

**N/MCI Contract N00024-00-D-6000
Awarded 6 October 2000**



**Attachment 6
Security Functions
Concept of Operations
Version 4.0**

Table of Contents

1	Purpose.....	4
1.1	Fleet Information Warfare Center (FIWC)	4
1.2	NCTF-CND	4
1.3	Commander, Naval Computer and Telecommunications Command (Nctc)	5
	The NCTC shall:.....	5
1.4	Naval Criminal Investigative Service (NCIS).....	5
1.5	Chief of naval operations (CNo) n6.....	5
1.6	PEO-it.....	6
1.7	SPAWAR PMW-161.....	6
1.8	PMW 162.....	7
1.9	SPAWAR System Centers (SSC).....	7
1.10	NMCI CONTRACTOR.....	7
1.11	Commander, Naval Security Group Command (COMNAVSECGRU)	8
1.12	Communications, Information Systems, and Networks (CISN) Training Working Group.....	8
1.13	Chief of Naval Education and Training (CNET).....	8
1.14	Director, Office of Naval Intelligence (ONI).....	8
1.15	Director, COMSEC Material System (DCMS)	8
2	The Threat	10
2.1.1	Network	10
2.1.2	Computer Systems	11
2.1.3	Applications	13
2.1.4	Inadvertent Disasters.....	13
2.1.5	Natural Disasters.....	13
2.1.6	Acts of War	14
3	security OPERATIONS	15
3.1	network operations CENTER(s) (NOc).....	15
3.2	Security Assessment teams	15
3.2.1	Green Teams	15
3.2.2	Red Teams.....	15
3.3	Government Program office security team	15
3.4	IAVA.....	15
3.5	INFOCON	15
3.6	C&A.....	15
3.6.1	Program Manager	15
3.6.2	The Certification Authority (CA)	16
3.6.3	The Certification Agent.....	16
3.6.4	The User Representative (UR).....	16
3.6.5	The Designated Approving Authority (DAA or Accreditor).....	16
3.7	Incident Response	16
3.7.1	Data Collection.....	16
3.7.2	Response	16
3.8	Policy.....	16
3.8.1	Static Policy	16
3.8.2	Dynamic Policy	16
3.9	Configuration Control.....	16
3.10	Lab Testing	16
3.11	Service Provisioning.....	17

BackGround

Although the Department of Navy (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, Department of Defense (DoD), and Federal requirements and exercising essential command authority over DoN defensive Information Warfare (IW) activities.

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

- Security Architecture
- Security critical product selections
- Network connectivity plan
- Security procedures
- 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.

Also, DoD/DoN red teaming will be utilized in the form of design, product, and configuration reviews. Authorized simulated attacks against operational NMCI networks will take place in order to ensure that the NMCI satisfies the Service Level Agreements (SLAs) and both DoN and DoD Security requirements. DoN will seek assistance from Defense Information Systems Agency (DISA) and National Security Agency (NSA) for these red teaming efforts as needed.

With respect to Computer Network Defense (CND), responses to network threats and attacks constitute IW defense command decisions that as a minimum shall be authorized by designated, uniformed DoN personnel. Along this line, the DoN uniformed command structure shall retain directive authority over all NMCI threat responses. These DoN military personnel shall also be the conduits for authorized responses to directives received from Commander, Joint Task Force for Computer Network Defense (JTF-CND) or Joint Service regional CINCs, for coordinated Joint Service response to threats. In particular, as the level is raised during time of conflict, DoN uniformed personnel will retain command decision authority.

Leadership of the Red Teams shall be government based, and can be augmented by contractor support. The Red teams shall be a critical factor in determining compliance with some of the SLAs.

DoN should be the approving authority for the security architecture since government personnel will still 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.

In summary, DoN personnel shall retain only essential command authority and approval authority of security significant changes. Also, with the constraints outlined above, the contractor is still responsible for the overall performance of the NMCI in accordance with the SLAs.

