

Site Security Requirements

1	Executive Summary	1
1.1	Overview	1
1.2	Background and Scope	1
2	Requirements	2
2.1	Border Protection	2
2.1.1	General	2
2.1.2	Border router(s)	2
2.1.2.1	Interface management and control	2
2.1.2.2	Traffic Management	3
2.1.2.3	Connectivity Management	3
2.2	Network Based Intrusion Detection System (IDS)	4
2.3	DMZ	4
2.3.1	General description	4
2.3.2	Minimum security requirements for systems located in the DMZ	4
2.3.3	Typical services available in the DMZ	5
2.3.3.1	Domain Name Service	6
2.3.3.2	Publicly accessible web servers	6
2.3.3.3	Publicly accessible FTP servers	6
2.4	Firewall	6
2.4.1	General	6
2.4.2	Management	6
2.4.3	Rules	6
2.4.4	Content screening	7
2.4.5	Logging and reporting	7
2.4.6	Access	7
2.4.7	Capabilities	8
2.4.8	Services permitted through the site firewall	8
2.4.8.1	DNS	8
2.4.8.2	Electronic mail	8
2.4.8.3	HTTPS	8
2.4.8.4	FTP	8
2.4.8.5	NNTP	9
2.4.8.6	SSH	9
2.4.8.7	Others (e.g., encryption devices, special services)	9
2.4.9	Firewall modification process	9
2.5	Site Network(s)	9
2.5.1	Network Addresses	9
2.5.1.1	General	9
2.5.1.2	Address Management	9
2.5.1.3	Names for network entities	10
2.5.1.4	Network domains (Internet)	10
2.5.2	Routers	10
2.5.3	Network Audit Trails	10
2.5.4	Internal Firewalls	10
2.5.5	Dial in Access	11
2.5.5.1	Location and configuration	11
2.5.5.2	Account eligibility	11
2.5.5.3	Authentication and telephone line audit trails	11
2.5.5.4	Network dial in audit trails	11
2.5.5.5	Operator requirements	11
2.5.6	Dial out Access	11
2.6	Computers	12
2.6.1	All	12

2.6.2	Servers	12
2.6.3	High Value Enclaves and/or mission critical servers	13
2.7	Services and applications	13
2.7.1	All services.....	13
2.7.2	Legacy Services	13
2.7.3	New services	13
2.7.4	Services accessible from outside the activity	13
2.7.4.1	Email.....	13
2.7.4.2	Web.....	14
2.7.4.3	FTP.....	14
2.7.4.4	Telnet	14
2.7.5	Services accessible only from within the activity	14
3	Classified Information Protection	14
3.1	General.....	14
3.2	Processing / Access within Specific Areas	15
3.2.1	Open Storage Area	15
3.2.1.1	Computers	15
3.2.1.2	Networks	15
3.2.2	Controlled Access Area	15
3.2.2.1	Computers	15
3.2.2.2	Networks	15
3.2.3	Other Areas	15
3.2.3.1	Computers	15
3.2.3.2	Networks	15
3.3	Processing at more than one classification level	15
3.3.1	General	15
3.3.2	Marking and handling	16
3.3.3	Reading up/writing down prohibited.....	16
3.3.4	Human Interface Device (HID) switches	16
3.3.5	State/periods processing	16
3.4	Transmission between Controlled Access Areas	16
4	Vulnerability Assessments	16
4.1	General.....	16
4.2	Authorized personnel	17
4.3	Unauthorized vulnerability assessments	17
5	Incident Handling	17
6	Training.....	17
6.1.1	General	17
6.1.2	Specific areas	17

Site Security Plan

1 Executive Summary

Information assurance is an integral part of the organization's mission. Our challenge is to make needed services available to authorized users concurrently with minimizing both the amount of information we freely disclose to others as well as minimizing the attack profile we present to our adversaries. This can be achieved by implementing a "defense in depth" - layered protection consisting of complementary countermeasures which provides protection (a robust infrastructure), detection (identifying attempts to compromise the network and / or computers connected thereto), containment (isolation of the problem or compromise), and recovery from incidents. Protection for existing (legacy) systems must be implemented using a meaningful and balanced approach.

1.1 Overview

A well-designed defense-in-depth strategy will accomplish the following:

- block attempts to map the site network;
- detect attempts to probe the network or mount attacks against the infrastructure or connected computers;
- minimize information disclosure;
- masquerade computer identity;
- protect information during transmission and at rest;
- protect against malicious code;
- limit inbound traffic to that which is destined for and meets acceptance criteria for the site; and
- limit outbound traffic to that originating from the site and meeting transmission criteria for the site.

Other countermeasures include (and are not limited to) effective training / awareness programs and periodic meaningful vulnerability assessments of systems and networks with appropriate follow-up to rectify identified deficiencies. There must exist a methodology to implement new services (or applications) when the benefit from the new service outweighs the risk(s) associated with it. The computers in use at the site must be configured to present the minimum risk while providing optimum capability.

