out	Yes
	Allow In	No
	Discussion	<i>Outgoing NNTP requests are proxied through the firewall to external servers. Inbound requests are not allowed.</i>

**Table 3. Electronic Messaging Services**

'r' commands	Allow Out	No (REXEC, RSHELL, RLOGIN, RUSER, RHOST, RPC)
	Allow In	No (REXEC, RSHELL, RLOGIN, RUSER, RHOST, RPC)
Telnet	Allow Out	Yes.
	Allow In	No.
X	Allow Out	No
	Allow In	No
RPC	Allow Out	No
	Allow In	No
	Discussion	This prevents the use of RPC-based applications such as MS Exchange. RPC has inherent security vulnerabilities.
PPTP	Allow Out	Conditional
	Allow In	Conditional
	Discussion	Conditional means that the firewall will only be configured to allow this protocol if there is a validated operational requirement for use. These will not be set by default. Additional mitigation steps are required.

**Table 4. Remote Access Services**

HTTP	Allow Out	Yes.
	Allow In	No.
	Discussion	Outgoing HTTP requests are proxied through the firewall to external servers. Optionally, a filter may be integrated to prevent the accessing of objectionable sites. Inbound requests are not allowed. Information intended to be publicly available should be placed on a public HTTP server on the outside of the firewall.
SHTTP	Allow Out	Yes
	Allow In	No
	Discussion	SHTTP is permitted via the HTTP proxy.
Gopher	Allow Out	No
	Allow In	No
	Discussion	
WAIS	Allow Out	No
	Allow In	No
Archie	Allow Out	No
	Allow In	No

**Table 5. Network Information Discovery and Retrieval Services**

FTP	Allow Out	Yes
	Allow In.	No
	Discussion	FTP is an inherent risk to the non-classified LAN and is a known vulnerability. Filtering FTP to prevent the accessing of objectionable servers provides added safeguards. Information intended to be publicly available should be placed on a public FTP server on the outside of the firewall. Current technology utilizes Web browser and E-mail. FTP will be allowed in through the firewall only with strong authentication.
TFTP	Allow Out	No
	Allow In	No
NFS	Allow Out	No
	Allow In	No
Printing	Allow Out	No
	Allow In	No
SQL*Net for Database Replication	Allow Out	Conditional
	Allow In	Conditional
	Discussion	Conditional means that the firewall will only be configured to allow this protocol if there is a validated operational requirement for use. These will not be set by default. Approval requires that each user must be approved, with all required IP addresses individually specified. Must be Oracle ver 8.0 or higher. Additional mitigation steps are required.

**Table 6. File Transfer Services**

Talk	Allow Out	No
	Allow In	No
IRC	Allow Out	No
	Allow In	No
Mbone	Allow Out	No
	Allow In	No
Real Audio	Allow Out	No
	Allow In	No
Lotus Notes for Database Replication	Allow Out	Conditional
	Allow In	Conditional
	Discussion	Conditional means that the firewall will only be configured to allow this protocol if there is a validated operational requirement for use. These will not be set by default. Each user must be approved, with all required IP addresses individually specified. Additional mitigation steps are required.
MSNetMtg	Allow Out	No
	Allow In	No.
Commercial ISP	Allow Out	No
	Allow In	No
	Discussion	Direct connectivity to any commercial ISP (AOL, COMPUSERVE, etc) will not be allowed

**Table 7. Collaborative Services**

JAVA	Allow Out	Conditional
	Allow In	Conditional
	Discussion	Conditional means that the firewall will only be configured to allow this protocol if there is a validated operational requirement for use. These will not be set by default. Requires user(s) to have a web browser that supports restricting to trusted sites with Java only allowed at those trusted sites. The only authorized wild card in the trusted sites list is *.mil
JAVA SCRIPT	Allow Out	No
	Allow In	No
ActiveX	Allow Out	No
	Allow In	No

**Table 8. Mobile Code Services**

SSL	Allow Out	Yes
	Allow In	Yes
	Discussion	
Secure Shell	Allow Out	No.
	Allow In	No.
NES traffic	Allow Out	Yes.
	Allow In	Yes.
	Discussion	NES encrypted traffic is allowed through the firewall via packet filtering (e.g., AuthenIP) on an as-needed basis.

**Table 9. Encrypted Services**

|

|

|

|

|

|

|

|

|

|

|

|

|

|



## 1.2.4 NMCI SIPRnet Boundary 1 through 4 Firewall Policy

The following paragraph provides a proposed NMCI SIPRnet Boundary One Firewall Policy. For SIPRnet Boundaries Two, Three and four, and other proposed protection layers, the Offeror shall propose a firewall policy, which will be subject to government approval as part of the certification and accreditation process.

