Defense Security Service
Office of the Designated
Approving Authority

MASTER SYSTEM SECURITY PLAN (MSSP) TEMPLATE FOR PEER-TO-PEER NETWORKS

June 2011
Version 3.0

MASTER SYSTEM SECURITY PLAN (MSSP)
GENERAL PROCEDURES

Compliant with the
Defense Security Service
Office of the Designated Approving Authority
Implementation Procedures based on
National Industrial Security Program
Operating Manual (NISPOM)

For Peer to Peer Networks

Contractor:

Address:

Cage Code:

ODAA Unique Identifier:

MSSP Revision Log		
Revision	Description of Baseline Change	Date

Information Systems Security Policy

The NISPOM requires that company management establish and promulgate an IS Security Policy. Following is an example that can be used as a guide in developing a policy for your facility.

The policy of **[enter contractor facility name & location]** is to safeguard all classified information as required in the National Industrial Security Program Operating Manual (NISPOM). As such, **[enter contractor facility name & location]** has published **[enter contractor facility security manual title],** which outlines the security program at our facility. Additionally, all employees of **[enter contractor facility name & location],** who are involved in the processing of classified information on an Information System (IS), shall comply with the following IS Security policies in accordance with NISPOM paragraph 8-101.b.

- The Information System Security Manager (ISSM) is the primary point of contact for all matters regarding the processing of classified information on an IS.
- The ISSM will publish a **[Master]** System Security Plan (**[M]**SSP) for all ISs to be used for classified processing and obtain the accreditation from the Defense Security Service (DSS) who is the designated approving authority (DAA).
- Only accredited ISs shall be used for the processing of classified information
- All accredited ISs shall be operated in compliance with the **[Master] [M]**SSP.
- Any employee of **[enter contractor facility name & location],** who fails to comply with facility security procedures, to include those defined in the **[Master]** SSP, shall be subject to disciplinary action up to and including termination of employment.

_____

[enter manager's name]
[enter manager's title]
[enter contractor facility name & location]

SAMPLE LETTER

Click on sample letter to upload image of signed letter.

1 Introduction 1
1.1 Purpose 1
1.2 Scope 1
1.3 Contract or Program Name and Description of IS Purpose 1
2 Personnel Responsibilities 1
2.1 Contractor Management 1
2.2 Information System Security Manager (ISSM) Responsibilities 2
2.3 Information System Security Officer (ISSO) Responsibilities 2
2.4 Users 3
2.4.1 Privileged Users 3
2.4.2 General Users 4
3 Certification and Accreditation 4
3.1 Certification 4
3.2 Accreditation 4
3.3 Reaccreditation 4
3.4 Security Testing 4
3.5 Self-Inspections 5
3.6 Self-Certification of Similar Systems 5
4 Information System Profile 5
4.1 Pure Servers 6
4.2 Tactical, Embedded, Data-Acquisition, and Special Purpose Systems 6
4.3 Mobile Systems 6
5 Protection Measures 6
5.1 Accounts and Logons 6
5.1.1 Identification and Authentication Management 6
5.1.2 Requirements for Passwords 6
5.1.3 Guidelines for User-Generated Passwords 7
5.1.4 Generic or Group Accounts 7
5.2 Session Controls 7
5.2.1 Logon Banner Requirements 7
5.2.2 Successive Logon Attempt Controls 8
5.2.3 System Entry Conditions 8
5.3 Access Controls 8
5.4 Audit Requirements 8
5.5 System Recovery and Assurances 9
5.6 Virus and Malicious Code Detection 10
5.7 Data Transmission Protection 10
5.8 Clearance & Sanitization 10
5.8.1 Clearing 10
5.8.2 Sanitization 11
5.9 Protection Measure Variances 11
5.10 Managing Wireless and other I/O Devices 11
6 Personnel Security 11

6.1 Personnel Access to IS....11
6.2 Security Education....11
6.2.1 Initial Training Requirements....11
6.2.2 Ongoing IS Security Education Program....12
7 Physical Security....12
8 Maintenance....12
8.1 Cleared Maintenance Personnel....12
8.2 Uncleared (or Lower-Cleared) Maintenance Personnel....13
9 Media Controls....13
9.1 Classified Media....13
9.2 Protected Media....13
9.3 Unclassified or Lower Classified Media....13
9.4 Media Destruction....14
10 Output Procedures....14
10.1 Hardcopy Output Review....14
10.2 Media Review and Trusted Download....14
11 Upgrade and Downgrade Procedures....14
11.1 Upgrading/Startup Procedures....14
11.2 Downgrading/Shutdown Procedures....15
11.3 Periods Processing....15
12 Markings....15
12.1 IS Hardware Components....15
12.2 Media....15
12.2.1 Unclassified Media Marking....16
12.2.2 Classified Media Marking....16
13 Configuration Management Plan and System Configuration....16
13.1 Hardware Description....16
13.2 Hardware Requirements....17
13.3 Change Control Procedures for Hardware....17
13.3.1 Addition of Hardware....17
13.3.2 Removal of Hardware....18
13.3.3 Reconfiguration of Hardware....18
13.4 Software Description....18
13.5 Software Requirements....18
13.6 Change Control Procedures for Software....19
13.6.1 Addition of Software....19
13.6.2 Removal of Software....19
13.7 Other MSSP Changes....19
14 System-Specific Risks and Vulnerabilities....19
14.1 Risk Assessment....19
15 System Protection Profile....20

1 Introduction

1.1 Purpose

This document serves as the general procedures of a Master System Security Plan (MSSP) for Protection Level 1 peer to peer network systems utilized within an area that is accredited by the Defense Security Service ("DSS"). This MSSP has been written in accordance with DoD 5220.22-M, "National Industrial Security Program Operating Manual, (NISPOM)" Chapter 8 dated February 28, 2006 and ISL 2007-01, ISL 2009-01, Standardization of Baseline Technical Security Configurations, and the ISFO Process Manual. This MSSP consists of these general procedures in addition to the IS Profile and necessary attachments, which describes each accredited IS. The attachments are composed of the following:

- Information System (IS) Profile (required)
- DSS Form 147, Record of Approval for Closed Area (required for Closed Area)
- IS Security Seal Log (for Restricted Areas, if needed)
- Configuration Management Documentation
    - Configuration Diagram (required)
    - Hardware Baseline (required)
    - Software Baseline (required)
- Sample Maintenance, Operating System & Security Software Change Log (required)
- Sample Briefing Acknowledgement Form (required)
- Trusted Download Procedures (required for Trusted Downloads)
- Upgrade/Downgrade Procedures (required for Periods Processing)
- DSS Configuration Tool Output Report or ISSM System Certification Test Checklist (required)
- Sample Relocation Letter (required for Mobile Systems to Government Site)

1.2 Scope

This plan applies to those peer to peer network systems that are accredited for Protection Level 1. This requires all users of the system to have the appropriate personnel security clearance (PCL), formal access approvals, and need-to-know for all information stored or processed by the IS at the time of their access. The confidentiality level of concern for this system is specified in the Section 15. Integrity or availability levels of concern are specified in the Section 15. This plan does not address controlled interfaces and disaster recovery planning as defined in NISPOM paragraphs 8-700.d. and 8-615, respectively.

1.3 Contract or Program Name and Description of IS Purpose

Contract information and IS description are contained in the IS Profile.