1.2 Background and Scope

As noted above, Information Assurance is a critical mission element. This document identifies the minimum security requirements that sites must meet to have an effective Information Assurance Program. It is based on the concept that an activity commander is responsible and accountable for events within the activity and that no command or activity has the authority to place another command or activity at risk. In that paradigm, the trust model boundary is the site electronic chain link fence, which is identified as those systems within the physical control and responsibility of the activity commander at a single geographic location. This line of demarcation applies to current services and applications as well as services and applications under development. The requirements described in this document must be applied to all new systems. Compliance for systems that are presently operational will be addressed on a case-by-case basis within the current accreditation timeframe. Owners of non-compliant systems are responsible and accountable for developing and verifying means to contain and recover in the event of an incident.

This plan applies to all information systems under the purview of the Activity Commander. Exceptions to the plan will be considered by the Information Systems Security Manager (ISSM) on a case-by-case basis.

Requirements and discussions that pertain to systems that are (or will be) used to process and / or transmit classified information will be conveyed in this font throughout this document with the exception of the section specifically devoted to Classified Information Protection.

2 Requirements

Protection must be applied at multiple locations in the infrastructure. Typical examples include the following:

- connection points to the site,
- computers internal to the site,
- services allowed on the computers at the site,
- information entering or leaving the site.

Protection for all connection points includes, and is not limited to, the following:

- a border router (or routers) with appropriate traffic management,
- a network-based intrusion detection system (IDS) with sensors located outside and inside the firewall,
- a demilitarized zone (DMZ), and
- one or more firewalls.

Requirements identified below are based on the following criteria:

- network address block(s) do not span geographic disparate sites,
- addresses for all external connections are in a range that is not a subset of the address block(s) used at the site proper. For example, if the site uses X.Y as the address space for the computers and network infrastructure, the addresses used for external connections would be A.B.C where X.Y and A.B.C constitute legally assigned addresses, and
- only legally assigned addresses are used.

2.1 *Border Protection.*

2.1.1 General

This section defines requirements for all network connections to the activity. Typical examples include and are not limited to:

- connections to the site Internet Service Provider(s) (ISP),
- connections to other sites (such as tenants and/or partners (e.g., contractor sites)),
- dial up telephone (dial in and dial out) lines,
- ISDN connections (leased or dial-up).

All such connections will terminate on site in a DMZ as described below.

Telephone lines are authorized for voice only unless specifically approved by the cognizant Designated Approving Authority (DAA) for use with a computer.

Any classified traffic leaving the site via any type of network or network interface shall be encrypted using an encryption device approved for the purpose.

An approved encryption device shall protect telephone lines used for transmission of classified information.

2.1.2 Border router(s)

2.1.2.1 Interface management and control

Site personnel will configure and manage all interfaces that connect to site network(s) as described below.

2.1.2.2 Traffic Management.

Border router(s) shall be configured to block the following:

- All non-Internet Protocol (IP) traffic, (e.g. Appletalk, NetBEUI, IPX, etc.)
- Broadcast IP packets destined for the site.
- Broadcast IP packets leaving the site.
- Any IP packet with the source routing options set.
- Incoming IP packets with source addresses used only inside the site or connected activities.
- Outgoing IP packets with destination addresses used only inside the site or connected activities.
- Outgoing IP packets with source addresses not used inside the site or connected activities.
- TCP or UDP packets with a source port of zero.
- Incoming IP packets with a destination address not within the addresses of the site or its connected sites.
- IP packets from, or destined for, non-routable addresses. These include and are not limited to the following:
 - a) 0.0.0.0 through 0.255.255.255 (Historical Broadcast);
 - b) 10.0.0.0 through 10.255.255.255 (RFC 1918 Private Network);
 - c) 127.0.0.0 through 127.255.255.255 (loopback interfaces)
 - d) 169.254.0.0 through 169.254.255.255 (Link Local Networks)
 - e) 172.16.0.0 through 172.31.255.255 (RFC 1918 Private Network);
 - f) 192.168.0.0 through 192.168.255.255 (TEST-NET);
 - g) 224.0.0.0 through 239.255.255.255 (Class D Multicast);
 - h) 240.0.0.0 through 247.255.255.255 (Class E Reserved);
 - i) 248.0.0.0 through 248.255.255.255
 - j) 255.255.255.255 (Broadcast)
- Incoming ICMP echo request packets.
- Incoming host unreachable packets.
- Outbound ICMP echo reply packets.
- Outbound ICMP host unreachable packets.
- SNMP except to those specific infrastructure machines necessary for site Internet Service Providers (ISPs) to check connectivity.

Border router(s) shall be configured to permit only traffic as required by connectivity agreements (described below).

Border routers shall be configured to record to a log server located inside the site firewall the following events:

- Incoming IP packets with source addresses used only inside the site or connected activities.
- Outgoing IP packets with destination addresses used only inside the site or connected activities.
- Outgoing IP packets with source addresses not used inside the site or connected activities.