### 1.2.4.1 NMCI SIPRnet Boundary 1 Firewall Policy

NMCI Boundary 1 SIPRnet Policy (Tables 10 through 18) display services that are to be permitted or denied for NMCI-SIPRnet boundary 1 firewalls. If a service is not listed, the service is denied. The tables categorize services as follows:

- Table 10 - Network Infrastructure/Management Services
- Table 11 - Electronic Messaging Services
- Table 12 - Remote Access Services
- Table 13 - Network Information Discovery and Retrieval Services
- Table 14 - File Transfer Services
- Table 15 - Collaborative Services
- Table 16 - Mobile Code Services
- Table 17 - Navy Unique Services
- Table 18 - Encrypted Services

For each service, the tables:

- indicate whether the service is allowed from the NMCI enterprise network out to the SIPRnet,
- indicate whether the service is allowed into the NMCI enterprise network from the SIPRnet, and
- provide additional discussion regarding the use of the service between the NMCI and the SIPRnet, if necessary.

SNMP	Allow Queries Out	No.
	Allow Replies In	No.
DNS	Allow Out	Restricted
	Allow In	Restricted
	Discussion	Permitted through firewall via a split DNS configuration that consists of an internal server and an external server. The external server is located on the bastion host of the firewall. The internal server resolves queries from host machines on the internal protected network(s) and forwards queries for external names to the bastion <del>host which</del> <u>host that</u> forwards the queries to other external DNS servers. The external server on the bastion host resolves queries from the internal server and presents a restricted DNS database to external systems.
NTP	Allow Out	No.
	Allow In	No.
Syslog	Allow Out	No.
	Allow In	No.
Finger	Allow Out	No.
	Allow In	No.
ICMP	Allow In	No.
	Allow Out	No.
NIS	Allow Out	No.
	Allow In	No.
Routing	Allow Out	No.
	Allow In	No.
Netbios	Allow Out	No.
	Allow In	No.

Vines IP	Allow Out	No.
	Allow In.	No.

**Table 10. Network Infrastructure/Management Services**

SMTP	Allow Out	Yes
	Allow In	No (See Discussion)
	Discussion	All electronic smtp-based mail is proxied through a secure mail forwarder on the bastion host of the firewall. The requirements are unique in that a "split email" configuration will be utilized, providing separate inbound and outbound smtp proxies so that email can still reach ships that have moved outside the firewall.
X.400	Allow Out	Yes (As DMS sites come online)
	Allow In	Yes (As DMS sites come online)
X.500	Allow Out	Yes (As DMS sites come online)
	Allow In	Yes (As DMS sites come online)
POP3	Allow Out	Yes
	Allow In	No
	Discussion	Outgoing POP3 requests are proxied through the firewall to external servers. An authenticated POP3 proxy (APOP) can be used to allow inbound requests.
NNTP	Allow Out	Yes.
	Allow In	No.
	Discussion	<i>Outgoing NNTP requests are proxied through the firewall to external servers. Inbound requests are not allowed.</i>

**Table 11. Electronic Messaging Services**

'r' commands	Allow Out	No. (REXEC, RSHELL, RLOGIN, RUSER, RHOST, RPC)
	Allow In	No. (REXEC, RSHELL, RLOGIN, RUSER, RHOST, RPC)
Telnet	Allow Out	Yes.
	Allow In	No
	Discussion	Telnet is allowed out via proxy and allowed in via a proxy with strong authentication, e.g. using secure shell.
X	Allow Out	No.
	Allow In	No.
RPC	Allow out	Yes.
	Allow In	No.
	Discussion	<i>GCCS and CTAPS require RPC on the SIPRnet. RPC is allowed out through the firewall via packet filtering (e.g., AuthenIP)</i>
PPTP	Allow Out	Conditional
	Allow In	Conditional
	Discussion	Conditional means that the firewall will only be configured to allow this protocol if there is a validated operational requirement for use. These will not be set by default. Additional mitigation factors are required.

**TABLE 12. REMOTE ACCESS SERVICES**

HTTP	Allow Out	Yes
	Allow In	No
	Discussion	Outgoing HTTP requests are proxied through the firewall to external servers. Optionally, a filter may be integrated to prevent the accessing of objectionable sites. Inbound requests are not allowed. Information intended to be publicly available should be placed on a public HTTP server on the outside of the firewall.
SHTTP	Allow Out	Yes
	Allow In	No
	Discussion	SHTTP is permitted via the HTTP proxy.
Gopher	Allow Out	No
	Allow In	No
WAIS	Allow Out	No
	Allow In	No
Archie	Allow Out	No
	Allow In	No

**Table 13. Network Information Discovery and Retrieval Services**

FTP	Allow Out	Yes
	Allow In.	No
	Discussion	FTP is allowed out via proxy and allowed in via a proxy with strong authentication. Optionally, a filter may be integrated to prevent the accessing of objectionable servers.
TFTP	Allow Out	No
	Allow In	No
NFS	Allow Out	No
	Allow In	No
Printing	Allow Out	No
	Allow In	No
SQL*Net	Allow Out	Conditional
	Allow In	Conditional
	Discussion	Conditional means that the firewall will only be configured to allow this protocol if there is a validated operational requirement for use. These will not be set by default. Approval requires that each user must be approved, with all required IP addresses individually specified. Must be Oracle ver 8.0 or higher. Additional mitigation factors are required.