2 Personnel Responsibilities

2.1 Contractor Management

a. Management has established an IS Security Policy addressing the classified processing environment. This policy has been promulgated on company letterhead to all cleared personnel. This policy includes a company commitment to protect classified information and to adhere to the IS requirements of the NISPOM. The policy also provides for disciplinary actions for those personnel who do not comply.

b. Management has appointed an IS Security Manager (ISSM) with oversight responsibility for the development, implementation, and evaluation of the facility's IS Security Program. The ISSM and their contact information is specified in the IS Profile. The ISSM has been trained to a level commensurate with the complexity of the facility's ISs, and management shall ensure that ongoing training occurs as needed.

c. In the absence or unavailability of the ISSM, an ISSO or the FSO may be contacted. A contact list with information for this person(s) is provided in the IS Profile.

2.2 Information System Security Manager (ISSM) Responsibilities

The ISSM has ultimate responsibility for the entire information security program. Following is the list of specific duties the ISSM will perform:

(1) Ensures the development, documentation, and presentation of IS security education, awareness, and training activities for facility management, IS personnel, users, and others, as appropriate.
(2) Establishes, documents, implements, and monitors the IS security program and related procedures for the facility and ensures facility compliance with requirements for IS.
(3) Contacts the Defense Security Service to determine if a risk management evaluation and report is available. The ISSM will then identify and document unique local threats/ vulnerabilities to IS.
(4) Coordinates the facility IS security program with other facility security programs.
(5) Ensures that periodic self-inspections of the facility's IS program are conducted as part of the overall facility self-inspection program and that corrective action is taken for all identified findings and vulnerabilities. Self-inspections are to ensure that the IS is operating as accredited and that accreditation conditions have not changed.
(6) Ensures the development of facility procedures to:
    a) Govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information.
    b) Properly implement vendor supplied authentication (password, account names) features or security-relevant features.
    c) Report IS security incidents to DSS. Ensure proper protection or corrective measures have been taken when an incident/vulnerability has been discovered.
    d) Require that each IS user sign an acknowledgment of responsibility for the security of the IS.
    e) Implement security features for the detection of malicious code, viruses, and intruders (hackers), as appropriate.
(7) Certifies in writing to DSS that each MSSP has been implemented; that the specified security controls are in place and properly tested; and that the IS is functioning as described in the MSSP and IS Profile.
(8) Ensures notification to DSS when an IS no longer processes classified information, or when changes occur that might affect accreditation.
(9) Ensures that personnel are trained on the IS's prescribed security restrictions and safeguards before they are initially allowed to access a system.
(10) Develops and implements general and remote maintenance procedures based on requirements provided by DSS.

2.3 Information System Security Officer (ISSO) Responsibilities

a. Information System Security Officers (ISSOs) may be appointed for each individual IS. The name, phone number and email address of each ISSO is listed in the IS Profile.

b. Following are the responsibilities that may be delegated to ISSOs, at the discretion of the ISSM:
    (1) Develop and implement certification tests as required.
    (2) Prepare, maintain, and implement an MSSP and/or IS Profile that accurately reflects the installation and security provisions.
    (3) Ensure:
        a) That each IS is covered by the facility configuration management program, as applicable.

b) That the sensitivity level of the information is determined prior to use on the IS and that the proper security measures are implemented to protect this information.
c) That unauthorized personnel are not granted use of, or access to, an IS.
d) That system recovery processes are monitored to ensure that security features and procedures are properly restored.

(4) Document any special security requirements identified by the Government Contracting Agency (GCA) and the protection measures implemented to fulfill these requirements for the information contained in the IS.
(5) Implement the facility procedures developed by the ISSM (refer to item 6 above).
(6) Conduct ongoing security reviews and tests of the IS to periodically verify that security features and operating controls are functional and effective.
(7) Evaluate proposed changes or additions to the IS, and advise the ISSM of their security relevance.
(8) Ensure that all active user IDs are revalidated at least annually.

2.4 Users

All IS users shall:

(1) Comply with the IS security program requirements.
(2) Be aware of and knowledgeable about their responsibilities in regard to IS security.
(3) Be accountable for their actions on an IS.
(4) Ensure that any authentication mechanisms (including passwords) issued for the control of their access to an IS are not shared and are protected at the highest classification level and most restrictive classification category of information to which they permit access.
(5) Ensure they protect all output of the IS to the level of processing until reviewed.
(6) Receive an initial user briefing prior to being granted access to the IS and acknowledge, in writing, their responsibilities for the protection of the IS and classified information.
(7) Receive an annual refresher AIS briefing and acknowledge same in writing.

2.4.1 Privileged Users

a. Privileged users (i.e., system, network, and database administrators) are those persons who have the authorizations and accesses to change the configuration of the IS and administer the accounts and access rights of general users. This also includes individuals who make changes to security relevant software. A privileged user shall be cleared to the highest level of IS accreditation and shall be the only person who may have access to those portions of the ISs hardware, software, or firmware that perform security functions.

b. Administrators who are also general users will have two accounts, one account as a general user and one account as a privileged user.

c. Because of their unique role, privileged users are often responsible for performing security-related duties such as escorting maintenance personnel and documenting system hardware and software changes. Privileged users will receive training on when they are required to notify or obtain approval from the ISSM or ISSO when making system changes or performing maintenance.

d. Privileged users have a greater responsibility than ordinary users to ensure they perform their duties in a secure manner. Their actions often set the example for general users. Additionally, their level of access poses the greatest threat of damage to the IS in the event of a mishap. For example, a mistyped command from a privileged account can shut down an IS or delete an entire file system, or leaving a workstation unattended while logged into a privileged account can provide the opportunity for someone to perform a malicious act. Following are guidelines for privileged users to follow:

(1) Privileged accounts are not for casual use. All privileged users will have a non-privileged general access account in addition to their privileged account. The privileged account should only be accessed when special privileges are required to complete specific

actions. Upon completion of these actions, the privileged account should be exited.

(2) The passwords to privileged accounts will be changed at least every 60 days; the exact frequency will be specified in the IS Profile.

(3) When executing privileged commands or programs, privileged users are advised to use full path names to protect from executing strategically placed malicious code. This is primarily applicable to Unix.

(4) Privileged users are advised to make copies of system configuration files before modifying them in order to revert to the saved copy in the event your change causes a system problem. This is primarily applicable to Unix.

(5) System privileges are not to be used for purposes other than gaining access to information or files maintaining the system. Privileged administrators are required to have access to classified information in order to understand and provide service for the systems they administer. System privileges are not to be used for any other purpose. The requirements for "all users" also apply to privileged users.

2.4.2 General Users

General users are all individuals who can input information to or modify information on an IS or who can receive information from an IS without a reliable human review. General users have no additional responsibilities besides those listed for "all users" and are limited from access to security relevant software.

3 Certification and Accreditation

3.1 Certification

Prior to submitting an MSSP, the ISSM will certify by signature on the attestation page that the information presented in the plan is accurate and that all protection measures described in the general procedures have been implemented and are operational. The ISSM System Certification Test Checklist demonstrates the compliance of the IS's configuration to certification requirements.

3.2 Accreditation

Classified processing will not commence on an IS until written accreditation from DSS has been obtained. Accreditation is based upon analysis and evaluation of an IS's hardware and software, its operations, and security safeguards with respect to security risks. This information is documented in the MSSP and submitted to DSS with a formal request for accreditation.