Electronic and hard copies of router configurations shall be escrowed and stored in an alternate location in a storage area approved for the corresponding classification / sensitivity level.

2.1.2.3 Connectivity Management

Each network link that is (or will be) used to provide access to another party (e.g., business partner, customer, or supplier) shall be approved by the ISSM prior to any development and /or procurement leading to such a connection.

Each network link (as described above) shall be documented by an appropriate Memorandum of Agreement (MOA) that stipulates as a minimum the following:

- description (and classification) of the data transmitted via the link,
- clearance levels of the users,
- safeguards to be implemented prior to, and during activation of the link,
- designation of the resolving party in the event of conflicts regarding the link, and

- typical minimum risk management practices employed by both parties.

The MOA shall be reviewed and approved by the appropriate risk manager and signatory for each party. For NSWCDD, the risk manager is the ISSM and the signatories are the Commander, the Executive Director, and the cognizant Designated Approving Authority (DAA).

Each link shall be configured to support collection and analysis of network level audit trails.

When encryption is employed on the link, decryption shall take place outside the corresponding firewall.

2.2 Network Based Intrusion Detection System (IDS)

Network-based IDS sensors shall be placed both inside and outside the site firewall. The IDS shall be selected and implemented in such a way as to produce a very low (less than 1%) false alarm rate concurrent with reliable detection of anomalous activity. Criteria for selection and implementation are as follows:

- The eavesdropping sensor network interface outside the firewall shall be configured to listen only (stealth). It shall not respond to any connection requests or attempts to identify.
- Sensor data shall be transferred to an analysis station via a second network interface connected inside the firewall.
- Filters for analysis of networked traffic shall be user configurable to meet site conditions.
- The IDS shall be capable of generating plain text reports which can be sent via email from the analysis station / console directly to appropriate activities (NAVCIRT, CERT, etc.) When such reports are transmitted unencrypted, the addresses in use for the reporting activity shall be obfuscated so as to preclude identification of computers and network entities that responded to a given stimulus. When actual addresses are required for reports transmitted outside the activity, the report shall be encrypted using public key cryptography.
- The IDS shall support sensors located between the border router and firewall (in a classical DMZ) and inside the firewall (to verify proper firewall operation) as well as a sensor located outside the border router.

2.3 DMZ

2.3.1 General description

These requirements are based on the implementation of a classical DMZ between the border router(s) and a choke firewall. Requirements may be modified as appropriate for alternate configurations. Typical services that are fielded in the DMZ include servers with publicly released information such as:

- externally accessible DNS servers,
- web servers,
- anonymous FTP servers, and
- others as deemed appropriate by the cognizant Designated Approving Authority.

2.3.2 Minimum security requirements for systems located in the DMZ

These requirements are in addition to those listed below for all computers.

Each server (computer) shall be configured and accredited as a single purpose server. This means that if a machine's purpose is to be a web server, only services required for the web server functionality may be run. Services that are not required to support the system's primary functions must be disabled. Typical examples of services to be disabled include (and are not limited to): X-windows, Sunrpc, mail, DNS, NIS, FTP, NFS, tooltalk, and calendar manager. Other high-risk services are identified by CERT and the cognizant CIRT. Systems Administrators and the ISSM shall conduct periodic reviews to verify installed services.

The Operating System and application(s) must be robust. Patches for both the OS and the application must be updated at least monthly and within four working hours of notice by CERT / NAVCIRT / IAVA that a problem needs to be corrected.

Administration and configuration of machine shall be accomplished from the console or through a secure mechanism which requires strong authentication and uses 128 (minimum) bit encryption (e.g., SSH or equivalent).

All operating system and application binaries, application configuration files, and static data files shall be protected by a file integrity assessment tool (e.g., Tripwire or equivalent). It must be run on a weekly basis to check file integrity. Older versions that do not keep the databases encrypted on disk must have databases stored on removable media to prevent tampering.

There shall be no compilers of any kind installed on any computers located in the DMZ.

Sample code / scripts provided with applications shall be removed prior to deployment in the DMZ. Typical examples include sample cgi-bin scripts provided with web servers.

User accounts shall be limited to the minimum number, and access will be granted only to appropriately trained personnel. Root or administrator access is granted only to properly trained administrators and those administrators are approved by the ISSM. The ISSM will maintain an escrow of the root password for purpose of being able to shut down or investigate the machine in the case of an incident.

The root password shall be different from that of any computer internal to the firewall.

Audit logging shall be performed on all externally available services. For example, an FTP server will log all connections to FTP - this will include source IP address and all files being retrieved and stored. In addition to any automated analysis, the system administrator must review the logfiles daily for abnormalities and / or intrusions or intrusion attempts.