**Table 14. File Transfer Services**

Talk	Allow Out	No.
	Allow In	No.
IRC	Allow Out	Yes
	Allow In	Yes
	Discussion	<i>GCCS requires IRC on the SIPRnet. IRC is allowed out through the firewall via the strongest possible security countermeasure, either a generic proxy or packet filtering.</i>
Mbone	Allow Out	No.
	Allow In	No.
Real Audio	Allow Out	Yes.
	Allow In	No.
	Discussion	<i>RealAudio is required for COMPASS on the SIPRnet. RealAudio is allowed out through the firewall via a proxy.</i>
Lotus Notes for Database Replication	Allow Out	Conditional
	Allow In	Conditional
	Discussion	Conditional means that the firewall will only be configured to allow this protocol if there is a validated operational requirement for use. These will not be set by default. Approval requires that each user must be approved, with all required IP addresses individually specified. Additional mitigation factors are required.
MS NetMtg	Allow Out	No.
	Allow In	No.

**Table 15. Collaborative Services**

JAVA	Allow Out	Conditional
	Allow In	Conditional
	Discussion	Conditional means that the firewall will only be configured to allow this protocol if there is a validated operational requirement for use. These will not be set by default. Requires user(s) to have a web browser that supports restricting to trusted sites with Java only allowed at those trusted sites. The only authorized wild card in the trusted sites list is *.mil.
JAVA SCRIPT	Allow Out	No
	Allow In	No
ActiveX	Allow Out	No
	Allow In	No

**Table 16. Mobile Code Services**

GCCS-M	Allow Out	Yes
	Allow In	Yes
	Discussion	GCCS-M requires specific ports and range of ports to be open to support CST Multicasting,
MDX	Allow Out	Yes
	Allow In	No
	Discussion	<i>GCCS requires MDX and MDXNet on the SIPRnet. These services are allowed out through the firewall via a generic proxy (e.g., plug-gw) and packet filtering (e.g., AuthenIP).</i>

**Table 17. Navy Unique Services**

SSL	Allow Out	Yes
	Allow In	Yes
Secure Shell	Allow Out	No
	Allow In	No.
NES traffic	Allow Out	Yes
	Allow In	Yes
	Discussion	NES encrypted traffic is allowed through the firewall via packet filtering (e.g., AuthenIP) on an as-needed basis.

**Table 18. Encrypted Services**

**NIPRnet**

### 1.2.5 TCP and UDP Ports

SERVICE	PORT	PROTOCOL	NOTES
WINS	0	TCP	WINDOWS INTERNET NAMING SERVICE
TCP PORT	1	TCP	TCP PORT MULTIPLEXOR
ECHO	7	UDP,TCP	ECHO SERVER
DISCARD	9	UDP,TCP	/DEV/NULL OF THE INTERNET. HARMLESS
SYSTAT	11	TCP	REPORTS ACTIVE USERS ON SYSTEM
NETSTAT	15	TCP	SEE SYSTAT
CHARGN	19	UDP,TCP	CHARACTER STREAM GENERATOR
FTP	21	TCP	FTP CONTROL CHANEL
SSH	22	TCP	SECURE SHELL
TELNET	23	TCP	ALLOWS FOR REMOTE LOGIN
SMTP	25	TCP	SIMPLE MAIL TRANSFER PROTOCOL
TIME	37	UDP,TCP	TIME OF DAY
WHOIS	43	TCP	RETURNS INFO ABOUT A SITE
DOMAIN	53	UDP,TCP	DOMAIN NAME SERVICE
BOOTP	67	UDP	PROVIDES TOO MUCH INFO ABOUT A SITE
TFTP	69	UDP	OFTEN USED TO BOOT DISKLESS WORKSTATIONS
GOPHER	70	TCP	
FINGER	79	TCP	USED TO GET INFO ON A USER OR USERS LOGGED ON TO A SYSTEM
HTTP	83	TCP	WORLD WIDE WEB
LINK	87	TCP	PRIVATE TERMINAL LINK. USED BY HACKERS
KERBERO	88	UDP	OFFICIAL KERBERROS PORT
SUPDUP	95	TCP	SIMILAR TO TELNET. RARELY USED EXCEPT BY HACKERS
POP2	109	TCP	POST OFFICE PROTOCOL LEVEL 2
POP3	110	TCP	POST OFFICE PROTOCOL LEVEL 3
SUNRPC	111	UDP,TCP	SUN RPC PORTMAPPER
NNTP	119	TCP	NETWORK NEWS TRANSPORT PROTOCOL
NTP	123	UDP	NETWORK TIME PROTOCOL
NETBIOS	137	UDP,TCP	NETBIOS NAME SERVICE
NETBIOS	138	UDP,TCP	NETBIOS DATAGRAM SERVICE
NETBIOS	139	UDP,TCP	NETBIOS SESSION SERVICE
NEWS	144	TCP	SUN NETWORK WINDOW SYSTEM
SNMP	161	UDP	SIMPLE NETWORK MANAGEMENT PROTOCOL AGENT
SNMP-TRAP	162	UDP,TCP	SIMPLE NETWORK MANAGEMENT PROTOCOL SERVER
XDMCP	177	UDP	X DISPLAY MANAGER CONTROL PROTOCOL
GCCS-M	389	TCP	PORT REQUIRED FOR GCCS-M
EXEC	512	TCP	CAN BE USED WITH A REMOTE COPY PROGRAM VARIANT
LOGIN	513	TCP	REMOTE LOGIN.
SHELL	514	TCP	SIMILAR TO REXEC. VULNERABLE TO SPOOFING
PRINTER	515	TCP	BERKELEY LPR REMOTE PRINTER
WHO	513	UDP	
SYSLOG	514	UDP	IF OPEN, YOUR LOGS CAN BE ATTACKED
TALK	517	UDP	TALK SERVICE ALLOWED BETWEEN RANDOM