3.3 Reaccreditation

a. All security relevant changes to an IS's hardware and software baseline, its physical security and access controls, and safeguarding policies will be reviewed and approved by the ISSM. These changes will be documented as they occur in the appropriate attachment(s). The ISSM will submit an update for reaccreditation whenever changes occur to the original baseline that impact previously accredited procedures. Security relevant changes can not be made on the system until ODAA has reviewed the change and determined if a reaccreditation is required.

b. Each IS will be re-evaluated for reaccreditation every 3 years. If no changes were made, the ISSM will notify DSS by electronic mail. After verifying the original accreditation was valid, the Designated Accrediting/Approving Authority (DAA) may provide a new accreditation letter to the ISSM.

3.4 Security Testing

a. Security testing verifies the correct operation of the technical and non-technical (procedural) protection measures of the IS. Prior to certification, the ISSM will validate that all safeguards are implemented and operational, and notate the same on the ISSM System Certification Test Checklist or submission of the DSS configuration tool output report.

b. Retesting will occur upon implementation of a new major version of software that supports technical security features and randomly during self-inspections.

3.5 Self-Inspections

a. The ISSM will conduct self-inspections of the IS program as part of the overall facility self-inspection program. Corrective action will be taken for all identified findings and vulnerabilities. Self-inspections shall be performed at least annually on each IS, or as determined necessary/ needed by the ISSM. The following are examples of incidents wherein this may be warranted: 1) a suspected compromise, 2) multiple security violations on the system, or 3) following significant changes in system security requirements.

b. At a minimum, the following will be verified during a self-inspection: authorized users and briefing records; configuration management (i.e., Is the IS current and certified?); technical and procedural security features; and audit records and logs.

3.6 Self-Certification of Similar Systems

a. Self-certification is based on similar systems. A similar system is defined as a system that operates in the same operating environment, classification level, system type (Single-User Non-networked, Multiuser, Non-networked and Peer to Peer LAN, or Domain Controlled LAN), similar operating system(s), and similar operations (trusted downloads, periods processing, mobile system, etc) as indicated in Section 15 of the MSSP or the IS Profile accredited by DSS which will be the basis for all self-certified systems under the approved master plan.

b. Self-certification authority must be specified in writing in the accreditation letter received from the DAA. ISSMs who have demonstrated an appropriate level of training and knowledge of IS requirements for the complexity of ISs within their facility may be granted self-certification authority. Self-certification is no longer valid if the ATO granting the self-certification expires, is withdrawn, or revoked.

c. The ISSM will self-certify new information systems. The ISSM must update/maintain a listing of all systems accredited by the Cognizant Security Agency (CSA) and those self-certified by the ISSM under an approved MSSP since the last annual security review. The MSSP IS tracking form from the ISFO Process Manual is to be used to maintain this list. When a system is self certified, the following documentation must be included with the self certification packet maintained with the IS:
   - Copy of the MSSP Accreditation letter.
   - Copy of the approved MSSP.
   - Signed self-certification letter identifying the date of certification and the MSSP used for certification.
   - Complete IS Profile and supporting documents

d. Master plans will not be written for any system requiring a variance or waiver. Only those systems that are NISPOM compliant may be self-certified.

e. The ISSM will follow the detailed guidance in the DSS ISFO Process Manual for the managing and reporting requirements of self-certified systems.

4 Information System Profile

Refer to individual IS Profiles for information on the purpose and usage of each IS including contact information and system identification. Section 15 of this document describes the specifics of the non-technical security features and safeguards to be implemented on the IS. This includes clearance and sanitization procedures, sensitivity level, user information, system specific risks and vulnerabilities, and special procedures.

4.1 Pure Servers

As this MSSP is for peer to peer network systems, this plan does not include pure servers, as referenced in NISPOM Chapter 8, paragraph 503.

4.2 Tactical, Embedded, Data-Acquisition, and Special Purpose Systems

As this MSSP is for standard peer to peer network systems, this plan does not include these types of systems, as referenced in NISPOM Chapter 8, paragraph 504.

4.3 Mobile Systems

If this peer to peer network system includes a component that is a mobile system it will be specified in Section 15. The specific guidance from the ISFO Process Manual will be followed for any mobile system.

5 Protection Measures

5.1 Accounts and Logons

5.1.1 Identification and Authentication Management

a. Logon authentication has been implemented on all ISs. Each user of an IS will be assigned a unique identifier, commonly referred to as an user ID. Each user ID has an associated personal password that serves as an authenticator. Prior to being granted access to an IS or any of its resources, users must present their uniquely assigned user ID and authenticator as proof of their identity. Their unique user ID will be associated with all auditable actions taken by that individual.

b. Following are the requirements for identification and authentication management:
   (1) User IDs will be established after the user's clearance and need-to-know has been validated and they have received an AIS briefing from the ISSM/ISSO regarding their IS security responsibilities.
   (2) The ISSM/ISSO or delegated privileged user may establish the initial password, relay same to the user, and the user shall be required to establish his/her own unique password upon their initial login. It is preferable that this is done as soon after the account creation as possible.
   (3) Active user IDs shall be revalidated at least annually. This will be accomplished by verifying the clearance and need-to-know of each user associated with each active account.
   (4) Prior to reuse of a user ID, all previous access authorizations will be removed from the system. This will include file ownerships (accesses) for that user ID.
   (5) When an IS user terminates, loses access to the system for cause, or no longer has a reason to access the IS, that individual's user ID will be disabled or removed from the system.
   (6) Individual authenticators will not be shared with anyone.
   (7) Access to authentication data will be restricted to authorized personnel through the use of encryption or file access controls, or both.

5.1.2 Requirements for Passwords

Following are requirements for all passwords:

(1) Shall be protected at the highest classification level and most restrictive classification category of information to which they permit access.
(2) Shall contain a minimum of fourteen alpha/numeric upper/lower case and special characters.
(3) Users will be briefed not to use dictionary definable passwords to include sport names, pets, or family members.
(4) Shall be changed at least every 60 days; the exact frequency will be specified in the IS Profile.
(5) Shall be changed when compromised.

(6) Shall not be displayed to the screen when input, and users shall take measures to prevent others from viewing their password while being entered.
(7) The operating system shall provide technical enforcement of password requirements.

5.1.3 Guidelines for User-Generated Passwords

Following are some guidelines for selecting user-generated password

(1) Do not include personal information like the name of the street you live on or the model of your automobile.
(2) Do not use phone numbers or special dates (e.g., birthday, anniversary), license plate numbers, etc.
(3) Choose a password that is both difficult to guess, but is easy to remember so there will be no temptation to write it down.
(4) It is easy to choose a good password; for example, Time4U2go2bed!, ifly2High4U2C!, bigb&sR2hip4me, ih2Prcnp4s4or! (acronym for "I hate to pick really complex new passwords for security for obvious reasons!").

5.1.4 Generic or Group Accounts

Operating systems and many commercial off the shelf (COTS) applications come pre-installed with generic or group accounts (group authenticators). Many generic or group accounts (e.g. system, root, and administrator) have special accesses or privileges associated with them. For the purpose of this MSSP, all generic or group accounts (i.e., GUEST, FIELD, NOBODY, etc.) will be deleted or disabled, with the following exceptions only:

(1) Although extremely rare, generic or group accounts may be permitted where required by software or otherwise necessitated for work to be accomplished. A statement certifying this must be provided in writing by the ISSM and receive the approval of the CSA. When group accounts are used, manual logs (or other methods) should be utilized to assure individual accountability.

5.2 Session Controls

5.2.1 Logon Banner Requirements

The following DSS approved banner will be displayed prior to initial user login. The user will be required to take positive action to remove the banner from the screen.

DoD Warning Banner

Use of this or any other DoD interest computer system constitutes a consent to monitoring at all times.