Although machines in the DMZ may trust internal machines, no internal machine shall trust any machine located in the DMZ. In this case, trust is defined as using identification and authentication accepted by a computer in the DMZ as the basis for granting access to a computer elsewhere (such as a computer located inside the firewall). An exception to this condition is the information contained on (or provided by) the external DNS servers that provide host name resolution for computers located inside the firewall.

Computers in the DMZ shall not reference (either directly or indirectly) any internal computers, (i.e. they don't have local hosts tables or alias files that reference internal machines). An exception to this condition is the information contained on the external DNS servers. This information provides host name resolution for computers located inside the firewall such that those internal computers can accept inbound connections from computers external to the site

Dynamic routing shall be disabled on all computers located in the DMZ. Each machine shall have only static routes to its default router.

File transfer applications in the DMZ may permit a "get" or "put" operation, but not both in the same file system in a computer.

Any information available for anonymous access other than Domain Name Service lookup (i.e. web or ftp) on a server shall be approved by Public Affairs Office (PAO) prior to being released. The process for PAO approval must be established, maintained, and audited.

2.3.3 Typical services available in the DMZ

2.3.3.1 Domain Name Service

The external Domain Name Service (DNS) servers (primary and secondary) shall resolve only those hosts to which the firewall permits connections from outside the site. A process for creating, maintaining, approving, removing, and auditing this list of hosts is the responsibility of the organization that provides Domain Name System service for the activity and shall be incorporated into the accreditation process for the external DNS servers.

2.3.3.2 Publicly accessible web servers

2.3.3.3 Publicly accessible FTP servers

2.4 Firewall

2.4.1 General

The firewall shall support the site security policy, not impose one.

Firewalls shall be configured to deny all services by default, and only permit those services approved by the ISSM. The approval is contingent on an operational requirement (validated by the cognizant manager) and a balanced risk management process. See below for implementation of services commonly allowed through a site firewall.

The firewall shall use an operating system that has been configured to be resistant to external or internal unauthorized access or exploit.

The firewall shall be configurable regarding queries to which it responds (e.g., SNMP, traceroute, ping, etc.).

The firewall shall accommodate new services and needs as the site security policy or risks to the site change.

2.4.2 Management

The ISSM (or designee) shall manage all firewalls.

The firewall administrator (and / or the ISSM staff) shall use an auditing mechanism (tools and process) approved by the ISSM to verify firewall configuration and the protection the firewall provides.

Rulesets for all firewalls shall be periodically reviewed and approved (or required modifications identified) by the ISSM. Site firewall review is typically conducted at least every three months. Ruleset review of internal firewalls may be done less frequently, but at least annually.

2.4.3 Rules

The system should use a flexible and user-friendly rule specification language that is easy to program and easy to read.

Filters and rules must be displayable in human readable form on a console separate from the firewall.

Filter and rule files must have the capacity to include (contain) comments.

Filters and rule specification language must support ranges of IP addresses, subnets, and ports.

The rule specification language should support the capacity to specify domain names and wild cards.

The system must support the ability to assume different configurations via input files.

The system must have the capacity to permit dynamic modification of rules without stopping and restarting the system.

2.4.4 Content screening

The firewall must have the capacity to inspect (and block or allow) various types of mobile code including, but not limited to, Java applets and ActiveX. Scanning of email attachments (text and binary) is also highly desirable.

2.4.5 Logging and reporting

The system must have flexibility in the configuration of logging and reporting, i.e., the ability to specify the amount of logging, which events to log, and the mechanism for logging (e.g., both failed and successful connection attempts can be logged with the appropriate configuration).

Logfiles must be easily accessible in non-proprietary displayable ASCII format, from authorized remote systems as well as the console.

The firewall must have the capability to generate an automatic alert to a configurable list of recipients (e.g., the firewall administrator, network operations manager, etc.) when logfiles reach a selectable percentage of storage capacity.

When logfile capacity is reached, the firewall must deny further connections (both inbound and outbound) except connections to the console from remote authorized systems.

The firewall will support automatic generation and delivery of monthly reports of the firewall configuration (rule sets) to the administrator and ISSM staff.

The firewall must support administrator configurable reporting capabilities to include bandwidth usage, statistical breakdowns of traffic by protocol, service (port), subnets, and hosts. This may be accomplished by third party software packages.

Alert reporting must have the option of providing summarized reports (i.e., only one alert email for 100 probes where the address is being varied or where a range of ports is being scanned). Summary reporting of similar probes during a specified time period (e.g., during the last minute or last five minutes) will be an available option.

Alert and alarm reporting should be user configurable to include paging, email, and SNMP.

2.4.6 Access

Remote access to the firewall shall be via a mechanism with strong authentication and encryption (e.g., secure shell or a PKI-enabled application).

All configuration capabilities of the firewall available at the console must be available to authorized remote systems on an assignable basis.

Authorized users on authorized remote systems must be permitted to examine or download the firewall log and configuration files without entering the firewall application.

2.4.7 Capabilities

The firewall must be either an application-proxy firewall or a network-level firewall with stateful packet inspection. Application-proxy is preferred.