			TCP PORTS
NTALK	518	UDP	SEE TALK
ROUTE	520	UDP	IF LEFT OPEN, ROUTING TABLES ARE OPEN TO OUTSIDERS
GCCS-M	522	TCP	GCCS-M APPLICATIONS
UUCP	540	TCP	UNIX TO UNIX COPY PROTOCOL
UUCP	541	UDP,TCP	UNIX TO UNIX COPY PROTOCOL RLOGIN
STARS FL	1365	TCP	OUTGOING FTP CONNECTIVITY
GCCS-M	1024	TCP,UDP	
LISTENER	1025	TCP	USUSAL PORT FOR SYSTEM V REL 3. BLOCK INCOMING CALLS TO PORT
OPENWIN	2000	TCP	OPEN WINDOWS
GCCS-M	2001	TCP,UDP	TDBM.UNIX
GCCS-M	2006	TCP,UDP	LDBM
GCCS-M	2007	TCP,UDP	LDBM1
GCCS-M	2008	TCP,UDP	LDBM2
GCCS-M	2009	TCP,UDP	LDBM3
GCCS-M	2010	TCP,UDP	ICM
GCCS-M	2011	TCP,UDP	ICM.UNIX
GCCS-M	2020	TCP,UDP	WAN
GCCS-M	2021	TCP,UDP	WAN.UNIX
GCCS-M	2030	TCP,UDP	PCM
GCCS-M	2031	TCP,UDP	PCM.UNIX
GCCS-M	2040	TCP,UDP	OCM
GCCS-M	2041	TCP,UDP	OCM.UNIX
GCCS-M	2050	TCP,UDP	BCST
GCCS-M	2051	TCP,UDP	BCST.UNIX
GCCS-M	2060	TCP,UDP	MPS
GCCS-M	2061	TCP,UDP	MPS.UNIX
GCCS-M	2065	TCP,UDP	MPR
GCCS-M	2066	TCP,UDP	MPR.UNIX
GCCS-M	2070	TCP,UDP	PRT
GCCS-M	2071	TCP,UDP	PRT.UNIX
GCCS-M	2080	TCP,UDP	ALERTD
GCCS-M	2081	TCP,UDP	ALERTD.UNIX
GCCS-M	2090	TCP,UDP	FINDER
GCCS-M	2091	TCP,UDP	FINDER.UNIX
GCCS-M	2095	TCP,UDP	IMPORTER
GCCS-M	2096	TCP,UDP	IMPORTER.UNIX
GCCS-M	2100-2199	TCP,UDP	COMM CHANNELS
GCCS-M	2200-2299	TCP,UDP	COMM BROADCASTS
GCCS-M	2300	TCP,UDP	MAP SERVER
GCCS-M	2301 – 2307	TCP,UDP	CHART, CHART 0-5
GCCS-M	2311	TCP,UDP	CHART 6
GCCS-M	2917	TCP,UDP	CST PROC MGR
GCCS-M	2918	TCP,UDP	CSTGDBM
GCCS-M	2919	TCP,UDP	CSTCOP
GCCS-M	3031	TCP,UDP	AMP SERVER
GCCS-M	3100	TCP,UDP	WSM0
GCCS-M	3110	TCP,UDP	WSM1

GCCS-M	3120	TCP,UDP	WSM2
GCCS-M	3450	TCP,UDP	ELVIS CHART
GCCS-M	3451	TCP,UDP	ELVIS TRACKMAN
GCCS-M	3452	TCP,UDP	ELVIS GDBM
GCCS-M	3456	TCP,UDP	ELVISII CHART
GCCS-M	3457	TCP,UDP	ELVISII GDBM
GCCS-M	6016	TCP,UDP	L16DBMC
GCCS-M	6017	TCP,UDP	L16DBM1
GCCS-M	6018	TCP,UDP	L16DBM3
GCCS-M	8010	TCP,UDP	CSI
GCCS-M	8011	TCP,UDP	CSI1
GCCS-M	8016	TCP,UDP	RX
GCCS-M	8088	TCP,UDP	EWCSGDBM
GCCS-M	8089	TCP,UDP	EWCSRIU
GCCS-M	8090	TCP,UDP	EWCSRIUST
GCCS-M	8091	TCP,UDP	EWCS CROSSFIX
GCCS-M	8200	TCP,UDP	ALERT1
GCCS-M	8600	TCP,UDP	ALERT2
GCCS-M	9000	TCP,UDP	ELVIS HTTP
GCCS-M	9120	TCP,UDP	CSTMCAST
GCCS-M	9121	TCP,UDP	CST MCAST
GCCS-M	9122	TCP,UDP	CSTMULT3
GCCS-M	9123	TCP,UDP	CSTMULT4
GCCS-M	9124	TCP,UDP	CSTMDPV21
GCCS-M	9125	TCP,UDP	CSTMDPV22
GCCS-M	9126	TCP,UDP	CSTMDPV23
GCCS-M	9127	TCP,UDP	CSTMDPV24
GCCS-M	9128-9199	TCP,UDP	CST
GCCS-M	9200	TCP,UDP	ELVISII HTTP
GCCS-M	9202	TCP,UDP	ELVISII VTMD
GCCS-M	9204	TCP,UDP	ELVISII TSEWSERVER
GCCS-M	9206	TCP,UDP	ELVISII SERVER
GCCS-M	9500	TCP,UDP	GFCP LAN
GCCS-M	9600	TCP,UDP	ALERT4
GCCS-M	2019	TCP	CST POINT TO POINT
GCCS-M	2020	TCP	NETPROC (OPNOTES)
NFS	2049	UDP	NETWORK FILE SYSTEM
LISTEN	2766	TCP	SYSTEM V LISTEN. LIKE TCPMUX.
X11	6000-6XXX	TCP	
IRC	6667	TCP	INTERNET RELAY CHAT

**Table 22 TCP AND UDP PORTS**

## Appendix 1

### Naval VPN Selection Criteria 22 March 2000

#### 1.0 Requirements.

All VPN hardware and software clients used within the NMCI shall meet the following target criteria, unless the government provides interim approval.

1. Cryptographic modules (hardware and software at least level 2 certified (excluding VPN clients) –FIPS 140-1.. Interim approval may be provided if the device is nearing completion of FIPS 140-1 testing. Note: Target criteria for hardware-based VPNs for NMCI is FIPS 140-1 Level 3 certified. All hardware-based VPNs implemented within NMCI after June 30, 2002 shall be FIPS 140-1 Level 3 certified.
2. Cryptographic modules (software clients)-FIPS 140-1, level 1 certified.
3. Key generation-FIPS 140-1 level 2
4. Key distribution-DOD medium assurance PKI for public key distribution using class 4, X.509 version 3 certificates, with hardware tokens for protection of private keys used by system and security administrators or remote users. Interim approval will allow for class 3 certificates and software private key storage until DOD PKI roadmap and token implementation.
5. PKI tokens-DOD PKI roadmap and FIPS 171 key management using ANSI X9.17. Interim approval will allow for class 3 certificates and software private key storage until full DOD PKI roadmap and token implementation. *Shared secret key distribution is not an acceptable authentication means.*
6. Key destruction-within the device, FIPS 140-1, level 2.
7. Data encryption-Either SKIPJACK (FIPS 140-1 level 2) or 3-DES (draft FIPS pub 46-3). User may select the algorithm. System should allow for future migration to the Advanced Encryption Standard (AES) algorithm upon NIST approval.
8. Protocol-Internet Engineering Task Force (IETF) IPsec RFC 2401 and 2406, *Encapsulated Security Protocol (ESP) tunnel mode only*. The Authentication Header (AH) shall not be implemented. Signature functions-RSA per PKCS-1 with cryptographic key size modules of at least 1024 bits/group 2, e=65537 meeting ANSI standards or DSS FIPS 386.
10. Data hashing functions-Secure Hash Algorithm-1 (SHA-1 FIPS 180-1) and cryptographic key size 160 bits or greater.
11. Key exchange functions-Diffie-Helman algorithm and cryptographic key size of either 1024 bits/IPsec group 2, or 1536/IPsec Group 5 meeting IETF RFCs 2401, 2406 and 2409, for IPsec IKE, tunnel mode, main mode, and public key signatures.
12. Fully comply with IETF RFC 2401-RFC 2407.
13. International Computer Security Association (ICSA) IPsec or Virtual Private Network Consortium (VPNC) certified. Interim approval may be given if the device is nearing completion of either certification.
14. VPNs used at boundary 1 should never be configured to operate in a bypass (unencrypted) mode.-

#### 2.0 VPN Lab Testing.

All VPN products shall be tested in accordance with the single sided and dual sided configurations as outlined in Section 3.0 below.