This is a DoD interest computer system. All DoD interest computer systems and related equipment are intended for the communication, transmission, processing, and storage of official U.S. Government or other authorized information only. All DoD interest computer systems are subject to monitoring at all times to ensure proper functioning of equipment and systems including security devices and systems, to prevent unauthorized use and violations of statutes and security regulations, to deter criminal activity, and for other similar purposes. Any user of a DoD interest computer system should be aware that any information placed in the system is subject to monitoring and is not subject to any expectation of privacy.

If monitoring of this or any other DoD interest computer system reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring of this or any other DoD interest computer systems reveals violations of security regulations or unauthorized use, employees who violate security regulations or make unauthorized use of DoD interest computer systems are subject to appropriate disciplinary action.

Use of this or any other DoD interest computer system constitutes a consent to monitoring at all times.

5.2.2 Successive Logon Attempt Controls

Repeated unsuccessful logon attempts may indicate someone attempting to access an account by guessing the password. In order to prevent someone from being able to do this until the password is guessed (possibly by use of a program) most operating systems provide the ability to thwart these attempts. Lockouts for multiple failed logins will occur after no more than 3 unsuccessful attempts. The account will remain locked for at least 60 minutes or must be unlocked by an administrator. Refer to the IS Profile of each for specifics on the configuration of logon attempt controls.

5.2.3 System Entry Conditions

IS entry is based upon users having an account (i.e. user profile) on each system to which they require access. Users' initial logins must include the entry of both their unique user ID and password. It shall always be required that each and every user authenticate into the IS using an unique user ID and password.

5.3 Access Controls

a. All persons granted an IS user account will have the requisite clearance and need-to-know for all information in the IS. Technical access control features are not required to segregate access to classified information within the system. File permissions will be used to prevent general users from accessing security relevant operating system files.

b. The following types of files and directories will be protected from access by non-privileged general users:

(1) Files containing authentication data (passwords) will be protected from modification. If passwords are not encrypted within the file, they will be protected from viewing.
(2) Files containing system and network configuration data will be protected from modifications.
(3) System startup and shutdown files will be protected from modifications.
(4) Applications or commands that provide the ability to change the system or network configuration will be protected from execution and modification.
(5) Applications or commands that provide the ability to add, remove, or change user access information will be protected from execution and modification.
(6) Files that contain audit information will be protected from viewing and modification.
(7) Applications or commands that provide the ability to change the audit configuration or to access audit information will be protected from execution and modification.
(8) Virus detection software will be protected from modification.

c. Boot proms and setup memory (e.g. BIOS) will be protected from modification by general users by the establishment of passwords which shall contain fourteen characters (when technically capable). The BIOS shall be configured so that no bootable media or device unknown to the ISSM/ISSO may boot the system and compromise the security of the system and the data thereon.

5.4 Audit Requirements

a. Audit records will be maintained and reviewed from the date of IS approval until withdrawal of accreditation. Audit records shall include the following.
(1) Enough information to determine the action involved, the date and time of the action, the system on which the action occurred, the system entity that initiated or completed the action, and the resources involved (if applicable).
(2) Successful and unsuccessful logons and logoffs.
(3) Unsuccessful accesses to security-relevant objects and directories.
(4) Changes to user authenticators.
(5) The blocking or blacklisting of a user ID, terminal, or access port.
(6) Denial of access from an excessive number of unsuccessful logon attempts.

Audit records will be protected against unauthorized access, modification, or deletion and will be retained for the previous 12 months.

b. The IS has been configured to automatically create and maintain an audit trail or log to record security-relevant activities of the IS.

c. In addition to the above security relevant system events, audit records will be maintained for the activities listed below. A single record or log may document multiple types of activities.
   (1) User briefing statements.
   (2) Additions, deletions, reconfiguration, and repair actions to accredited hardware.
   (3) Installation, modification or testing of operating system and security related software.
   (4) Actions taken to sanitize IS components.
   (5) The placement and destruction of security seals.

d. A review of all IS audit records will be performed weekly by the ISSM or ISSO, if appointed. If analysis of the audit records reveals unauthorized actions that are not easily explainable, the details will be reported to the ISSM for review and further action as necessary. Any incident that involves suspected compromise of classified information will be immediately reported to DSS. Below are guidelines for reviewing automated audit records:
   (1) Verify that the automated audit functions are performing properly and there are no time periods during which audit data is missing.
   (2) Review all failed logins. Question multiple failed login attempts and account lockouts.
   (3) Review a sampling of successful logins to ensure those persons were actually present and using their account during the recorded time periods. For example, if you are aware of someone being on travel or on vacation during the week, verify his or her account was not accessed.
   (4) Question login sessions that occur at unusual times (e.g. 2 am) or sessions that are left open for long periods of time (i.e., over 24 hours)
   (5) Scrutinize direct logins to generic or group accounts. Verify they are within the guidelines specified in the MSSP.
   (6) If applicable, verify accesses to privileged group/generic accounts were made from authorized user IDs.
   (7) Depending on the available audit mechanism, failed attempts to access objects may be all inclusive rather than limited to security-relevant objects. Attempt to focus your review on identifying any user ID that consistently has failed access attempts to privileged system files.

5.5 System Recovery and Assurances

a. The IS has been configured to ensure that all security mechanisms (e.g., auditing, virus detection) are automatically enabled during the IS startup/boot process.

b. System assurance includes maintaining the reliability of those components of a system (hardware, software and firmware) that are essential to enforcing the security policies of the system. Procedures for maintaining the reliability of the hardware are provided in Section 7, “Physical Security”, and Section 13, “Configuration Management and System Configuration.” Procedures for maintaining the reliability of the IS software are outlined in Section 5.3 “Access Controls” and Section 13, “Configuration Management and System Configuration”. Procedures for maintaining the reliability of the IS communications are provided in Section 5.7 “Data Transmission Protection”. The ISSM, or if designated, the ISSO is responsible for ensuring that system assurance is maintained.

c. System recovery is performed by the ISSM or designee only by using either:
   (1) Protected copies of the original operating system disks.
   (2) Images (ghost) from original configuration or full recovery disks.
   (3) Restored data files from system backups.

(4) Once restored, an ISSM System Certification Test Checklist (attachment 12) will be completed and all security settings verified before the system is returned to service.

d. If system recovery operations do not work or any abnormal operation arises during recovery, the system will be powered off and all classified media (including hard disk drive (HDD)) will be removed. It will be the responsibility of the ISSM or designee to determine if the remainder of the system hardware (unclassified 'sanitized') is usable at which point a new HDD can be procured and the recovery operation can be resumed.

5.6 Virus and Malicious Code Detection

a. Malicious code is a broad term for any software that is detrimental to the operation of an IS. A virus is a specific type of malicious code that replicates itself from one file or system to another and may infect an entire network very rapidly if not detected.

b. Virus detection software shall be employed and configured to automatically check all files that are opened or accessed on the IS.

c. The following policies and procedures to detect and deter incidents caused by malicious code, such as viruses or unauthorized modifications to software will be implemented.
   (1) All files and media will be checked for viruses using a current virus detection tool prior to, or at the time of introduction to an IS.
   (2) Virus signature files will be updated at an interval not to exceed 30 days.
   (3) The antivirus executable software will be updated within 30 days of being available.
   (4) When a virus is detected, the user will discontinue interaction with the infected IS and immediately notify the ISSM and/or ISSO. If a preliminary investigation reveals compromise or suspected compromise, the ISSM will immediately notify DSS.
   (5) COTS software will be tested to provide reasonable assurance that malicious code or security vulnerabilities do not exist. This will be accomplished by installing and using the product in an unclassified environment prior to usage in a classified environment.
   (6) Vendor-provided security patches will be installed on a periodic basis.
   (7) Contractor software that is not developed by cleared personnel will be reviewed by cleared personnel.