If the firewall type is application-proxy, it must use hardened "application aware" daemons.

No inbound connection shall pass unrestricted (e.g. telnet from all addresses outside the site to all addresses inside the site will not be permitted).

The firewall must support network address translation (NAT) and split DNS.

The firewall must use a verifiably hardened operating system, or allow hardening of the underlying operating system. Verification of the operating system status will be accomplished by vulnerability scanning.

The firewall should have VPN support for all IPsec compliant VPN clients.

The firewall should have the capability to detect and report port scans.

2.4.8 Services permitted through the site firewall

See "Services and applications" for additional information.

2.4.8.1 DNS

Outbound queries shall be permitted only from DNS servers that are located inside the firewall to external DNS servers that are located outside the firewall.

2.4.8.2 Electronic mail

Inbound email to the site shall be permitted only on port 25 (SMTP) and only to corporately managed server(s) located in the DMZ. Each of these servers shall only transfer email to a server (cluster) located inside the firewall on a screened subnet.

Outbound email shall be permitted only from corporate servers located in the DMZ. Each of these servers accepts outbound requests only from computers located inside the firewall.

2.4.8.3 HTTPS

Outbound HTTPS is permitted unrestricted within the bounds of the command acceptable use policy.

Inbound connections shall be permitted only to accredited internal HTTPS servers.

2.4.8.4 FTP

Outbound FTP is permitted unrestricted within the bounds of the command acceptable use policy.

Inbound connections shall be permitted only to legacy FTP servers as approved by the ISSM.

2.4.8.5 NNTP

Inbound connections shall be permitted only to corporate server(s) from a list authorized by the ISSM.

Outbound connections shall be permitted only from corporate NNTP servers.

2.4.8.6 SSH

Outbound connections are allowed to pass unrestricted within the bounds of the command acceptable use policy.

Inbound connections shall be permitted only to information systems accredited to accept connections from computers external to the activity.

2.4.8.7 Others (e.g., encryption devices, special services)

In accordance with the Firewall modification process specified below, access to other ports via their access control lists shall be implemented on an as-needed basis once the firewall modification has been approved.

2.4.9 Firewall modification process

Firewall rule sets may be modified to meet a valid operational requirement endorsed by the cognizant business area manager. The requestor will identify the need (service/port) and source and destination addresses necessary, anticipated duration of the request, the benefit to the corporation, and any associated risks potentially encountered by permitting the service as requested. The request shall also identify how the risk will be mitigated and managed. The process must contain provisions for the following (as a minimum):

- Review and concurrence by the ISSO for affected system(s),
- Review and concurrence by the ISSM staff after evaluation of risks and proposed countermeasures.
- Approval by the ISSM.

2.5 Site Network(s)

2.5.1 Network Addresses

2.5.1.1 General

Addresses for all networks and network elements/entities under the cognizance of the activity commander shall be addresses assigned to the activity unless the ISSM has granted a specific written waiver.

Addresses for networks that connect to, or provide connectivity for, networks under the cognizance of the activity commander shall use addresses different from the address spaces identified above.

2.5.1.2 Address Management

Addresses for all networks and network elements/entities under the cognizance of the activity commander shall be assigned by a central agent approved by the ISSM. Addresses shall be assigned subject to the following conditions:

- the network entity (computer, printer, network device) is properly accredited as condition for obtaining an address.
- subnets in the address space are assigned such that subnets do not span buildings.
- the address block assigned to the site will not be use at another geographic site or another activity at the site.

The organization assigning addresses is also responsible for management and auditing of network address usage per the following:

- Auditing shall be conducted to identify unregistered addresses in use. A report is to be sent to the cognizant Information Systems Security Officer with a date by which the condition is to be corrected or service discontinued (blocked at the router local to the invalid address).
- Assigned addresses shall be validated at least annually (verify that the address is still in use under the condition it was assigned - type of device, operating system, valid accreditation, and that the need for the address still exists).

2.5.1.3 Names for network entities

Names for network entities (e.g., hostnames) shall consist only of alphanumeric and the dash characters.

2.5.1.4 Network domains (Internet)

All entities on the network shall be named as hostname.domain where domain is the domain assigned to the activity. The use of sub-domains (or host names that have the appearance of sub-domains) is prohibited.

2.5.2 Routers

Routers internal to the site shall be configured to block broadcast packets and addresses listed in "Border router(s)" above.

Routers shall be configured to permit management (e.g., SNMP) connections only from computers approved by the site ISSM.

Routers shall be configured to detect and record connections originating from or destined for a network at a different classification level (e.g., the routers on the unclassified network shall be configured to log connection attempts to or from the address space in use for a classified network). Such events shall be written to a syslog file (or equivalent). The syslog file shall be reviewed automatically at least hourly with email notification to the cognizant Security Officer and the 'incidents' email alias.

Routers shall be configured to block all invalid / unregistered addresses assigned to the site and detected on the network.

2.5.3 Network Audit Trails

Operators of networks shall collect and store network audit trails for all common protocols in use on the network. In a TCP/IP based network, these include (as a minimum) TCP, UDP, and ICMP.

Audit trails shall record (at a minimum) date, time, source address (and port as applicable), and destination address (and port as applicable).

Audit trails shall be digitally signed and usable as evidence (if needed) and shall be maintained for at least one year.

Networks that have computers that employ state processing (processing information at different classification levels, one level at a time) connected to them shall have implemented (by the network operator) sufficient audit trail infrastructure to detect addresses for networks at a different classification level (i.e., the unclassified network shall have a mechanism to detect and report the presence of an address used on the secret network).

2.5.4 Internal Firewalls

Internal firewalls will be selected and implemented as protection requirements indicate. Permitted services will be identified on a case-by-case basis to provide protection as needed.

Operators of internal firewalls shall grant access to members of the ISSM staff for the staff to conduct vulnerability assessments (described below). Exceptions to this will be considered on a case-by-case basis.

2.5.5 Dial in Access

2.5.5.1 Location and configuration

All dial-in facilities shall be logically located inside the firewall that is connected to the Internet. All dial-in facilities shall be implemented only for dial-in access to a network. Connection of a dial-in capability on other configurations (e.g., user desktop) is prohibited.

2.5.5.2 Account eligibility

Dial-in access will be offered only to validated users (employees via line management; contractors via the Contracting Officers Representative) who sign an agreement to abide by the activity security and acceptable use policies. Violation shall constitute grounds for account termination and potential disciplinary action.

2.5.5.3 Authentication and telephone line audit trails

Users shall be required to identify and authenticate themselves prior to being granted access to the network. The following activity shall be recorded in an audit log:

- User identification as entered by the person attempting to authenticate.
- Both successful and failed connection attempts.
- The telephone number from which the call originated.
- The time of start and end of dial up activity.

2.5.5.4 Network dial in audit trails.

All connection attempts to or from the dial-in and other network resources shall be recorded regardless of success or failure. Information collected (minimum) shall include the following: date, time, protocol, source address and port, destination address and port).

Network connection audit trails shall be retained for at least one year.

2.5.5.5 Operator requirements

Operators of any dial-in facility shall audit dial-in accounts at least quarterly. Accounts not in use will be removed in a timely fashion.

Operator(s) of any dial in access facility will audit access logs to identify and resolve the following anomalous activity:

- five (or more) failed login attempts using the same login ID within a 30 minute time frame
- five (or more) failed login attempts within a 30 minute time frame from the same telephone number
- any attempt to use accounts historically known to be used for penetration attempts such as: guest, root, anonymous, etc.

The reviewer will report any unresolved activity that appears to be unauthorized to the ISSM in accordance with established incident handling procedures described below.

2.5.6 Dial out Access

Dial out access is permitted only from standalone computers (i.e., not connected to a network at any time) that are specifically accredited for that purpose. Waivers to this practice will be considered on a case-by-case basis. Required documentation includes a Standard Operating Procedure identifying the risks and they will be mitigated. The SOP must be reviewed and approved by the ISSM prior to accreditation by the cognizant DAA.

2.6 Computers

2.6.1 All

A trained system administrator who is responsible for maintaining security-related patches for the operating system and all applications in use will be assigned to every computer. The administrator will also be responsible for monitoring the health of the computer system by periodic frequent examination of the system logs and audit trails.

A trained Information System Security Officer (ISSO) responsible for all issues related to Information Assurance will be assigned to every computer. ISSO responsibilities are described in the appointment letter signed by the cognizant Department Head or designee.

Every computer shall incorporate a mechanism for identification and authentication of each user permitted to use the computer.

An approved warning banner (with at least an abbreviated version of the acceptable use policy and consent to monitoring) shall be displayed upon login or access.

Modems are prohibited in computers connected to the site network. Exceptions are granted on a case-by-case basis in accordance with guidance and approval from the ISSM.

Anti-viral software shall be installed, operational, and current for all operating systems covered by the DOD-wide license. Anti-viral signatures must be updated at least weekly or within 4 working hours of receipt of update notification. Anti-viral signatures on computers that are used infrequently (e.g., not powered up frequently) shall have the signatures updated as soon as they connected to a network and prior to exchanging any information with another computer.

Every computer shall have in place a mechanism approved by the ISSM to remove/sanitize inappropriate material such as classified and/or sensitive material not intended for storage on said computer.

Network services not needed to provide required functionality shall be disabled. For example, a typical desktop computer does not need the FTP server service operational.

Patches for the operating system and applications shall be maintained and updated at least quarterly or within a timeframe required by an applicable Information Assurance Vulnerability Alert or the cognizant DAA as appropriate.

Access control lists for all services in use shall be implemented and monitored. The default policy shall be to deny access to all services and allow access to only those services approved as part of the accreditation process. The logging of all accesses to the system is required along with a review of those logs (weekly, minimum; daily, preferred). Exceptions to this element will be considered on a case-by-case basis. Contact the Information Systems Security Office for additional information.