1 PURPOSE

This document provides an outline to amplify and define the security roles and responsibilities that the government and contractor will have in this partnership. Specifically, the operations outlined in section five of this document are areas that the government will retain directive control Roles and RESPONSIBILITIES

1.1 FLEET INFORMATION WARFARE CENTER (FIWC)

The FIWC shall:

- A. Manage the Naval Computer Incident Response Team (NAVCIRT) for Navy; The NAVCIRT, located at FIWC, serves as the Navy primary computer incident response capability to provide assistance in identifying, assessing, containing, and countering incidents that threaten Navy information systems and networks. On request NAVCIRT will offer hands-on assistance to selected naval activities, such as deployed ships, that are under cyber-attack. FIWC will collaborate and coordinate Navy efforts with other Government and commercial activities to identify, assess, contain, and counter the impact of computer incidents on national security communications and information systems, and to minimize or eliminate identified vulnerabilities.
- B. Provide Chief of Naval Operations (CNO) (N64) with monthly, quarterly, and annual summaries of reported Navy computer incidents.
- C. Provide timely advisories of newly identified vulnerabilities.
- D. Conduct on-line surveys for fielded systems.
- E. Provide vulnerability assessments and Red and Blue Team operations to requesting commands. Coordinate resources provided by Commander, Naval Security Group (COMNAVSECGRU) and Commander, Space and Naval Warfare Command (COMSPAWARSYSCOM) PMW-161 as required.
- F. Provide intrusion detection monitoring, on-line surveys, and activity analysis and assessment in support of the Navy Component Task Force (NCTF)-CND.

1.2 NCTF-CND

The NCTF-CND shall:

- A. Coordinate the defense of Navy computer networks and systems as directed by the JTF-CND.
- B. Defend computer networks and systems within the Navy's elements of the Defense Information Infrastructure, as directed by the JTF-CND.
- C. When tasked, be responsible for the monitoring, restoral, and security of Navy networks.
- D. Monitor the Navy's Information Assurance Vulnerability Alert (IAVA) compliance and act as the Navy's Reporting Agent for IAVA.
- E. Coordinate/direct appropriate actions to ensure Navy web pages resident on the World Wide Web (WWW) are in compliance with prescribed Department of Defense and Navy guidance.
- F. Make Information Operations Condition (INFOCON) recommendations to the Navy Command Center in response to a Computer Network Attack and report the Navy INFOCON status.

1.3 COMMANDER, NAVAL COMPUTER AND TELECOMMUNICATIONS COMMAND (NCTC)

The NCTC shall:

- A. Coordinate Defense Information Infrastructure (DII) connection approval with the DISA for Navy information systems and sites. Ensure sites with DII connections meet DISA accreditation requirements.
- B. As required, provide Internet web-hosting and demilitarized zone (DMZ) services for Afloat units and small shore commands. A DMZ is a dedicated network segment that is used to separate public services from internal services.
- C. Ensure shore-based infrastructure solutions incorporate appropriate Information Assurance (IA) safeguards.
- D. Provide network operations, including monitoring and restoral functions in support of the NCTF-CND.

1.4 NAVAL CRIMINAL INVESTIGATIVE SERVICE (NCIS)

The Naval Criminal Investigative Service (NCIS) shall provide law enforcement and counter-intelligence support to the NCTF-CND and FIWC.

1.5 CHIEF OF NAVAL OPERATIONS (CNO) N6

The CNO (N643) shall:

- A. Oversee the Navy IA Program. Provide streamlined, simplified and standardized security guidance and policy.
- B. Approve and issue the Navy IA Master Plan.
- C. Represent IA Requirements submitted by Fleet Commanders-in-Chief and other Echelon II Commanders to the CNO N64 Attack, Protect, Exploit Requirements Action Forum (CAPER AF).
- D. In coordination with COMSPAWARSYSCOM (PMW-161), develop and issue standards for critical IA components (e.g. firewalls, virtual private networks (VPNs), intrusion detection systems (IDSs)), for use within Navy information systems and networks. Critical IA components are those which, to ensure interoperability with other Navy, joint or other DoD systems, must be standardized and managed at a service level. Standards will be documented in the DoN CIO Information Technology Standards Guidance, Chapter 3.
- E. Represent CNO as the Designated Approving Authority (DAA) for Navy-wide and joint service information systems (where Navy is the assigned lead). Assign DAAs and ensure the accreditation of all Navy information technology resources. CNO (N643) further delegates DAA authority to second echelon commanders for acquisition and development of information systems within their cognizance. Further delegation of this DAA authority is limited to officers of the grade of O-6 or above and civilians of grade GS-15 or equivalent except by prior coordination with and authorization from CNO (N643).

- F. Provide Navy representation to the DoD Information Assurance Panel, subordinate working groups and other DoD-level working groups and study groups relating to IA.
- G. Coordinate Navy submission of reports on IA postures, to include training initiatives and overall progress in meeting IA goals and objectives.
- H. Oversee Navy IA training requirements and provide requirements to the Communications, Information Systems, and Networks (CISN) Training Working Group.

1.6 PEO-IT

The PEO-IT will integrate information assurance requirements into the contract requirements of NMCI and ensure that all systems are delivered to naval customers with certification documentation to support accreditation requirements.

1.7 SPAWAR PMW-161

SPAWAR PMW-161 is the DoN IA Program Manager. As such PMW-161 shall:

- A. Ensure full coordination of Navy IA program execution with CNO (N643), COMNAVSECGRU, COMSPAWARSYSCOM (PMW-162) and Headquarters, United States Marine Corps (USMC).
- B. Draft and maintain the Navy IA Master Plan as requested by CNO (N643), and in coordination with CNO N64 Attack/Protect/Exploit Requirements (CAPER) Action Forum, Headquarters Marine Corps, COMNAVSECGRU, and other Naval Systems Commands. The IA Master Plan shall include identification and formal documentation of IA goals and objectives for Navy, a strategy for achieving those goals and objectives, a description of IA programs, projects and initiatives that will result in the capabilities needed, and an IA risk management plan. The Navy IA Master Plan and updates as required will be submitted to CNO (N643) for approval and issuance.
- C. Submit Program Objectives Memorandum (POM) requirements to support IA programs as delineated in the Navy IA Master Plan.
- D. Execute Navy IA programs as defined in the Navy IA Master Plan.
- E. As the technical lead for Navy IA, provide systems and security engineering and integration testing and support for Navy information systems and networks with IA requirements. Provide input, review, and recommended updates to IA Publications. Establish and execute capability to provide on-site assessments to Navy commands, including vulnerability assessments coordinated by FIWC.
- F. Maintain a Navy IA research and development program to meet Navy requirements in accordance with the Non-Acquisition Program Decision Document (NAPDD) and as delineated in the Navy IA Master Plan.
- G. Coordinate IA R&D activities with the Office of Naval Research to ensure maximum and smooth transition of new technologies to operating forces, fully integrated for maximum cost effectiveness with existing technologies.
- H. As the Navy's Certification Authority, Provide high-level oversight and standardization for the system certification and accreditation process for all Service, Joint, development and acquisition programs across Navy.

- I. Advise program managers and DAAs in their responsibility to assign a capable Certification Agent responsible for completing the certification and accreditation process in accordance with the Defense Information Technology Security Certification and Accreditation Process (DITSCAP), reference (f).
- J. Establish and maintain a master file of Navy accredited systems and major Network Operations Centers (NOCs). Ensure supporting certification and accreditation documents are analyzed for lessons learned, identification of system deficiencies and for incorporation in process improvements and the Navy IA Master Plan.
- K. Develop and centrally acquire Navy standard and specified IA products. Provide life cycle management support for centrally procured IA products and systems, to include operations and maintenance funding.
- L. Maintain the Navy Information Security (INFOSEC) Web Site and IA Help Desk as directed by CNO (N643).
- M. Support Navy Computer Network Defense by providing network analysis and management tools to support the NCTF-CND mission.