5.7 Data Transmission Protection

As this IS is a standard peer to peer network implementation, no communication to another IS is permitted.

5.8 Clearance & Sanitization

5.8.1 Clearing

a. Clearing is the process of removing the data on media or devices before permitting access by personnel without the proper clearance, need-to-know, or formal access approvals. All internal memory, buffer, or other reusable memory shall be cleared to effectively deny access to previously stored information.

b. IS devices will be cleared during upgrade and downgrade of an IS, when individual devices are added or removed from an IS, and when required for maintenance purposes. The cleared devices/media will remain within the approved IS physical safeguards. Clearance actions include visual inspection, removal of classified media and materials, and removal of power to clear classified data from volatile memory.

5.8.2 Sanitization

a. Sanitization actions include visual inspection, the removal of classified media and materials, removal of power from volatile memory devices, and the destruction of non-volatile memory (see section 9.4).

b. IS systems will be sanitized when the system is no longer needed for classified processing.

5.9 Protection Measure Variances

A description of any approved variances from protection measures will be included in individual IS Profiles including a copy of the approval documentation received from DSS. Implementation of any variances may not begin until written approval is received from DSS.

5.10 Managing Wireless and other I/O Devices

Wireless and other devices such as infrared (IR), bluetooth and firewire are not permitted on this information system.

6 Personnel Security

6.1 Personnel Access to IS

a. Prior to being provided a classified user account the ISSM or ISSO will verify the personnel security clearance and need-to-know of the user and brief the user on their responsibilities for using the IS.

b. Each user will be required to complete and sign the “Acknowledgement of Briefing for AIS Users” Form. This form will serve as the user's acknowledgement of their responsibilities for the protection of the IS and classified information, and documents their clearance level and access privileges.

c. Access termination to an IS will occur in a timely manner whenever an user is no longer employed, has a reduction in level of clearance or no longer possesses the appropriate need-to-know. The user or his/her supervisor will be responsible for notifying the ISSM or ISSO of changes in an IS user's status. The ISSM or ISSO will ensure user IDs are disabled or removed from the IS.

6.2 Security Education

The ISSM shall develop and implement an ongoing IS security education program. Security awareness training will be provided prior to authorizing an individual access to an IS and updated as needed.

6.2.1 Initial Training Requirements

Initial security awareness training will encompass all IS security requirements for which an individual will be responsible. Depending on job function, responsibilities will vary. Anyone who is designated as an ISSO or alternate will receive an in-depth briefing from the ISSM prior to assuming the responsibilities of that position. IS users will be briefed by the ISSM or ISSO. At minimum, authorized IS users will be aware of the company’s IS security policy, methods for controlling access to the area and the IS, password requirements, limitations on removing IS hardware and software from the controlled area, requirements for review of output from the IS, and procedures for reporting security related incidents. If responsible for maintaining hardware or software on the IS, the user will additionally be briefed on hardware and software configuration control and maintenance procedures. All users will read and sign the “Acknowledgement of Briefing for AIS Users” acknowledging their responsibility to protect the IS and classified information.

6.2.2 Ongoing IS Security Education Program

At a minimum, IS security re-briefings shall occur annually and records of these re-briefings shall be maintained. Additional re-briefing shall occur whenever an IS user is directly involved in or responsible for the breech of any IS security policy, or when there is a change to the security procedures for which an IS user is responsible.

7 Physical Security

Safeguards have been established to prevent or detect unauthorized access to the IS and unauthorized modification of the IS hardware and software. Hardware integrity of the IS shall be maintained at all times. The location of the IS system will be specified in the IS Profile.

(1) Restricted areas may be established for an IS when the IS has all removable media and classified processing will always be attended by an appropriately cleared individual. A restricted area must have an identifiable boundary (for example, walls, signs, tape on floor, ropes or chains) where it is obvious that the area is restricted to authorized personnel. During classified processing sessions, users will exercise constant surveillance and control of the IS and safeguards will be in place to prevent visual access to classified information by unauthorized individuals. When the IS has been downgraded (cleared) and all classified media removed, safeguards will remain in place to detect or prevent tampering or theft of the IS hardware

(2) Closed areas are required for ISs that have non-removable media and/or will remain in a classified mode while unattended. All personnel granted unescorted access to an IS closed area will have an appropriate security clearance and need-to-know for the area. Should the integrity of a closed area be violated, or if unauthorized modification of hardware or software is suspected, the ISSM will be notified prior to the continuance of classified processing. The ISSM will conduct an investigation and take appropriate actions as needed.

8 Maintenance

Maintenance should always be performed by cleared personnel. The ISSM must be notified when an IS requires maintenance. Maintenance may involve reaccreditation, as outlined in Section 3.3 “Reaccreditation”. The following requirements apply to all maintenance actions, regardless of the clearance level of the person performing the maintenance:

(1) Addition and removal of hardware and software will be in accordance with the change control procedures discussed in Section 13, “Configuration Management and System Configuration”.

(2) If security seals have been broken as a result of maintenance, they will be re-applied with actions documented in the security seal log.

(3) Prior to release, accredited IS equipment having memory or data retention capabilities will be sanitized as described in Section 5.8 “Clearance and Sanitization.”

(4) All maintenance to the accredited IS equipment will be documented in the Maintenance, Operating System and Security Software Change Log.

(5) Vendor-supplied software used for maintenance must reside on read-only or write-protected media marked “For Maintenance Use Only”.

8.1 Cleared Maintenance Personnel

Maintenance personnel who are cleared to the highest classification level of information on the system and have formal access approvals for all information processed on that system will not be escorted if need-to-know controls can be implemented. When cleared maintenance personnel do not have a need-to-know for the classified information on the IS an appropriately cleared and technically knowledgeable person will be present within the area where the maintenance is being performed to ensure that security procedures are being followed. Refer to individual IS Profiles for a description of cleared personnel performing maintenance and escort requirements employed.

8.2 Uncleared (or Lower-Cleared) Maintenance Personnel

When appropriately cleared personnel are unavailable to perform maintenance, an uncleared or lower-cleared person may be used. An appropriately cleared and technically knowledgeable escort will monitor their activities. Refer to individual IS Profiles for a description of uncleared personnel performing maintenance and escort requirements employed. Uncleared maintenance personnel must be U.S. citizens.

When scheduling an outside repair person for maintenance, question them as to the type of equipment/ materials they will need for evaluation of the problem. ISSM approval will be obtained to bring in any maintenance tool, diagnostic or any other device to be used to service an accredited IS. Special attention should be given to portable units containing memory and/or have retention capabilities. These devices may require accreditation by DSS.

Prior to admittance of any uncleared maintenance personnel, the area will be inspected to verify that no classified material is remaining within visual access.

Prior to maintenance, the IS will be downgraded and all non-volatile data storage media will be removed or physically disconnected and secured. The separate, "UNCLASSIFIED – FOR MAINTENANCE ONLY", copy of the operating system and diagnostic routines will be loaded. If it is not feasible to clear the IS or if clearance will impede maintenance activities, the following procedures will be followed: The technically knowledgeable escort will log into their account. If possible, the escort will remain in control of the keyboard and take instructions from the maintenance person on activities to perform. If the uncleared person is given keyboard access the escort will monitor all input and output to the IS (i.e. keystroke monitoring) to ensure only system files are accessed and no user files are viewed.