The individual responsible for logfile review shall report to the ISSM or designee all unresolved anomalous activity detected during review of the system logs.

2.6.2 Servers

Information not approved for public release shall be placed only on servers accredited for that purpose and which utilize a PKI-compliant authentication and encryption mechanism.

Every server shall have in place a tested contingency/recovery plan.

2.6.3 High Value Enclaves and/or mission critical servers.

Internal firewalls will be implemented to protect high value enclaves as program needs dictate.

The need for encrypted traffic will be evaluated and approved on a case-by-case basis. If the traffic to and from the enclave is encrypted at the network level (e.g., a virtual private network) an IDS meeting the criteria specified in “Network Based Intrusion Detection System” (above) shall be installed, operational, and maintained.

A file integrity analysis program shall be implemented for all critical servers.

2.7 Services and applications

2.7.1 All services

Prior to obligating funds for any hardware, software, or labor that will be used to provide a new service (application), or upgrade (or replace) an existing service (application) the service developer/provider shall contact the ISSM to review the proposal. The ISSM will review the proposal and approve the proposal or identify any shortcomings to be mitigated prior to proceeding. A description of the process is located at http://www.nswc.navy.mil/ISSEC/Guidance/server_setup.html.

2.7.2 Legacy Services

Existing services and applications are subject to a risk management process for identifying and managing risk. Existing services will be made compliant with best practice for new service within 180 calendar days of publication of this plan. For those services and applications that cannot be made compliant due to reasons beyond the users control, the user will develop a mechanism for containment and recovery as appropriate and obtain endorsement by the ISSM.

2.7.3 New services

Any new services will use fixed ports to allow for tracking and auditing.

Data not approved for public release must be encrypted for off-site transmission using a PKI-compliant mechanism. If a PKI-compliant solution is not available, a secure shell that forwards TCP connections is an acceptable alternative.

Each site will implement PKI as a part of the information assurance program. Certificates will be at least Class 3.

2.7.4 Services accessible from outside the activity

2.7.4.1 Email

Only SMTP (port 25) shall be used for the transport of email in the conduct of official business.

All incoming and outgoing SMTP traffic for the site shall be routed through a set of SMTP gateways managed by one set of administrators.

The email server shall be configured to refuse ‘spam’ email.

Incoming email that contains forged headers shall be rejected. A typical example of an email messages with forged headers is an email from outside the site domain with a “from” address that is inside the site.

Only email destined for users at the site shall be accepted by the SMTP gateways. Email shall not be forwarded automatically without review.

Indirect addressing of email will be denied by email server configuration.

Servers will enable full audit trails such that message headers are preserved each time an email message is forwarded.

Anti-viral software that scans and cleans attachments shall be implemented on all mail servers.

2.7.4.2 Web

All web servers containing information not approved for public release and accessible from locations external to the site will use 128 bit (minimum) encryption and server certificates issued by a DOD Certificate Authority.

Servers that require identification and authentication will use a PKI-enabled mechanism. In the event that users do not have PKI certificates, an alternate method approved by the ISSM may be used in the interim.

2.7.4.3 FTP

Identification/authentication and data transmission in the clear between the site and external locations is not an acceptable risk. Such conditions shall not be approved for new applications. See "New Services" below.

FTP will be permitted inbound only to computers approved by the ISSM. Conditions for approval include the following:

- submission and approval of plan to migrate to a secure mechanism that incorporates strong identification and authentication as well as encrypted data transmission.
- use of a mechanism that manages (controls) and records access.
- automated logfile analysis

2.7.4.4 Telnet

Telnet shall be managed similar to FTP (above).

2.7.5 Services accessible only from within the activity

See "All Services" above.

3 Classified Information Protection

3.1 General

In this section (Classified Information Protection) the term computer refers to an information system that accesses, or processes classified information, or is connected to a network on which classified information is transmitted.

In this section the term network refers to a collection of components including, and not limited only to: media (wiring/cabling), hubs, routers, switches, media converters, etc. used to transmit classified information or provide connectivity to computers that process classified information or have classified information stored on them.

Network media for unclassified and classified networks shall not be bundled together.

Only systems accredited by the cognizant DAA shall be used to process classified information.

3.2 Processing / Access within Specific Areas

3.2.1 Open Storage Area

An open storage area is an approved space with sufficient protection such that a classified document may be left in the open.

3.2.1.1 Computers

May contain fixed, non-removable hard drives which are left unattended. This is based on the premise that all persons with access to the area are cleared or escorted.

3.2.1.2 Networks

Good installation practices apply. Network components may be installed without the benefit of any mechanical protection beyond what is done as a standard installation practice.

3.2.2 Controlled Access Area

A Controlled Access Area is the complete building or facility area under direct physical control within which unauthorized persons are denied unrestricted access and are either escorted by authorized persons or are under continuous physical or electronic surveillance.