1.8 PMW 162

PMW-162 of SPAWARSSYSCOM shall conduct IA Vulnerability Assessments in support of the DITSCAP Certification and Accreditation process for developing systems.

1.9 SPAWAR SYSTEM CENTERS (SSC)

The SPAWAR Systems Centers provide engineering, acquisition, security certification & accreditation, and life cycle support to PMW 161 in the execution of its IA responsibilities

1.10 NMCI CONTRACTOR

The NMCI contractor shall assist these DoN organizations in the execution of IA responsibilities as defined in the NMCI Request for Proposal (RFP) and subsequent contract.

1.11 COMMANDER, NAVAL SECURITY GROUP COMMAND (COMNAVSECGRU)

COMNAVSECGRU will provide support, as coordinated by FIWC, in the conduct of vulnerability assessments and Red and Blue Team operations.

1.12 COMMUNICATIONS, INFORMATION SYSTEMS, AND NETWORKS (CISN) TRAINING WORKING GROUP

The CISN Training Working Group shall:

- A. Identify Navy IA billet and training requirements.
- B. Ensure development of Navy training plans for information systems.
- C. Establish IA training requirements for military and civilian personnel.

1.13 CHIEF OF NAVAL EDUCATION AND TRAINING (CNET)

The CNET shall:

- A. Develop Navy schoolhouse IA training and education.
- B. Ensure IA training is incorporated into all pertinent Navy training and appropriate formal schools.

1.14 DIRECTOR, OFFICE OF NAVAL INTELLIGENCE (ONI)

The ONI shall:

- A. Assist CNO (N643) and COMSPAWARSYSCOM (PMW-161) by gathering relevant threat information to assist in defining system security requirements.
- B. Provide all-source, fused intelligence support to the NCTF-CND.

1.15 DIRECTOR, COMSEC MATERIAL SYSTEM (DCMS)

The DCMS shall:

- A. Maintain Central Office of Record (COR), ensuring the proper storage, distribution, inventory, accounting, and overall safeguarding of COMSEC materials for the Navy, Marine Corps, and Coast Guard, Military Sealift Command (MSC), and joint and allied commands, as required.
- B. Maintain the IA Publication Library as directed by CNO (N643).
- C. Control, warehouse, and distribute cryptographic equipment, ancillaries and associated keying material for all Navy.
- D. Under CNO (N643) direction, issue, publish and distribute guidance necessary to ensure National level (e.g., NSA) policies are followed and enforced.
- E. Act as the Navy High Assurance (Class 4) PKI Certificate Approving Authority. Communications Security (COMSEC) Material Issuing Office (CMIO) Norfolk provides a Navy Centralized CAW Facility (NCCF) to support DMS for other than Organizational Messaging and non-DMS FORTEZZA® requirements.

F. Act as Navy Registration Authority for Medium Assurance (Class 3) PKI.

2 THE THREAT

NMCI will face many threats during its operation. These threats may occur during peacetime or wartime. Primary peacetime threats will arise from both natural and man-made sources. Earthquakes, tornadoes, flooding, and other natural disasters may cause outages of network services. Unintended internal actions by users can also effectively damage network connectivity, or cause delays in service. Other peacetime threats include information operations, including deliberate actions by adversaries or unauthorized users to destroy, corrupt, or divulge information. Hostile intelligence collection and sabotage efforts are also likely. During wartime, these threats may be more focused on damaging or destroying the infrastructure, or embarrassing and discrediting the U.S.

2.1.1 Network

2.1.1.1 Active Network Threats – Requires attacker participation in the transaction.

Loss of Integrity – Communication pathways are lost due to technical problems such as loss-of-signal and line noise. Loss of Integrity would have little impact for commodity users, but would have high impact on mission critical and mission support systems.

Retransmission of Data (“Replay”) – Unauthorized retransmission of data on the network (multiplicity). For most applications, retransmission of data would have little effect on operations. However, for financial and mission essential systems, replay of data may cause serious problems. Within a network this could result in a denial of service for the users, which would have a significant impact.

Modification of Data (“Modify in Transit”) – Unauthorized addition, deletion, or modification of information as it crosses the network. Modification of data would have a much greater impact on all operations than simply retransmission of data.

Masquerading (“Spoofing”) – Unauthorized sending/receiving of messages using valid, but unauthorized, identity. Masquerading would have some considerable effects on all operations. Spoofing also include use of compromised authentication keys.

Man-in-the-middle – Unauthorized interception and retransmission of data on a network. This attack is usually the precursor to Modification of Data and Masquerading, and can also include insertion of bogus data.

Denial of Service Attacks – Attempting to limit or destroy capabilities of a network by denying services on network devices to authorized users. A network denial of service attack would have a considerable effect on all operations.

Network Virus (“Worms”) – Distribution of computer code designed to self-replicate across the network. Worms can have a payload, but usually do not. Worm attacks could have a considerable effect on all operations.

Protocol Subversion (“Hijacking”)– Modifying protocols to exploit protocol handling capabilities of devices on the network. Protocol subversion will have major impact on most operations; however, protocol subversion is usually a precursor to a denial of service attack, which may have significant impact.

Covert Channels – Unauthorized transmission of data through hidden means. This would establish a pathway for the extraction of data or other forms of attack.

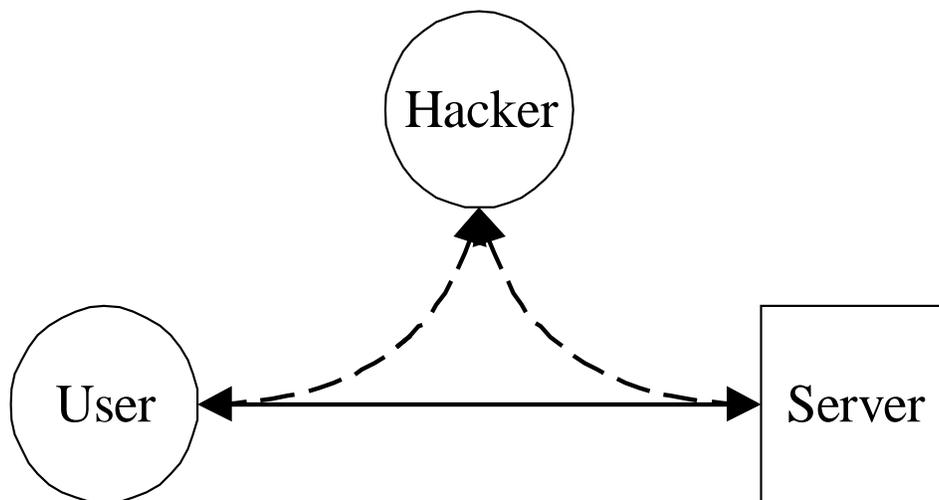


Figure 1 Man-in-the-Middle Attacks

2.1.1.2 Passive Network Threats – Does not require attacker active participation.

Eavesdropping and Wiretapping – Unauthorized listening to private communications, usually through special hardware or software, such as a sniffer. Eavesdropping and Wiretapping would have little impact for ongoing operations, but have a large impact for on current and future operations.

Open Source Accumulation – Legal accumulation of unclassified data via Radio Frequency or public domain sites from multiple sources that, in aggregate, allow listeners to assemble information of a much higher level of classification.

Scanning and Mapping – Unauthorized data collection of network topology, which could then be used to attack computers on the network. This type of threat would have little impact on most operations, but is usually a precursor to the other network attacks.

2.1.2 Computer Systems

2.1.2.1 Active Computer Threats

Physical Sabotage or Vandalism – Destruction or sabotage of computer hardware. While this would have little effect on operations beyond the computer involved, it could have a high impact on critical systems.

Denial of Service – Attempts to limit or destroy capabilities of a network by denying services to users. While this would have little effect on operations beyond the computer involved, it would have a high impact on critical systems.

Computer Viruses & Trojan Horses – Viruses consist of malicious code designed to replicate itself and infect other computers. It may, or may not, carry a payload. Trojan Horses are code designed to exploit the user, which then subverts security when run. Both would have a considerable effect on all operations.

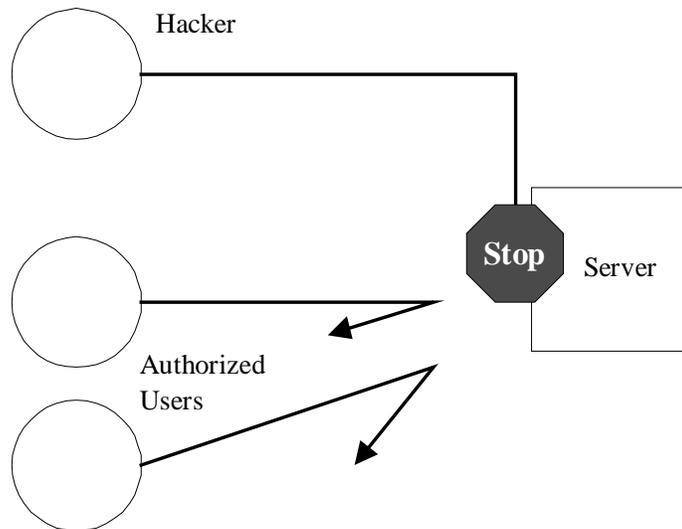


Figure 2 Denial of service Attacks

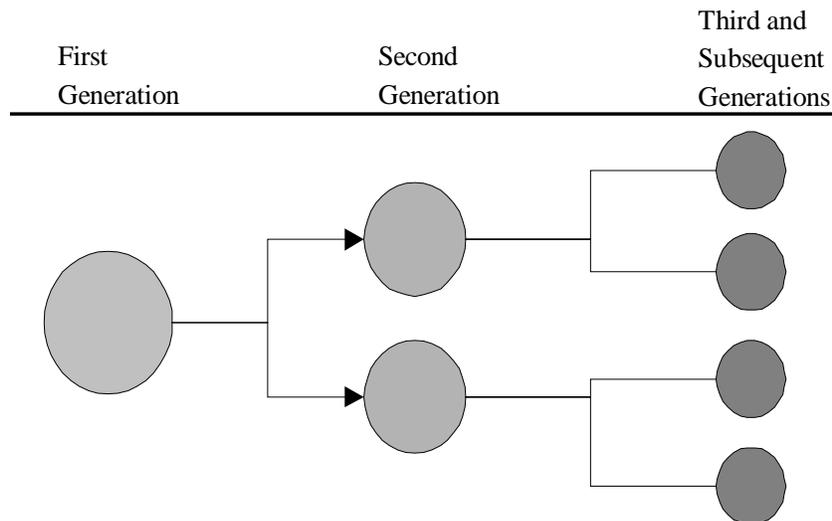


Figure 3 Virus Infections

Port Scanning – Mapping port usage of a computer. This type of threat would have little impact on most operations, but is usually a precursor to Denial of Service Attacks, Computer Exploitation, and Password Cracking.

Computer Exploitation – Exploiting security flaws in the System Architecture, Network Protocols, Operating Systems, Commercial Off-The-Shelf (COTS) products, or Security Policies, to gain unauthorized access to the computer or infrastructure. While this would have little effect on operations, beyond the computer involved, it would have a high impact on critical systems.

Password Cracking – Exploiting the human tendency to choose passwords poorly. While this would have little effect on operations, beyond the computer involved, it could have a high impact on critical

systems.

Audit Log Exploits – Audit Logs are records of computer and network activity. Following a compromise, destruction, deletion, or modification of audit logs hides or masks the severity of an incident.

Trusted System – any of the exploits described above could be launched from a trusted site or system. This would have a high impact on critical systems. An IW attack could be launched against a U.S. site from another U.S. site that has already been compromised.

2.1.2.2 Passive Computer Threats

Power Loss – Temporary or permanent loss of power. While this would have little effect on operations, beyond the computer involved, it would have a high impact on critical systems.

Voltage Spikes – Refrigerators, microwaves, and even coffee makers, can create huge currents which can damage network hardware and computer systems. This would have little effect on operations beyond the computers involved, but would have considerable impact on critical systems.

Overheating – Operating temperatures higher than 110° F. This would have little effect on operations beyond the computers involved, but would have considerable impact on critical systems.

2.1.3 Applications

Application Sabotage ("Trap Doors" and "Back Doors") – Modifying the code to either discontinue working after an event (such as the termination of the developer), or to allow unsecured access to the program or computer by unauthorized individuals. While this would have an impact on critical systems, it would not have a large impact on commodity users. For government developing facilities, this would be a concern for development teams.

Application Exploits – Using security flaws in an application to gain unauthorized access to the computer or data. While this would have an impact on critical systems, it would not have a large impact on commodity users. For government development facilities, this would be a concern for development teams.

Cryptanalytic Recovery – Recovery of keys and/or digital certificates via cryptanalytic means.

2.1.4 Inadvertent Disasters

User Incompetence – Damage or loss of service caused by users not fully aware of design or operation features of the system or network. This would have little effect on operations if all users were adequately trained.

Accidental Subversion – Damage or loss of service caused by developers not fully aware of design protocols they are using, by creating security flaws in their software. This would have little effect on operations.

Incorrect Disposal of Sensitive Media – Disposal of classified or sensitive data through non-approved methods that provide potential attackers with technical or operational information on the network. Proper training to all NMCI users and NMCI contractor personnel will mitigate the impact on operations.

Social Engineering – Providing a potential attacker with information they need to attack a computer system, which may include user ids and passwords, version numbers of software, and other important information. This would not have much of an effect with proper training of all NMCI users and NMCI contractor's personnel.

2.1.5 Natural Disasters

Earthquakes - Damage or loss of service caused by earthquake.

Tornadoes and Hurricanes - Damage or loss of service caused by tornadoes and hurricanes.

Flooding - Damage or loss of service caused by flooding.

Lightning - Damage or loss of service caused by lightning.

Fire - Damage or loss of service caused by a fire.

Electrical outage - Damage or loss of service caused by electrical outage.

Meteorite or Asteroid impact - Damage or loss of service caused by impact.

2.1.6 Acts of War

Nuclear Detonation - Damage or loss of service caused by nuclear detonation.

Ordinance Explosion - Damage or loss of service caused by an explosion.

Sabotage - Damage or loss of service caused by Sabotage.

Physical Overrun - Damage or loss of service caused by an adversary physically taking over a computer or node.

Terrorism-Damage or loss of service caused by a terrorist.

4.2 DISASTER RECOVERY PLANNING

Any of the threats defined in this section, as well as future and unknown threats, have the potential to cause substantial loss of network availability, applications, data, and specific NMCI services. The NMCI contractor must have fully developed, rehearsed, and implemented Disaster Recovery Plans tailored to the regions in which the NMCI will operate and that mitigate the risks defined in this section. The contractor shall provide a report, as required by paragraph 3.4.6 of Attachment 1, on the results of individual site critical infrastructure assessments to include: identification of critical infrastructures (cyber and physical), an assessment of risk of loss of service availability, and actions taken to ensure operational availability is protected.

3 SECURITY OPERATIONS

3.1 NETWORK OPERATIONS CENTER(S) (NOC)

The NOC Mission is to provide network management services and maximum security for the NMCI. The NOC is responsible for maintaining network equipment for the NMCI and for diagnosing/troubleshooting network related problems. Network Operators will be available 24 hours a day 7 days a week for reporting network problems/security issues and outages. Network Operators can provide the NMCI with current information about the network and the modem pool. Central reporting to a higher echelon command of intrusion attempts will be processed at this level. This will include management and operation of all network security components, including but not limited to firewalls, IDSs, VPNs, HAGs, ACLs, etc.