9 Media Controls

IS media is any material with retention capability on which IS software or data is stored. Media includes, but is not limited to, disks, battery backed RAM, FLASH, PROMS, EEPROMS, UVPROMS as well as analog, video, and digital tapes. Refer to section 12 for media marking requirements.

9.1 Classified Media

Classified media is any media which fits any of the following descriptions:

1) Media containing classified data
2) Media that was or is mounted without write-protection enabled on a classified IS

This is most often media that has been specifically designated for the storage of classified information. This may also include media containing software that writes scratch or paging files and therefore will not operate in a write-protected mode. Immediately upon the loading/creation of classified information, the media/device will be labeled with all required markings, safeguarded, and brought into accountability.

9.2 Protected Media

Protected media is any UNCLASSIFIED media dedicated to and repeatedly used for the operation of the IS, such as diagnostics, "UNCLASSIFIED – FOR MAINTENANCE USE ONLY", boot media, and software installation media. This media will always be mounted on the IS in a write-protected state.

9.3 Unclassified or Lower Classified Media

Unclassified or lower classified media will be write-protected during use. If not write-protected, it must be considered classified to the level of information on the IS. Write-protection mechanisms will be verified each session (i.e. once per day) during which unclassified media is used. Write-protect mechanisms are tested by attempting to write to the media.

9.4 Media Destruction

a. IS media may be destroyed by incinerating, smelting, mutilation, chemical decomposition, or pulverizing (e.g. hammer mills, choppers, and hybridized disintegration equipment).

b. When destruction is performed, the action of removing any media specified in the hardware baseline from the IS controlled area and delivering it to the security office or FSO for destruction will be documented in the Maintenance, Operating System and Security Software Change Log.

c. Media destruction methods will be specified in Section 15 of this document.

10 Output Procedures

All output from an IS will be handled at the level of system processing until a comprehensive review (in human-readable form) is performed by an appropriately cleared and knowledgeable person. Classified output will be properly marked, protected, and brought into accountability. This section provides the requirements for the proper review of unclassified and lower classified materials from the IS. The reviewer is responsible for determining the proper classification of any output. When large volumes of unclassified/ lower classified materials need to be output from an IS, alternative methods for performing automated or sampling reviews shall be accredited by DSS on a case-by-case basis.

10.1 Hardcopy Output Review

If a user is familiar with a file and is familiar with its contents, the user may review by scanning the output to verify this is indeed the unclassified file the user has been working with. If the user generates a hardcopy of information they are not familiar with or have not recently accessed, they must review the output to verify it contains no information classified higher than intended. All documents must be examined in their entirety, unless the document exceeds 25 pages, then a 20% sampling rate must be implemented.

10.2 Media Review and Trusted Download

For the purpose of this MSSP, the use of trusted downloading will be specified in Section 15.

If authorized, trusted download procedures will be the DSS trusted download procedures available at http:// www.dss.mil. All users who have a need to perform trusted download will be trained and authorized in writing by the ISSM/ISSO. An administrative record of each trusted download action will be generated and retained.

11 Upgrade and Downgrade Procedures

Prior to and after processing classified information, actions will be taken to ensure the security and reliability of the IS, its associated media, and the physical area in which it resides. The following are the general procedures for performing upgrade and downgrade. Refer to the IS Profile for specific upgrade/ downgrade procedures.

11.1 Upgrade/Startup Procedures

To adjust the IS to a higher security level, the following will be performed:

(1) All unauthorized personnel will be removed from the IS area or precluded access to the IS.
(2) The physical integrity of the area will be verified and any required modifications/controls will be imposed such as placing covers over windows.
(3) Obtain from approved storage all classified/protected media and material needed to perform the upgrade.
(4) Ensure that all previous processing on the IS has ceased. Then, shutdown the system to be upgraded.

(5) If used, inspect IS security seals.
(6) Physically disconnect and/or switch all non-accredited networks, systems or components. Verify that all remaining communications links are to ISs that will be processing at the same sensitivity level.
(7) Clear the volatile memory of the IS and all peripheral devices by removing power for 30 seconds.
(8) Install required classified media on the IS.
(9) Power on and boot the system, verifying no errors.
(10) Ensure that applicable audit records (automated and/or manual) are initiated.

11.2 Downgrade/Shutdown Procedures

To adjust the IS to a lower security level, the following will be performed:

(1) Ensure that all previous processing on the IS has ceased.
(2) Ensure that all classified media/material which was created or utilized during the classified processing session, but which is not needed for the downgrade process, is removed from the IS. This includes a visual inspection of printer paper paths to ensure they are clear.
(3) Ensure this material is properly marked, and then either secured in an approved container or disposed of as classified waste.
(4) Any media which will be utilized for an unclassified or lower classified processing session will be sanitized.
(5) Perform an orderly system shutdown.
(6) Physically remove all classified disk drives.
(7) Clear the volatile memory of all remaining devices by removing power for 30 seconds.
(8) Remove and store in an approved container all classified/protected media/material, such as printer ribbons, internal wax roll cartridges, disks, and media required for clearing procedures.
(9) Ensure that all applicable records and logs have been completed.

11.3 Periods Processing

Periods processing is a method of sequential operation of an IS that provides the capability to process information at various levels of sensitivity at distinctly different times. For example, using an IS with all removable media for unclassified processing in the morning and classified processing in the afternoon. An IS employed in periods processing will have separate media for each period of processing, including copies of operating systems, utilities, and applications software. The appropriate upgrade/downgrade procedures will be performed before transitioning from one period to the next and the action will be documented. Periods processing will be specified in the IS Profile for this IS.

12 Markings

Markings on classified hardware, hardcopy output (paper, film and other printed media), and media will conform to the requirements of Chapter 4 of the NISPOM. It is recommended that internal file markings be included in electronic files to facilitate proper markings upon output.

12.1 IS Hardware Components

a. IS hardware components that have the potential to retain classified information will have a conspicuous external label identifying the highest level of classified processing.
b. Co-located unclassified systems will be conspicuously labeled to indicate they are for unclassified processing.

12.2 Media

All media will have the appropriate markings clearly labeled on the exterior. When media is contained within another component, the outermost surface should also be labeled if the interior label is not visible. When the surface or size of the media is not appropriate for all required markings, contact the ISSM for guidance. The required markings for all media are outlined below. Media will be handled in accordance with the details of Section 9.

12.2.1 Unclassified Media Marking

All unclassified media within the IS controlled area will be clearly marked upon breakage of the original external wrapping or when introduced into the IS area. The media will be labeled “Unclassified”. Vendor media that retains its original markings and that has not been altered is considered to be unclassified and does not require additional marking.

12.2.2 Classified Media Marking

Classified media will be marked in accordance with NISPOM 4-200. As a general rule, the following markings are required for all classified media:

Overall classification level
Applicable special markings e.g., NATO
Name and address of originating facility
Unclassified title
Creation date
"Derived from" line
"Declassify on" line
Control number

13 Configuration Management Plan and System Configuration

This section describes a process of using the baselines and revision log for documenting all security relevant IS changes. This is normally the official record of security approval of IS changes.

a. The configuration management (CM) program ensures that protection features are implemented and maintained on the IS. CM is defined as the formal change control process of all security relevant aspects of the IS.

b. The following CM procedures describe the approval and documentation process for changes to any IS hardware, software, and security documentation. The ISSM or ISSO will be responsible for authorizing all security relevant baseline changes to the IS Profile to include hardware, software, procedures, reports, and audit records. In cases where the change impacts upon previously accredited procedures, reaccreditation by DSS will be required prior to implementation. The hardware and software lists will show the current baseline.

c. The CM program will be periodically verified during internal self-audits to ensure it is working effectively and that changes outside the CM process are not permitted. Verification will be accomplished by a physical audit of the hardware and software currently in use on the IS against the hardware and software baselines.