3.2.2.1 Computers

Computers shall not contain fixed, non-removable hard drives. When unattended, any media must be secured in an approved container.

3.2.2.2 Networks

Good installation practices apply. Media (e.g., cabling) and components (hubs, routers, switches) may be installed without the benefit of any mechanical protection beyond what is done as a standard installation practice.

3.2.3 Other Areas

These areas are typically uncontrolled (no clearance required to gain access).

3.2.3.1 Computers

Computers shall not contain fixed, non-removable hard drives. When unattended, any media must be secured in an approved container.

3.2.3.2 Networks

Networks that transmit unencrypted classified information in other than a controlled access area or open storage area must utilize a Protected Distribution System as described in Navy Information Assurance Publication 5239-22.

3.3 Processing at more than one classification level

3.3.1 General

When information at more than one classification level must be extractable (i.e., written to media at the respective classification level), separate computers shall be used to meet operational requirements.

If information at more than one classification level must be stored on a computer, the computer shall be operated standalone (not connected to a network) or connected only to a network accredited for the highest classification level to be processed.

Computers shall not be connected simultaneously to networks at different classification levels.

3.3.2 Marking and handling

All information on any computer shall be protected and marked to reflect the highest classification level processed or accessible by the computer or the network to which the computer is connected, as applicable.

3.3.3 Reading up/writing down prohibited

As a general rule, any media inserted into a computer at a classification level higher than unclassified must be marked, handled, and stored at the highest classification level available on the system. Exceptions include media that is demonstrably write-protected (e.g., CD-R in a read-only drive) and a computer using a trusted operating system capable of maintaining segregation.

As a general rule, removing information from a system that is operating at (or connected to a system operating at) a classification level higher than unclassified and marking said information (or the media on which it resides) as unclassified is prohibited. Exceptions include systems that incorporate trusted operating systems designed and approved for that purpose and downwrite routines approved by the activity DAA.

3.3.4 Human Interface Device (HID) switches

Use of a keyboard/video/mouse (KVM) switch to server computers at different classification levels (e.g., unclassified and secret) is permitted subject to the following conditions:
initial wiring installation is verified by a second person,
all components are color coded to reflect the classification level of the individual item,
wiring is checked the first working day of each month, and
the ISO is notified immediately of any problems

3.3.5 State/periods processing

As a general rule, state processing shall not be used. The ISSM will consider exceptions on a case-by-case basis where all of the following conditions are met:

- Space constraints preclude the use of separate computers.
- Separate (or no) hard drives are used for unclassified and classified processing.
- Detailed SOPS are approved by the ISSM and used to preclude incidents.
- Two persons are present to verify proper state change.
- Requisite network audit trails are in place to detect an improperly connected system (e.g., an unclassified system connected to a classified network)

3.4 *Transmission between Controlled Access Areas*

When classified information must leave a controlled access or open storage area and traverse an uncontrolled access area, it shall be protected by either NSA approved encryption devices or an approved Protected Distribution System in accordance with in Navy Information Assurance Publication 5239-22.

4 Vulnerability Assessments

4.1 *General*

The ISSM staff (or designees authorized by the ISSM) will conduct periodic unannounced vulnerability assessments against computers and network infrastructure components to identify services in use and potential vulnerabilities present.

Results of the assessment will be emailed to the cognizant ISSO for follow up and resolution during a time period specified by the assessor. Timely correction of deficiencies is necessary for continued operation of the computer.

ISSOs are responsible for advising line managers of potential risks and impact of removal from the network.

Modem sweeps will be conducted by the ISSM staff on a semi-annual basis. Departmental Administrative Officers are responsible for disconnecting any telephone lines not authorized for modem use.

4.2 Authorized personnel

Only persons authorized by the ISSM will conduct vulnerability assessments. Typical personnel include the ISSM staff (for site wide assessments) and system administrators and network administrators (for systems under their cognizance).

System and network administrators may request that other persons be authorized to conduct a vulnerability assessment on systems for which they are responsible. Such requests will be forward to the ISSM for review. Upon approval of the request, the administrator is responsible for ensuring that the assessment is coordinated with the ISSM.

4.3 Unauthorized vulnerability assessments

Conduct of vulnerability assessments by individuals other than those authorized by the ISSM will be handled as an incident. Such action may result in disciplinary action, termination of employment, or criminal prosecution or a combination of these.

5 Incident Handling

Incidents will be handled in accordance with NAVSO P-5239/19 and local procedures published on the activity Information Assurance intranet web page.

6 Training

6.1.1 General

Training will be provided in a number of ways: onsite, no cost instruction prepared and delivered by the ISSM and staff, as well as fee based training both on and off site.

6.1.2 Specific areas

Typical areas in which training will be provided include: IA Awareness, Auditing, Incident Handling, Malicious Code Protection (anti-viral software), Personal Internet Safety, and Processing Classified Information in a Computing and Network Environment