The following items are to be evaluated for the features identified below. The items are listed in sequence of importance. Some items are tested concurrently.

## 2.1 PERFORMANCE

Latency / Overhead using DES/3DES

- A. Tunnel Mode
- B. Optimum Packet Size

## 2.2. PRIORITIES

- A. Closed enclave to closed enclave
- B. Software client to closed enclave
- C. SW client and closed enclave to single sided vpn
- D. Single sided vpn to single sided vpn
- E. Double sided vpn to single sided vpn
- F. Management station closed enclave to closed enclave

## 3.0 Virtual Private Network configurations

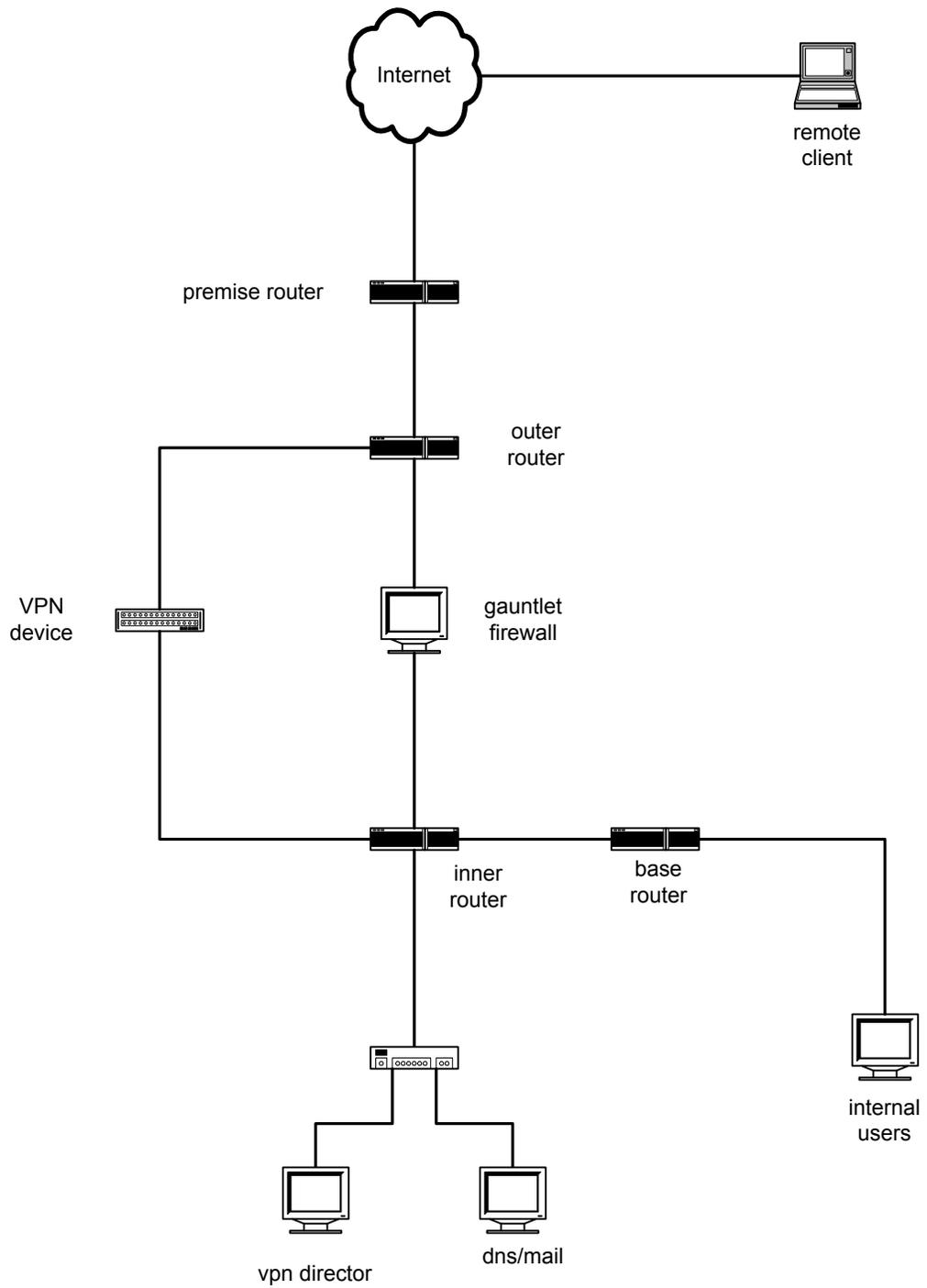
This section provides a brief description of two Virtual Private Network configurations that have been designed by the Space and Naval Warfare Systems Command, PMW 161, for implementation in all Navy Network Operation Centers. The VPN configurations are referred to as Single-sided VPN and Dual-sided VPN architectures.

The VPN configurations provide secure remote access to internal applications such as email and internal web servers. In addition the VPN provides secure LAN to LAN or VPN device to VPN device tunneling via the Internet/NIPRnet. The VPN configurations also maintain the security of the firewall in that applications with known vulnerable protocols can be routed through the VPN tunnels rather than implementing packet screening rules or creating plug proxies on the firewall. This allows a command to implement a strong security policy and provide maximum security to its internal networks.

### 3.1 Single-sided VPN Architecture

The single-sided VPN architecture, shown in Figure 1, uses a VPN device that is placed in parallel with an application proxy firewall. The encrypted or BLACK side of the VPN device is connected to the outer router and the unencrypted or RED side of the VPN device is connected to the inner router. An outer screening router directs the appropriate data to the correct destination. The IP addresses for the external interface of the firewall as well as the encrypted interface of the VPN Gateway are advertised in the routing table of the outer router so no static routes are required to be entered into the outer router to route incoming packets (this is true for both the single-sided and dual-sided architectures).

LAN to LAN or VPN device to VPN device ~~are~~ typical uses of the single sided VPN architecture. Prior to data being passed between one VPN device from another VPN device an encrypted session or tunnel needs to be established. The VPN gates exchange either a shared secret password or digital certificates as a means of authentication. Incoming VPN traffic is then received and decrypted by the VPN device that is parallel to the firewall. Once decrypted, the traffic passes to an internal network router and is then routed via normal network protocols to its destination. Remote access requires the installation of VPN software on a laptop or ~~desktop~~ ~~which desktop that~~ will then allow the end user to access the VPN device. The remote client must first be authenticated with the VPN device by providing a shared secret password or by exchanging digital certificates with the VPN device. Upon authentication the encrypted tunnel will be established and the remote client receives a virtual IP address that makes the client appear to be connected directly to the RED subnet of the VPN device.



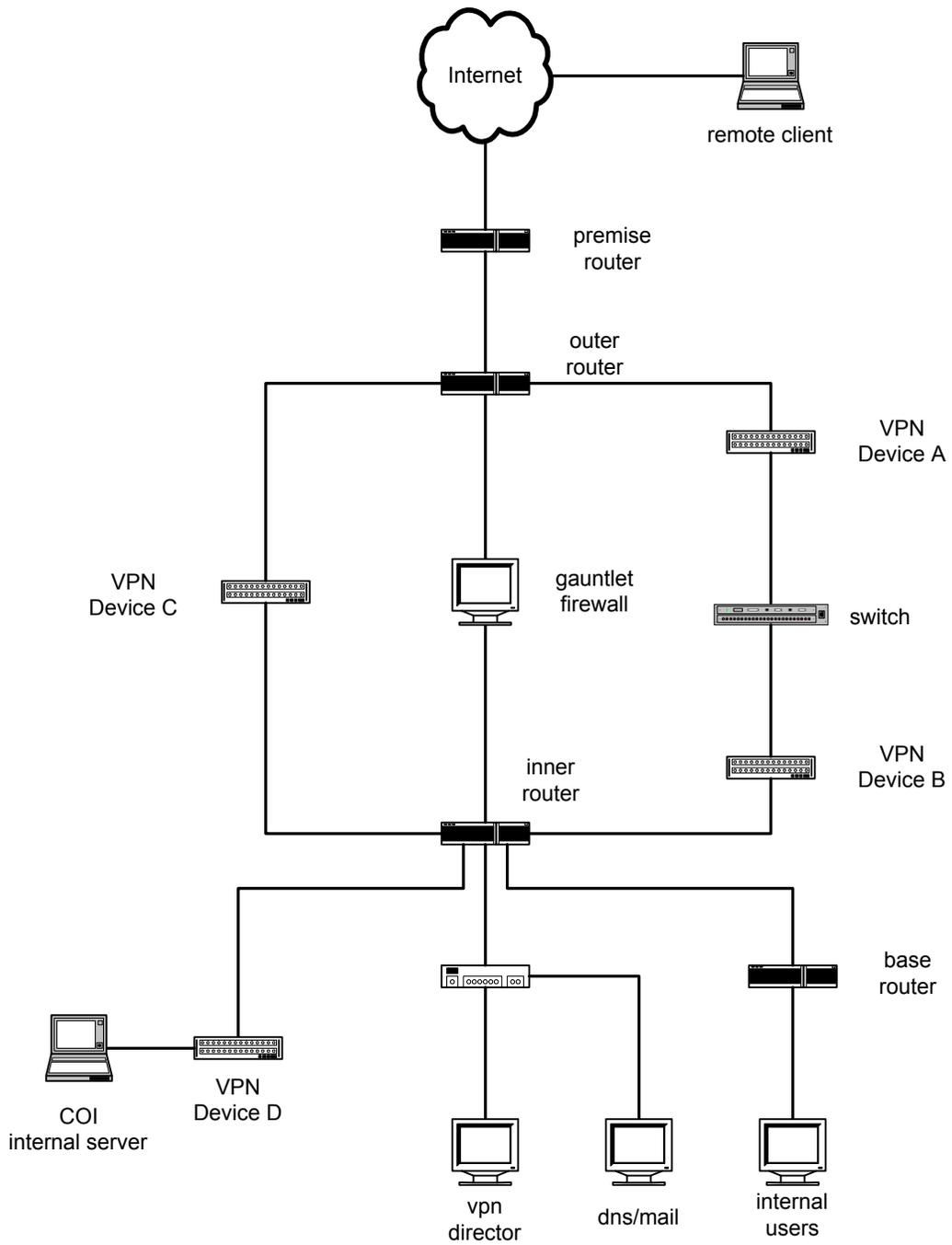
**Figure 1**  
**Single-sided VPN Architecture**

### 3.2 Dual-sided VPN Architecture

The Dual-sided VPN design, shown in Figure 2, differs from the single-sided architecture in that the VPN components form a second or dual path parallel around the firewall. This second path is designed to interface with either a LAN to LAN or remote user that requires access to an internal network but whose traffic does not need to be known by others uses of the trusted network. The Dual-sided design allows for community of interest separation to send and receive sensitive information that is required or desired to be isolated from the rest of the network.

For example, the remote user wishes to transfer medical records to VPN Device D but this type of sensitive information should not be shared over the Internet/NIPRNET or within the trusted network behind the firewall. The remote user would establish a security association with VPN Device A either by a shared secret password or by exchanging digital certificates. Once the encrypted tunnel is established encrypted data is passed. The traffic is decrypted and passed on to VPN Device B which then re-encrypts the traffic and directs the packets to the inner router which then routes the packets to VPN Device D. A switch or hub in series with VPN Device A and B allows for intrusion detection at the network operations center.

For remote clients, the process remains the same as described in the Single-sided design. Regardless of which VPN design the remote user is contacting, the security policy set for the VPN Gateway will determine what networks the remote user can access.



**Figure 2**  
**Dual-Sided VPN Architecture**

1. Purpose: To propose a Designated Approving Authority (DAA) and other accreditation participants for the NMCI so that accreditation planning can begin.
2. Proposal:
- |                              |   |
|------------------------------|---|
| Program Manager (PM)         | CAPT Bry, PMW 152 and PM, MARCORSSYSCOM   |
| Certification Authority (CA) | CAPT Galik, PMW 161   |
| User Representatives (UR)    | A council of the major DoN claimants, chaired by Commander, NMCI Operations and Governance Organization DAA<br>Commander, NMCI Operations and Governance Organization |
3. Background: Accreditation in DoN is governed by DODI 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP). In the DITSCAP, there are four principals--the Program Manager, Certification Authority, User Representative(s) and the Designated Approving Authority. Per its definitions, the Program Manager is the person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the IT system. The Certification Authority is the official responsible for performing the comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meet a set of specified security requirements. The User Representative is the individual or organization that represents the user or user community in the definition of information system requirements. The Designated Approving Authority (DAA or Accreditor) is the official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk. The four principals must agree on the planning, statements of security requirements, security engineering, analyses and tests for accreditation to be successful. This agreement is signified through signatures on the governing document for an accreditation, the System Security Authorization Agreement (SSAA).
4. Discussion: Selection of the first two principals is fairly straightforward. The Program Manager is always someone from the program office. There is a little more latitude for the Certification Authority; however, the CA must have credibility in the security community and be acceptable to the DAA. CAPT Galik, PMW 161, performs this role for most of the systems at SPAWAR and selected systems for other SYSCOMs. As the DoN Program Manager for Information Assurance, he has the appropriate credibility.
- The selection of the User Representative has more latitude yet. A panel consisting of the major claimants in the USN and USMC, chairmanship of which is proposed as Commander, NMCI Operations and Governance Organization. Its also proposed that DoN components of the Joint Task Force for Computer Network Defense (JTF-CND) have

membership on this panel of user representatives. These components are Navy Component Task Force for CND (NCTF-CND), and Marine Forces Task Force for CND (MARFOR-CND).

DAA responsibilities are proposed to reside with Commander, NMCI Operations and Governance Organization.

5. Recommendation: Proceed with accreditation planning using these proposed principals.