13.1 Hardware Description

a. The hardware baseline includes a list of all IS components that process classified information and contain memory.

b. A configuration diagram depicting the system architecture, with all component and system interconnections, is attached to the MSSP.

c. The type of information required is based upon whether the device retains classified information when power is removed. Following are guidelines to make this determination.
   (1) Disks (e.g. floppy, hard, zip, jazz, CDs, etc.) that are not write-protected during classified processing sessions shall be treated as classified.

(2) If the device contains media or components intended to store classified information, it shall be treated as classified. For example, an EEPROM loaded with classified software by the contractor.
(3) If the device contains non-volatile memory that is not writable as installed within the component (e.g. PROM, UVPROM), and contains unclassified information (e.g. configuration or calibration data), it may be treated as unclassified.
(4) If the device contains non-volatile components that are intended for the storage of unclassified information and is only accessible through a controlled menu driven program (e.g. PC boot configuration) that only provides selectable options and does not provide the ability for the user or system to input information, this may be treated as unclassified.
(5) If the device contains non-volatile components that are writable (e.g. EEPROM, FLASH) but requires specialized software in order to access the component, and this software is not installed on the system, this may be treated as unclassified.
(6) If the system or users have the ability to write information of their choosing to non-volatile components, this must be treated as classified.
(7) Optical disk devices (e.g., CD, DVD) require evaluation to determine if they have write capabilities.
(8) Test equipment often has non-volatile components with storage capabilities and requires additional considerations. You must ascertain whether the data being stored is classified under the applicable security classification guide. For example, a digital power meter that stores power measurements. If power measurements are classified according to the contract, the device is considered classified. If power measurements are not classified, the device may be treated as unclassified.

d. The IS hardware baseline shall include all components that may be sanitized by removal of power: device type, manufacturer and model, and types of memory. For each device that has a sanitization procedure other than removal of power, the following additional information must be provided: the size/capacity of all memory and media that retains classified information, and an identifier (e.g. serial number, inventory control #) suitable for tracking changes. The physical location of each system and/or device shall be specified in the baseline, or an equivalent system (for example bar-coding) shall be used which can locate the IS components.

13.2 Hardware Requirements

a. Hardware will be examined to determine that it appears to be in good working order and has no elements that might be detrimental to the security operation of an IS when placed under facility control and cognizance. For example, the following will be considered: the existence of infrared ports, RF antennas, and built-in microphones on systems/equipment to be accredited, or on unclassified systems resident within the area. Subsequent changes and developments that affect security may require additional examination.

b. Physical protection of the device will begin prior to, or immediately after examination.

c. Installation of hardware will be performed by authorized and technically knowledgeable personnel.

d. Hardware containing memory or media that has the potential to retain classified information must be treated as classified unless alternative methods such as write-protection are employed to prevent storage of classified information. A firmware password protection mechanism shall be used in the BIOS of the IS and shall contain fourteen characters (if technically capable).

13.3 Change Control Procedures for Hardware

13.3.1Addition of Hardware

When new components or devices are required for classified usage the following procedures will apply:

(1) Verify the new system or device has been authorized through the CM process.

(2) If the device retains information when power is removed, label the component or media per Section 12.
(3) Connect the device and perform the upgrade procedure.
(4) If the system or device has security relevant features configure those features in accordance with the MSSP.
(5) Document these actions on the Maintenance, Operating System and Security Software Change Log.
(6) Notify the ISSO or ISSM to complete the required certification to validate the correct operation of technically implemented security features.

13.3.2 Removal of Hardware

If an accredited device is being removed from the IS the following procedures will apply:

(1) Perform the downgrade procedure. If the device is to be removed from physical controls it must be sanitized as described in Section 5.8, "Clearance and Sanitization".
(2) If present, remove all seals classification labels.
(3) If accreditation is being withdrawn, contact the ISSO or ISSM for updating of the hardware baseline.
(4) Document removal and/or sanitization of the device on a Maintenance, Operating System and Security Software Change Log.

13.3.3 Reconfiguration of Hardware

While the ISSO or ISSM shall primarily perform these duties, appropriately cleared individuals may be delegated to reconfigure accredited systems provided no currently accredited security procedures are affected. When moving devices from one accredited system to another under, appropriate clearance procedures must be performed unless both source and destination systems are operating at the same sensitivity level. All reconfiguration actions will be documented in the Maintenance, Operating System, and Security Software Change Log.

13.4 Software Description

The IS software baseline includes the name, vendor, and major version number or release number of all security-relevant software (e.g. operating system, access control, sanitization, virus scanning software, etc.)

13.5 Software Requirements

a. Software from unknown or questionable sources will not be used on an IS.

b. The use of personal or public domain software is discouraged and each installation of such software will be approved by the ISSM.

c. From the earliest feasible time all IS software will be stored on media that is safeguarded to the highest level of intended processing.

d. Installation and modification of software will be performed by authorized personnel who are knowledgeable of the computer system and the software being installed.

e. Software will be loaded from media that is write-protected.

f. Per section 5.6 "Viruses and Malicious Code Protections", software will be screened and/or tested for malicious code or logic.

g. Unclassified software that will eventually be used during classified processing periods must either be developed by cleared, knowledgeable personnel or reviewed and/or tested by cleared, knowledgeable personnel. This includes operating system, virus detection, and software sanitization software. The best method to safeguard is to develop the software on the classified system. If developing the software in an unclassified environment you must restrict uncleared persons

from having the ability to access the software. This can be accomplished through strict control of file permissions. You must ensure that all users with access, including privileged administrators, have the appropriate clearance.

h. Software disconnects are not permitted on ISs that process at the TOP SECRET level.

13.6 Change Control Procedures for Software

13.6.1 Addition of Software

a. Verify the software to be added has been authorized through the CM process.

b. Verify that all software requirements as specified in Section 13.5, “Software Requirements" have been met.

c. If the software includes security relevant features, verify that the ISSM or ISSO has completed the required certification tests to validate the correct operation of technically implemented security features.

d. Document the installation of operating system and security relevant software in the Maintenance, Operating System, and Security Software Change Log.

13.6.2 Removal of Software

a. Removal of any security-relevant software (operating system, access control, sanitization) will be reported to the ISSO or ISSM.

b. The ISSO or ISSM will be responsible for updating the software baseline and ensuring a certification test is conducted and documented if the change will impact the IS.

13.7 Other MSSP Changes

All other non-hardware and software changes to the MSSP will be reviewed and approved by the ISSO or ISSM. The review will assure that the proposed change complies with the IS security requirements of the NISPOM. If the change impacts previously accredited procedures, reaccreditation by DSS will be required. The ISSM will assure that the MSSP revision log is used to document the review and certification of all changes by DSS and/or the ISSM.

14 System-Specific Risks and Vulnerabilities

14.1 Risk Assessment

Systems under this MSSP have no known threats or vulnerabilities requiring mitigation. All NISPOM Chapter 8 requirements are met or exceeded and signified by the ISSM’s signature to the ISSM System Certification Test Checklist.