3.2 SECURITY ASSESSMENT TEAMS

3.2.1 Green Teams

The purpose of this team(s) will be to determine effectiveness of contract fulfillment by the vendor against a pre-determined and agreed upon range of SLAs. These teams will also verify configuration management and aid in maintaining the security integrity of the NMCI.

3.2.2 Red Teams

The purpose of this team(s) is to perform a vulnerability and risk assessment to analyze the actual risk that users of the NMCI are managing given the current set of unbounded network attacks.

3.3 GOVERNMENT PROGRAM OFFICE SECURITY TEAM

This team will review and approve:

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

3.4 IAVA

In the DoN, IAVA's are promulgated by DISA via Navy Message. The NMCI service provider will be required to follow/implement these time sensitive directives.

3.5 INFOCON

Like DEFCONs, the DoD has implemented information operations conditions that are predicated on the cyber threat against the United States. The NMCI service provider will be required to implement, follow and dynamically support INFOCONs as they are promulgated.

3.6 C&A

Security services provided by NMCI shall provide for a sufficient level of assurance that allows the respective components within NMCI to be certified and accredited in accordance with DoD Policy.

Any product deployed by the vendor as part of NMCI used to separate classification levels shall be a high-grade cryptographic device that meets DoD defined requirements. Also, the contractor shall support the role of certifying agent for NMCI.

3.6.1 Program Manager

Program Manager (PM) is the person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the IT system. The proposed PMs are PMW 152 and PMO-IT for USMC.

3.6.2 The Certification Authority (CA)

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 proposed CA is PMW 161.

3.6.3 The Certification Agent

The Certification Agent aids the CA in collection and gathering of technical evidence and data. The proposed Certification Agents will consist of the NMCI service provider and other government and non-government entities.

3.6.4 The User Representative (UR)

The User Representative (UR) is the individual or organization that represents the user or user community in the definition of information system requirements. The proposed URs are comprised of a council of the major claimants co-chaired by NCTF-CND and MARFOR-CND.

3.6.5 The Designated Approving Authority (DAA or Accreditor)

The Designated Approving Authority is the official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk. The proposed developmental DAA is PEO IT. The proposed operational DAA is the NMCI Chief Operating Officer.

3.7 INCIDENT RESPONSE

3.7.1 Data Collection

The NMCI service provider shall collect incident data and provide that data to DoN CND entities (FIWC, NCTF-CND, MARCIRT, MARFOR-CND, and other organizations that the Government may specify) for analysis as to whether an incident has occurred as well as the magnitude of the incident.

In some scenarios, the NMCI service provider may be requested by DoN CND entities to analyze incident data which would then be forwarded to appropriate DoN entities. This will be based on security policy as set by NMCI Operations and Governance organization.

3.7.2 Response

After analysis of the incident data at the DoN CND entities, an incident response will be promulgated from the DoN CND entities to the NMCI service provider. The NMCI service provider shall then react and respond to the incident response.

3.8 POLICY

3.8.1 Static Policy

NMCI security policy will be administered and promulgated by NMCI Governance and Operations Organization and DoN CIO. There will be an agreed upon implementation plan for incorporation of these changes.

3.8.2 Dynamic Policy

JTF CND through NCTF-CND and MARFOR CND will also provide dynamic security policy changes that will need to be incorporated real time within the NMCI.

3.9 CONFIGURATION CONTROL

The NMCI service provider will be required to apply applicable security policies to the NMCI configurations. The NMCI service provider will manage their own compliance and be tested by the Red and Blue Teams outlined above to verify.

3.10 LAB TESTING

A test environment will be utilized to test newly developed and discovered attacks, new products (software and hardware), compatibility issues, and legacy support.

3.11 SERVICE PROVISIONING

The NMCI service provider will ensure networking components, workstations, servers, etc. are initially configured securely. The service provider will also be responsible for improving future security configurations with timely application of security patches and fixes.