Risk is the possibility that a particular threat will adversely impact an IS by exploiting a particular vulnerability. A threat may be defined as a potential for the accidental or deliberate compromise of security. A vulnerability is a weakness or lack of controls that would facilitate or allow a threat to actuate. Risk assessment is the process of analyzing threats and vulnerabilities of an IS and the potential impact resulting from the loss of information or capabilities of a system. This analysis is used as a basis for identifying appropriate and cost-effective security countermeasures.

a. NISPOM Chapter 8 requires the ISSM to determine if any unique local threats or vulnerabilities exist for an IS. At minimum, this will include an evaluation to determine if any requirement of Chapter 8 has not been fully implemented for the IS; including requirements which have an “if technically feasible” caveat. If present, the ISSM will consider the use of countermeasures to mitigate the risk associated with the vulnerability.

b. There are no unique threats or vulnerabilities to this IS, or if present, a description of the vulnerability and the countermeasures implemented will be described.

15 System Protection Profile

The following information specifies the configuration for the IS that is to be accredited. Each MSSP includes a section that describes the IS and specifies the non-technical security features and safeguards to be implemented on the IS. This includes clearance and sanitization procedures, sensitivity level, user information, physical location and safeguards, identification & authentication management, IS maintenance procedures, software protections, system specific risks and vulnerabilities, and special procedures.

Operating Systems	
Operating System Name (e.g., Microsoft Windows XP)	Version # or Release (e.g., SP3)

Protection, Sensitivity Level, and User Information	
Protection Level ☒ **1** **Highest classification level of data:** ☐ Confidential, Basic Confidentiality Level of Concern ☐ Secret, Medium Confidentiality Level of Concern ☐ Top Secret, High Confidentiality Level of Concern **Category(s) of Info:** ☐ COMSEC ☐ RD ☐ FRD ☐ FGI ☐ Other: **Formal access approvals:** ☐ No ☐ Yes. If Yes, indicate ☐ NATO ☐ CNWDI ☐ Crypto	**Levels of Concern**: Integrity ☐ High ☐ Medium ☐ Basic ☒ Not Contractually Imposed Availability ☐ High ☐ Medium ☐ Basic ☒ Not Contractually Imposed **Minimum clearance level of users:**
IS Maintenance	
IS Maintenance will routinely be performed by: ☐ Cleared System Administrator who routinely maintains the IS ☐ Cleared company employee ☐ Uncleared company employee escorted by technically knowledgeable cleared employee ☐ Cleared outside vendor: ☐ Escorted ☐ Not Escorted, need-to-know controls enforced by: ☐ Uncleared outside vendor escorted by technically knowledgeable cleared employee ☐ Other, Specify:	**IS Maintenance Procedures:** Systems and/or components will be downgraded prior to maintenance: ☐ Yes ☐ No An unclassified for maintenance only copy of the operating system will be loaded prior to maintenance: ☐ Yes ☐ No The IS operates classified 24x7 and will not be downgraded for maintenance: ☐ Yes ☐ No
Clearance and Sanitization Methods	
Clearance and sanitization of non-volatile memory or media: ☐ No ☐ Yes, If Yes, Refer to Attachments(s):	**Degaussing Used:** ☐ No ☐ Yes If Yes, Degausser Make/Model:

Software Protections	
COTS Software Protections: COTS software will be verified to be free of obvious indications of malicious code by the following method:	**Contractor Developed Software Protections:** ☐ No contractor developed software ☐ All contractor software is developed on the classified IS ☐ Cleared contractors develop software on an unclassified IS Protections during development: ☐ Uncleared contractors develop software on an unclassified IS Process for review or test:

Media Destruction Methods	
Destruction method(s) to be used for each type of media: *Floppy:* ☐Incinerate ☐Smelting ☐Pulverize ☐Chemical Decomposition *Rigid media:* ☐Incinerate ☐Smelting ☐Pulverize ☐Chemical Decomposition *Tapes:* ☐Incinerate ☐Smelting ☐Pulverize ☐Chemical Decomposition *Optical Media:* ☐Incinerate ☐Smelting ☐Pulverize ☐Chemical Decomposition *Chips/Proms/Integrated Circuits:* ☐Incinerate ☐Smelting ☐Pulverize ☐Chemical Decomposition	**Other Methods:** ☐Disintegrator Make /Model ☐Send to Customer ☐Send to NSA NSA Destruction Registration #: ☐Other NSA approved method:

Identified Threats and Vulnerabilities
Identified Threats: Risk Management Evaluation and Report identifying threats provided by DSS: ☐No ☐Yes **Identified IS Vulnerabilities:** The IS is capable of implementing <u>all</u> NISPOM Chapter 8 protection measures: ☐No ☐Yes If no, describe protection measure short-comings: **Risk Mitigation:** No unique threats or vulnerabilities have been identified: ☐True ☐False If false, describe the procedures implemented to mitigate these risks:

Special Procedures	
Trusted download: ☐No ☐Yes DSS authorized procedures ☐No ☐Yes, Refer to attachment: Customer approved alternate procedures: ☐No ☐Yes, Refer to attachment:	**Waivers**: ☐No ☐Yes, Refer to Attachment:

This IS includes Mobile Systems: ☐ No ☐ Yes If Yes, Complete the following:

Description of system(s) that will move:
The IS will be moved:

☐ Temporarily for less than 8 days, only to Contractor facilities under DSS cognizance.
☐ For 8 days to 120 days to a Contractor facility under DSS cognizance.
☐ Temporarily for less than 8 days to a government facility, not under DSS cognizance.
☐ For 8 days to 120 days to a government facility, not under DSS cognizance.

Requirements for mobile systems to contractor locations: Both the IS Profile along with the MSSP and the DSS accreditation letter will be forwarded to the gaining ISSM in advance of IS relocation. The ISSM will provide the gaining ISSM training and/or briefings necessary to understand the required safeguards and operation of the IS. Mobile systems are limited to 120 days unless requested by the GCA in writing. A System Component Information Form will be used for this documentation. Additionally a Transportation Plan shall be completed for each relocation.

Requirements for mobile systems to government locations: DSS IS accreditations are only valid for the security of classified information at appropriately cleared contractor locations. However, the government activity *may* decide to accept reciprocity in lieu of having to reaccredit these systems themselves. Regardless of whether the government uses DSS' accreditation to facilitate their own use of a contractor's accredited IS for classified performance while the IS is resident at their location, DSS is not responsible for security cognizance at government locations. The contractor will provide the applicable government sites with a copy of the DSS IS Accreditation Letter along with a letter acknowledging relocation (if between 8 and 120 days) of the IS to the particular government activity/site. The letter will specify to the government activity that movement and use of the DSS accredited IS outside of the contractor's facility to the government site, requires the transfer of security oversight to the government activity. A System Component Information Form will be used for this documentation. Additionally a Transportation Plan shall be completed for each relocation. *Prior to shipment*, the applicable government activity must formally concur in writing to accept security oversight for a specific IS while it is on that activity's installation(s). The documentation must be retained as part of the contractor's audit requirements.

Exception: In situations involving short-term (one week or less) relocation of any accredited mobile IS (e.g. laptops, etc.), to be used for processing classified information at a site outside of the contractor's facility to either a government or other contractor location, formal acceptance of oversight is *not* required.

Other Special procedures: ☐ N/A ☐ Yes If yes, describe:

Other Comments or Additional Information:

☒ This page is not applicable

Additional information/comments:

☒ This page is not applicable

Additional information/comments: