Defense Security Service

Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM

Version 3.3

May 21, 2016

Title Page

Document Name:	DSS Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM
Effective Date:	6 months from Revision
Document Owner:	Defense Security Service (DSS) Industrial Security Field Operations (ISFO) Office of the Designated Approving Authority (ODAA)
Point of Contact:	Questions regarding the publication of this manual should be directed to the Office of the Designated Approving Authority at ODAA@dss.mil Specific questions related to the implementation of the DSS Process Manual at contractor facilities, to include the status of C&A packages submitted, should be sent to the assigned ISSP or local DSS Field Office. Defense Security Service Office of the Designated Approving Authority 27130 Telegraph Road Quantico, VA 22134 www.dss.mil

1.0 Introduction 5
1.1 Preface 5
1.2 Responsibility 6
2.0 CERTIFICATION AND ACCREDITATION PROCESS 7
3.0 MANAGEMENT CONTROLS 7
3.1 Roles and Responsibilities 7
3.1.1 Information Systems Security Professional 7
3.1.2 Information Systems Security Manager 7
3.1.3 Information Systems Security Officer 8
3.1.4 Network (Host) ISSM/ISSO 8
3.1.5 Users of Information Systems 9
3.2 Certification and Accreditation Process 12
3.2.1 Certification and Accreditation Life Cycle 12
3.2.2 Validation 13
3.2.3 Plan of Action & Milestones 14
3.2.4 Interim Approval to Operate 15
3.2.5 Approval to Operate 15
3.2.6 Reaccreditation and Reevaluation of an IS 16
3.2.7 Revocation of an IATO or ATO 16
3.2.8 Termination/Disestablishment of an IS under an (M)SSP 17
3.2.9 Multi-User Standalone Systems and Single-User Standalone Systems 17
3.2.10 Special Categories 18
3.2.11 Local Area Networks 21
3.2.12 Interconnected System/Wide Area Network 21
3.2.13 Government to Contractor Networks 29
3.3 Types of Security Plans 30
3.3.1 Master Systems Security Plan 30
3.4 System Security Plan Submission Process 37
3.5 Configuration Management Process 38
3.6 Risk Assessment Requirements 38
4.0 OPERATIONAL CONTROLS 39
4.1 Training and Awareness 39
4.1.1 Security Education 39
4.1.2 Contractor Training 39
4.2 Contingency Planning 40
4.3 System Recovery and Assurances 40
4.4 Clearing and Sanitization 41
4.4.1 Clearing 41
4.4.2 Sanitizing 41
4.4.3 Magnetic Tape 41
4.4.4 Organization Destruction Options 42
4.4.5 DSS Clearing and Sanitization Matrix 42
4.5 Incident Response 43
4.5.1 Classified Spills 43
4.5.2 Incident Response Plan 44
4.5.3 Classified Spill Cleanup Procedures 44
4.5.4 Wiping Utility 45
4.5.5 DSS-Approved Classified Spill Cleanup Plan 45

4.5.6 Contamination Cleanup Procedures......47
4.6 MAINTENANCE......49
4.6.1 Maintenance......49
4.6.2 Cleared Maintenance Personnel......49
4.6.3 Uncleared (or Lower-Cleared) Maintenance Personnel......50
4.6.4 Remote Maintenance......50
4.7 MEDIA......50
4.7.1 Media Protection......50
4.7.2 Removable Media Restrictions......51
4.7.3 Hardware Marking......52
4.7.4 Trusted Download......52

5.0 PHYSICAL AND ENVIRONMENTAL PROTECTION......60

5.1 PHYSICAL SECURITY......60
5.1.1 Hardware and Software Protections......61
5.1.2 Mobile Systems......61
5.1.3 Software Protections......66
5.1.4 Emergency Procedures......66
5.1.5 Transient Electromagnetic Pulse Emanation Standard (TEMPEST)......66
5.1.6 Personnel Security......67
5.1.7 Personnel Sanctions......67
5.2 SYSTEM AND INFORMATION INTEGRITY......67
5.2.1 Flaw Remediation......67
5.2.2 Unclassified Software Review......67
5.2.3 Antivirus......68

6.0 TECHNICAL CONTROLS......68

6.1 ACCESS CONTROL......68
6.1.1 Separation of Function......68
6.2 NISPOM COMPLIANT LOGON BANNER FOR DSS ACCREDITED NON-DOD SYSTEMS......68
6.2.1 DoD Warning Banner for SIPRNet......69
6.3 SESSION CONTROLS......70
6.3.1 Successive Login Attempt Controls......70
6.3.2 User Inactivity......70
6.3.3 Logon Notification (PL-2/PL-3 only)......71
6.4 USB DEVICES AND PORTS......71
6.5 RADIO FREQUENCY ID TAGS......71
6.6 SECURE WIRELESS LANS......71
6.7 AUDIT AND ACCOUNTABILITY......71
6.7.1 Audit Requirements......71
6.7.2 Weekly Audit Reviews – Definition......72
6.8 SECURITY SEALS......72
6.9 IDENTIFICATION AND AUTHENTICATION......73
6.9.1 Identification and Authentication Management......73
6.9.2 Generic or Group Accounts......73
6.9.3 Password Policy......73
6.9.4 BIOS Password......74
6.10 SYSTEM AND COMMUNICATIONS PROTECTION......74
6.10.1 Data Transmission Protection......74
6.10.2 Protected Distribution Systems......74
6.10.3 Network Management and Protections......76

6.10.4 Controlled Interfaces ... 76
6.11 CLASSIFIED VOICE OVER INTERNET PROTOCOL/VIDEO TELECONFERENCING ... 77
6.12 THIN CLIENT SYSTEMS ... 77
6.13 VIRTUALIZATION ... 78
6.14 MASKING/CODING/DISASSOCIATION ... 78

7.0 VARIANCES ... 79

8.0 ENHANCED CONTROLS ... 81

9.0 SYSTEMS/NETWORKS WITH ENHANCED CONTROLS OR PROCESSES ... 81

9.1 SIPRNET ... 81
9.1.1 SIPRNet Systems ... 81
9.1.2 Command Cyber Readiness Inspections ... 82
9.1.3 NISP SIPRNet Circuit Acquisition Process ... 82
9.2 DEFENSE INDUSTRIAL BASE CYBER SECURITY ACCREDITATION PROCESS (DIBNET) ... 84
9.3 INTERNATIONAL SYSTEMS SECURITY PLANS ... 85

10.0 NIST 800-53 CONTROL MAPPING ... 86

11.0 REFERENCE ... 86

12.0 ACRONYMS LIST ... 87

13.0 GLOSSARY ... 89

14.0 REFERENCE MATERIALS ... 94

14.1.1 Flow Diagram: Initial (M)SSP ... 94
14.1.2 Flow Diagram: Reaccreditation and Re-evaluation ... 95
14.1.3 Example ODAA Disestablishment Letter ... 96
14.1.4 Plan of Action and Milestones Template ... 97
14.1.5 NSP Accreditation Process Diagram ... 99
14.1.6 Overall Network Security Profile ... 100
14.1.7 NSP Architecture Diagram Example ... 102
14.1.8 Network Host Security Profile ... 103
14.1.9 Network Node Security Profile Form ... 105
14.1.10 Memorandum of Understanding Template ... 107
14.1.11 Flow Diagram for Self-Certification under an MSSP ... 110
14.1.12 Table for Self-Certification ... 111
14.1.13 MSSP IS Tracking Form ... 112
14.1.14 Table of Subject Line Requirements for Plan Submissions ... 113
14.1.15 E-mail to ODAA Mailbox Template and Sample ... 114
14.1.16 Clearing and Sanitization Matrix ... 116
14.1.17 Main Cleansing Process Checklist ... 118
14.1.18 Microsoft Exchange Server Cleansing Checklist ... 119
14.1.19 Novell GroupWise Server Cleansing Checklist ... 123
14.1.20 Desktop Client Workstation Cleansing Checklist ... 126
14.1.21 Process for Clearing a Blackberry ... 127
14.1.22 Trusted Download Authorization Form ... 130
14.1.23 Trusted Download Record ... 131
14.1.24 Alternate Trusted Download Risk Acceptance Letter (RAL) Example ... 132
14.1.25 Table of DSS Authorized File Type/Formats ... 133
14.1.26 Mobile System Relocation Form ... 134
14.1.27 Authorized Alternate Site Locations ... 135
14.1.28 Authorized Sites for Mobile Processing ... 136

14.1.29 System Component Information Form 137
14.1.30 Mobility Plan Sample 139
14.1.31 Protected Distribution System Approval Request 141
14.1.32 WAN Accreditation Boundaries....142
14.1.33 Tunneling....143

1.0 Introduction

1.1 Preface

The Defense Security Service (DSS), Office of the Designated Approving Authority (ODAA), has been delegated the responsibility for providing Certification & Accreditation (C&A) oversight of the National Industrial Security Program (NISP) contractor information systems (IS) that process classified information. This process manual is for cleared contractors under DSS cognizance. In addition, this process manual is designed to provide a full spectrum of resources to newly appointed contractor Information Systems Security Managers (ISSM) and well-seasoned Information Systems Security Officers (ISSO) alike.

Specifically, the intent of this process manual is to explain process standards, management control standards, operation control standards, technical configuration standards, and (M)SSP standard templates. Adherence to the standards in this process manual, by NISP contractors, is highly recommended in order for DSS to expeditiously issue Interim Approvals to Operate (IATO) and Approvals to Operate (ATO).

Stakeholders in the DSS C&A process are responsible for being familiar with the processes and requirements to ensure systems are accredited and maintained in the proper manner. The DSS Process Manual provides a consistent approach to be applied when submitting systems to DSS for accreditation across the NISP.

This manual includes and incorporates minimum standards for contractors' insider threat programs, as they relate to information systems. The ISSM plays an important role in the contractors' insider threat program and reports information system activities related to the program to the contractor's Insider Threat Senior Official (ITSO).

The following items are key elements that support industry insider threat programs. Although not all new to the ODAA requirements, Insider Threat initiatives have created a renewed emphasis on the following items and in some cases require the use of additional security controls to be applied by the contractor. Click on the heading to access the information within the manual:

- *User Training (4.1.1)*: All classified IS users will be trained on their responsibilities and include information related to the insider threat program
- *Use of System Logon Banners (6.2)*: Classified IS users will be notified at logon that their activity is subject to monitoring
- *User Activity Monitoring/Auditing (6.7.1)*: Contractors will monitor and review user activity for the detection of insider threat activity and protect the methods used and information obtained

This process manual is not intended to be relied upon or construed to create any right or benefit, substantive or procedural, enforceable at law against the United States, its agencies, officers or employees. The Federal Government reserves the right, and has the obligation, to impose any security method, safeguard, or restriction it believes necessary to verify that unauthorized access to classified information is effectively precluded and that performance of classified contracts is not adversely affected.

DSS Process Manual guidance should be applied to new systems and reaccreditations by the end of the published revision transition period. Systems under a current accreditation will retain accredited status and will generally be required to update to new requirements at the next reaccreditation event.

1.2 Responsibility

The Director, DSS is responsible for C&A oversight of cleared NISP contractors' Information Systems. The Designated Approving Authority (DAA) is the government official with authority to formally accredit the operation of a contractor's IS and assumes residual risk for the government on behalf of DSS. Under the NISP, the Director, Industrial Security Field Operations for DSS is the delegated DAA for NISP contractors and has further delegated those responsibilities to the Deputy Director, ODAA and to the Regional Designated Approving Authorities (RDAAs). Other DSS components may support DSS in executing its DAA responsibilities, when approved by the Deputy Director, ODAA.

2.0 Certification and Accreditation Process

C&A process guidance is divided into three areas corresponding to sections from prevailing national level guidance and further support the protection measures outlined in the NISPOM. The three areas define the basic structure of an information assurance program, including:

- Management Controls
- Operational Controls
- Technical Controls

3.0 Management Controls

3.1 Roles and Responsibilities

The ODAA is the accrediting authority for contractor classified systems under DoD or those agencies and/or departments which have entered into agreements with the Secretary of Defense for rendering industrial security services. ODAA C&A oversight is comprised of reviewing the (M)SSPs and supporting documentation, performing onsite validations and assessments to verify system controls are in place and operating as intended, providing advice and assistance to cleared contractors, and promulgating guidance and policy interpretation. The ODAA oversees the C&A of contractor classified systems to verify it is consistent with national computer security information assurance (IA) policy and performed in an efficient and effective manner. The ODAA also ensures contractors' maintain the security posture of their accredited systems throughout their life cycle by conducting onsite validations and annual assessments. The ODAA includes DSS Field Operations staff known as Information Systems Security Professionals (ISSP).

3.1.1 Information Systems Security Professional

The primary role of the ISSP is technical in nature. The ISSP will evaluate, certify, and assess all IS technical features and safeguards for all contractor ISs processing classified information under the NISPOM. Additionally, the ISSP will review the (M)SSPs to determine if the management, operational, and technical controls identified in the plans are adequate to protect the classified information resident on the IS. The ISSP will conduct onsite validations and assessments to verify that the protection measures, as certified by the ISSM, have been implemented on the Information Systems. The ISSP is also responsible for providing guidance and assistance to cleared contractors in their efforts to protect classified information.

3.1.2 Information Systems Security Manager

The ISSM (NISPOM 8-103) is a contractor employee who is responsible for daily supervision of the contractor's IS security program.

ISSM training includes both technical and administrative aspects. If the ISSM is not technically competent to securely configure the systems under his or her purview, there must be a local ISSO that can configure and manage the information systems to verify their controls are in place and operating in accordance with established policies. During onsite validation visits and security assessments, DSS staff will verify that the ISSM is trained to a level commensurate with the overall complexity of the systems, or that the ISSM has appointed a technically knowledgeable local ISSO. If it is determined during an IS onsite validation visit or a security assessment that the ISSM (1) does not have eligibility for access to classified information, (2) does not understand their duties and responsibilities, (3) does not possess adequate technical skills to manage the systems under their authority, or (4) has not appointed a local ISSO with the requisite technical skills, it will be noted in the "IS Certification Report," or as a security review vulnerability, and may be cause for a denial of approval to operate (DATO) or withdrawing a current accreditation. The DSS ISSP or qualified IS Rep will document such determinations in the Industrial Security Facilities Database (ISFD) and ODAA system records.

A primary and alternate ISSM may be appointed by the contractor and may operate simultaneously with all the same rights and privileges. A primary ISSM may establish subordinate ISSMs at other contractor locations under their authority. However, the primary ISSM will be held responsible for the security of the systems at each contractor location. Each site is required to have a local ISSM to handle the day-to-day operations and be able to effectively and quickly respond to security instances, therefore the ISSM must be within a reasonable commuting distance. DSS considers up to four hours travel time between locations as a reasonable distance.

3.1.2.1 ISSMs for Multiple Facility Organizations

In a Multiple Facility Organization (MFO), the ISSM can be assigned oversight responsibility for multiple contractor locations within the MFO. The ISSM, in addition to the above requirements, must have the ability to effectively manage all of IS programs. The ISSM who has been granted self-certification authority for like systems under approved MSSP may self-certify systems for those facilities where he or she has been designated as the ISSM in associated system security plans and accreditation letters. There are no restrictions on an experienced ISSM assisting another ISSM in a different geographical location, but the local ISSM is responsible for the local system and must meet the requirements for self-certification. Emergency situations will be reviewed by DSS on a case-by-case basis. Within an MFO, contractor management can appoint an employee to serve as the ISSM for multiple facilities if the following conditions are met:

- Facilities are in close proximity to, or within a reasonable commuting distance from, the ISSM's duty station.
- The ISSM is trained to a level commensurate with the overall complexity of the systems under his/her purview at the assigned facilities.
- Each remote facility has at least one appointed ISSO who has been assigned the duties identified in NISPOM paragraph 8-104.

3.1.3 Information Systems Security Officer

One or more Information Systems Security Officers (ISSOs) may be appointed by the ISSM when the contractor has multiple accredited Information Systems, in an MFO in which the ISSM has oversight responsibility for multiple contractor locations, or when the technical complexity of the contractor's IS program warrants the appointment. The ISSO must ensure and/or be able to configure and manage the security configuration of the systems under their purview. For further guidance refer to Table 1.2: Industry Roles and Responsibilities.

3.1.4 Network (Host) ISSM/ISSO

In many cases there are requirements for cleared contractors to collaborate and share information in support of a large contract (or multiple contracts) through establishment of a wide area network (WAN). An ISSM at one of the connecting sites is designated the lead site, or "Host ISSM" for the WAN. In order for contractors to exchange classified information the Host ISSM must verify that each connected site (node) has an accredited system to join this interconnected system, or WAN. A network security plan (NSP) must be submitted and accredited by DSS before any classified information can be exchanged across the WAN. Generally, the prime contractor will be established as the Host for the WAN, but not in all cases. The host ISSM may appoint an individual located at the host site as the Network ISSO. The duties of a Network ISSO or Host ISSM are as follows:

- Verify that all security measures on the network are appropriate, outlined in the NSP and that the network is in compliance with NISPOM Chapter 8 and other applicable guidance.
- Serve as focal point for the network and the connecting node ISSM/ISSOs, to include collecting network security profiles.
- Generate and maintain approvals for the NSP and, if applicable, assist in coordinating the Memorandum of Understanding (MOU) if government nodes are connected to the WAN.
- Verify all systems on the WAN are accredited.
- Ensure proper network security procedures are developed and implemented.
- Perform or oversee weekly reviews of the WAN and verify that only connections that are accredited and exhibited on the topology diagram are connecting to the system.
- Evaluate the impact of system and network changes and apply for re-approval of the NSP and MOU, as appropriate.
- Recommend DSS rescind the MOU and NSP, if necessary, and report any anomalies or violations to DSS and any other accrediting authorities with nodes on the network.
- Submit a written request to DSS in order to disestablish the accredited NSP and any associated MOU(s) when the WAN is no longer needed.

3.1.5 Users of Information Systems

There are two types of IS users, 1) privileged, and 2) general. From a security standpoint, this is the most basic user structure. Depending on the complexity and number of accredited IS(s) at the contractor facility, users can have multiple roles. Each role has unique requirements that are vital to successful IS operations. The ISSP, IS Rep, and the ISSM will review the various user roles and responsibilities.

Table 1.1: DSS Roles and Responsibilities

Participant(s)	Responsibilities
HQ Office of the Designated Approving Authority (ODAA)	▪ Accreditation authority for contractor IS processing classified information under DSS cognizance ▪ Provides advice and assistance on the C&A process and other IS matters ▪ Approval signatory on all MOUs/MOAs ▪ Coordinates cyber incident responses related to classified information systems under DSS cognizance
Regional Designated Approving Authority (RDAA)	▪ Responsible for the accreditation of ISs used to process classified information ▪ Provides advice and assistance on the C&A process and other IS matters ▪ Coordinates regional cyber incident responses related to classified information systems under DSS cognizance ▪ Subject matter expert on information systems ▪ Coordinates with the field on C&A issues ▪ DAA responsibilities and authority within their region ▪ Reports to the Regional Director ▪ Coordinates with HQ as needed
Information Systems Security Professional (ISSP)	▪ Primary DSS POC on Industry information systems ▪ Provides advice and assistance on the C&A process and other IS matters ▪ Coordinates cyber incident responses related to classified information systems under DSS cognizance at field office level ▪ Subject matter expert in information systems ▪ Reviews (M)SSPs, NSPs, and MOU/As ▪ Notifies the DAA on system compliance ▪ Performs certification, validation, and annual reviews on ISs ▪ First level of inquiry for cleared contractor issues and questions
Regional Director (RD)	▪ Directs the Field Office Chiefs (FOC) and RDAAs
Field Office Chief (FOC)	▪ Directs industrial security oversight activities at the field office level to include annual assessment reviews
Industrial Security Specialist (IS Rep)	▪ Primary DSS POC for Industry ▪ Coordinates with Government Contracting Authorities (GCAs) ▪ Provides advice and assistance on the C&A process (if qualified) and other IS matters
Counterintelligence Specialist	▪ Collects, analyzes, integrates and provides timely threat assessment and CI reports to RD, RDAA, ISSP and IS Rep

Table 1.2: Industry Roles and Responsibilities

Participant(s)	Responsibilities
Contractor Management	▪ Appoint ISSMs trained to a level commensurate with the complexity of the contractor's ISs and granted access and need-to-know for all information processed on all accredited ISs ▪ May appoint an alternate ISSM to act with full authority in the absence of the primary ISSM or simultaneously. However, the primary ISSM is still responsible ▪ Publishes and promulgates an IS security policy addressing the classified processing environment ▪ Notifies DSS and other government agencies as appropriate for cyber incidents and suspicious contacts in accordance with the NISPOM
Information Systems Security Manager (ISSM)	▪ Oversight responsibility for the development, implementation, and evaluation of the IS security program ▪ Develops (M)SSPs which comply with the NISPOM ▪ Verifies IS(s) are configured in accordance with security requirements and the (M)SSPs ▪ Informs DSS of security relevant changes to accredited systems ▪ Must be trained to a level commensurate with the complexity of the contractor's IS or have a local ISSO who is trained ▪ May appoint the ISSO in contractor facilities with multiple accredited IS or when the complexity of the IS technical features exceeds the capability or knowledge of the ISSM to assist in the daily operations of the IS programs
Information Systems Security Officer (ISSO)	▪ If appointed, supports the ISSM in their efforts to implement security requirements as mandated by the NISPOM ▪ ISSO must ensure and/or be able to configure and manage the security configuration of the systems under their purview ▪ ISSO must be local with the systems they manage
Network ISSM/ISSO	▪ Verifies that all security measures on the network are appropriate, outlined in the NSP, and that the network is in compliance with NISPOM Chapter 8 ▪ Focal point for the network and for the connecting node ISSM/ISSO, to include collecting network security profiles ▪ Coordinate and track approvals for the NSP and the MOU, if applicable ▪ Verifies all systems on the network are accredited ▪ Assures proper network security procedures are developed and implemented ▪ Reports anomalies or violations to DSS and any other accrediting authorities with nodes on the network
General User	▪ Authorized by the ISSM or ISSO to process classified information on an accredited IS ▪ Subordinate to the ISSM or ISSO on all matters related to IS security
Privileged User	▪ A user with access to system controls, documentation, monitoring, and/or administration functions ▪ Must have working knowledge of system functions, security policies, technical security safeguards, and operational security measures ▪ Subordinate to the ISSM or ISSO on all matters related to IS security
System/Network Administrator	▪ Privileged user with complete control of an IS ▪ Authority to control and change other users' access to data or program files ▪ Set up and administer user accounts and authenticators ▪ Troubleshooting or monitoring an IS' security functions
Facility Security Officer (FSO)	▪ Supports the ISSM in their efforts to implement security requirements for classified information systems as mandated by the NISPOM

3.2 Certification and Accreditation Process

3.2.1 Certification and Accreditation Life Cycle

The Certification and Accreditation (C&A) Process (NISPOM 8-200) is an integral part of the contractor IS life cycle. Protection measures are identified during system design and development. Certification conducted by the ISSM serves to attest that the protection measures described in the (M)SSP have been implemented and are functioning properly. Accreditation is the DAA's formal authorization for the contractor's IS to process classified information at one of three Protection Levels (PLs), using a prescribed set of safeguards, at an acceptable level of risk. Accreditation is based on the ISSM's certification and an onsite validation by the ISSP. IAW NISPOM 8-200, accreditation is the approval for processing. Therefore, if accreditation expires or is withdrawn, the system is no longer approved for processing. Interim Approval to Operate (IATO) and Approval to Operate (ATO) are the two accreditation actions that authorize the IS to operate and permit the IS to begin classified processing.

By accrediting the contractor's IS, the DAA officially declares that the protection measures and the environment the contractor has identified in the (M)SSP will effectively protect classified information from unauthorized access, disclosure, and modification. The DAA's accrediting decision represents that adequate controls are in place to fulfill the security requirements of the NISPOM, and that the DAA accepts the operation of the contractor's IS under the stated parameters of the accredited (M)SSP. The DAA will invalidate or withdraw the contractor's IS accreditation, including self-certification authority, if the contractor's procedures and controls are not implemented, ineffective, or there has been an unacceptable change in the IS or security configuration. These actions are taken after appropriate coordination within DSS.

3.2.1.1 Certification Process

An ISSM of record submits an (M)SSP for an IS that will process classified information to ODAA using the instructions within this manual and per the NISPOM.

The ISSM is required to certify, in writing, that the IS has undergone a comprehensive evaluation of all technical and non-technical security features and safeguards.

The ISSM's certification process must outline the assessment and test procedures used to demonstrate compliance with the security requirements associated with the Protection Level (PL) assigned to the IS. The certification test will be administered during the certification process and must verify correct operation of the protection measures in the IS.

By signing the certification test results, the ISSM is affirming in writing that the system is currently installed and configured as described in the (M)SSP. The DSS accreditation decision relies heavily on the accuracy of the ISSM's certification. Additionally, the certification test results and required NISPOM 8-610(a) DOC 1 Requirements must accompany the (M)SSP to support an accreditation decision. This signature is required to accompany the plan in an electronic format for digital storage.

Reminder

The electronic format can be:

- ✓ *Digital certificate*
- ✓ *An ink signature that has been scanned and saved as a PDF*

ODAA reviews the plan and makes the following recommendation:

- ▪ Accept the plan requiring no corrective action
- ▪ Accept the plan requiring some corrective action
- ▪ Deny the plan (NOTE: in this case the lifecycle restarts)

Examples of reasons to deny an IATO:

- Missing or incomplete UID
- ISSM did not sign the IS Security Package Submission and Certification Statement
- Missing Hardware List / Software List / Configuration Diagram
- Physical security not adequately explained
- No signed DSS Form 147 (Record of Controlled Area) if the system is in a closed area
- No Certification Test Guide Results were provided
- Missing letter from GCA if any variances are needed
- Missing MOU/MOA when required
- Identification and authentication not adequately addressed
- Any unique matters or concerns that would require denial of the IATO

When updates are required, once the security plan has been revised in accordance with the provided DSS comments, the ISSM will forward the revision to ODAA@dss.mil, the ISSP, and the IS Rep.

The ISSM will be given three opportunities for successful security plan submission. After the third unsuccessful attempt, the security plan will be rejected and NISP facility management will be notified of the need for assistance with the process.

The ISSM is responsible for resubmitting a corrected plan within the six-month IATO period when corrections are required. The corrections should be submitted in a timely manner allowing enough time for the ISSP to review updated documents prior to expiration of the IATO.

After the plan is reviewed and accepted, the RDAA may grant an IATO to allow the cleared contractor to begin classified processing.

During the period identified in the IATO, an onsite validation will take place to determine if the protective security measures noted in the SSP match the actual technical and physical settings of the system, the ISSP will make one of the following determinations:

- Recommend issuing an ATO for final accreditation with no corrections required to the system
- Recommend issuing an ATO after the ISSM has made minor corrections to the system
- Reschedule another onsite validation to review the system again after corrective action has been taken

In cases when it is practical to do so, the ISSP may schedule and conduct on onsite validation immediately after reviewing the plan, before recommending an IATO. Completing the site validation prior to granting an IATO may allow the system's accreditation to go straight to ATO status.

The ISSM should immediately notify the ISSP of the need to disestablish an accredited system when it reaches the end of life cycle. Upon receipt of the ISSM's notification, the ISSP should:

- Verify the system has been properly sanitized in accordance with the security plan
- Ensure the disposition of program data is in accordance with the SSP, NISPOM, and guidance from the government data owner
- Forward a system disestablishment recommendation to the RDAA

Upon receipt of the recommendation to disestablish, RDAA should issue a letter addressed to the ISSM officially disestablishing the system (and the associated accreditation)

Reminder

Prior to disestablishing a system, the ISSM should verify self-certification authority (if applicable) is granted under a different system plan. Disestablishing the system granting self-certification authority cancels the ATO and the associated authority to self-certify "like" systems.

3.2.2 Validation

Onsite validation will take place during the period authorized by the IATO to determine whether or not protective security measures noted in the (M)SSP match the actual configuration and physical environment documented in the security plan.

During the onsite system validation, minor discrepancies between the plan and system configuration should be corrected by the ISSM when discovered to the extent practical. If the discrepancies reveal a significant difference between the system's configuration and the approved plan, placing classified information at risk, the ISSP will notify the ISSP Team Lead, RDAA, IS Rep, FOC and FSO. If an IATO is rescinded due to significant discrepancies, a corrected system security plan will be resubmitted. However, systems will not be considered for IATO upon resubmission to correct significant discrepancies discovered during the onsite validation.

In rare cases, when justified and approved by the RDAA, a second IATO may be issued to allow a system to operate while corrections are made. Second IATOs under these circumstances are rare and will only be considered when the discrepancies do not place classified information at risk. In these cases, the ISSM initiates a request through the ISSP along with a plan of action and milestones (POA&M). The POA&M should detail the actions and timetable for correcting the discrepancies.

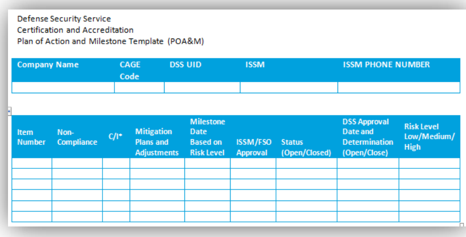
3.2.3 Plan of Action & Milestones

The purpose of POA&M is to facilitate a disciplined and structured approach to mitigating risks in accordance with NISPOM requirements and CSA priorities.

POA&Ms are used by the DAA to monitor progress in correcting weaknesses or deficiencies noted during the C&A lifecycle, including: initial submissions; those discovered during ongoing security reviews and tests by the ISSM; self-assessments; potential configuration changes; and DSS security assessments.

The POA&M identifies: (i) the tasks to be accomplished with a recommendation for completion either before or after information system implementation; (ii) the resources required to accomplish the tasks; (iii) any milestones in meeting the tasks; and (iv) the scheduled completion dates for the milestones.

Example
Plan of Action Milestones Template



Defense Security Service
Certification and Accreditation
Plan of Action and Milestone Template (POA&M)

Company Name	CAGE Code	DSS UID	ISSM	ISSM PHONE NUMBER

Item Number	Non-Compliance	C/I*	Mitigation Plans and Adjustments	Milestone Date Based on Risk Level	ISSM/FSO Approval	Status (Open/Closed)	DSS Approval Date and Determination (Open/Close)	Risk Level Low/Medium/ High

An example Plan of Action and Milestones Template (POA&M) is located in the Reference Materials (14.1.4), page 97.

When a system is updated and resubmitted to conform to a new baseline configuration or a new system is submitted after new baseline requirements have been implemented:

- The ISSM may use a POA&M when the baseline configuration requirements are not yet fully implemented.
- The first step with the POA&M is to identify the high risk, medium risk and low risk items. The high risk items need to be addressed within 90 days, medium risk within 180 days, and low risk within 365 days.
- If the POA&M and the (M)SSP are acceptable, the RDAA will issue an IATO for the system.
- After all POA&M items have been completed, and the ISSP has conducted a successful onsite validation, the RDAA will issue an ATO for the system.

3.2.4 Interim Approval to Operate

After the security plan has been reviewed and determined to be acceptable, DSS may issue an interim approval to operate. If minor corrections are required, a comments form will be attached with the IATO letter. Corrections must be resolved during the IATO period prior to the validation visit for granting an ATO.

An IATO is a temporary approval allowing the systems to be used to process information in support of the program prior to onsite validation. In cases when the ISSM needs to make changes to the system during IATO, the ISSP must be contacted to coordinate the changes. It is not necessary to issue a new IATO for the system due to minor updates or changes to the system.

Reminder

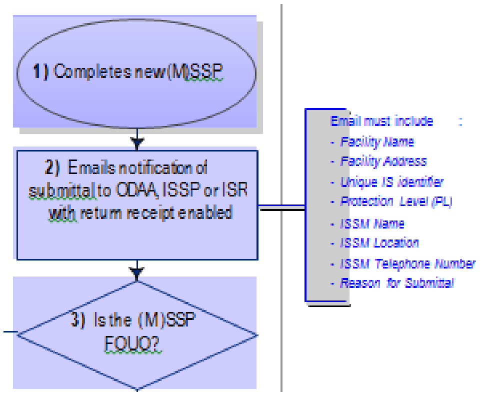
The (M)SSP and all changes will be frozen one week before the ISSP conducts the onsite validation/assessment to ensure that the IS is operating as accredited and that accreditation conditions have not changed.

Reminder

The ISSM should forward all accreditation documentation to ODAA 30 days prior to the expiration of an IATO or ATO. Failure to do so could result in lapse of accreditation resulting in the system being unavailable for processing. Initial accreditation requests should be forwarded to ODAA for review and approval as soon as possible and in advance of the "required" date for use. Generally, security plans should be submitted a minimum of 30 days prior to the date the system is required to be operational.

IATOs may be granted for a period up to 180 days to allow for using the system while an onsite validation visit is scheduled. In rare cases, an RDAA may issue a second IATO for another 180 days (360 total) if there is justification for doing so.

Example
Initial (M)SSP



A Flow Diagram for Initial (M)SSP is located in the Reference Materials (14.1.1), page 94.

3.2.5 Approval to Operate

ATO is the official management decision to allow a system to operate as documented in the SSP. An ATO may be granted as a result of the onsite validation if no significant security discrepancies are discovered.

Information systems may be approved to process classified information in one of two ways:

1. DSS ODAA accredits the by granting ATO
2. An authorized ISSM self-certifies the system based on parameters established in an existing accredited system for which an ATO was granted to the ISSM (or as an Alternate ISSM) with self-certification authority included.

The RDAA may grant final ATO for a period of time up to three years in duration. During this period, the ISSM is required to notify the assigned ISSP of proposed security relevant modifications to the system. Security relevant changes will be reviewed by ODAA to determine if reaccreditation is necessary.

The term "Master" is associated with the system's security plan that grants self-certification authority to an ISSM. When an MSSP is accredited, the date of the ATO letter starts the three-year cycle. Each self-certified system profile added to the MSSP begins its own separate three-year certification cycle as of the self-certification date.

This reaccreditation/recertification date will be established in one of three ways:

- Three years from the date an initial ATO is issued by the RDAA for the MSSP and associated system profiles
- Three years from the date an ATO is granted by the RDAA for reaccreditation of a system profile
- Three years from the date an authorized ISSM self-certifies a system and adds it to an existing ATO for an MSSP

3.2.6 Reaccreditation and Reevaluation of an IS

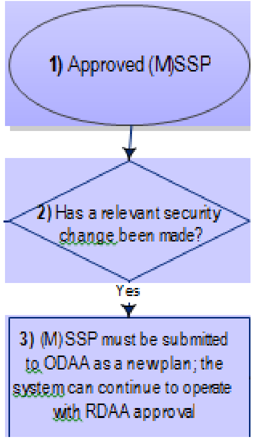
Reaccreditation must be initiated when security relevant changes occur. The ISSM must document all security relevant changes within the security plan and submit to ODAA@dss.mil with a copy to the assigned ISSP and IS Rep. The documentation will be reviewed to determine if reaccreditation is required. Examples of a security relevant change include: when a sniffer (LAN Analyzer) is added to a network; a new operating system is added to the accredited IS; a change in physical environment from restricted to closed area; changes in the protection level; other changes affecting security posture of the accredited system.

Reminder

Assignment of a new ISSM by itself does not meet the threshold of a security relevant change to the system. However, the new ISSM does not inherit self-certification authority from the previous ISSM. The new ISSM should resubmit the MSSP or SSP when the next security relevant change occurs.

Re-evaluation will occur three years from the issuance date of the ATO. If there are no system changes, re-evaluation reviews will be handled via e-mail from the ISSM to the ODAA@dss.mil, with a copy to the ISSP and IS Rep, stating that there have been no security relevant changes. The e-mail must include the facility name, address, unique (M)SSP identifier, NISPOM protection level, and ISSM name, location, and telephone number. Based on the ISSM's statement, a new ATO will be granted for the system. See Flow Diagram Reference (15.1.1) for Initial (M)SSP.

Example
Reaccreditation and Re-evaluation


1) Approved (M)SSP
2) Has a relevant security change been made?
Yes
3) (M)SSP must be submitted to ODAA as a new plan; the system can continue to operate with RDAA approval

A Flow Diagram for a reaccreditation and Re-evaluation is located in the Reference Materials (14.1.2), page 95.

If there are significant changes to the system, the revised (M)SSP and system profile must be resubmitted using the appropriate procedures. Proposed security relevant changes cannot be made on the system until ODAA has reviewed the change and determined if a reaccreditation is required. It is the ISSM's responsibility to ensure that plans submitted for reaccreditation with changes are submitted with enough time to permit ODAA to conduct a review and validation of the plan and system components. A minimum of 30 days prior to expiration is expected to ensure other operational commitments are met. If the system's accreditation expires during the review time, the ISSM must stop processing classified information until the plan is approved. The RDAA may grant an IATO for the system after receipt of the reaccreditation package to allow time for reviewing the system's security plan.

3.2.7 Revocation of an IATO or ATO

If the ODAA determines that conditions exist that place classified information at risk or if gross non-compliance with the approved (M)SSP is discovered, an IATO or ATO can be revoked. If an IATO or ATO is revoked, the ISSM will be notified by letter via e-mail from the RDAA with a copy to the ISSP, ISR, FOC, FSO, and RD. The e-mail and/or attached letter will clearly state all security issues to be resolved. When an ATO (or IATO) is revoked, withdrawn, or expires, processing on the accredited system should cease immediately. In some rare cases, the critical nature of a program may be justification to continue processing; however, the ISSM shall submit a POA&M

immediately. The ISSM should provide information to support the need to continue processing with concurrence from responsible government program personnel.

3.2.7.1 Reaccreditation of an IS after a Revocation

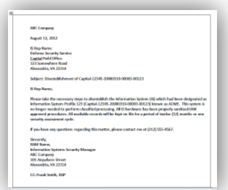
Before an (M)SSP can be reaccredited after a revocation, the FSO and the ISSM must submit a clear POA&M that addresses all the security concerns addressed by the revocation notification. An onsite review will be conducted by the ISSP or IS Rep in coordination with the RDAA and FOC before processing will be allowed to continue. The ISSP or IS Rep will submit their recommendation for reaccreditation to the RDAA who will determine reaccreditation. Any changes required in the (M)SSP must be resubmitted to the ODAA by the appropriate method. If it is determined that security concerns have been addressed, the RDAA will issue a new ATO for the system.

3.2.8 Termination/Disestablishment of an IS under an (M)SSP

When an IS has come to the end of its lifecycle, due to the end of a contract or program, etc., accreditation for the system is withdrawn. Storage media and memory associated with the IS must be sanitized, destroyed or disposed of in accordance with the procedures outlined in the system's (M)SSP. Records and logs associated with the IS must be retained for one review cycle.

To disestablish an IS, the ISSM notifies the ISSP and/or IS Rep of the need to disestablish, to include the UID for the system, reason for disestablishment, and the disposition of the hard drive(s) and media. After review the ISSP will forward the recommendation to terminate the accreditation to the RDAA. Disestablishments will be validated to show that the IS has been effectively declassified in accordance with the approved procedures in the (M)SSP.

Example
ODAA Disestablishment Letter



ABC Company

August 13, 2012

IS Rep Name
Defense Security Service
Captial Field Office
123 Somewhere Road
Alexandria, VA 22314

Subject: Disestablishment of Captial-12345-20080310-08003-00123

IS Rep Name,

Please take the necessary steps to disestablish the Information System (IS) which had been designated as Information System Profile 123 (Captial-12345-20080310-08003-00123) known as ACME. This system is no longer needed to perform classified processing. All IS hardware has been properly sanitized IAW approved procedures. All available records will be kept on file for a period of twelve (12) months or one security assessment cycle.

If you have any questions regarding this matter, please contact me at (212) 555-4567.

Sincerely,
ISSM Name,
Information Systems Security Manager
ABC Company
101 Anywhere Street
Alexandria, VA 22314

CC: Frank Smith, ISSP

An example ODAA Disestablishment Letter is located in the Reference Materials (14.1.3, page 96).

Reminder

Weekly system audit trail analysis should be conducted until the day the system is officially removed from service and sanitized. Audit trails should be retained for at least one review cycle (per NISPOM) and a minimum of 12 months.

Information Systems Types

There are many Information Systems types and system configurations that operate within cleared contractor facilities. However, the three predominant IS types are the Multi-User Standalone (MUSA), the Local Area Network (LAN) and the WAN.

3.2.9 Multi-User Standalone Systems and Single-User Standalone Systems

The NISPOM defines systems that have one user at a time, but have a total of more than one user with no sanitization between users, as multiuser systems, and the Cognizant Security Agency (CSA) will consider the systems as such in determining the protection level and the resulting security requirements. ODAA further defines Multiuser-Standalone (MUSA) systems as having more than one general user on the system. The privileged users (systems administrators) should not be included when determining the number of users on the system. The NISPOM requires there be accountability of users on classified IS(s). Therefore, at a minimum, a MUSA configured with Protection Level 1 specifications requires the technical security features for identification and authentication (I&A), session controls and auditing be enabled. A Single-User Standalone (SUSA) has only one user that is held accountable; therefore, technical security features are not required. Because of the vast differences between the technical security requirements of the MUSA and SUSA, forethought should be given to potential future growth in the number of users. In other words, if there is only one person using the IS but there are intentions of adding users in the near future, it is advisable to submit an (M)SSP for a MUSA rather than a SUSA.

General characteristics of MUSA:

- Two or more general users (SUSA is only one general user)
- Physical security environment may be either a closed or restricted area
- Operating system must be NISPOM compliant, or have a risk acknowledgement and acceptance letter (RAL) from the GCA

3.2.10 Special Categories

The requirements of NISPOM Chapter 8 are written for the general purpose or office automation systems and personal computers. Implementing the same security requirements for components such as weapons or tactical systems, test stands, simulators, or embedded components that can be integral elements of a larger IS may not always be possible. To apply the general requirements of Chapter 8 in these instances may result in unnecessary costs and adversely impact operations.

Examples of special categories or types of systems include:

- Single-User Standalone (SUSA)
- Systems utilizing periods processing
- Test Equipment
- Pure Server
- Test Equipment
- Special Purpose, Tactical, Embedded Systems
- Copiers

3.2.10.1 Single-User, Standalone Systems

Distinct differences exist between single-user standalone and multi-user standalone systems. The information's classification level, and the user's access level and need-to-know are the controlling factors in determining whether technical or non-technical (e.g., administrative and/or environmental measures) security features are required. The emphasis is on protecting classified information and sanitizing memory and media. For most standalone systems, sanitizing memory is the standard requirements for changing between classification levels, information sensitivity, or users.

Extensive technical protection measures are normally inappropriate and inordinately expensive for single-user, stand-alone systems. Administrative and environmental protection measures are sometimes employed as appropriate for such systems, in lieu of technical controls. Typically, a single-user standalone system is assigned to one general user; other general users are not allowed to use the system. System administrators may also have an account for access on a single-user standalone system for maintenance and/or auditing purposes; however this does not constitute a system being considered a MUSA. Automated audit trails should be enabled on single-user standalone systems to capture events that may become relevant if the system is discovered to be compromised. When the system is not capable of automated audit logging, manual logging of system activities shall be implemented. Weekly audit trail analysis should be conducted when the system is capable of automated auditing.

3.2.10.2 Periods Processing

Periods processing systems have one user at a time. These systems are sanitized between uses to allow for differing levels of user access controls, classification levels, or segregation of program data onto separate media. Periods processing systems require an upgrade/downgrade procedure for switching between modes.

- Periods processing is a method of sequential operation that provides the capability to process information at various levels of classification or different general users at different times. It also can include upgrading to the classified level or downgrading to the unclassified level.
- One advantage to periods processing is that an information system is not required for every general user. Different processing periods can be established for different classifications of information and for users with different need-to-know for single user standalones. The ISSP will verify with the ISSM that different processing times are established for the different classifications, sensitivity of information, or users.
- When an information system is being used for periods processing it only requires the submission of one profile, with each hard drive addressed in the hardware baseline by associating it with the classification level and the contract number.
- Periods processing requires sanitization of system resources before and after distinct periods of processing. Sanitization is also required prior to releasing the system from classified information controls or for re-use at a lower classification level. Sanitization for releasing a system typically includes destruction of the fixed media for the system.
- Clearing is required if the information system is not being released to users with a lower access or clearance levels. Systems may be cleared (e.g., hard drive wiped) and then re-used at the same or a higher classification level. Clearing should not normally be employed for systems at the TOP SECRET or higher level.
- Separate media may be used for each period processing session at a different classification level or with different user access.
- During the validation process and on security reviews, the ISSP or IS Rep will observe the contractor’s procedures for upgrading and downgrading the system and ensure that sanitization before and after use is accomplished when periods processing is involved. During the visit, the physical environment should be evaluated to ensure only appropriate personal may view the information being processed.

3.2.10.3 Pure Servers

Pure servers do not fit into standard protection level criteria. As an example, a pure server does not have general users in the traditional sense; however, it does have clients. The only user accounts on a pure server are for privileged users maintaining the device. The software maintenance of pure servers is frequently performed remotely. The system or network administrators no longer have to be physically located at the pure server in order to perform maintenance. Instead, the administrator logs into the device remotely and performs the maintenance. I&A mechanisms, auditing, and access controls are required when conducting remote maintenance.

Reminder

Each pure server is different and serves a specialized purpose; therefore, each pure server must be reviewed by the ISSP before a determination can be made as to what, if any, technical security features are required.

3.2.10.4 Test Equipment

Test equipment with non-volatile memory that is going to process or retain classified information requires accreditation. In cases where there are no technical security features associated with the test equipment, abbreviated procedures may be used in lieu of the standard (M)SSP template to identify areas such as clearing/sanitization procedures and physical security. Sanitization procedures (i.e., Certificate of Volatility from the manufacturer) for all test equipment, classified or unclassified (volatile memory included) should be included in the (M)SSP.

3.2.10.5 Special Purpose, Tactical, Embedded Systems

NISPOM Chapter 8 identifies special purpose, tactical and embedded systems as "special category," and allows for protection measures and safeguards to be implemented on a case-by-case basis, based on the needs of the program. Special purpose and/or tactical equipment are typically designated as such by the GCA/customer. Written designation with security requirements to be implemented should be provided by the GCA/customer and included with the (M)SSP. If the entire system is designated special purpose or tactical no (M)SSP is required, only Standard Operating Procedures (SOP) along with the letter from the GCA stating that the system has been designated as a special purpose or tactical system will be required.

In rare cases when the GCA/customer is unable to provide special purpose or tactical system designation documentation, the ISSM should consult with the ISSP and provide recommended security guidance. The ISSP will discuss the situation with the ISSP Team Lead and RDAA for an evaluation of the system and recommended security controls.

- The ISSP, along with the IS Rep, will assist the ISSM/ISSO in developing protection and safeguarding measures emphasizing the protection of classified information and the sanitizing of memory and media.
- For special purpose systems which are not part of a larger system the ISSM will be required to explain the need to the GCA and get a RAL to include GCA security requirements for the system. The facility will need to retain the RAL and any other GCA provided accreditation documentation for security assessments.
- The GCA letter will be sufficient documentation to identify the system as special purpose. A GCA may provide a consolidated RAL to cover systems at multiple contractor sites.
- Because of calibration and frequency of use in testing environments, removing the battery at the end of the classified processing is not normally an option for the contractor. The contractor must have some type of clearance or sanitization procedure in order to use the equipment for other unclassified processing. Test equipment manufacturers have published clearing and sanitization procedures for their test equipment. The ISSP should ensure these documents meet the requirements for sanitization. In situations where user accessible or configurable data is contained in EEPROM or Flash EPROM, the only approved procedures are those provided by the manufacturer. Additional requirements in the clearing and sanitization matrix also apply. The ISSP will verify sanitization procedures are properly implemented to ensure the equipment is properly sanitized. In some cases, additional requirements may be applied if the sanitization procedure does not address all memory on the system.
- There are instances where test equipment is connected to the classified system but not processing or retaining classified data. There are systems that have a portion of the equipment processing classified, but also have test equipment connected to other equipment (sometimes in racks) that never process classified data. The test equipment in this case must be under Configuration Management (CM) as part of the overall system. However, its presence does not require the system to be reaccredited or the test equipment sanitized.

3.2.10.6 Copiers

Multifunction copiers are basically a PC, printer, and scanner combined into one container. These devices typically have non-volatile memory, hard drives, an operating system, and networking capability. Some utilize RFID technology for device inventory or status management. Copiers with these features are to be accredited. Separate accreditation is only required for standalone devices. Separate accreditation is not required for these devices when connected to an IS as a peripheral device. In these instances, the multifunction device should be included in the connected system's accreditation plan. The SSP should address maintenance, clearing, and sanitization among other things. In particular, area upgrade and monitoring may be necessary to ensure physical security. (NISPOM Chapter 5, Section 6 (Reproduction)) is applicable to these systems. Copiers that do not have non-volatile memory or hard drives do not require accreditation. However, the requirements of NISPOM paragraph 5-600 thru 5-603 apply.

3.2.11 Local Area Networks

A LAN consists of two or more connected workstations for the purpose of sharing information. The physical security parameters within (M)SSPs vary between closed areas and various configurations of restricted areas. However, to avoid the use of removable hard drives on multiple systems, LANs that reside in a closed area are left up and running when unattended. A LAN can be as simple as two interconnected laptops through a category 5 cross-over cable in a peer-to-peer configuration and as complex as a thousand desktops connected by multiple switches and routers traversing several buildings using Active Directory to push group security policies throughout the domain. The defining characteristics of LANs, in contrast to WANs, include their much higher data transfer rates, smaller geographic range, and lack of a need for leased telecommunication lines.

General characteristics of a LAN:

- Two or more computers
- Connection devices:
  - Hubs
  - Switches
  - Routers
- Physical security:
  - Closed area
  - Restricted area
- Peer-to-peer
- Client-server/Active Directory

Operating system must be NISPOM compliant, or have a risk acceptance letter.

3.2.12 Interconnected System/Wide Area Network

3.2.12.1 Unified Networks

A unified network applies when all involved DAAs concur that there will be a single security policy for the entire WAN. For WANs where all the nodes are accredited by DSS, the RDAA of the host node will accredit the network. The network can have an SSP for a unified network that outlines all the requirements contained in NISPOM paragraph 8-610. The plan review and system validation process will be coordinated between DSS offices to ensure each connected site is visited.

3.2.12.2 Interconnected Networks

An interconnected network consists of two or more separately accredited systems connected together. Interconnected networks may be contractor-to-contractor or government-to-contractor connections, or a combination of both. It is very important for ODAA to review the access levels, categories and classification of the information, and need-to-know for all connecting sites. A Protection Level (PL) 1 system at one site connecting to a PL 1 system at another site could create a PL 2 or a PL 3 network. For uniformity purposes, the PL of the network will equal the PL of the highest node on the network. For example, if one of the nodes requires PL 2, the network will then be accredited at PL 2. The network can be configured at PL 2 by use of a controlled interface. However, only the node that requires PL 2 will be required to meet all the PL 2 requirements. Other nodes on the network that are PL 1 will be required to meet PL 1 requirements.

A WAN is a computer network that covers a broad area (e.g., any network whose communications links cross metropolitan, regional, or national boundaries), or, less formally, a network that uses routers and public communications links. This is in contrast with personal area networks (PANs), local area networks (LANs), campus area networks (CANs), or metropolitan area networks (MANs) which are usually limited to a room, building, campus or specific metropolitan area (e.g., a city, state) respectively. The largest and most well-known example of a WAN is the Internet.

WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations. Many WANs are built for one particular organization and are private. Others, built by Internet service providers, provide connections from an organization's LAN to the Internet.

3.2.12.3 Contractor to Contractor Networks

Network Security Plans

A NSP must be written for any interconnection between two or more separately accredited information systems including two or more systems owned by the same ISSM at the same facility or campus (CAGE code).

The NSP is used to document the security posture of the interconnecting systems in a standalone document separate from the associated profiles for the interconnected systems. The NSP provides the DAA with an overall view of the WAN and interconnections along with the associated security requirements. The NSP is assigned its own ODAA Unique Identifier and is accredited as an information system. Utilizing an NSP for a WAN enables the ODAA to add new connections or nodes to the system without requiring the existing nodes to be reaccredited.

The NSP is submitted and managed by the designated host ISSM. The NSP is submitted into the process like standard system security plans. The host ISSM and responsible DSS office are responsible for accrediting, and reaccrediting, the interconnected network's NSP.

NSP Content

The responsibility for creating, gaining accreditation, and maintaining an NSP belongs to the ISSM responsible for the "host" node. If the WAN is accredited by DSS, the accreditation document for the WAN will be referred to as the NSP. If the WAN is not accredited by DSS, the name and content of this document may be different from a standard DSS NSP. This is typically encountered when a DSS-accredited information system is connecting to a WAN accredited by another government entity or DAA. This type of connection also requires an MOU or an MOA signed by all DAAs with systems connected. MOAs/MOUs are covered in detail in the Government Interconnection Agreements section *3.2.13.1*.

As a minimum, an NSP should include the following information for the WAN:

1. ODAA Unique ID and IS name
2. Physical addresses for connected sites
3. Point of contact (POC) information for each site
4. Protection level (PL) and the highest classification of data with any caveats or formal access requirements identified
5. Minimum clearance level required for user access to the WAN
6. Description of the system along with a diagram showing all connections
7. Encryption method and devices in use
8. Security responsibilities for the WAN and nodes
9. Network connection rules including a statement from the ISSM as to whether or not full node accreditation will be required for connection or if an interim approval is sufficient. This only applies to WANs identified as PL 1
10. Signed and dated statement from the ISSM attesting that there are no additional connections to the WAN not identified in the NSP
11. A network participation data sheet for each node which includes requirements listed in bullets 1-8 above and a description of the node system. This must be signed by the node ISSM
12. For any node not accredited by DSS an accreditation letter or a signed MOU/MOA. If the node is under a DSS accredited MSSP, the profile associated with the node must be identified
13. NISPOM Chapter 8 compliant security policies and procedures for any systems or components seeking accreditation as part of the NSP
14. Controlled Interfaces (Firewall) description with ports and protocols
15. Access control lists (if applicable)
16. Intrusion Detection System (IDS) requirements (if any)
17. For auditing purposes, record activities occurring across the interconnection
18. Identify any I&A methods used to authenticate users across the interconnection
19. Specific virus scanning or anti-virus requirements (if any)
20. Identify physical security requirements (e.g., closed or restricted area)

The Network ISSM/ISSO will submit the NSP and include copies of current accreditation letters for all nodes connected to the WAN. The DSS reviewer will verify all nodes have a current accreditation letter in the NSP package. In addition, a signed copy of each node ISSM's participant data sheet will be included with the NSP submitted to DSS for review and accreditation. When the NSP is subsequently submitted for reaccreditation (e.g., when adding a new node) the Network ISSO will include current accreditation letters for all nodes submitted. If the NSP is submitted with copies of expired accreditation letters, review and approval will be delayed until updated copies are obtained.

NSPs covering two or more separately accredited systems at the same facility, campus or CAGE and managed by the same ISSM can be simplified. In such cases, the ISSM can submit a single page NSP that address requirements 1-7, 10 and 13 above and includes each nodes' ODAA UID (and IS profile if under a MSSP), protection level, location, if different from facility address, classification of data processed with any additional caveats, minimum clearance of users and node name.

Under these circumstances, the NSP should also contain the following WAN connection rules:

- All personnel will be briefed on the use of the WAN and will be knowledgeable of the NSP security requirements
- WAN configuration changes must be approved by the ISSM to determine if the reconfiguration constitutes a security relevant change which requires approval or reaccreditation by the DAA
- Any configuration changes affecting the node's protection level, classification or categories of information processed, formal access approvals, or the clearance level of users must be approved by the DAA for both the node and the WAN before the change can be made
- Other WAN connection rules could be added at the discretion of the ISSM and/or DAA.

Submitting the NSP to DSS for accreditation – Step-by-Step

1. The need for interconnection or WAN establishment is noted by two or more information systems to support contractually related work or programs.
2. One ISSM is designated "host" node and assumes role of "Network ISSO" for the WAN or interconnected system.
3. Host node ISSM or "Network ISSO" prepares the NSP.
   - Collects signed participant data sheets and local accreditation letters from all node ISSMs
   - Provide e-mail addresses in the package for all node ISSMs
   - Ensures encryption devices are in place at all nodes. Some nodes may need to get reaccredited locally when adding the encryptor and WAN connection to the profile
   - Determines if an MOU is needed. If yes, uses the DSS template to create an MOU customized for the requirements. Obtains and inserts DAA signature blocks onto the MOU form
   - Completes the NSP document and diagram, etc. Attaches MOU (if required), accreditation letters and signed participant data sheets for each node
   - Assigns an ODAA Unique Identifier to the NSP
   - Documents any devices or components that are to be accredited with the NSP instead of in an associated profile. This is rare, but all NISPOM required information is required. Typically, an SSP attachment to the NSP may be used
   - E-mails the completed package to DSS ODAA and copies DSS personnel as required by the process manual
4. The ISSP will review the NSP for completeness and make certain all required documentation is included.
   - If the NSP includes components/devices not accredited under an associated profile (rare), the ISSP will schedule a visit to validate these components
   - There may be cases where an NSP is granted an IATO, but typically, an NSP is issued an ATO when all documentation is correct

- Any required MOUs based on node connections documented in the NSP must be signed by all DAAs before the NSP is approved

5. RDAA will sign and distribute the NSP's ATO. The NSP ATO will be sent back to the Network ISSO and responsible DSS personnel.
6. Network ISSO provides each node with a copy of the NSP, its accreditation letter, and any associated MOUs.

Connecting to a WAN Accredited by DSS

The NSP for a DSS-accredited WAN is processed in the same manner as an (M)SSP. The Network ISSO is responsible for creating and submitting the NSP through the review process for accreditation by the host DAA.

Realizing that adding nodes to a WAN could potentially change the security posture of the WAN, each node to be added must be evaluated for clearance and need-to-know concerns. When DSS is the WAN DAA a connection determination must be made. In order to provide consistency, the following rules will be applied. The final node connection determination is still subject to the discretion of the ODAA.

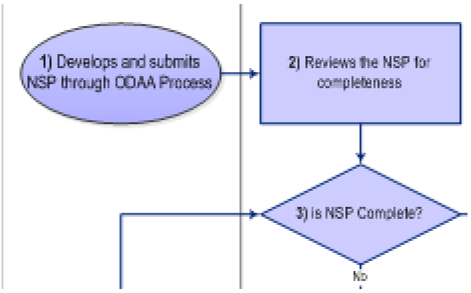
Connection	Example
True Protection Level (PL) 1 WAN If the WAN and all connecting nodes are at PL-1, all users across the WAN and all nodes have the same need-to-know (NTK) for all of the information processed on the WAN and all nodes, a node can be allowed to connect while under an IATO provided that the WAN ISSM has not indicated otherwise in the NSP. This will be referred to as a True PL-1 WAN.	A PL-1 WAN called TC-WAN owned by Tech Company processing SECRET collateral has two PL-1 nodes owned by Tech Company. Tech Company subcontracts the construction of a widget to IT Security Inc. To facilitate in this endeavor IT Security Inc. requests to be allowed to connect their SECRET collateral PL-1 node to the TC-WAN. The reviewer for the IT Security node (M)SSP notes that all the nodes and the TC-WAN only processes SECRET Collateral and that all users of the node and WAN have the same NTK. The IT Security Inc. (M)SSP is reviewed and granted an IATO. After consulting the NSP for TC-WAN, the reviewer determines that there is no objection by the Tech Company ISSM (Network ISSO) for connecting the PL-1 IT Security Inc. node to TC-WAN while under IATO. The Network ISSO submits an updated NSP along with the accreditation letter for the new node. After approval of the connection and issuance of an updated ATO for the NSP authorizing the connection, it is the responsibility of the ISSMs to coordinate the connection and notify their respective IS Reps and ISSPs of the connection status for the node(s).
PL-2+ Node Connecting to a PL-1 WAN (NTK protections/controlled interface are provided by the node) When all users on a node do not have the NTK for the all information on the WAN or when all the users of the WAN do not have the NTK all the information processed on the node, the node will not be allowed to connect to the WAN until it receives full accreditation status or ATO. The node can be given an IATO so that it can begin processing as a local system. After a satisfactory onsite validation is completed by the ISSP, an ATO may be issued for the node. The Network ISSO will submit an updated NSP along with a copy of the node's ATO. This requirement ensures the NTK protections provided	A PL-1 WAN called TC-WAN owned by Tech Company processing SECRET collateral has two PL-1 nodes owned by Tech Company. Tech Company subcontracts the construction of a widget to IT Security Inc. for "Really Big Project" (RBP). To facilitate in this endeavor IT Security Inc. requests to be allowed to connect their SECRET collateral node to the TC-WAN. The IT Security Inc. ISSM determines that some of the users on his node do not have the NTK for the RBP information that will be passing to some of the users on his IT Security Inc. node. The IT Security Inc. ISSM submits a security plan for his node as a PL-2 and provides the necessary requirements to prevent the users without the NTK for RBP information from accessing this information on his node or accessing any portion of the TC-WAN. After

at the node are in place and working properly. The new node may connect after the NSP is issued an updated ATO reflecting approval for the connection is issued by the DAA.	reading the IT Security node's (M)SSP, the ISSP (through the DAA) may issue an IATO for the node. However, since the node is at PL-2, some of the users are not permitted access the TC-WAN and RBP data. In this case, the node will not be allowed to connect until it has received an ATO. This ensures the node has been inspected and the NTK protection measures validated. The Network ISSO will submit an updated NSP along with the ATO for the new node. Once the updated ATO for the NSP is issued, the node will be allowed to connect.
PL 2+ WAN **(NTK protection/controlled interface provided by the WAN)** A WAN at PL-2 level or greater must be granted an ATO before a node can connect if the NTK protections are provided as part of the WAN. This may be encountered in cases where the WAN NSP includes actual devices or equipment not accredited as part of a node. This requires the NSP to gain full accreditation before allowing a connection and ensures NTK protections are properly configured and working on the WAN. In this scenario, the ISSP will complete an onsite validation visit for the NSP. This type of arrangement would not be encountered when accrediting a "conceptual WAN" described earlier where no actual network devices are accredited under the NSP. Most of the DSS-accredited WANs are of the conceptual type and would not usually require an onsite validation.	A PL-2 WAN called TC-WAN owned by Tech Company processing SECRET collateral has three nodes Tech Company node A, Tech Company node B and Tech Company Security node C. Node A and node B have the NTK for Project 1 information. Node A and node C users have the NTK for information related to project 2. A server farm, firewall and Layer 3 switch are accredited as part of the WAN NSP. The WAN configuration and network devices will ensure only users on nodes A and B can see project 1 data and users on nodes A and C can see project 2 data. Before any node is authorized to connect, the WAN's NTK protection/devices must be validated by the ISSP and the WAN NSP must be granted an ATO. After the NSP is granted an ATO, the nodes will be allowed to connect in accordance with the NSP's ATO.
PL 2+ WAN **(NTK protection/controlled interface provided by the WAN and nodes)** In rare cases where NTK protection are provided by a combination of devices on the WAN and one or more nodes, both the WAN and the nodes must achieve an ATO before a connection is permitted. Adding a Node Under IATO to a WAN - Adding a node that is operating under an IATO requires issuance of an updated ATO for the NSP to authorize the connection. Adding a node under IATO to the WAN will not cause the WAN to revert to an IATO. Remember that a node will not be allowed to connect while under IATO if the node provides NTK protections for the WAN connection. Therefore, all NTK protections for the WAN will remain intact even when a node is allowed to connect while under IATO.	A PL1 WAN owned by Company "A" has an ATO and is processing SECRET collateral. It has two Company "A" PL1 nodes one with an ATO and one with an IATO. Company "B" has a PL1 node also only processing SECRET collateral and wishes to connect to the WAN. It is determined that this node has the same NTK as the WAN and the other two nodes and that it can connect to the WAN while under IATO. When this node connects, it does not change the WAN's ATO to an IATO.

Adding a node to an existing DSS WAN – Step-by-Step

1. Host node ISSM or "Network ISSO" updates the NSP.
   - Collects signed participant data sheets and local accreditation letters from the new node ISSM(s)
   - Verifies all existing nodes' participant data is current and requests updated information as needed
   - Provides e-mail addresses for all node ISSMs
   - Ensures encryption devices are in place at new nodes. NOTE: Some nodes may need to be reaccredited locally when adding the encryptor and WAN connection to the profile
   - Determines if an MOU is needed for the new nodes' connection. If yes, uses the DSS template to create an MOU customized for the requirements. Obtains and inserts DAA signature blocks onto the MOU form
   - Updates the NSP document and diagram, etc. Attaches MOU (if required), local accreditation letters for new node(s) and any updated local accreditation letters or signed participant data sheets
   - E-mails the completed package to DSS ODAA and CCs DSS personnel as required by the process manual
2. The ISSP will review the NSP for completeness and ensure all required documentation is included.
   - If the NSP includes components/devices not accredited under an associated profile (rare), the ISSP will schedule a visit to validate these components if there were changes (rare)
   - Required MOUs must be signed by all DAAs before the node is allowed to connect to the WAN
3. The ISSP will forward the updated draft ATO for the NSP to the RDAA.
   - RDAA will sign and send the signed ATO for the NSP back to the Network ISSO
   - The Network ISSO will update all nodes with a copy of the ATO and updated NSP along with any new or modified MOUs

Example
NSP Accreditation


1) Develops and submits NSP through ODAA Process
2) Reviews the NSP for completeness
3) Is NSP Complete?
No

NSP Accreditation Flow Diagram illustrates the general process flow for DSS NSP accreditation and connecting nodes to the WAN. Other DAAs will have their own specific processes that may be similar. The contractor ISSM wishing to establish a connection to a non-DSS WAN is responsible for contacting the appropriate WAN DAA or representative for resolving issues related to those connections.

An example of the NSP Accreditation Flow Diagram is located in the Reference Materials (14.1.5), page 99.

Changes in Status – From IATO to ATO or From ATO to IATO

After the node is connected to the WAN, the node ISSM is required to notify the Network ISSO of any changes in local accreditation status. Similarly, the Network ISSO is required to notify node ISSM(s) of any changes in the WAN's accreditation status.

The typical scenario is that a new node connects to the WAN while under an IATO. Once the node gets an ATO for the local accreditation, the node ISSM is required to forward a copy to the Network ISSO. The Network ISSO should maintain a copy of the ATO with the NSP. When the NSP is updated and submitted for reaccreditation, the updated letter should be included. The same process is followed if a node gets downgraded to IATO status from an ATO.

Withdrawal or Invalidation of Accreditations

If the accreditation for a WAN is terminated for any reason, all connections to that WAN must be severed. Nodes that later reconnect to a DSS accredited WAN that had its IATO or ATO withdrawn or invalidated need not be revalidated unless security relevant changes have occurred. When connections to the WAN are again allowed, the

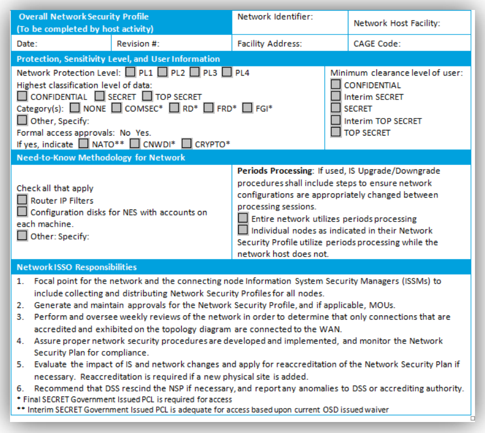
NSP's ATO will be updated and re-issued. The ATO will list all authorized node connections. The Network ISSO should keep all node accreditation letters updated as necessary prior to submitting the NSP.

When a node's IATO or ATO is withdrawn or invalidated, the node is no longer authorized to be connected to any WAN or process information locally. The DAA may require the node to gain full accreditation (ATO) before an approval is issued for the node to again connect to the WAN(s).

Connecting to a WAN not accredited by DSS

When a DSS-accredited node is connecting to a non-DSS accredited WAN, the approval to connect is granted by the non-DSS DAA. An MOA or MOU is required to document security responsibilities for the connection. The MOA/MOU's content should be limited to information systems security/DAA responsibilities only and not include other information such as funding requirements. DSS has a standard MOU/MOA template that should be used. The MOU or MOA should state whether a full ATO is required before a DSS controlled contractor node can be connected to the WAN and provide point of contact (POC) information. The MOU/MOA must require all nodes and the WAN be accredited in accordance with the respective certification and accreditation requirements documents.

Example
Overall Network Security Profile



Overall Network Security Profile **(To be completed by host activity)**		Network Identifier:	Network Host Facility:
Date:	Revision #:	Facility Address:	CAGE Code:

Protection, Sensitivity Level, and User Information

Network Protection Level: □ PL1 □ PL2 □ PL3 □ PL4
Highest classification level of data:
□ CONFIDENTIAL □ SECRET □ TOP SECRET
Category(s): □ NONE □ COMSEC* □ RD* □ FRD* □ FGI*
□ Other, Specify:
Formal access approvals: No Yes.
If yes, indicate □ NATO** □ CNWDI* □ CRYPTO*

Minimum clearance level of user:
□ CONFIDENTIAL
□ Interim SECRET
□ SECRET
□ Interim TOP SECRET
□ TOP SECRET

Need-to-Know Methodology for Network

Check all that apply
□ Router IP Filters
□ Configuration disks for NES with accounts on each machine.
□ Other: Specify:

Periods Processing: If used, IS Upgrade/Downgrade procedures shall include steps to ensure network configurations are appropriately changed between processing sessions.
□ Entire network utilizes periods processing
□ Individual nodes as indicated in their Network Security Profile utilize periods processing while the network host does not.

Network ISSO Responsibilities

1. Focal point for the network and the connecting node Information System Security Managers (ISSMs) to include collecting and distributing Network Security Profiles for all nodes.
2. Generate and maintain approvals for the Network Security Profile, and if applicable, MOUs.
3. Perform and oversee weekly reviews of the network in order to determine that only connections that are accredited and exhibited on the topology diagram are connected to the WAN.
4. Assure proper network security procedures are developed and implemented, and monitor the Network Security Plan for compliance.
5. Evaluate the impact of IS and network changes and apply for reaccreditation of the Network Security Plan if necessary. Reaccreditation is required if a new physical site is added.
6. Recommend that DSS rescind the NSP if necessary, and report any anomalies to DSS or accrediting authority.

* Final SECRET Government Issued PCL is required for access
** Interim SECRET Government Issued PCL is adequate for access based upon current OSD issued waiver

An example of the Overall Network Security Profile is located in the Reference Materials (14.1.6), page 100.

The contractor can write an MSSP for the node under DSS cognizance provided that it is not explicitly denied in the MOU/MOA. The addition of a like system to the contractor node under a DSS approved MSSP must be approved by the WAN DAA or designated WAN POC. The contractor must contact the WAN POC to seek permission to add the like system prior to the addition unless otherwise directed by the WAN DAA. The decision of the WAN POC must be communicated to the IS Rep, ISSP and FOC for the contractor node. If the WAN POC or DAA determines that like systems can be added to the DSS approved MSSP for the node without seeking further approval of the WAN CSA, the contractor is still required to notify their IS Rep of the addition of self-certified systems.

Non-DSS WAN Connection Example: Army is the DAA for the Big Army Wan (BAW). The DSS-accredited contractor node IS# 123 has a contractual reason to connect to the Army WAN. If the Systems Security plan for IS# 123 has not identified that a WAN connection exists, the contractor must update and submit the security plan to DSS ODAA for reaccreditation with a WAN connection documented in the plan. An MOU has been signed between the Army DAA and the DSS DAA. The MOU requires all nodes to be accredited before connection to the WAN but does not state full accreditation of the node is required. The DSS DAA has granted an IATO for IS#123's SSP (reflecting a WAN connection). Upon receipt of the IATO, the contractor for node IS# 123 contacts the Army POC for the BAW and requests approval to connect. The Army POC requests a copy of the DSS issued IATO for node #123 from the contractor and decides that the IATO will be sufficient for the contractor node to connect. The contractor notifies the IS Rep, ISSP and FOC that the connection has been made to the BAW.

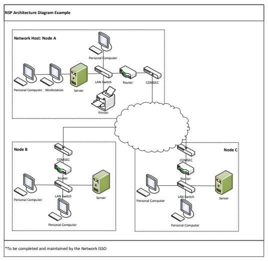
Self-certification of a workstation on the DSS-accredited node when DSS is not the WAN DAA Example: The profile for contractor node IS# 123 is under a MSSP for a small development LAN. The ISSM has been granted self-certification for like systems on the local node. The ISSM contacts the BAW POC to request permission to self-certify an additional workstation on the IS# 123 node. The BAW POC allows the self-certified system to be connected to the WAN node. The ISSM for IS# 123 contacts the IS Rep and ISSP to inform them the BAW POC is allowing the connection of a self-certified workstation to IS# 123. The ISSM then follows up this notification by sending the IS Rep the statements of self-certification for adding like workstations to the node in the manner and frequency agreed upon by the ISSM and IS Rep.

Example
NSP Architecture Diagram and Network Security Forms

The following examples are located in the Reference Materials:

- *NSP Architecture Diagram Example (14.1.7), page 102*
- *Network Host Security Profile (14.1.8), page 103*
- *Network Node Security Profile Form (14.1.9), page 105*

NSP Architecture Diagram Example



*To be completed and maintained by the Network ISSO

Network Host Security Profile (To be completed by Network Host) | Network Identifier: | Network Host Facility:

Date: | Facility Address: | CAGE Code:

IS Contact Information

Network DAA: Phone Number: | Network ISSP: Phone Number: | Network ISSO: Phone Number: | ISSM: Phone Number:

Contracts Supported (Contract Numbers):

Describe role in supporting the above contract(s):

Reason for network participation ☐ Access other nodes ☐ Other nodes access your node

This node is accessible by (check/describe all that apply): ☐ O/S Login ☐ Other:

Specify all nodes accessing your node:

If applicable, describe procedures for remote users to gain access to your site:

Description of local systems/network:

☐ Terminal Node (no backside connections) ☐ Backside connections, separately accredited WAN:

IS Protection, Sensitivity Level, and User Information

Accredited Protection Level: ☐ PL1 ☐ PL2 ☐ PL3 ☐ PL4

Highest classification level of IS data:
☐ CONFIDENTIAL ☐ SECRET ☐ TOP SECRET

Category(s):☐ NONE ☐ COMSEC* ☐ RD* ☐ FRD* ☐ FGI*
☐ Other Specify:

Formal access approvals: ☐ No ☐ Yes

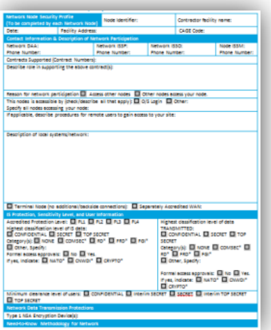
If yes, indicate: ☐ NATO* ☐ CNWDI* ☐ CRYPTO*

Highest classification level of data TRANSMITTED:
☐ CONFIDENTIAL ☐ SECRET ☐ TOP SECRET
Category(s): ☐ NONE ☐ COMSEC*
☐ RD* ☐ FRD* ☐ FGI*
☐ Other Specify:

Formal access approvals: ☐ No ☐ Yes
If yes, indicate: ☐ NATO* ☐ CNWDI*
☐ CRYPTO*

Minimum clearance level of users: ☐ CONFIDENTIAL ☐ Interim SECRET ☐ SECRET ☐ Interim TOP SECRET
☐ TOP SECRET

Network Data Transmission Protections



Network Node Security Profile (To be completed by each Network Node) | Node Identifier: | Contractor facility name:

Date: | Facility Address: | CAGE Code:

Contact Information & Description of Network Participation

Network DAA: Phone Number: | Network ISSP: Phone Number: | Network ISSO: Phone Number: | Node ISSM: Phone Number:

Contracts Supported (Contract Numbers):

Describe role in supporting the above contract(s):

Reason for network participation ☐ Access other nodes ☐ Other nodes access your node.

This nodes is accessible by (check/describe all that apply): ☐ O/S Login ☐ Other:

Specify all nodes accessing your node:

If applicable, describe procedures for remote users to gain access to your site:

Description of local systems/network:

☐ Terminal Node (no additional/backside connections): ☐ Separately Accredited WAN:

IS Protection, Sensitivity Level, and User Information

Accredited Protection Level: ☐ PL1 ☐ PL2 ☐ PL3 ☐ PL4
Highest classification level of IS data:
☐ CONFIDENTIAL ☐ SECRET ☐ TOP SECRET
Category(s): ☐ NONE ☐ COMSEC* ☐ RD* ☐ FRD* ☐ FGI*
☐ Other, Specify:
Formal access approvals: ☐ No ☐ Yes
If yes, indicate: ☐ NATO* ☐ CNWDI* ☐ CRYPTO*

Highest classification level of data TRANSMITTED:
☐ CONFIDENTIAL ☐ SECRET ☐ TOP SECRET
Category(s): ☐ NONE ☐ COMSEC* ☐ RD* ☐ FRD* ☐ FGI*
☐ Other, Specify:

Formal access approvals: ☐ No ☐ Yes
If yes, indicate: ☐ NATO* ☐ CNWDI*
☐ CRYPTO*

Minimum clearance level of users: ☐ CONFIDENTIAL ☐ Interim SECRET ☐ SECRET ☐ Interim TOP SECRET
☐ TOP SECRET

Network Data Transmission Protections

Type 1 NSA Encryption Device(s):

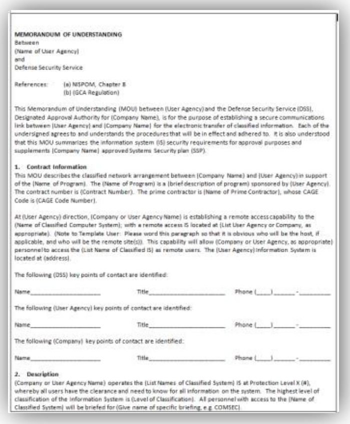
Need-to-Know Methodology for Network

3.2.13 Government to Contractor Networks

3.2.13.1 Government Interconnection Agreements

For the purposes of this manual, Memorandum of Understandings (MOUs), Memorandum of Agreements (MOAs) and Interconnection Agreements are used interchangeably. The term MOU may be used generically throughout this document in reference to all three types of agreements. MOUs created for other purposes (e.g., sharing a space or closed area) are not addressed in this manual.

Example
Memorandum of Understanding



MEMORANDUM OF UNDERSTANDING
Between
(Name of User Agency)
and
Defense Security Service

References: (a) NISPOM, Chapter 8
(b) (GCA Regulation)

This Memorandum of Understanding (MOU) between (User Agency) and the Defense Security Service (DSS), Designated Approval Authority for (Company Name), is for the purpose of establishing a secure communications link between (User Agency) and (Company Name) for the electronic transfer of classified information. Each of the undersigned agrees to and understands the procedures that will be in effect and adhered to. It is also understood that this MOU summarizes the information system (IS) security requirements for approval purposes and supplements (Company Name) approved Systems Security plan (SSP).

1. Contract Information

This MOU describes the classified network arrangement between (Company Name) and (User Agency) in support of the (Name of Program). The (Name of Program) is a (brief description of program) sponsored by (User Agency). The contract number is (Contract Number). The prime contractor is (Name of Prime Contractor), whose CAGE Code is (CAGE Code Number).

At (User Agency) direction, (Company or User Agency Name) is establishing a remote access capability to the (Name of Classified Computer System); with a remote access IS located at (List User Agency or Company, as appropriate). (Note to Template User: Please word this paragraph so that it is obvious who will be the host, if applicable, and who will be the remote site(s)). This capability will allow (Company or User Agency, as appropriate) personnel to access the (List Name of Classified IS) as remote users. The (User Agency) Information System is located at (address).

The following (DSS) key points of contact are identified:

Name____________________ Title______________________ Phone (____)______-_________

The following (User Agency) key points of contact are identified:

Name____________________ Title______________________ Phone (____)______-_________

The following (Company) key points of contact are identified:

Name____________________ Title______________________ Phone (____)______-_________

2. Description

(Company or User Agency Name) operates the (List Names of Classified System) IS at Protection Level X (#), whereby all users have the clearance and need to know for all information on the system. The highest level of classification of the Information System is (Level of Classification). All personnel with access to the (Name of Classified System) will be briefed for (Give name of specific briefing, e.g. COMSEC).

Using this document to create an MOU will reduce the time required for review and processing by DSS.

An approved template or sample MOU document is located in the Reference Materials (14.1.10), page 107.

An MOU between DSS and the GCA is required for all government to contractor connections to include connections over STE, and Secure Data Devices. MOUs following the DSSMOU template format do not require approval by the DSS Office of the General Counsel (OGC). MOUs using other template formats must be reviewed and approved by the DSS OGC and the Office of Policy.

An MOU is not required for contractor to contractor connections if DSS is the DAA for both accredited ISs, only an NSP is required for such connections. If the contractor requires an MOU, that is between the two contractors who require the connection. The purpose of an MOU is to adjudicate the differences in requirements of different DAAs and to establish roles and responsibilities. Many GCAs and program offices have standard MOU formats that are routinely utilized for all MOUs. The GCA may use their format if they'd like; however, DSS may levy additional requirements in order to be NISPOM compliant.

Interconnected systems that result in the requirement for an MOU may range from complex WANs to simple connections between two standalone systems.

All MOUs must be sent to the ODAA Headquarters for coordination and signature. ODAA requires a minimum of 30 days to coordinate and properly staff all MOUs for signature. MOUs are valid for a maximum of three years, at which time they must be resubmitted for both GCA and DSS review, and signature. They may be rescinded by either party (DSS or GCA) with prior notification to, DSS or the GCA, at any time.

3.2.13.2 MOU Content

If an MOU is submitted in a format other than the DSS approved format, more DSS internal reviews are required prior to approval. Processing and approval time within DSS will be impacted greatly. It is recommended that the DSS approved MOU format be used.

All MOUs must contain the following minimum information:

- Date of the MOU
- Names and signatures of Designated Accrediting/Approving Authorities
- Name of Network ISSM/ISSO and responsibilities
- High-level description of and usage of the network
- Contract or program name
- Name and location of facilities involved
- Network type: Unified or Interconnected (usually interconnected)
- Documentation of any existing connections to DISN circuits
- A statement that there is no further connection to any DISN network not outlined in the MOU and none will be added in the future (SIPRNet, SDREN,

- Security points of contact and phone numbers
- Names, numbers or system identifiers for systems involved
- Highest classification of data
- MOU expiration date or review frequency (if applicable)
- Network protection level
- Minimum clearance level required of users
- Categories and formal access approvals (if applicable)

DISN-LES, etc.)

- Encryption method
- A statement regarding required accreditation status for interconnected sites and informing Network ISSO about any changes in accreditation status
- A start and end date
- MOU valid for a maximum of up to three years
- A requirement to be signed by all parties before the MOU is effective

MOU Changes and Invalidations

MOUs are valid for three years or until system changes occur that affect the security posture and agreement defined in the MOU. Some MOUs specify a pre-determined review frequency. During the review, security parameters, the need for the MOU, POC information and DAA signatory information should be verified. If changes are required, a new MOU should be vetted and routed for signatures.

MOUs may become invalid if the security posture of a node or the WAN itself changes. Changes must be evaluated by the signing DAAs to determine the impact (if any) on the accreditation of the WAN and/or the validity of the MOU.

Changes that may affect the security posture of the WAN or a node should be approved by the DAAs prior to implementation.

3.3 Types of Security Plans

Plans submitted to DSS must be submitted using the applicable DSS-provided system security plan templates in order to accommodate timely reviews. The templates can be requested from the DSS web site. Once completed, plans should be kept from public disclosure, as they can provide adversaries insight to how classified information is being protected.

There are three types of plans that can be submitted to the ODAA:

- System Security Plan (SSP)
- Master Systems Security Plan (MSSP)
- Network System Plan (NSP)

One system security plan may include IS that are being accredited to support multiple program areas as long as the users have the proper authorization and need-to-know for all information on the system. If some users are not authorized access to all data, a PL2 system is required. It is recommended that data from different programs remain separated to facilitate potential removal of data at the end of contract.

The SSP is the formal document used by the government contractor to identify the protection measures to safeguard information being processed in a classified environment. The process flow for submitting SSPs is explained in the C&A Process. The submission format is outlined in the Systems Security Plan Submission Process section.

The ISSM will make the SSP accessible to authorized personnel.

3.3.1 Master Systems Security Plan

The term “Master” indicates the authorization to add like systems to an approved plan by an ISSM. The ISSM may add like systems to the MSSP after the ODAA has determined the ISSM has the requisite knowledge and skills to manage multiple IS under one master plan. Upon determination that the ISSM has met the requisite requirements, self-certification authority may be granted in the ATO. If self-certification has not been granted the plan will follow the procedures for submitting an SSP.

The following is included in this section:

- Defining “Similar”
- Managing added IS
- Self-certification

The concept of the MSSP allows two or more IS that operate in equivalent operational environments (e.g., the levels of concern and protection level are the same, the users have at least the required clearances and access approvals for all information on the IS(s), the IS configurations are essentially the same, and the physical security requirements are similar) to be protected by one plan. For instance, if a plan was submitted for a MUSA IS in a closed area and it was determined that a MUSA IS in another closed area could be adequately protected using the same plan, that IS can be added to the plan (assuming the ISSM was authorized to do so through the use of self-certification). An MSSP may be written by the ISSO, certified by the ISSM, and then approved by the CSA to cover all such IS. This type of approval applies only to IS(s) operating at PL 1 or 2.

Master Plan Structure

The use of an MSSP is offered to expedite the processing of system additions and deletions. MSSPs are specific and will apply to all the systems that fall under the MSSP (e.g., the levels of concern, protection level, need-to-know, system type, protection measures, systems configurations and physical security). If there are any changes to the MSSP, those changes will affect every IS that fall under, and are protected by, that MSSP.

After the RDAA grants approval for an MSSP, an IATO may be issued based on the protection measures for the IS submitted by the ISSM. During the IATO period, the ODAA copy of the MSSP is the official copy. The ISSP for the facility will validate the IS(s) represented in the MSSP and approved in the IATO as soon as practical, but not more than 180 days from the time the IATO was granted. After a successful onsite validation, the RDAA will issue an ATO for the system, system type(s), operating system(s), operations, and operating environment that the ISSM is approved to self-certify. Like systems that meet the requirements of the MSSP and are “like” the accredited system as defined in the MSSP may be self-certified by the ISSM as meeting the conditions of the approved MSSP. This self-certification authorizes the individual IS to operate under the ATO issued by DSS for the MSSP.

Self-certification will not be granted for an IS in an IATO status. ISSMs with self-certification authority granted through an MSSP ATO may continue to self-certify systems under the MSSP during reaccreditation activities resulting in the system reverting to IATO status. If the system is disestablished, or expires, self-certification authority under the MSSP is removed.

ISSMs may consider combinations of conditions from multiple accredited MSSPs granting self-certification authority to determine whether or not he/she may self-certify a system. For example, if an ISSM has authority to self-certify MS Windows under an MSSP for restricted areas and has as separate MSSP for closed areas, he/she may self-certify MS Windows for a closed area.

When adding new operating systems or configurations not currently addressed in MSSPs granting self-certification authority, the ISSM must submit the approved MSSP as an attachment with the new IS profile being submitted for accreditation.

The ISSM must include the certification test results and a signed statement by the ISSM attesting that the security features are implemented and operational on this system as attachments to the e-mail. At least one system of

each OS, system type, or configuration must be certified by the CSA to receive an ATO and self-certification authority. A copy of each certification report must be retained with the approved copy of the MSSP.
The ISSM must maintain a listing of all systems accredited by the CSA and those self-certified by the ISSM under an approved MSSP since the last annual security review. The format to be used is provided at the end of this section (see the MSSP Tracking Form). This listing/form will be presented to the ISSP prior to the start of a security review and provide enough information to uniquely identify the new systems. This listing does not replace the requirement for the ISSM to work with their ISSP to determine submission frequency of self-certified IS and any other required notifications.

Information Systems certified under an MSSP remain certified until the MSSP is changed, the ATO for the (M)SSP is rescinded/withdrawn or three years have elapsed since the IS was certified.

If there are no security relevant changes, the three-year reevaluation (reauthorization) may be based on an e-mail from the ISSM to the ODAA stating that there have been no security relevant changes to the system described in the (M)SSP.

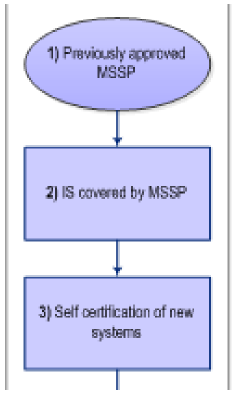
General Guidelines for MSSPs and Self-Certification

Self-Certification Requirements

Self-certification authority may be granted for an ISSM who has demonstrated the requisite level of knowledge and competence necessary to properly manage the information systems security program. Self-certification will be under constant review to ensure the program is properly managed. Self-certification authority may be rescinded at the discretion of the Regional DAA. Completion of the following items is recommended prior to an ISSM seeking self-certification authority.

- Completion of the following DSS online courses:
  - Introduction to the NISP Certification and Accreditation (C&A) Process
  - NISP C&A Process: A Walk-Through
  - Technical Implementation of Certification and Accreditation (C&A)
- Completion of appropriate IT specific training (e.g., Security +, Microsoft, UNIX etc.)

Example
Flow Diagram for Self-certification under a MSSP


1) Previously approved MSSP
2) IS covered by MSSP
3) Self certification of new systems

A Flow Diagram for Self-Certification under a MSSP is located in the Reference Materials (14.1.11), page 110.

MSSP General Requirements

An MSSP must be specific to the operating environment. For example, a separate plan must be prepared for restricted areas and closed areas. An MSSP must also reflect operating systems approved for self-certification.

A separate MSSP must be written for each classification level of processing; TOP SECRET, SECRET, and CONFIDENTIAL. Information systems that have caveated information, e.g., Foreign Government Information (FGI) or NATO, do not need to be covered under separate MSSPs, but can be put into an MSSP at the appropriate classification level.

A separate plan must be submitted for single user and multiuser systems.

Separate plans are NOT required for a single system/computer with multiple hard drives. Each drive should be listed in the hardware baseline section.

A IS profile under a MSSP is written for a system type (single-user non-networked, multiuser non-networked, peer-to-peer LAN, or domain controlled LAN) and similar operations (trusted downloads, periods processing, mobile system, etc.). Each IS profile must be accredited by the CSA before the ISSM can self-certify a similar system.

Systems including certain variances may be included in an MSSP. New instances of the variance may not be self-certified by the ISSM. When a system is accredited under an MSSP with an approved variance in place, the ISSM may be granted self-certification authority for like systems that do not include the audit variance.

All networks must be appropriately identified by type as either domain controlled (centralized authentication) or peer-to-peer. An MSSP for domain controlled networks cannot be used to self-certify peer-to-peer networks or any standalone (non-networked) workstation.

Categories of information must be identified in the IS profile of the MSSP and will be addressed in the accreditation letter.

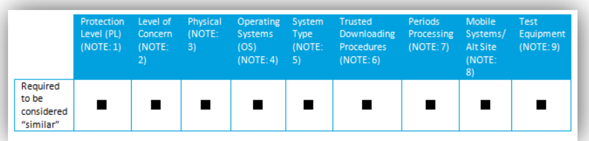
Examples of MSSP types:

- CONFIDENTIAL MUSA in a restricted area
- CONFIDENTIAL MUSA in a closed area
- CONFIDENTIAL LAN in a restricted area
- CONFIDENTIAL LAN in a closed area
- SECRET MUSA in a restricted area
- SECRET MUSA in a closed area
- SECRET LAN in a restricted area
- SECRET LAN in a closed area
- TOP SECRET MUSA in a restricted area
- TOP SECRET MUSA in a closed area
- TOP SECRET LAN in a restricted area
- TOP SECRET LAN in a closed area

Self-Certification of Similar Systems

Self-certification approval may be granted by the DAA in the MSSP ATO. Self-certification authority is only authorized as long as the ATO is valid.

Example
Table for Self-certification



	Protection Level (PL) (NOTE: 1)	Level of Concern (NOTE: 2)	Physical (NOTE: 3)	Operating Systems (OS) (NOTE: 4)	System Type (NOTE: 5)	Trusted Downloading Procedures (NOTE: 6)	Periods Processing (NOTE: 7)	Mobile Systems/ Alt Site (NOTE: 8)	Test Equipment (NOTE: 9)
Required to be considered "similar"	■	■	■	■	■	■	■	■	■

A table providing parameters governing self-certification by industry under a DSS-approved MSSP is located in the Reference Materials (14.1.12) page, 111.

Self-certification is not allowed under an IATO because the system must first be validated by DSS to verify that the system is properly configured.

ISSMs with self-certification authority may only self-certify systems that are compliant with all applicable requirements.

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, multi-user non-networked, 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 the IS profile accredited by DSS which will be the basis for all self-certified systems under the approved MSSP.

If the ISSMs are unsure of whether or not they can self-certify a particular IS, it is their responsibility to contact the ISSP to get clarification.

When a system is self-certified, the following documentation MUST be included with the self-certification packet maintained with the IS and also submitted to ODAA@dss.mil:

- Copy of the MSSP ATO Letter
- Copy of the approved MSSP
- A signed self-certification letter identifying the date
- The complete IS profile and supporting documents
  - Certification test results
  - A signed statement by the ISSM that security

of certification, the MSSP and IS profile used for certification. The format that the ISSM chooses to use to document the self-certified system is not defined. However, they are encouraged to use the same format as the original ATO letter and it must be obvious to any user or reviewer that the system was self-certified.	features; including access controls and configuration management are implemented and operational. This is often included as part of the statement of self-certification – Any documentation uniquely identifying the self-certified system, e.g., location information, system administrator (SA) or ISSO information, network diagrams, hardware list and software list, etc.

Reminder

- ✓ *The facility MUST have the proper documentation for the self-certified system. The ISSM cannot simply state that the system was self-certified.*
- ✓ *A list must be kept for all systems and all self-certified systems must be identified separately. This list must be given to the ISSP when each information system is self-certified.*
- ✓ *This list of systems does not alleviate the ISSM from having to notify their ISSP/IS Rep when a new system is self-certificated. Self-certification notification should occur immediately upon completion of the self-certification of the IS unless directed otherwise by ISSP.*

Limitations on Self-Certification of Similar Systems

See examples below and required documentation and procedures.

SIPRNet	An ISSM cannot self-certify a SIPRNet node, but can self-certify a workstation on a node providing all self-certification requirements are met and there are IP addresses available within the assigned scope.
Interconnected Systems/WANs	An ISSM cannot self-certify a WAN. An ISSM can self-certify a new workstation on a WAN node providing all self-certification requirements are met. ISSM cannot self-certify a connection to a WAN. To add a self-certified node to an existing WAN, the ISSM responsible for the node must submit the following artifacts to the WAN host ISSM: ▪ Copy of the MSSP ATO Letter ▪ Copy of the approved MSSP ▪ A signed self-certification letter identifying the date of certification, the MSSP and IS profile used for certification. The format that the ISSM chooses to use to document the self-certified system is not defined. However, they are encouraged to use the same format as the original ATO letter and it must be obvious to any user or reviewer that the system was self-certified. ▪ The complete IS profile and supporting documents. – Certification test results – A signed statement by the ISSM that security features; including access controls and configuration management are implemented and operational. This is often included as part of the statement of self-certification – Any documentation uniquely identifying the self-certified system, e.g., location information, system administrator (SA) or ISSO information, network diagrams, hardware list and software list, etc. The WAN host must request approval of additional nodes by resubmitting an updated NSP for approval. If a WAN node is later removed from a WAN to become a LAN again, the local ISSM

needs to submit a withdrawal message to the ODAA mailbox, and submit an updated MSSP or IS profile for the LAN with a new UID at the same time. An explanation for the reason for the submission should be included. This will keep the ODAA database up-to-date concerning the status of the LAN. The system can continue processing while waiting for the updated accreditation.

Systems requiring variances

A contactor cannot self-certify systems with variances in place. All variances must be approved by ODAA. An ISSM may self-certify systems based on an ATO for a system with a variance, provided the self-certification is for a fully compliant system. If the newly self-certified system requires a variance, a separate approval for the variance must be obtained from ODAA.

Systems with audit variances

Systems requiring an audit variance should first be self-certified under an approved MSSP as a compliant system. The ISSM must then request an audit variance in writing through the assigned ISSP. The variance cannot be applied to the system until approval is granted by the RDAA.

The variance approval request letter must identify the following information:

- Copy of the self-certification letter identifying the system UID and associated MSSP
- Detailed procedures explaining physical and technical audit procedures
- Frequency the technical audits will be performed

Once approved, the procedures and DSS audit variance approval letter must be retained as an attachment in the IS profile for the specific system approved for the variance. The approval letters will be system specific and will expire when the associated MSSP or IS profile expires, unless rescinded.

A system security plan for a specific system not under a MSSP may include the audit variance procedures in the plan narrative. The variance is approved when the system is granted an accreditation by the RDAA.

Systems with Alternate Trusted Download Procedures

Any system requiring the use of alternate trusted download procedures may first be self-certified under an approved MSSP as a compliant system. The ISSM must then send a request for approval in writing to the ISSP for the facility, and provide a copy of the customer-accepted alternate trusted download procedures along with the customers RAL. The alternate trusted download procedures cannot be implemented on the system until approval is granted by the ODAA.

The written request must include the following:

- Copy of the approved MSSP ATO Letter
- Copy of the self-certification letter identifying the system ID and associated MSSP
- A signed copy of the RAL on Government letterhead stating they are willing to assume the residual risk for the alternate trusted download procedures
- The alternate procedures must include a statement that the ISSM has observed these procedures, and they have been performed as documented in the RAL
- Detailed procedures and file types applicable under the alternate procedures

Once approved, the procedures, the RAL and the ODAA approval letter must be retained as an attachment in the IS profile for the specific system approved for use. Note that RALs must be updated when the plan is reaccredited every three years.

The approval letter will be system specific and will expire when the associated MSSP expires unless rescinded.

Systems with Legacy (non-compliant) Operating Systems

Any system requiring the use of non-compliant operating systems may not be self-certified under an approved MSSP. (There is an exception for single–user systems since they do not require technical security features such as I&A, and auditing).

Systems operating with Test Equipment

Any system requiring the use of test equipment may be self-certified under an approved MSSP IS profile as a long as the test equipment associated with the system being self-certified is identical in make and model to the equipment which is identified in previously accredited IS profiles.

ISSMs may find it beneficial to maintain a comprehensive list of all test equipment used across the local programs to include manufacturer, nomenclature, model, type and amount of memory, and clearing and sanitization procedures for each piece of equipment.

Once the list is compiled, the ISSM may submit the completed document along with a cover letter requesting authority to self-certify any piece of equipment from this list. The list of equipment will be dated and the cover letter will identify the list by a unique identifier and revision number. The list of test equipment will require re-approval when additional equipment is acquired by the facility and added to the list. A new approval letter will be provided once the clearing and/or sanitization procedures have been demonstrated for newly acquired equipment. The new equipment cannot be added or used on any approved system until approval is granted by the CSA.

The test equipment documentation must include the following information:

- Cover letter identifying the facility, ISSM points of contact, purpose of the letter, and UID for the test equipment document
- Listing of test equipment, matching the UID specified in the cover letter detailing manufacturer, nomenclature, model, types and amount of memory, and detailed clearing and sanitization procedures

The CSA will evaluate the listing and when approved provide an approval letter for listing by unique ID and revision. Once approved, the ISSM may self-certify any piece of test equipment from the approved listing on any system that is self-certified.

The approval letter and list of test equipment will be considered security relevant documentation and must be maintained with the system.

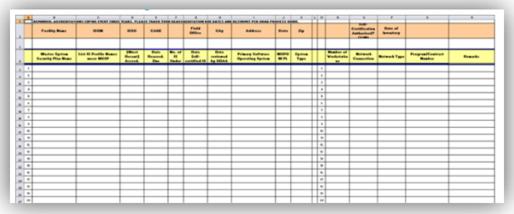
Reaccreditation and Re-evaluation of an MSSP

Reaccreditation must be completed when security relevant changes occur. Re-evaluation of the conditions which accreditation was originally granted will occur every three years

If no significant changes have occurred, re-evaluations will be handled via e-mail from the ISSM to the ODAA with a carbon copy to the IS Rep and ISSP stating that there have been no significant changes. The e-mail must include the facility name, address, unique MSSP identifier, NISPOM protection level, and ISSM name, location, and telephone number. See Reaccreditation and Re-evaluation Flow Diagram Reference (15.1.4).

If a re-evaluation occurred and discovered significant unauthorized changes, the ISSP should be immediately notified to determine risk

Example
MSSP IS Tracking Form



REMINDER: ACCREDITATIONS EXPIRE EVERY THREE YEARS. PLEASE TRACK YOUR REACCREDITATION DUE DATES AND ACCOUNT PER ODAA PROCESS GUIDE.

	Facility Name	ISSM	ISSO	CAGE		Field Office	City	Address	State	Zip				Self-Certification Authorized? (Y/N)	Date of Inventory		
	Master System Security Plan Name	List IS Profile Names under MSSP	(Most Recent) Accred.	Date Reaccred. Due	No. of IS Under	Date Self-certified IS	Date reviewed by ODAA	Primary Software Operating System	MSSP M PL	System Type			Number of Workstations	Network Connection	Network Type	Program/Contract Number	Remarks
1												1					
2												2					
3												3					
4												4					
5												5					
6												6					
7												7					
8												8					
9												9					
10												10					
11												11					
12												12					
13												13					
14												14					
15												15					
16												16					
17												17					
18												18					
19												19					
20												20					

An example of the MSSP IS Tracking Form is located in the Reference Materials 14.1.13, page 112.

associated with the changes and provide guidance to the ISSM and feedback to the DAA. However, the facility can continue to use the system for classified processing provided the system is still operating under a valid IATO or ATO. Security relevant changes cannot be made on the system until the ODAA has reviewed the change and determined if a reaccreditation is required. It is the ISSM's responsibility to submit plans for reaccreditation at least 30 days prior to expiration to allow the ODAA to review the plan and respond to the ISSM. If the accreditation expires during the review time, the ISSM must stop processing classified information until the plan is approved.

Withdrawal of self-certification authority

Self-certification authority can be withdrawn if it is determined that there is evidence of incompetency, or if the ISSM does not have adequate experience or has violated trust in the past. Additionally, if it is determined that the ISSM cannot adequately manage the self-certified IS, self-certification can be withdrawn (e.g., discovery of undocumented self-certified systems).

3.4 System Security Plan Submission Process

ISSM E-mail Validation

It is extremely important that the ISSM follow the instructions for plan submissions properly. Any deviation/omission makes it difficult for HQ personnel to quickly and efficiently input the required information into the ODAA database. If the ISSP and/or IS Rep are not identified in the e-mail, significant delays may occur in processing the plan for review. If the necessary information cannot be readily obtained, the e-mail will be rejected and returned for administrative correction.

The following procedure should be used for submitting an initial (M)SSP. Once an ISSM develops an (M)SSP in accordance with the NISPOM Chapter 8, it can be submitted to the ODAA for approval using the following methods.

▪ The first method of submittal is by:	Sending an e-mail from the corporate e-mail address with the (M)SSP as an attachment to the ODAA mailbox at ODAA@dss.mil with the subject line as explained in the example that follows. The subject line unique identifier format is mandatory for the proper routing of the (M)SSP. The region must be the first variable in the subject line. The body of the e-mail must include the facility name, address, unique identifier of the system, NISPOM protection level, and ISSM name, location, telephone number, and reason for submittal (i.e., initial, reaccreditation, review, re-evaluation, informational). If the system is being reaccredited, please include a list of changes made to the plan to assist in reaccreditation processing.
▪ The second method of submittal for (M)SSPs marked FOUO or (M)SSPs larger than 10MB:	They must be forwarded to the ODAA using the address on the title page of this document via carrier (FedEx, UPS, US Postal, etc.) on a compact disk (CD). ODAA will ONLY accept electronic copies of (M)SSPs.

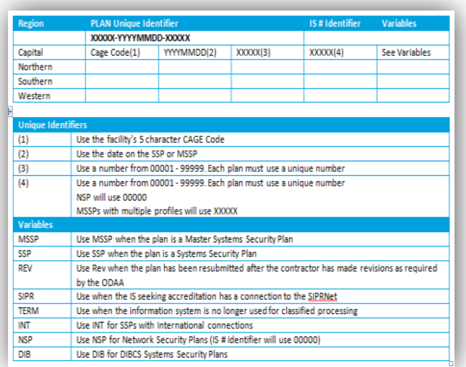
Regardless of the method used, the ISSMs must copy on the e-mail to ODAA, the local ISSP and IS Rep stating that the plan has been submitted. If the ISSMs are unsure of the personnel to be notified, they should contact the local IS Rep, FOC or ISSP. Their information will be provided on the DSS web site. The e-mail will include the facility name, address, ODAA unique identifier of the system, NISPOM protection level, and ISSM name, location, telephone number and reason for submittal, (i.e., initial, reaccreditation, review, re-evaluation, informational). The ODAA Unique Identifier (UID) applies to the (M)SSP and the IS Profile. The IS Profile will be uniquely identified with a five digit identifier determined by the ISSM or other facility personnel. This allows more than one IS to be protected by one (M)SSP.

Reminder

The ODAA mailbox has a size limit of 10MB. Please use compression tools to ensure that the submission is below this threshold.

UIDs will not change when plans are rejected and subsequently resubmitted to the ODAA. Changes in the UID may result in delays, and will result in multiple entries in the ODAA database for the same physical system. The table that follows shows the correct format to use in the subject line of the e-mail to ODAA when submitting the plan. The correct format for the UID in all other cases, such as the title page of the plan, is the Plan Unique Identifier for (M)SSPs, and the Plan Unique Identifier together with the IS # Identifier for IS Profiles.

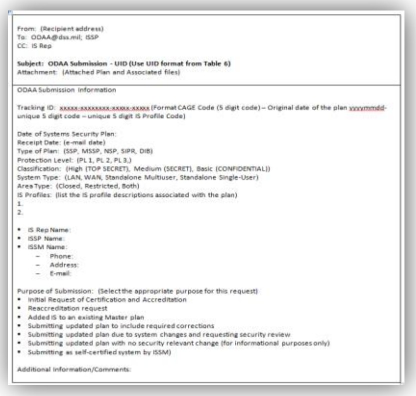
Example
Subject Line Requirements for Plan Submissions and E-mail to ODAA Mailbox



Region	PLAN Unique Identifier			IS # Identifier	Variables
	XXXXX-YYYYMMDD-XXXXX				
Capital	Cage Code(1)	YYYYMMDD(2)	XXXXX(3)	XXXXX(4)	See Variables
Northern					
Southern					
Western					

Unique Identifiers	
(1)	Use the facility's 5 character CAGE Code
(2)	Use the date on the SSP or MSSP
(3)	Use a number from 00001 - 99999. Each plan must use a unique number
(4)	Use a number from 00001 - 99999. Each plan must use a unique number NSP will use 00000 MSSPs with multiple profiles will use XXXXX
Variables	
MSSP	Use MSSP when the plan is a Master Systems Security Plan
SSP	Use SSP when the plan is a Systems Security Plan
REV	Use Rev when the plan has been resubmitted after the contractor has made revisions as required by the ODAA
SIPR	Use when the IS seeking accreditation has a connection to the SIPRNet
TERM	Use when the information system is no longer used for classified processing
INT	Use INT for SSPs with International connections
NSP	Use NSP for Network Security Plans (IS # Identifier will use 00000)
DIB	Use DIB for DIBCS Systems Security Plans

An example of the Subject Line Requirements for Plan Submissions is located in the Reference Materials (14.1.14), page 113.



From: (Recipient address)
To: ODAA@dss.mil; ISSP
CC: IS Rep

Subject: ODAA Submission - UID (Use UID format from Table 6)
Attachment: (Attached Plan and Associated files)

ODAA Submission Information

Tracking ID: xxxxx-xxxxxxxx-xxxxx-xxxxx (Format CAGE Code (5 digit code) – Original date of the plan yyyymmdd-unique 5 digit code – unique 5 digit IS Profile Code)

Date of Systems Security Plan:
Receipt Date: (e-mail date)
Type of Plan: (SSP, MSSP, NSP, SIPR, DIB)
Protection Level: (PL 1, PL 2, PL 3,)
Classification: (High (TOP SECRET), Medium (SECRET), Basic (CONFIDENTIAL))
System Type: (LAN, WAN, Standalone Multiuser, Standalone Single-User)
Area Type: (Closed, Restricted, Both)
IS Profiles: (list the IS profile descriptions associated with the plan)
1.
2.

- IS Rep Name:
- ISSP Name:
- ISSM Name:
  - Phone:
  - Address:
  - E-mail:

Purpose of Submission: (Select the appropriate purpose for this request)
- Initial Request of Certification and Accreditation
- Reaccreditation request
- Added IS to an existing Master plan
- Submitting updated plan to include required corrections
- Submitting updated plan due to system changes and requesting security review
- Submitting updated plan with no security relevant change (for informational purposes only)
- Submitting as self-certified system by ISSM)

Additional Information/Comments:

A sample e-mail to ODAA Mailbox and subject-line requirements is located in the Reference Materials (14.1.15), page 114.

3.5 Configuration Management Process

The configuration management (CM) process ensures that the protection features are implemented and maintained on the system. For the purposes of this document, the CM is defined as the formal change control process of all security relevant aspects of the IS. The (M)SSP will describe the CM procedures and documentation process for changes to any IS hardware, software and security documentation. The ISSM and/or ISSO will be responsible for authorizing all security relevant baseline changes to the applicable ISs profile(s) to include hardware, software, procedures, reports, and audit records. In cases where change impacts previously accredited procedures, reaccreditation by DSS will be required prior to implementation. The hardware and software lists will show the current baseline. The CM process will be periodically verified during a contractor self-assessment to ensure it is working effectively and that changes outside the CM process are not permitted. Validation will be accomplished by a physical audit of the hardware and software currently in use on the IS against the hardware and software baselines listed in the accredited (M)SSP.

3.6 Risk Assessment Requirements

Risk is the possibility that a threat will adversely impact an IS by exploiting a vulnerability. A threat may be defined as a potential for the accidental or deliberate compromise of security. A weakness or lack of controls that could facilitate, or allow, a compromise is considered a vulnerability. 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.

NISPOM paragraph 8-610 requires the ISSM to determine if any unique local threats or vulnerabilities exist for an IS. At a 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.

4.0 Operational Controls

4.1 Training and Awareness

4.1.1 Security Education

The ISSM will develop and implement an ongoing IS security education program for all IS users. Security training and awareness will be provided prior to authorizing an individual access to an IS and updated as needed. All IS authorized users will receive training on the security risks associated with their user activities and responsibilities under the NISP. The contractor will determine the appropriate content of the security training taking into consideration, assigned roles and responsibilities, specific security requirements, and the IS to which personnel are authorized access. It is the responsibility of the ISSM to coordinate with the contractor's FSO and the contractor's Insider Threat Program Senior Official to ensure insider threat awareness is addressed within the contractor's IS program. ISSMs will include insider threat awareness to their security education, awareness, and training for general users.

In addition to their information system security responsibilities, ISSMs and ISSOs will be trained on their responsibilities associated with the contractor's insider threat program.

Initial security training and awareness 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 a 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 IS Users" acknowledging their responsibility to protect the IS and classified information and that their activity on classified systems is subject to monitoring which could be used against them in a criminal, security or administrative proceeding.

At a minimum, IS security briefings will occur annually and records of these briefings will be maintained. Additional briefing will 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.

4.1.2 Contractor Training

Cleared contractors should take every training advantage available from the following sources:

- The Center for Development of Security Excellence (CDSE)
- ODAA staff
- Contractor seminars, workshops, conferences, etc.
- Internal company/corporate training

ODAA Tools

To reduce processing delays, there are several tools available to promote efficiency and consistency in the C&A process. These tools can be beneficial for training personnel as well. The following tools are available by following the procedures listed on the DSS web site:

(M)SSP Templates	(M)SSP templates assist in developing System Security Plans that are tailored toward a particular facility. These templates, which were designed for the majority and most typical IS systems, will allow the contractor to facilitate the submission process. In addition, the benefits of using the (M)SSP templates provide the ODAA a familiar format tailored to a set configuration under a set environment, which results in an efficient (M)SSP evaluation. Plans submitted to DSS must be based upon the DSS-provided plan templates. Significant delays and/or denial will result and should be expected if these templates are not used.
ODAA Standardization of Baseline Technical Security Configurations	ODAA has developed system hardening standards based on computer security standards from the National Security Agency (NSA), Defense Information Security Agency (DISA), National Institute of Standards and Technology (NIST), and original equipment manufacturers. The use of these standards is required and designed to strengthen IS security controls, protection of classified data, and accountable system access controls. Also, the technical configuration standards are designed in conjunction with the (M)SSP templates. Any deviation from these configuration standards will require further DSS reviews to verify appropriate system controls are in place and operating in lieu of the recommended configuration standards. A lack of adherence will significantly lengthen the IATO and ATO process resulting in delays in obtaining authority to process classified. Use a POA&M if the Baseline Technical Security Configurations are not fully implemented. A Plan of Action & Milestones template is located in the Reference Materials 15.1.4.

4.2 Contingency Planning

When considering availability controls, the principal consideration is the need for the information on the system in question to be available in a fixed time frame to accomplish a mission. Availability protection requirements, when contractually imposed, will be described in the IS profile. If disaster recovery planning is contractually mandated, the ISSM will develop a plan that identifies the facility's mission essential applications and information, procedures for the backup of all essential information and software on a regular basis, and testing procedures.

4.3 System Recovery and Assurances

The IS will be configured to ensure that all security mechanisms (e.g., auditing, virus detection) are automatically enabled during the IS startup/boot process. 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, IS software and IS communications are documented in the (M)SSP. The ISSM or designated ISSO will be responsible for ensuring that system assurance is maintained. System recovery will be performed by the ISSM or designated ISSO only by using either: protected copies of the original operating system disks, images (ghost) from original configuration or full recovery disks, or restored data files from system backups.

Once restored, a certification test will be completed by the ISSM, which verifies all security settings before the system is returned to service. If system recovery operations are unsuccessful 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.

4.4 Clearing and Sanitization

4.4.1 Clearing

NISPOM 8-301(a) refers to a procedure by which classified information is removed in such a manner that known non-laboratory attacks such as keyboard attacks, will be unable to recover the information. Clearing memory and media is required before and after periods of processing as a method of ensuring need-to-know protection, as well as before maintenance personnel who have been authorized access to classified information are present. The clearing procedure must be evaluated and approved by the ISSP or be on an authorized DoD list. Cleared equipment must continue to be safeguarded at all times, and carry the highest, most restricted information category type until sanitized.

4.4.2 Sanitizing

NISPOM 8-301(b) refers to a procedure by which the classified information is completely removed and even a laboratory attack using known techniques or analysis will not recover any information. Sanitizing removes information from media to render the information unrecoverable by technical means. Overwriting, degaussing, and sanitizing are not synonymous with declassification. Declassification is a separate administrative function which requires GCA approval. Spills at all classification levels will be cleaned up following these procedures at a minimum, but will require GCA approval either prior to (preferable) or after the spill occurs (the GCA may require destruction). If the GCA does not answer within 30 days it will be taken as a concurrence with the procedures.

4.4.3 Magnetic Tape

Magnetic tape can be cleared using a Type I, II, or III approved tape degausser, as referenced in the Matrix for Degaussing Media below. As a degaussed tape can be released through unclassified channels, the selection of the degausser is critical. Using an approved tape degausser of the same level or higher can sanitize all three types of magnetic tape that are in use. A list of degaussers appears in the latest version of the NSA Information Systems Security Products and Services Catalog. In addition NSA regularly posts an updated Evaluated Product Listings (EPL) of equipment that securely erases the most common types of storage devices that retain classified or sensitive data on its web site (http://www.nsa.gov/ia/government/index.cfm).

Reminder

The terms "Type I, II or III" are being replaced by the actual media coercivity rating.

If a degausser not listed on the NSA EPL was used, the only method of verifying whether the tape was properly degaussed is to have the tape or degausser tested at a NSA certified laboratory. Degaussers should be tested periodically using the timetable established by DSS and NSA. The degausser must be tested within six months after the initial "new" purchase or immediately if purchased used. Even products on the EPL must be re-tested twice a year for the first two years, then once a year thereafter. If the results are marginal, the degausser must be re-tested within six months.

The destruction of optical media, compact disc (CD), and DVD media present unique destruction issues. There are two categories of CD and DVD media types that are recordable (e.g., CD-R, DVD-R, CD-RW, DVD-RW) and one that is not (i.e., CD-ROM). CD-R and DVD-R media are broken down into two categories: write-once (WO) and re-writeable (RW). Each type is uniquely constructed and must be examined separately in the destruction process to be certain that the process or equipment to be used is adequate. If any of the ancillary components of the CD or DVD package (e.g., CD/DVD case, jewel case, paper insert) are marked with, or contain any classified information, those materials must be destroyed. A copy of the latest NSA evaluated and approved optical destruction devices can be found on the ODAA web site.

Floppy disks are not allowed to be destroyed by shredding per NISPOM 5-705.

A record of destruction is required when TOP SECRET memory or media is destroyed. An audit log entry is required when any classification level of memory or media is cleared or sanitized. Destruction records for TOP SECRET must be retained for two years.

4.4.4 Organization Destruction Options

With the ever increasing use of computers, the destruction of classified hard drives that are no longer needed is becoming an issue. NSA has discontinued accepting classified hard drives unless they were Government Furnished Equipment (GFE) and the appropriate Contracting Officer Representative (COR) submits a request for NSA to handle the destruction. Most GCA client organizations do not want to accept old hard drives for destruction.

There are four options available to organizations for the destruction of classified hard drives:

Options	Details
Return to customer	Unless specifically prohibited from doing so in their contract, organizations can return all media (including hard drives) to their government customer for destruction. The Contract Manager should coordinate with the Contracting Officer's Representative (COR) for the return of this equipment.
Send to NSA	If the media is Government Furnished Equipment (GFE), and approval is granted from NSA, the organization can send the items to NSA. The Contract Manager should call the NSA Media Destruction Customer Service Center (301) 688-6672 to register with NSA. The Contract Manager must fill out a Contractors Approval Form (provided by NSA) and follow the instructions provided by the destruction engineers at NSA.
Destruction by the organization	If the organization does not meet the criteria of option 1 or 2, the organization must destroy the materials.
Destruction by other organization	An organization can send the materials to another approved organization with an NSA approved method for destruction.

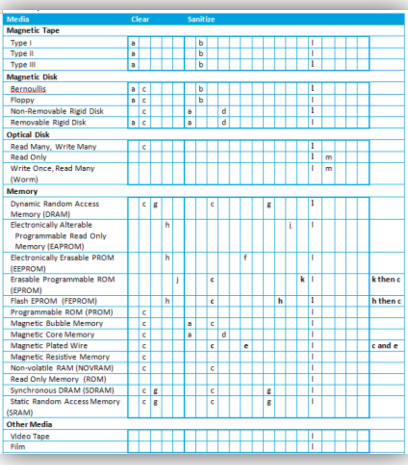
4.4.5 DSS Clearing and Sanitization Matrix

NISPOM paragraphs 5-704 and 5-705 set out requirements for the destruction of classified material that is no longer required, including media, memory, and equipment. The appropriate procedure to be used is based upon the classification sensitivity of the information and the type (size, capacity and connectivity) of the media.

This matrix provides guidance regarding clearance, sanitization (destruction) and disposition of the most common media, memory and equipment used for classified processing. In addition, NIST Special Publication 800-88, Guidelines for Media Sanitization, dated Sep 2006, can assist organizations and system owners in making practical sanitization decisions based on the level of confidentiality of their information, ensuring cost effective security management of their information technology resources, and mitigate the risk of unauthorized disclosure of information.

The contractor is required to document in the (M)SSP the clearing, sanitization and release of IS media and equipment to be used for the IS. If a contractor has memory, media, or equipment not identified in the matrix, or has a procedure that is more effective than the one identified, the IS Rep will contact the assigned ISSP to approve the method for sanitization or have the facility arrange with the GCA for return of the memory or media.

Example
Clearing and Sanitation Matrix



Media	Clear					Sanitize																
Magnetic Tape																						
Type I	a						b										l					
Type II	a						b										l					
Type III	a						b										l					
Magnetic Disk																						
Bernoullis	a	c					b										l					
Floppy	a	c					b										l					
Non-Removable Rigid Disk		c				a			d								l					
Removable Rigid Disk	a	c				a			d								l					
Optical Disk																						
Read Many, Write Many		c															l					
Read Only																	l	m				
Write Once, Read Many (Worm)																	l	m				
Memory																						
Dynamic Random Access Memory (DRAM)		c	g					c					g				l					
Electronically Alterable Programmable Read Only Memory (EAPROM)				h											i		l					
Electronically Erasable PROM (EEPROM)				h							f						l					
Erasable Programmable ROM (EPROM)					j			c								k	l					k then c
Flash EPROM (FEPROM)				h				c						h			l					h then c
Programmable ROM (PROM)		c															l					
Magnetic Bubble Memory		c				a		c									l					
Magnetic Core Memory		c				a			d								l					
Magnetic Plated Wire		c						c			e						l					c and e
Magnetic Resistive Memory		c															l					
Non-volatile RAM (NOVRAM)		c						c									l					
Read Only Memory (ROM)																	l					
Synchronous DRAM (SDRAM)		c	g					c					g				l					
Static Random Access Memory (SRAM)		c	g					c					g				l					
Other Media																						
Video Tape																	l					
Film																	l					

An example of the Clearing and Sanitation Matrix is located in the Reference Materials (14.1.16), page 116.

Destruction Methods for Classified Media and Equipment:

NISPOM paragraph 5-705 reflects requirements for destruction of classified material, including classified media and equipment. DSS recommends methods and procedures for destroying classified media and equipment to be reflected in the SSP and reviewed/approved in connection with the information systems certification and accreditation process.

The following summary information is provided for organizations in updating Systems Security procedures for destruction of classified media:

- Incineration using a licensed incinerator is the most common and recommended method for removing recording surfaces.
- Applying an abrasive substance to completely remove the recording surface (e.g., emery wheel, disk sander, belt sander, sand blaster) from the magnetic disk or drum. Make certain that the entire recording surface has been thoroughly destroyed before disposal. Ensure proper protection from inhaling the abraded dust.
- Degaussing or destruction using government approved devices. NSA publishes guidance on the sanitization, declassification, and release of IS storage devices for disposal or recycling in the NSA CSS Policy Manual 9-12, NSA/CSS Storage Device Declassification Policy Manual, dated 13 Mar 2006. It is recommended that prior to performing any process for disposal, recycling or release of storage, media, or equipment that users review the manual and/or check for any updates to the guidance. NSA publishes on a recurring basis, updated Evaluated Products Lists (EPL) for High Security Crosscut Paper Shredders, High Security Disintegrators and Optical Media Destruction Devices. Organizations may utilize NSA evaluated destruction devices for destruction of classified media and hardware without prior authorization from DSS. For use of non-NSA approved devices or procedures, prior approval from the CSA is required.
- Smelting, disintegrating, or pulverizing hard disks or drums at an approved metal destruction facility. Prior approval from the CSA is required.
- Destroying by the use of chemicals (e.g., application of concentrated hydriodic acid (55 to 58 percent solution). Chemical destruction is hazardous and should only be done by trained personnel in a proper environment (e.g., licensed facility, well-ventilated area, safety equipment and procedures, etc.). Prior approval from the CSA is required.
- Due to the proliferation, wide spread use, interoperability, low cost of USB technologies throughout the Global Information Grid (GIG), USB media and equipment no longer required to store or process classified information must be destroyed.

The National Security Agency (NSA) Classified Material Conversion (CMC) destruction facility may be utilized by approved and registered contractors. NSA CMC will accept all COMSEC hardware and materials (regardless of ownership), and classified Government Furnished Equipment (GFE) (including media), with the prior endorsement of a Government Contracting Officer (CO) or Contracting Officer Representative (COR) in accordance with NSA CMC contractor registration procedures reflected in NSA guidance "Contractor Request for NSA CDC Services”. Guidance for registration for NSA destruction services is also available on the DSS website.

4.5 Incident Response

GCA/Customer is the data owner and contractor should contact the GCA/Customer for procedures and guidance with regard to concerns related to the data that resides on the system. If GCA/Customer does not provide procedures/guidance then procedures/guidance contained in this process manual should be followed if the GCA/Customer concurs.

4.5.1 Classified Spills

Classified Spills (also known as contaminations or classified message incidents) occur when classified data is introduced to an unclassified computer system or to a system accredited at a lower classification than the data. Any classified spill will involve an Administrative Inquiry (AI) for the facility concerned.

4.5.2 Incident Response Plan

The contractor will develop an incident response plan that details the following information:

- Provides the contractor with a roadmap for implementing its incident response capability
- Describes the structure and organization of the incident response capability
- Provides a high-level approach for how the incident response capability fits into the overall organization
- Meets the unique requirements of the organization, which relate to mission, size, structure, and functions
- Defines reportable incidents
- Provides metrics for measuring the incident response capability within the organization
- Defines the resources and management support needed to effectively maintain and mature an incident response capability
- Reviewed and approved by designated officials within the organization

Copies of the incident response plan will be distributed to appropriate incident response personnel. The Incident Response Plan will be reviewed and revised when appropriate to ensure accuracy to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

Reminder

- ✓ *The tracking of hard drives involved in a spill cleanup is not required*
- ✓ *Wiping (overwriting) can be used for the cleanup of spills, but may not be used for sanitization of disks used with systems accredited to process classified*

The following procedures are aligned with National Institute for Standards and Technology (NIST) Special Publication (SP) 800-88, Guidelines for Media Sanitization, September 2006; Committee on National Security System Instruction (CNSSI) No. 1001, National Instruction on Classified Information Spillage, February 2008; Department of Defense Instruction (DoDI) 8500.2, Information Assurance Implementation, February 06, 2003; Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01E, IA and Computer Network Defense (CND), August 15, 2007; National Security Agency Central Security Service (NSA/CSS) Policy Manual 9-12, NSA/CSS Storage Device Declassification Manual, March 13, 2006; Assistant Secretary of Defense, Networks and Information Integration (ASD/NII) Memorandum, Disposition of Unclassified DoD Computer Hard Drives, June 04, 2001; and Air Force Systems Security Instruction 8580, Remanence Security, 17 November 2008.

4.5.3 Classified Spill Cleanup Procedures

The following procedures apply to all cleared facilities and all contractor systems involved in a classified data spill with information classified Secret and below. Data spills involving TOP SECRET information will be cleaned up following GCA procedures, but at minimum will include these procedures. The focus of cleanup procedures is to identify the degree of the spill, containing it, and cleaning it up.

Facility Security Officers (FSO), Information Systems Security Managers (ISSM), Information Systems Security Officers (ISSO), system administrators (SA), etc., are encouraged to become familiar with these procedures prior to an incident. These procedures will be incorporated into the NISPOM training.

4.5.4 Wiping Utility

Hard drives involved in a classified spill should be wiped using an NSA or NIAP-approved product, however if one is unavailable any commercially available wiping utility that meets the following requirements may be used:

- If wiping whole disks, it must be able to wipe the entire drive (e.g., partition tables, user data, operating systems and boot records)
- If wiping whole disks, it must be able to wipe Device Configuration Overlay (DCO) hidden sectors if ATA-6 disks are being used
- If wiping whole disks, it must be able to wipe a Host Protected Area (HPA)
- Must be able to sanitize by overwriting with a pattern, and then its complement, and finally with another unclassified pattern (e.g., “00110101” followed by “11001010” and then followed by “10010111” [considered three cycles]). Sanitization is not complete until three cycles are successfully completed
- Must be able to verify the overwrite procedure by randomly re-reading (recommend 10% if possible) from the drive to confirm that only the overwrite character can be recovered. If not, the use of an additional utility to accomplish this is acceptable
- Must be able to print the results of the overwriting operation showing any bad sectors or areas of the disk that could not be written to (if there are any bad sectors or blocks the disk must be destroyed or degaussed)

Cost Analysis

It is suggested that the company perform a cost analysis before using the option of wiping hard drives. Wiping can take many hours to perform and it may be more cost effective to dispose of hard drives by degaussing or destruction. NIST Special Publication 800-88, Guidelines for Media Sanitization can provide some assistance in this regard.

Additional Precautions

The hard drive may not be the only storage media in a system. Beware of floppy disks left in floppy disk drives, Zip disks in Zip drives, CDs and DVDs in optical drives, tapes in tape backup-units, thumb drives/compact flash drives, BIOS passwords, printing devices and the like. Include relevant documentation when an old system is wiped and then transferred from one department or division within the same company to another. Desktops and laptops aren't the only systems that need sanitizing. Pocket PCs, PDAs, some multifunction cell phones, and other devices may also contain sensitive information such as passwords or confidential data.

4.5.5 DSS-Approved Classified Spill Cleanup Plan

Purpose

This document describes a procedure for cleanup of Information Systems that have been contaminated with classified data. It defines the roles and responsibilities of personnel during incidents such as those caused by inadvertent transmission of classified e-mail over unclassified computer networks and e-mail systems, or by the introduction of data of a higher classification level onto an unaccredited system, or a system accredited at a lower level. The DSS ODAA may require additional or alternate cleanup procedures.

Scope

Equipment	The process outlined in this document includes both file servers and Exchange servers, laptops/desktops and other systems and peripherals that may have been contaminated with classified information.
Sender/Receiver	This procedure is intended to cover both the computing environment of the sender and receiver(s) of classified e-mails. The initial report of contamination could come from either the sender or receiver. In any event, all potentially contaminated computing environments must be included. In those cases where either the sender or the receiver are not local, the cognizant FSO will make notification to the appropriate security contact at the other known locations where the contamination may exist and include them in the coordination of cleanup actions. Notification of an e-mail spill will NOT be made to any uncleared company or individual that does not fall under the NISPOM (e.g., to a Yahoo user, or to an uncleared company).
Contaminated material	The cognizant FSO will establish the protection for all equipment or material that is believed to be contaminated with classified information. The FSO will determine when an item may be released back into service based on the review of the checklists from the IS team.

Role	Responsibilities
All Personnel	▪ Immediately communicate to each other any reports of e-mail security incidents or classified contaminations ▪ Participate in and support security incident meetings and response efforts ▪ Assess the risks of the contamination and follow any special guidelines of the data owner (customer) ▪ Assign appropriately cleared individuals to participate in the cleanup effort
FSO	▪ The originating facility FSO of the contamination will act as the incident lead. ▪ Notify applicable Government agencies of the security incident ▪ Determine the security classification level of the data and confirm the appropriate cleansing procedures ▪ Identify the sender/receiver(s) of the classified information ▪ Request cleanup assistance by appropriately cleared technicians ▪ Contact the appropriate security official at any distant locations where the contamination was received or from where it originated ▪ Determine if there was “bcc:” addressing or if the sender copied his/her own account ▪ Determine if the contamination was distributed via other paths such as print, ftp, electronic media, server storage, etc. ▪ Determine if recipient accounts have user-configured rules for auto-forward, auto-save or other special instructions ▪ Investigate possibility of proxy accounts, Blackberry access, remote access and any other possible “feeds” from the contaminated accounts ▪ Isolate any contaminated assets of the sender/receiver ▪ Notify company officials of the incident and the planned cleanup effort
ISSM/ISSO	▪ Assess the extent of contamination and plan cleanup actions with the local ISSM ▪ Conduct cleanup of contaminated systems and any peripherals using cleared personnel. Spills at all classification levels will be cleaned up following these procedures at a minimum, but will require GCA approval either prior to (preferable) or after the spill occurs (the GCA may require destruction). If the GCA does not answer within 30 days it will be taken as a concurrence with the procedures and declassification. ▪ Report findings, cleanup actions and any other pertinent information to local ISSM ▪ Protect and isolate any contaminated systems from further compromise ▪ Coordinate storage/transport of classified material or other evidence with the ISSM

Reminder

Notification should NOT include the classification of the spilled information or its location. This stems from the intent of not providing an unclassified notification of where someone could locate inadvertently released classified information. Including this information would make the notification CONFIDENTIAL.

4.5.6 Contamination Cleanup Procedures

Coordination

Communications – Employees or security managers who report the discovery of classified information on unclassified or lower classified information systems are not to delete the classified data, but to isolate the systems and contact the cognizant FSO, ISSM or ISSO immediately. Caution should be taken when discussing such incidents over unsecured telephones so as not to further endanger any classified information that may be at risk on unclassified systems.

Reporting (NISPOM 1-303)

The facility must make a Preliminary Inquiry immediately to the CSA when there is a loss, compromise, or suspected compromise of classified information, foreign or domestic.

Lead FSO – The originating facility FSO of the contamination leads the effort. The FSO will immediately coordinate and plan the investigation/cleanup considering detailed information such as sender, recipient(s), subject, time sent, day sent, systems and peripherals potentially affected, etc.

If the contractor's preliminary inquiry confirms that a loss, compromise, or suspected compromise of any classified information occurred, the contractor will promptly submit an initial report of the incident unless notified by the CSA. The initial report will be distributed via secure channels (STE, secure fax, cleared network, etc.). If secure channels are not available the initial report will not include location and/or classification of the spill only.

Additionally, the Lead FSO will prepare a final report (NISPOM 1-303c.) when the investigation is completed to the CSA.

The initial report should include the following (if known):

- Origination of data/message: Facility, location, point of contact
- Other facilities involved: Facility, location, point of contact
- Method of transmission
- All equipment involved: Servers (RAID or single), workstations, notebooks, e-mail servers, Blackberries, etc.
- Remote dial-in or network connection?
- Location of all equipment
- All Operating Systems involved
- Number of people involved (Identify the employee(s) and include clearance level)
- Are there backup tapes involved?
- Any audit logs available to determine access?
- Current status of all equipment involved.
- Data owner notified?
- Customer information: Name, Point of Contact, phone numbers, email address
- A copy of the customer approved clean-up procedures for of all equipment and media

Appropriately Cleared Team

It is essential that all persons who participate in the cleanup have the appropriate clearance/access if they could potentially be exposed to classified information. In cases where the company is a cleared company but without accredited IS and no cleared computer personnel, uncleared personnel will be required to sign a standard non-disclosure agreement.

Protection of classified data and hardware

The cognizant ISSM will interview all appropriate persons to determine the extent of the contamination and to recover any hardcopy or media copies of the classified information. Any contaminated systems such as printers or other peripherals with memory that cannot be readily sanitized will be moved into a controlled area until they can be cleaned. Backup tapes that are determined to contain potential classified material must be identified and secured appropriately until they can be sanitized.

Security Incident Response Procedures

Checklists – The following checklists describe the processes/procedures to sanitize Exchange and GroupWise e-mail servers and e-mail clients. Other e-mail systems must follow comparable processes that comply with the intent of the documented procedures. These standard procedures are to be followed for classification levels of TOP SECRET and below, unless directed by the Designated Approving Authority (DAA) to take more stringent measures.

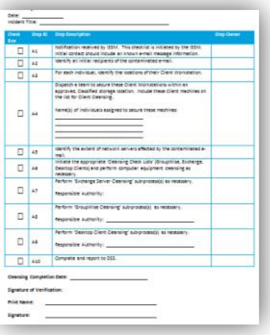
Transitory Devices – Data that is transmitted through transitory network devices such as mail hubs, routers, etc., is constantly overwritten through normal network operations. Therefore, these sanitization procedures are applicable only to the sending and/or receiving network servers and client workstations.

Example

Sample Checklists and Clearing Processes

The following checklists are located in the Reference Materials:

- *Main Cleansing Process (14.1.17), page 118*
- *Microsoft Exchange Server Cleansing (14.1.18), page 119*
- *Novell GroupWise Server Cleansing (14.1.19), page 123*
- *Desktop Client Workstation Cleansing (14.1.20), page 126*
- *Process for Clearing a Blackberry (14.1.21), page 127*



Date: ______________

Incident Title: ______________________________________

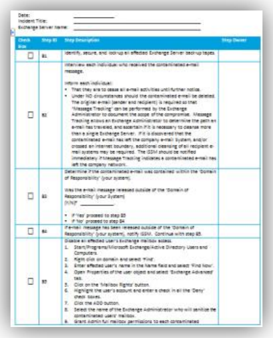
Check Box	Step ID	Step Description	Step Owner
□	A1	Notification received by ISSM. This checklist is initiated by the ISSM. Initial contact should include all known e-mail message information.	
□	A2	Identify all initial recipients of the contaminated e-mail.	
□	A3	For each individual, identify the locations of their Client Workstation.	
□	A4	Dispatch a team to secure these Client Workstations within an approved, Classified storage location. Include these Client machines on the list for Client Cleansing. Name(s) of individuals assigned to secure these machines: ______________________ ______________________ ______________________ ______________________	
□	A5	Identify the extent of network servers affected by the contaminated e-mail.	
□	A6	Initiate the appropriate 'Cleansing Check Lists' (GroupWise, Exchange, Desktop Clients) and perform computer equipment cleansing as necessary.	
□	A7	Perform 'Exchange Server Cleansing' subprocess(s) as necessary. Responsible Authority:	
□	A8	Perform 'GroupWise Cleansing' subprocess(s) as necessary. Responsible Authority: ______________________	
□	A9	Perform 'Desktop Client Cleansing' subprocess(s) as necessary. Responsible Authority: ______________________	
□	A10	Complete and report to DSS.	

Cleansing Completion Date: ______________________

Signature of Verification:

Print Name: ______________________

Signature: ______________________

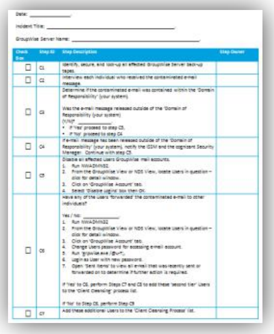


Date: ______________

Incident Title: ______________________________________

Exchange Server Name: ______________________________________

Check Box	Step ID	Step Description	Step Owner
□	B1	Identify, secure, and lockup all affected Exchange Server backup tapes.	
□	B2	Interview each individual who received the contaminated e-mail message. Inform each individual: • That they are to cease all e-mail activities until further notice. • Under NO circumstances should the contaminated e-mail be deleted. The original e-mail (sender and recipient) is required so that "Message Tracking" can be performed by the Exchange Administrator to document the scope of the compromise. Message Tracking allows an Exchange Administrator to determine the path an e-mail has traveled, and ascertain if it is necessary to cleanse more than a single Exchange Server. If it is discovered that the contaminated e-mail has left the company e-mail System, and/or crossed an Internet boundary, additional cleansing of all recipient e-mail systems may be required. The ISSM should be notified immediately if Message Tracking indicates a contaminated e-mail has left the company network.	
□	B3	Determine if the contaminated e-mail was contained within the 'Domain of Responsibility' (your system). Was the e-mail message released outside of the 'Domain of Responsibility' (your System) (Y/N)? ____________ • If 'Yes' proceed to step B5 • If 'No' proceed to step B4	
□	B4	If e-mail message has been released outside of the 'Domain of Responsibility' (your system), notify ISSM. Continue with step B5.	
□	B5	Disable all affected User's Exchange mailbox access. 1. Start/Programs/Microsoft Exchange/Active Directory Users and Computers. 2. Right click on domain and select 'Find'. 3. Enter affected user's name in the Name field and select 'Find Now'. 4. Open Properties of the user object and select 'Exchange Advanced' tab. 5. Click on the 'Mailbox Rights' button. 6. Highlight the user's account and enter a check in all the 'Deny' check boxes. 7. Click the ADD button. 8. Select the name of the Exchange Administrator who will sanitize the contaminated users' mailbox. 9. Grant Admin full mailbox permissions to each contaminated	

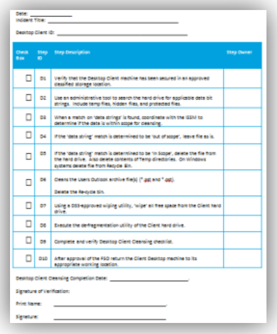


Date: ______________

Incident Title: ______________________________________

GroupWise Server Name: ______________________________________

Check Box	Step ID	Step Description	Step Owner
□	C1	Identify, secure, and lock-up all affected GroupWise Server back-up tapes.	
□	C2	Interview each individual who received the contaminated e-mail message.	
□	C3	Determine if the contaminated e-mail was contained within the 'Domain of Responsibility' (your system). Was the e-mail message released outside of the 'Domain of Responsibility' (your system) (Y/N)? ____________ • If 'Yes' proceed to step C5. • If 'No' proceed to step C4.	
□	C4	If e-mail message has been released outside of the 'Domain of Responsibility' (your system), notify the ISSM and the cognizant Security Manager. Continue with step C5.	
□	C5	Disable all affected Users GroupWise mail accounts. 1. Run NWADMN32. 2. From the GroupWise View or NDS View, locate Users in question – click for detail window. 3. Click on 'GroupWise Account' tab. 4. Select 'Disable Logins' box then OK.	
□	C6	Have any of the Users 'forwarded' the contaminated e-mail to other individuals? Yes / No: ____________ 1. Run NWADMN32 2. From the GroupWise View or NDS View, locate Users in question – click for detail window. 3. Click on 'GroupWise Account' tab. 4. Change Users password for accessing e-mail account. 5. Run 'grpwise.exe /@u-?'. 6. Login as User with new password. 7. Open 'Sent Items' to view all e-mail that was recently sent or forwarded on to determine if further action is required. If 'Yes' to C6, perform Steps C7 and C8 to add these 'second tier' Users to the 'Client Cleansing' process list. If 'No' to Step C6, perform Step C9	
□	C7	Add these additional Users to the 'Client Cleansing Process' list.	



Date: ______________

Incident Title: ______________________________________

Desktop Client ID: ______________________________________

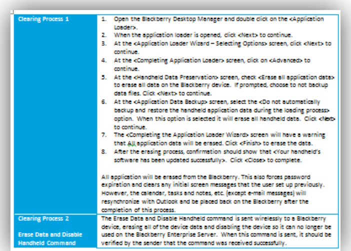
Check Box	Step ID	Step Description	Step Owner
□	D1	Verify that the Desktop Client machine has been secured in an approved classified storage location.	
□	D2	Use an administrative tool to search the hard drive for applicable data bit strings. Include temp files, hidden files, and protected files.	
□	D3	When a match on 'data strings' is found, coordinate with the ISSM to determine if the data is within scope for cleansing.	
□	D4	If the 'data string' match is determined to be 'out of scope', leave file as is.	
□	D5	If the 'data string' match is determined to be 'in Scope', delete the file from the hard drive. Also delete contents of Temp directories. On Windows systems delete file from Recycle Bin.	
□	D6	Cleans the Users Outlook archive file(s) (*.pst and *.ost). Delete the Re-cycle bin.	
□	D7	Using a DSS-approved wiping utility, 'wipe' all free space from the Client hard drive.	
□	D8	Execute the defragmentation utility of the Client hard drive.	
□	D9	Complete and verify Desktop Client Cleansing checklist.	
□	D10	After approval of the FSO return the Client Desktop machine to its appropriate working location.	

Desktop Client Cleansing Completion Date: ______________________

Signature of Verification:

Print Name: ______________________

Signature: ______________________



Clearing Process 1	1. Open the Blackberry Desktop Manager and double click on the <Application Loader>. 2. When the application loader is opened, click <Next> to continue. 3. At the <Application Loader Wizard – Selecting Options> screen, click <Next> to continue. 4. At the <Completing Application Loader> screen, click on <Advanced> to continue. 5. At the <Handheld Data Preservation> screen, check <Erase all application data> to erase all data on the Blackberry device. If prompted, choose to not backup data files. Click <Next> to continue. 6. At the <Application Data Backup> screen, select the <Do not automatically backup and restore the handheld application data during the loading process> option. When this option is selected it will erase all handheld data. Click <Next> to continue. 7. The <Completing the Application Loader Wizard> screen will have a warning that All application data will be erased. Click <Finish> to erase the data. 8. After the erasing process, confirmation should show that <Your handheld's software has been updated successfully>. Click <Close> to complete. All application will be erased from the Blackberry. This also forces password expiration and clears any initial screen messages that the user set up previously. However, the calender, tasks and notes, etc. (except e-mail messages) will resynchronize with Outlook and be placed back on the Blackberry after the completion of this process.
Clearing Process 2 Erase Data and Disable Handheld Command	The Erase Data and Disable Handheld command is sent wirelessly to a Blackberry device, erasing all of the device data and disabling the device so it can no longer be used on the Blackberry Enterprise Server. When this command is sent, it should be verified by the sender that the command was received successfully.

4.6 Maintenance

4.6.1 Maintenance

Maintenance should always be performed by cleared personnel. The ISSM must be notified when an IS requires maintenance to determine if the IS will require reaccreditation. The following requirements apply to all maintenance actions, regardless of the clearance level of the person performing the maintenance: Document the addition and removal of hardware and software in accordance with the (M)SSP. If security seals have been broken as a result of maintenance, they will be re-applied with actions documented in the security seal log. Prior to release, accredited IS equipment having memory or data retention capabilities will be sanitized as described in the (M)SSP. All maintenance to the accredited IS equipment will be documented in the Maintenance, Operating System and Security Software Change Log. Vendor-supplied software used for maintenance must reside on read-only or write-protected media marked "For Maintenance Use Only". Use of any diagnostic and test programs will be checked for malicious code before the media is connected to the system.

4.6.2 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.

4.6.3 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 Information System.

Special attention should be given to portable units containing memory and/or having 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, follow this procedure: A 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.

4.6.4 Remote Maintenance

Remote maintenance procedures (when required) will be developed by the ISSM and approved by the CSA before implementation. All other options will be explored before consideration is given to remote maintenance. Remote maintenance is defined as non-local maintenance and diagnostic activities conducted by individuals communicating through a network. Any remote maintenance will be described in the (M)SSP.

4.7 Media

4.7.1 Media Protection

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.

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

- Media containing classified data
- 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 if required (e.g., Top Secret). 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 and will be protected to the level of IS accreditation.

Unclassified or lower classified media brought into the classified processing environment 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 during which unclassified media is used. Write-protect mechanisms are tested by attempting to write to the media.

Media Destruction

IS media may be destroyed by incinerating, smelting, mutilation, chemical decomposition, or pulverizing (e.g., hammer mills, choppers, and hybridized disintegration equipment). When destruction is performed, the action of removing any media specified in the Hardware or Software 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.

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 if required (i.e., Top Secret). The output procedures provide 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 will be accredited by DSS on a case-by-case basis.

Hardcopy Output Review Procedure

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 you have been working with. If you generate a hardcopy of information you are not familiar with or have not recently accessed, you 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.

4.7.2 Removable Media Restrictions

NISP systems with requirements to write classified information to removable media will be restricted to personnel designated and briefed by the ISSM. The ISSM will disable the "write" capability for all forms of removable media devices on all information systems as a default setting using any and all feasible means. It is recommended to disable unnecessary ports (USB, Firewire, etc.) in the information systems Basic Input Output System (BIOS). It is not necessary to disable a USB port in the BIOS if its dedicated use is necessary for keyboard, mouse, and/or backup tape/disk drives. Removable media is defined as CD/DVD, Secure Digital (SD) cards, Tape, Flash Memory data storage devices, Multi Media Cards (MMC), removable hard drives, etc. The removable media restriction does not include items such as tape/disk backup, unless the media is intended for distribution.

The ISSM will establish a program to appoint and account for authorized personnel responsible for conducting data transfers. All media is required to be marked appropriately and in accordance with NISPOM 8-306 and 4-200.

Maintain a logbook for any document transferred and make available to DSS during security reviews:

- Date/time of transfer
- Document subject
- Name of individual who conducted the transfer
- Name of individual who authorized the transfer
- Mark media classification as appropriate
- Serial number and/or ID number of removable media

Reminder

The removable media restriction does not impact the ability to use "read-only" removable media.

4.7.3 Hardware Marking

All components of an IS, including input/output devices that have the potential for retaining information, terminals, standalone microprocessors, or work processors used as terminals, will bear a conspicuous, external label that states the highest classification level and most restrictive classification category of the information accessible to the component in the IS. In areas where classified and unclassified information are processed on collocated IS, unclassified hardware and media will also be marked.

Color Code Procedures

While color coded labels are not required, the following guidance should be used when color coding is used to indicate classification level.

- TOP SECRET – Orange
- SECRET – Red
- CONFIDENTIAL – Blue
- UNCLASSIFIED – Green

4.7.4 Trusted Download

Trusted download refers to a procedure, or series of procedures, that permits information to be released below the accredited level of the Information Systems (IS).

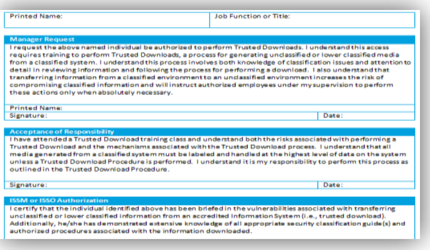
Almost without exception, the majority of contractors Information Systems that are accredited to process classified information operate at PL 1 or PL 2. As such, the protection requirements identified in Section 6 of the NISPOM Chapter 8 do not support more than one classification and/or sensitivity level of information. This is because the IS cannot recognize or distinguish information based on content. All information residing or processed on a PL 1, 2 or 3 systems are handled/treated at the classification/sensitivity level for which the information system is accredited. ODAA approved trusted download procedures listed below. Any alternate (non-DSS) procedures must first be documented, demonstrated to the ISSP, submitted to the government customer for approval and then included within the SSP.

4.7.4.1 Trusted Download Procedures

Example
Trusted Download Forms

The following forms are located in the Reference Material

- *Trusted Download Authorization Form (14.1.22), page 130*
- *Trusted Download Record (14.1.23), page 131*
- *Trusted Download Risk Acceptance Letter Example (14.1.24), page 132*



Printed Name:	Job Function or Title:

Manager Request

I request the above named individual be authorized to perform Trusted Downloads. I understand this access requires training to perform Trusted Downloads, a process for generating unclassified or lower classified media from a classified system. I understand this process involves both knowledge of classification issues and attention to detail in reviewing information and following the process for performing a download. I also understand that transferring information from a classified environment to an unclassified environment increases the risk of compromising classified information and will instruct authorized employees under my supervision to perform these actions only when absolutely necessary.

Printed Name:

Signature: Date:

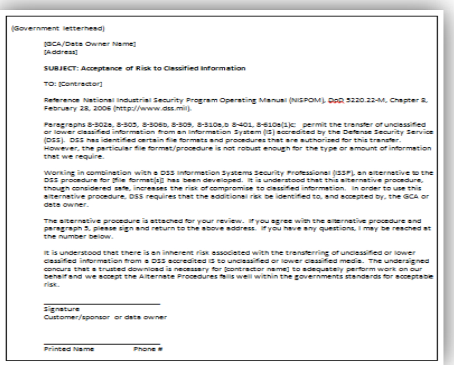
Acceptance of Responsibility

I have attended a Trusted Download training class and understand both the risks associated with performing a Trusted Download and the mechanisms associated with the Trusted Download process. I understand that all media generated from a classified system must be labeled and handled at the highest level of data on the system unless a Trusted Download Procedure is performed. I understand it is my responsibility to perform this process as outlined in the Trusted Download Procedure.

Signature: Date:

ISSM or ISSO Authorization

I certify that the individual identified above has been briefed in the vulnerabilities associated with transferring unclassified or lower classified information from an accredited Information System (i.e., trusted download). Additionally, he/she has demonstrated extensive knowledge of all appropriate security classification guide(s) and authorized procedures associated with the information downloaded.



(Government letterhead)

[GCA/Data Owner Name]
[Address]

SUBJECT: Acceptance of Risk to Classified Information

TO: [Contractor]

Reference National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M, Chapter 8, February 28, 2006 (http://www.dss.mil).

Paragraphs 8-302a, 8-305, 8-306b, 8-309, 8-310a,b 8-401, 8-610a(1)c: permit the transfer of unclassified or lower classified information from an Information System (IS) accredited by the Defense Security Service (DSS). DSS has identified certain file formats and procedures that are authorized for this transfer. However, the particular file format/procedure is not robust enough for the type or amount of information that we require.

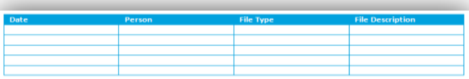
Working in combination with a DSS Information Systems Security Professional (ISSP), an alternative to the DSS procedure for [file format(s)] has been developed. It is understood that this alternative procedure, though considered safe, increases the risk of compromise to classified information. In order to use this alternative procedure, DSS requires that the additional risk be identified to, and accepted by, the GCA or data owner.

The alternative procedure is attached for your review. If you agree with the alternative procedure and paragraph 5, please sign and return to the above address. If you have any questions, I may be reached at the number below.

It is understood that there is an inherent risk associated with the transferring of unclassified or lower classified information from a DSS accredited IS to unclassified or lower classified media. The undersigned concurs that a trusted download is necessary for [contractor name] to adequately perform work on our behalf and we accept the Alternate Procedures falls well within the governments standards for acceptable risk.

Signature
Customer/sponsor or data owner

Printed Name Phone #



Date	Person	File Type	File Description

Scope

The February 2006 NISPOM Chapter 8 requirements for trusted download will be implemented by all newly accredited or reaccredited ISs at PL1, PL2, or PL3 that require the transfer of information with different sensitivities or information with unclassified or lower classified information. The implementation of the trusted download requirements will provide contractors with specific guidelines on how to perform this task while maintaining an acceptable level of risk during the creation of lower-than-system-level output.

In general, DSS trusted download requirements include:

- A comprehensive review by a "Knowledgeable User" (see Definitions below)
- The applicable DSS standard file type/formats and file transfer procedures documented in the IS (M)SSP
- Data owner/GCA acknowledgment and acceptance of additional risk for alternate trusted download procedures
  - Contract requirements
  - Letterhead memo signed by data owner or GCA.

NISPOM Requirements for Trusted Downloading

The following NISPOM Chapter 8 requirements apply to trusted downloading.

8-310a. **Human-Readable Output Review**	An appropriate sensitivity and classification review will be performed on human-readable output before the output is released outside the security boundary to determine whether it is accurately marked with the appropriate classification and applicable associated security markings.
8-310b. **Media Review**	Electronic output, such as files, to be released outside the security boundary will be verified by a comprehensive review (in human-readable form) of all data on the media including embedded text (i.e., headers and footer) before being released. Information on media that is not in human-readable form (e.g., embedded graphs, sound, video, etc.) will be examined for content using the appropriate software application. CSA-approved random or representative sampling techniques may be used to verify the proper marking of large volumes of output.

Definitions

Aggregation	The generation of a higher level overall classification of information when combining two or more lower level classified files (e.g., the combination of two unclassified files on a media producing Confidential or SECRET media hardware) based on Security Classification Guide(s) (SCG), restriction(s).
Acceptance of Risk	Alternate trusted downloading procedures that do not follow the DSS guidelines may be used only when the Government customer/data owner has formally (in writing) acknowledged and accepted the risk inherent in the alternate file type/format and procedures.
Comprehensive Review	A methodical review is established so that all higher level information has been removed prior to the data being released outside the IS's security boundary. Comprehensive reviews fall into two categories: Hardcopy and media. For hardcopy output a review will be performed by a "Knowledgeable User" to determine the correct classification and portion marking of the information. For large products in human-readable form, the comprehensive review must be done on no less than 20% of the output product. For media output, the media will be created by a "Knowledgeable User" following the DSS "File Transfer Procedure" as defined in the (M)SSP.
Knowledgeable User	An IS user (general or privileged) who is considered a subject matter expert (SME) with extensive knowledge of all appropriate security classification guide(s), and who can perform the "Comprehensive Review". The User will be trained by the ISSM or ISSO in understanding the vulnerabilities associated with producing lower-than-system-level output and file transfer procedures.
Sensitivity	Refers to formal access requirements (e.g., NATO, COMSEC, CNWDI) or caveats that specify handling or releasing restrictions (e.g., Foreign Government Information (FGI).
Slack Space	The data storage space that exists from the end of a file to the end of the last cluster assigned to the file. Slack space potentially can contain randomly selected bytes of classified data from computer memory.
Trusted download	A procedure, or series of procedures, that permits information to be released below the accredited level of the Information Systems (IS). Release of information outside the IS may take the form of hardcopy (or human-readable), digital/analog media, or electronic transfer.

File Type/Formatting Issues

The many different file formats represent a security challenge to the contractor, DSS, and in many cases the Government Contracting Activity (GCA) or data owner. Most applications, even those belonging to a professional software suite (e.g., Microsoft Office, Mat Lab, Claris) formats, stores, displays, and/or codes information differently. Some use proprietary coding techniques, some hide file related information (in binary and/or ASCII format) within the file, and some do things from a DSS security viewpoint that even the vendor cannot explain. However, to perform a reliable "trusted download", existing file format vulnerabilities must be considered.

While no security procedures can mitigate 100% of the risk involved, the DSS approved Trusted Download procedures mitigate an acceptable amount of risk and have been tested and that the procedures followed are reliable.

The only "SAFE" method of removing unclassified information from a classified system is to print and perform a comprehensive human review by a "Knowledgeable User". Once the printed output is reviewed, it is a simple process to scan the document into an unclassified or lower classified information systems. This will eliminate the vulnerabilities associated with electronic media.

No matter which file type/formats are used, the SSP must identify the file format(s) and specific procedures for reviewing and transferring those formats.

Legacy Operating Systems Slack Space Issues

In addition to file type/format issues, there is also an issue with how certain Operating Systems handle slack space that must be considered when copying information to media or during electronic transfers.

Systems that are known to produce slack space with non-predictable results are:

- MAC (Does not include MAC OS X)
- Windows 95/Windows 95, release A
- Some early versions of Windows 98

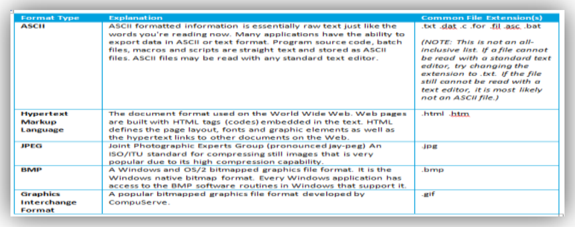
When copying to media or performing electronic transfers from these operating systems a DSS-authorized copy product/procedure must be used.

DSS Authorized File Type/Formats

This policy supports both hardcopy and media/electronic transfer file type/formats.

Hardcopy	All human-readable output sent to hardcopy devices, such as printers, copiers and faxes, independent of the original files format, fall into this category. This includes, but is not limited to, ASCII, HEX and Octal files, word processing, graphics, database and scientific files. As long as the file can be reviewed meeting the "Comprehensive Review" criteria it is eligible for release at a level (e.g., classified or unclassified) lower than the accredited IS level.
Media/Electronic Files	The following file formats are authorized by DSS to be released from the IS at or below the IS's accreditation level without an acceptance of risk from the government customer, but only after a comprehensive review.

Example
DSS Authorized File Types/Formats



Format Type	Explanation	Common File Extension(s)
ASCII	ASCII formatted information is essentially raw text just like the words you're reading now. Many applications have the ability to export data in ASCII or text format. Program source code, batch files, macros and scripts are straight text and stored as ASCII files. ASCII files may be read with any standard text editor.	.txt .dat .c .for .fil .asc .bat *(NOTE: This is not an all-inclusive list. If a file cannot be read with a standard text editor, try changing the extension to .txt. If the file still cannot be read with a text editor, it is most likely not an ASCII file.)*
Hypertext Markup Language	The document format used on the World Wide Web. Web pages are built with HTML tags (codes) embedded in the text. HTML defines the page layout, fonts and graphic elements as well as the hypertext links to other documents on the Web.	.html .htm
JPEG	Joint Photographic Experts Group (pronounced jay-peg) An ISO/ITU standard for compressing still images that is very popular due to its high compression capability.	.jpg
BMP	A Windows and OS/2 bitmapped graphics file format. It is the Windows native bitmap format. Every Windows application has access to the BMP software routines in Windows that support it.	.bmp
Graphics Interchange Format	A popular bitmapped graphics file format developed by CompuServe.	.gif

A Table of DSS Authorized File Types/Formats is located in the Reference Materials (14.1.25), page 133.

DSS File Transfer Procedures

For every file type or format, there are an endless number of transfer procedures that have been developed by industry and government. Some of the more common ones are identified at the end of this document. Any alternative procedure must get the GCA or data owner to accept the increased risk to classified information created by using one of the non-DSS authorized file types/formats and/or procedures.

No matter what file format or procedure is used, there are requirements that are common to all general media and to electronic transfers:

- The file types/formats and transfer procedures must be certified by DSS and documented in the SSP
- Target media must be factory fresh
- A comprehensive review must be performed so as to ascertain the sensitivity and classification level of the data
- Classified path/file embedded links and/or classified path/file name(s) are not used for source or target file(s)
- The compilation of all files on the target media does not cause an increased classification level due to "Aggregation"
- File(s) are transferred using a known, authorized utility or command
- The target media is verified to contain only intended source file(s)
- File(s) are verified on target media to contain the correct sensitivity of information and/or level of unclassified or lower classified information
- The appropriate security classification label is applied to the target media
- An administrative record of the transfer is created and maintained

If the ISSM is unable to implement the DSS Authorized Procedures, the SSP must include a description of how and why the contractor has deviated from the standard, and a RAL by the GCA. Note that RALs must be updated when the plan is reaccredited every three years.

DSS Authorized Procedure (Windows-Based)

1. The target media must be new.	
2. The procedure must be performed by a "Knowledgeable User".	
3. If multiple files are being transferred, create a designated directory for the transfer using the DOS make directory command (md [drive:] path) or the new folder command under Windows Explorer.	[Rationale: This will establish an empty directory which helps make certain that only intended files are transferred.]
4. If multiple files are being transferred, transfer all files into the newly created directory.	
5. As a general rule, files should be converted to one of the acceptable formats first (DSS Authorized File Type/Formats), then reviewed.	Drawings and presentation type files (e.g., PowerPoint, Publisher, and Visio) are an exception. These types of files within their native application may have layers of information, for example text on top of graphics, or multiple graphics layered together. Once exported into one of the authorized graphic formats (e.g., .bmp, .jpg, .gif) the layers will be merged together and will not be editable to remove any higher classified information. To review these files, use the native application used to generate the file and review every page, chart, slide, drawing etc. Within each page, chart, slide, drawing, etc., all layers are to be reviewed by ungrouping and moving objects around so everything is visible. Some applications may also have information in headers and footers, notes pages, etc. Below is a detailed procedure for reviewing one of the more commonly used presentation/graphic applications, review of MS Word and MS Excel files can follow the same instructions; however, some items may not apply. For PowerPoint:

	▪ Review Headers and Footers. To do this: Click on Header and Footer under the View menu. Click on and review both the Slide and the Notes and Handouts tab ▪ Review the Masters for the file. To do this: Click on Master under the View menu. Then select and review each of the Masters (Slide, Title, Handout, & Notes) ▪ For each slide, click on Edit, Select All. Once all objects are selected, click on Draw (bottom left of screen), then Ungroup, until the Ungroup option is no longer available (grayed out). Hit the tab key to outline each object (delineated by a box around a graphic or text), in the slide. If an object is outlined but not visible, move it, bring it forward or change its color until it is visible, or delete it. Repeat this process for each object in the slide. Use this process to find and delete all higher classified information ▪ After the review is complete, save the information in one of the authorized formats. To do this: Click on File Save As under the File menu. Select one of the DSS authorized formats from the drop-down menu of Save As Type
6. If any files are not in one of the following five formats, ASCII/Text, HTM/HTML, JPEG, BMP, GIF, convert it to one of these formats.	▪ Spreadsheet and database files must be exported as an ASCII text file(s) ▪ The graphics files within HTM/HTML files must be saved separately as JPG files. HTML files by themselves are text information and may be treated as a standard ASCII file format ▪ Executable programs may not be transferred. The source code (ASCII text) may be reviewed/transferred to a lower level IS then re-compiled into executable code
7. Review the file(s) using a compatible application. Review the entire file(s) not just random samples.	▪ BMP and JPG files may be reviewed with a graphics file viewer such as MS Photo Editor. (NOTE: because GIF files may contain a 3D/animation/multi-page image, you must use a program that will show all the information stored in GIF files. Web browsers can be used. MS Photo Editor will not display all the frames (images) and therefore is not adequate to view GIF files). You must right-click on the file, choose Properties, and select the Summary tab to ensure that no classified information exists in any field ▪ For ASCII text, the preferred application for reviewing is NotePad. However, these applications have file size limitations. If the file may not be opened with NotePad, then use MS Word (step d below) ▪ After completion of the review, remove all encoded formatting created by previous editing with MS Word. To do this: On the File menu, click Save As (Selected Approved Format) then click Save ▪ Review remaining ASCII files not viewable with NotePad with MS Word ▪ Ensure all hidden text and codes are viewable. To do this: Click Options on the Tools menu, click the View tab, then select every option under the Show section and All under the Formatting Marks section ▪ Verify all Tracked changes (Revisions in MS Word) are viewable. To do this: Click on Track Changes then Highlight Changes under the Tools menu. If Enabled, Disable the Track changes while editing. Enable the Highlight changes on screen ▪ Review the Summary and Contents sections of the file properties.

	To do this: Click Properties on the File menu, then click on the Summary and Contents tabs ▪ Review Headers and Footers. To do this: Click on Header and Footer under the View menu. Headers will be displayed at the top of each page, and any footers will be displayed at the bottom of each page. If a document has multiple sections, each section may have different Headers and Footers ▪ Review Comments. To do this: Click on Comments under the View menu. A comments pane will be displayed at the bottom of the screen. If Comments is grayed out under the View menu, this means there are no comments within the document ▪ Review Footnotes. To do this: Click on Footnotes under the View menu. If Footnotes is grayed out under the View menu, this means there are no footnotes within the document. If footnotes are not grayed out there are footnotes. If you are displaying the document in Normal layout or Web Layout, a footnote pane will appear at the bottom of the screen. If you are displaying the document in Print Layout, footnotes will already be visible at the bottom of each page, or at the end of the document ▪ Review the entire contents of the file including all Sections. All embedded objects except clipart and WordArt must be deleted. To be certain, review clipart and WordArt and text boxes to validate that there is no information hidden behind these objects. Embedded objects may be opened and saved separately prior to deletion. Each separately saved object is subject to this procedure prior to transfer ▪ When you are finished reviewing the file, make certain all hidden deleted information from Fast Save operations is removed. To do this: On the File menu, click Save As … (Selected Approved Format) then click Save. Also, if the file is not yet in one of the acceptable file format types, select one of the DSS approved formats from the drop-down menu of Save As Type ▪ For all file formats, verify the source and target file(s) names are not classified
8. Use the standard save or transfer command or utility (i.e., drag and drop, copy, etc.) to transfer the file(s) to the target media.	
9. Write-protect the media (physical or software) as soon as the transfer(s) are complete.	
10. Verify (dir/s [drive]: or Windows Explorer) that only intended file(s) were transferred.	
11. Compare the file(s) that were transferred to the original(s) [fc (pathname\filename) drive: (path\filename)].	
12. Apply the appropriate security classification label to the target media.	
13. Create an administrative record of	

the transfer and maintain with your audit records. The record must specify the data being released, the personnel involved and the date.	

DSS Authorized Procedure (Unix)

Reminder

These procedures should be tailored for the local environment. In particular, the Unix commands listed herein are for illustration purposes only and must be modified to account for the Unix OS version, hardware configuration, and software installation specifics.

1. Target media must be new.	
2. Procedure must be performed by a “Knowledgeable User”.	
3. If multiple files are being transferred, create a designated source directory for the transfer using the Unix make directory command (mkdir directory_name).	Rationale: This will establish an empty directory. This two-step process helps ensure that only intended files are copied.
4. If multiple files are being transferred, transfer all files into the newly created directory.	
5. Verify the source and target file(s) names are not classified.	
6. View the contents of all file(s) in the designated directory, not just “random samples.”	▪ For text files using software that displays the entire contents of the file. (e.g., Hex editor) Any unintelligible data is assumed to be classified at the accredited IS level ▪ For graphics or movie files review the file(s) using an appropriate file viewer. Ensure that the file format does not include internal annotations or other additional data (if present, this information can only be viewed with a specialized viewer, and poses a significant threat of inadvertent disclosure) ▪ For non-text files the sensitivity or classification of non-text, non-graphics files cannot generally be determined without intensive technical analysis. Such files must be assumed to be classified. Files in this category include binary database files, compressed archives, and executable code ▪ In the case of executable files, review and downgrade the source code, and then transfer the source code to a lower-classified machine for re-compilation ▪ In some cases, the source code will be classified, but the compiled code will be unclassified as specified in the classification guidance document. After compilation, the executable must be reviewed with HEX editor software to ensure that no classified information has escaped the compilation process ▪ In the case of binary database files, export the data to ASCII text format, then review and downgrade the text file for media migration

	▪ Compressed archives should be reviewed and transferred uncompressed
7. Use the Tar utility to create and write an archive of the source directory to the target media. The Unix command sequence will be as shown below (the exact command may vary depending on the Unix version, machine configuration, and the media used):	▪ mt -f /dev/rst0 rew Ensure tape is rewound (not required if using floppy) ▪ tar cvf /dev/rst0 /directory_name Create Tar file on tape
8. Write-protect the media as soon as the transfer(s) are complete.	
9. Verify that the media contains the expected data by printing a directory of the Tar file:	▪ mt -f /dev/rst0 rew Ensure tape is rewound (not required for floppy) ▪ tar tvf /dev/rst0 | lpr Print directory of file (| lpr may be omitted for on-screen review)
10. The output of the above command should match the contents of the source directory. To verify that they match, compare the output of the above command with the directory printed by the following command:	▪ ls -alR /source-directory | lpr (| lpr may be omitted for on-screen review)
11. Ensure the date, time, and file size(s) are as expected. If any unintended data was copied, the target media must be considered classified and cannot be used for a trusted down load again.	
12. Apply the appropriate security classification label to the target media.	
13. Create an administrative record of the transfer and maintain with your audit records. The record must specify the data being released, the personnel involved and the date.	

5.0 Physical and Environmental Protection

5.1 Physical Security

Safeguards will be established to prevent or detect unauthorized access to the IS and unauthorized modification of the IS hardware and software. Hardware integrity of the IS will be maintained at all times. The location of the IS system will be specified in the (M)SSP.

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.

All personnel granted unescorted access to an information system in a Closed Area is required to have an appropriate security clearance and need-to-know for the area (i.e. Visit Authorization Letter (VAL)). The contractor will document and retain a list of personnel with authorized access to the closed area. Persons without the appropriate level of clearance and/or need to know will be documented and escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented. 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.

Classified systems with non-removable media that remain in classified mode while unattended are to be secured in approved Closed Areas. When related classified removable media and/or associated materials are required to be stored with the classified IS the material is to be stored in a General Services Administration (GSA) approved security container. Where operational requirements are impacted by storing this material in approved containers, the Closed Area must be approved for open shelf or bin storage (i.e., open storage).

5.1.1 Hardware and Software Protections

Hardware should be inspected for any abnormalities prior to use in a classified environment. Software should be scanned for malicious software prior to use. Both hardware and software should be protected at its intended level of classification as soon as possible after the inspection and prior to use to prevent tampering such as stored in a closed area.

5.1.2 Mobile Systems

Systems accredited for processing classified data were not intended to be relocated to alternate sites for classified processing and are not addressed in the current version of the NISPOM. Due to the ongoing need to relocate systems, special procedures are required to document applicability, movement, operations, and security of classified systems that are relocated to alternate sites. If a mobile system is in place for 120 days or more, the contractor must submit a (M)SSP so that DSS can conduct the appropriate risk management evaluation.

Definition

A mobile system is a system that is accredited by the CSA or self-certified by the ISSM under an MSSP to process classified information at one location, and is temporarily relocated to another location for classified or unclassified processing. The mobile system may be a complete system or components of a larger more complex system. The mobile processing plan is included in the SSP and will be approved as part of the accreditation of the SSP.

Reminder

When relocated, systems that are connected to another system require an NSP.

Types of Mobile Systems

There are two categories of mobile systems; 1) systems that are relocated to other contractor sites, or 2) systems moved to government sites. Each of these system types are unique and require a specific set of operating procedures.

Duration of offsite processing

An accredited system may be offsite for no more than 120 days. If the system is required to be offsite for longer periods the ISSM must do one of the following:

- Transfer the system over to the gaining ISSM for accreditation under that CAGE code.
- Submit a request and justification from the customer concurring with the need to extend the relocation period beyond the 120 days and provide a date when the system or components will be returned or transferred. This may be either a formal letter or e-mail.
- Return the system back to the owning facility.

Accreditation Requirements

A system must have a final accreditation or self-certification by the ISSM prior to being relocated. Systems may be relocated while on an IATO under unique circumstances with RDAA approval.

Hard Drive Transfers

When transferring operating system hard drives for temporary use at another facility the following minimum procedures apply:

- Audit records from the drive must be downloaded on to a CD or other storage place and kept for review IAW Chapter 8
- The hard drive is removed from the system
- Hard drive is documented by serial number, and updated in the maintenance log
- Disk is sent offsite through proper NISPOM Chapter 5 procedures
- The transfer receipt is maintained
- When returned, the drive must be scanned for malicious code and go through certification process
- The drive is re-introduced as a maintenance item and documented in the maintenance log

Responsibilities of Receiving Facility

- The recipient organization must notify the dispatching organization and [Facility] Security of any security relevant problems that occur.
- The recipient organization must notify the dispatching organization and [Facility] Security of any discrepancies in the documentation or equipment.

Interconnected LANs

If a mobile system is connected to a separately accredited system at the remote location it will be treated as an interconnected LAN. As such it requires an approved NSP prior to connection.

Notification to DSS

The ISSM must notify DSS any time an accredited system or component is relocated from the facility. Only systems accredited with mobility can be relocated. Notification must be made to the assigned IS Rep and ISSP as soon as possible in advance of the movement to facilitate coordination with the IS Rep and ISSP at the relocation site. Prior concurrence of the movement by the IS Rep or ISSP is not required. Some relocation may be considered emergency movements to replace failed equipment or special needs. This should not be the norm and will be handled on a case by case basis.

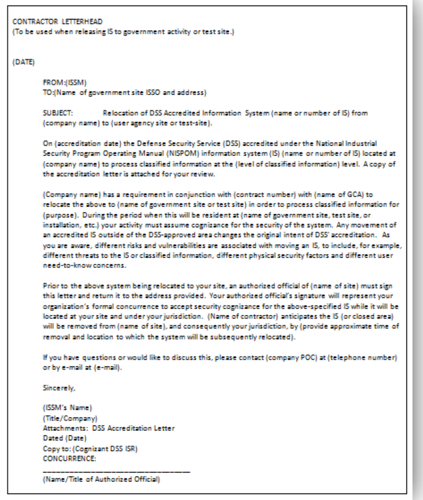
Mobile System Relocation Form

The Mobile System Relocation Form must be used for any accredited system or subset of a system that is being relocated to a Government site where the system will remain overnight or longer. The Letter 16 is not required for systems relocated to other contractor sites. A Mobile System Relocation Form will be valid for the life of the contract or system accreditation, whichever is less. The owning ISSM must provide a separate letter for each IS to be relocated by UID and operating environment.

Procedures

The SSP and IS profile must address mobile systems. The plan must explain the type of mobile system you have and identify where the procedures are located for each specific type of mobile system operated. For example, the SSP may include a statement that some systems or components of systems under this plan may be mobile systems that are relocated to other government sites, or contractor sites. Mobile processing procedures are contained in Attachment X of the specific system IS profile. The IS profile must identify whether or not the complete system is relocated as a unit or which component(s) of an accredited system may be relocated. This is especially important for large systems that are not relocated as a complete system.

Example
Mobile System Relocation Form



CONTRACTOR LETTERHEAD
(To be used when releasing IS to government activity or test site.)

(DATE)

FROM:(ISSM)
TO:(Name of government site ISSO and address)

SUBJECT: Relocation of DSS Accredited Information System (name or number of IS) from (company name) to (user agency site or test-site).

On (accreditation date) the Defense Security Service (DSS) accredited under the National Industrial Security Program Operating Manual (NISPOM) information system (IS) (name or number of IS) located at (company name) to process classified information at the (level of classified information) level. A copy of the accreditation letter is attached for your review.

(Company name) has a requirement in conjunction with (contract number) with (name of GCA) to relocate the above to (name of government site or test site) in order to process classified information for (purpose). During the period when this will be resident at (name of government site, test site, or installation, etc.) your activity must assume cognizance for the security of the system. Any movement of an accredited IS outside of the DSS-approved area changes the original intent of DSS' accreditation. As you are aware, different risks and vulnerabilities are associated with moving an IS, to include, for example, different threats to the IS or classified information, different physical security factors and different user need-to-know concerns.

Prior to the above system being relocated to your site, an authorized official of (name of site) must sign this letter and return it to the address provided. Your authorized official's signature will represent your organization's formal concurrence to accept security cognizance for the above-specified IS while it will be located at your site and under your jurisdiction. (Name of contractor) anticipates the IS (or closed area) will be removed from (name of site), and consequently your jurisdiction, by (provide approximate time of removal and location to which the system will be subsequently relocated).

If you have questions or would like to discuss this, please contact (company POC) at (telephone number) or by e-mail at (e-mail).

Sincerely,

(ISSM's Name)
(Title/Company)
Attachments: DSS Accreditation Letter
Dated (Date)
Copy to: (Cognizant DSS ISR)
CONCURRENCE:
____
(Name/Title of Authorized Official)

An example of a DSS Form Letter 16 is located in the Reference Materials (14.1.26), page 134

Requirements of a Mobile Processing Plan

The Mobile Processing Plan must address all aspects of security. This includes movement, physical security, and operations at the new location. The Mobile Processing Plan must address the following information.

Relocation to a Contractor Site

1. Identify the system.
2. List relocation site(s) and type of site (i.e., Government or Contractor).
3. Identify points of contact for each site, FSO and ISSM for contractors and government representative(s) when relocation is to a government site. (Name, address, phone number, and e-mail address).
4. How the equipment, dedicated software, and all classified information are to be transported and safeguarded.
5. A statement that every location must have adequate physical security safeguards to include supplemental controls, as necessary to protect the accredited IS, its software, and all classified information.
6. A statement that only an appropriately cleared employee of the contractor holding the Accreditation Letter will act as the ISSO for the system while it is relocated.
7. Before the accredited information system is relocated, the FSO or ISSM must notify the assigned IS Rep of the location(s) to which the IS will be moved and the scheduled departure and arrival times.
8. The FSO or ISSM must notify the receiving site when the equipment has been shipped and the method of shipment (FedEx, USPS, or hand carried).
9. The FSO or ISSM must provide the receiving location with a copy of the SSP and the IS Accreditation Letter. The ISSM of record or ISSM of facility where the IS was accredited must provide any training and/or briefings necessary to the receiving ISSM.
10. DSS retains security cognizance for IS under control of a cleared contractor while it is in-transit to or from the facility and/or a government installation.

Additional Requirements for relocating to Government Sites

- Prior to shipment, the applicable government activity must concur in writing (by signing and returning the Letter 16) to accept security oversight for a specific IS.
- The owning ISSM should re-certify the system upon its return from the government site.
- An MOU is not required when the DSS accredited system will connect to a government accredited system under oversight of the same office/program receiving the DSS system.

Documentation

- The contractor will provide the applicable government sites with a copy of the approved SSP, DSS IS Accreditation Letter, and a Mobile System Relocation Form acknowledging relocation of the IS to a particular government site if the system is to remain overnight or longer.
- The FSO or ISSM must provide the receiving location with a copy of the complete SSP and the IS Accreditation Letter. The ISSM of record or ISSM of facility where the IS was accredited must provide any training and/or briefings necessary to the receiving ISSM.
- Prior to shipment, the gaining facility must concur in writing (by signing and returning the Letter 16) to accept security oversight for a specific IS while at that facility.
- The owning ISSM must include the following documentation:
  - The signed Letter 16 which specifies the transfer dates and duration.
  - Accreditation letter and self-certification letter if applicable.
  - Copies of the approved security plan, IS Profile, and supporting documents.
  - A detailed listing of the components that are being relocated.
  - A list of responsible personnel managing the system at the relocation site and their duties.

Reminder

✓ *All documentation must be retained for at least one review cycle (per NISPOM) and a minimum of 12 months for auditing purposes.*

5.1.2.2 Mobile Processing Procedures

Alternate Site Processing within the facility

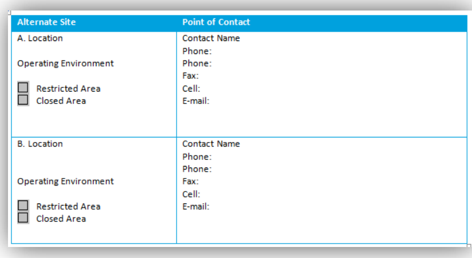
Classified computers may be temporarily relocated to the locations within the facility identified below for briefings, presentations, customer meetings, and related purposes. This temporary relocation will only be during the periods required and will be returned to the [specify closed or restricted] area immediately at the conclusion of classified processing. If the alternate site is a CSA approved closed area, the system can remain in the location over night for operations that require and extended stay period.

1. The system maintenance log will be used to record system movement, removal or addition of components from one system to another.
2. During the entire time the computer is outside of the [specify area] it must be accompanied by the cleared individual responsible for the system.
3. During classified operation at the temporary relocation site, access to the room will be restricted to those individuals with a verified clearance and need-to-know for the information being processed. If processing in a restricted area, a sign will be posted at all entrance points.
4. Only those individuals who have a valid signed user briefing statement will be allowed to operate the computer.

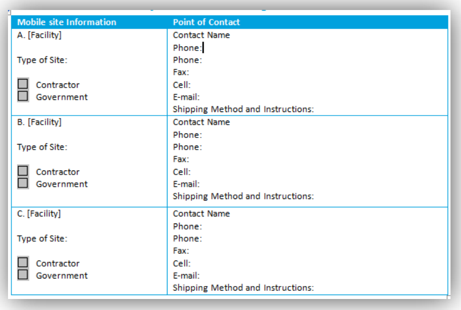
Example
DSS Authorized Sites and Locations

The following forms are located in the Reference Material

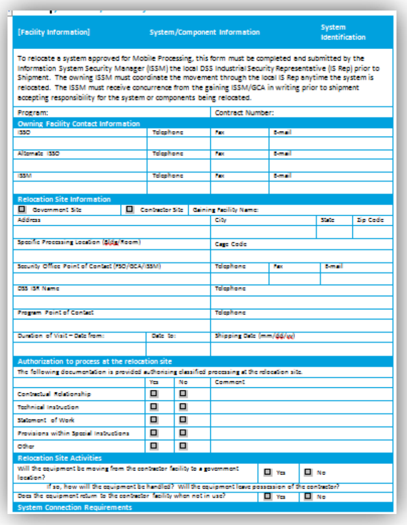
- *Authorized Alternate Site Locations (14.1.27), page 135*
- *Authorized Sites for Mobile Processing (14.1.28), page 136*
- *System Component Information Form (14.1.29), page 137*
- *Mobility Plan Sample (14.1.30), page 139*



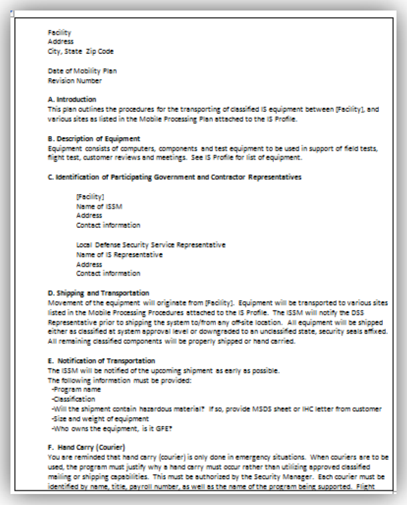
Alternate Site	Point of Contact
A. Location Operating Environment □ Restricted Area □ Closed Area	Contact Name Phone: Phone: Fax: Cell: E-mail:
B. Location Operating Environment □ Restricted Area □ Closed Area	Contact Name Phone: Phone: Fax: Cell: E-mail:



Mobile site Information	Point of Contact
A. [Facility] Type of Site: □ Contractor □ Government	Contact Name Phone: Phone: Fax: Cell: E-mail: Shipping Method and Instructions:
B. [Facility] Type of Site: □ Contractor □ Government	Contact Name Phone: Phone: Fax: Cell: E-mail: Shipping Method and Instructions:
C. [Facility] Type of Site: □ Contractor □ Government	Contact Name Phone: Phone: Fax: Cell: E-mail: Shipping Method and Instructions:



[Facility Information]	System/Component Information		System Identification
To relocate a system approved for Mobile Processing, this form must be completed and submitted by the Information System Security Manager (ISSM) the local DSS Industrial Security Representative (IS Rep) prior to Shipment. The owning ISSM must coordinate the movement through the local IS Rep anytime the system is relocated. The ISSM must receive concurrence from the gaining ISSM/GCA in writing prior to shipment accepting responsibility for the system or components being relocated.			
Program:		Contract Number:	
Owning Facility Contact Information			
ISSO	Telephone	Fax	E-mail
Alternate ISSO	Telephone	Fax	E-mail
ISSM	Telephone	Fax	E-mail
Relocation Site Information			
□ Government Site	□ Contractor Site	Gaining Facility Name:	
Address	City	State	Zip Code
Specific Processing Location (Bldg/Room)	Cage Code		
Security Office Point of Contact (FSO/GCA/ISSM)	Telephone	Fax	E-mail
DSS ISR Name	Telephone		
Program Point of Contact	Telephone		
Duration of Visit – Date from:	Date to:	Shipping Date (mm/dd/yy)	
Authorization to process at the relocation site			
The following documentation is provided authorizing classified processing at the relocation site.			
	Yes	No	Comment
Contractual Relationship	□	□	
Technical Instruction	□	□	
Statement of Work	□	□	
Provisions within Special Instructions	□	□	
Other	□	□	
Relocation Site Activities			
Will the equipment be moving from the contractor facility to a government location?	□ Yes	□ No	
If so, how will the equipment be handled? Will the equipment leave possession of the contractor?			
Does the equipment return to the contractor facility when not in use?	□ Yes	□ No	
System Connection Requirements			



Facility
Address
City, State Zip Code

Date of Mobility Plan
Revision Number

A. Introduction
This plan outlines the procedures for the transporting of classified IS equipment between [Facility], and various sites as listed in the Mobile Processing Plan attached to the IS Profile.

B. Description of Equipment
Equipment consists of computers, components and test equipment to be used in support of field tests, flight test, customer reviews and meetings. See IS Profile for list of equipment.

C. Identification of Participating Government and Contractor Representatives

[Facility]
Name of ISSM
Address
Contact information

Local Defense Security Service Representative
Name of IS Representative
Address
Contact information

D. Shipping and Transportation
Movement of the equipment will originate from [Facility]. Equipment will be transported to various sites listed in the Mobile Processing Procedures attached to the IS Profile. The ISSM will notify the DSS Representative prior to shipping the system to/from any off-site location. All equipment will be shipped either as classified at system approval level or downgraded to an unclassified state, security seals affixed. All remaining classified components will be properly shipped or hand carried.

E. Notification of Transportation
The ISSM will be notified of the upcoming shipment as early as possible.
The following information must be provided:
-Program name
-Classification
-Will the shipment contain hazardous material? If so, provide MSDS sheet or IHC letter from customer
-Size and weight of equipment
-Who owns the equipment, is it GFE?

F. Hand Carry (Courier)
You are reminded that hand carry (courier) is only done in emergency situations. When couriers are to be used, the program must justify why a hand carry must occur rather than utilizing approved classified mailing or shipping capabilities. This must be authorized by the Security Manager. Each courier must be identified by name, title, payroll number, as well as the name of the program being supported. Flight

Offsite Processing

When equipment is relocated to an area outside of the facility, the System Information form must be completed for each location prior to shipment. This form must be maintained as part of this system's documentation. The ISSM will notify DSS no later than five days prior to shipping the system to/from any off-site location. All equipment will be shipped either as a classified system at the approved level classification or downgraded to an unclassified state. Security seals will be affixed when equipment is relocated to detect tampering. All remaining classified components will be properly shipped or hand carried.

The ISSM or alternate must make certain the following requirements are met:

- Designate, in writing to the DSS Representative who will be responsible for the system at the relocation site
- Maintain a complete copy of the system documentation to accompany equipment
- Update the system maintenance log to reflect movement to and from the facility
- Brief users accompanying the system on their responsibilities to include:
  - Maintaining the audit records of the system (automated or paper)
  - Responsibilities for maintaining the integrity of the security seals (if equipment is in an unclassified area)
  - Make certain that the equipment is properly downgraded (if not in an approved closed area at system approval level with appropriate need-to-know)
  - Establishing a process so that media (paper and magnetic) is properly reviewed and labeled
  - Ensuring that the weekly audit (review) is performed and annotated on the review record
  - Bringing any discrepancies to the attention of the ISSO
  - Responsibility that all records are returned with the system
- The ISSM must coordinate the relocation through the local DSS Representative. The DSS Representative for both sites must exchange information and authorization before the move occurs
- Make certain that the gaining activity acknowledges in writing, prior to the shipment, that they will accept oversight of the system during the relocation period

5.1.3 Software Protections

Software from unknown or questionable sources will not be used on classified information systems (IS). The use of personal or public domain software is discouraged and each installation of such software will be approved by the ISSM. From the earliest feasible time, all IS software will be stored on media that is safeguarded to the highest level of intended processing. Installation and modification of software will be performed by authorized personnel who are knowledgeable of the computer system and the software being installed. Software will only be loaded from media that is write-protected. Software will be screened and tested for malicious code or logic.

Unclassified software that will eventually be used during classified processing periods must be developed by cleared, knowledgeable personnel or reviewed and/or tested by cleared, knowledgeable personnel. This includes operating systems, 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 the ISSM must ensure uncleared persons are restricted from having the ability to access the software. This can be accomplished through strict control of file permissions. The ISSM must ensure that all users with access, including privileged administrators, have the appropriate clearance.

5.1.4 Emergency Procedures

Contractors will develop procedures for safeguarding classified material in emergency situations. The procedures will be as simple and practical as possible and should be adaptable to any type of emergency that may reasonably arise. Contractors will promptly report to the CSA any emergency situation that renders the facility incapable of safeguarding classified material.

5.1.5 Transient Electromagnetic Pulse Emanation Standard (TEMPEST)

TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. Compromising emanations are unintentional intelligence-bearing signals that, if intercepted and analyzed, will disclose classified information when it is transmitted, received, handled, or otherwise processed by any information processing equipment.

TEMPEST countermeasures will be applied only in proportion to the threat of exploitation and the resulting damage to the national security should the information be intercepted and analyzed by a foreign intelligence organization. It is the responsibility of the GCA to identify in writing what TEMPEST countermeasures may be required. The GCA will identify any TEMPEST requirements within the United States to the CSA for approval prior to imposing requirements for TEMPEST countermeasures on contractors. Contractors may not impose TEMPEST countermeasures upon their subcontractors without GCA and CSA approval.

The government is responsible for performing threat assessment and vulnerability studies when it is determined that classified information may be exposed to TEMPEST collection.

Contractors will assist the GCA in conducting threat and vulnerability surveys by providing the following information upon request:

- The specific classification and special categories of material to be processed/handled by electronic means
- The specific location where classified processing will be performed
- The name, address, title, and contact information for a point-of-contact at the facility where processing will occur

5.1.6 Personnel Security

5.1.6.1 Personnel Security Clearance Verification

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. Each user will be required to complete and sign the “Acknowledgement of Briefing for IS 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. 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 system when no longer necessary or allowed.

5.1.7 Personnel Sanctions

Contractor management will establish and enforce sanctions on personnel failing to comply with the established information security policies and procedures.

5.2 System and Information Integrity

5.2.1 Flaw Remediation

The ISSM will identify ISs containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The ISSM will install security-relevant software upgrades (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information systems error handling, are also addressed expeditiously. Maintaining security compliance (i.e., patching, service packs, and hotfixes) does not require reaccreditation as these are maintenance items and will be documented as such (e.g., Maintenance, Operating System & Security Software Change Log entries).

5.2.2 Unclassified Software Review

An unclassified software review and/or testing provides two options for examination of unclassified software prior to its introduction into the IS and use for classified processing; 1) the contractor may choose either a review or testing of the unclassified software, 2) an unclassified software review must be a line-by-line source code review. Unclassified software testing must include a validation of all functionality for security-relevant items. This includes security relevant software such as all OS software on an IS where I&A and/or auditing have been technically implemented, virus and malicious code detection and sanitization software, all security relevant information such as software and router tables, configuration settings, IS and OS documentation, audit data, etc. Security relevant hardware includes any hardware or IS component that contains, or has the potential of containing classified information as well as resolution of any discrepancies. For example, if the software writes to a file, the file must then be reviewed using a hexadecimal editor to ensure that only the intended information was written.

Unclassified software that will eventually be used during classified processing periods must be developed by cleared, knowledgeable personnel or reviewed and/or tested by cleared, knowledgeable personnel. The review and/or testing are done to provide reasonable assurance that security vulnerabilities do not exist.

5.2.3 Antivirus

Software for the detection of malicious code must be implemented. Antivirus definition files must be updated at least once every 30 days. The antivirus executable software must be updated within 30 days of being available (without the latest executable software some definitions will not be implemented and some malicious code may get through). It is preferred that Linux or Solaris systems use applicable antivirus software rather than utilizing an external Windows system for scanning prior to introducing data onto the Linux or Solaris system. The IS must employ the appropriate software to check all files and media for viruses and malicious code upon introduction to the system. Additionally, the ISSM will ensure that the IS prevents non-privileged users from circumventing malicious code protection capabilities.

6.0 Technical Controls

6.1 Access Control

The ISSM ensures the IS stores and preserves the integrity of the sensitivity of all information internal to the system. IS entry is based upon users having an account (i.e., User Profile) on each system to which they require access. All users must authenticate into the system using a unique User ID and password. For Generic or Group accounts, see Generic or Group Accounts Paragraph 6.9.2. The ISSM ensures the denial of physical access by unauthorized individuals unless under constant supervision of technically qualified, authorized personnel.

For Protection Level 2 (PL-2) systems, the ISSM will provide discretionary access controls. The PL-2 system will implement discretionary access controls when the security support structure defines and controls access between named users and named objects (e.g., files and programs) in the system. The discretionary access control policy includes administrative procedures to support the policy and its mechanisms.

For PL-3 systems, the ISSM will ensure some process or mechanism that allows users (or processes acting on their behalf) to determine the formal access approvals granted to another user. Furthermore, the ISSM ensures some process or mechanism that allows users (or processes acting on their behalf) to determine the sensitivity level of data.

6.1.1 Separation of Function

For PL-3 systems, the ISSM will ensure the functions of the ISSO and the system manager will not be performed by the same person.

6.2 NISPOM Compliant Logon Banner for DSS Accredited Non-DoD Systems

Banners will be included on all classified IS to notify users they are subject to monitoring and that such monitoring could be used against them in a criminal, security, or administrative proceeding.

On occasion the Department of Defense updates the logon banner for DoD systems. ISSM's for systems accredited by DSS/ODAA will receive a message from DSS when and if contractor systems need to be updated. The required Banner for DSS Accredited Non-DoD Systems follows.

DSS Accredited Non-DoD System Warning Banner

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

6.2.1 DoD Warning Banner for SIPRNet

NISP contractors having IS connected to the Defense Information Systems (DISN) SIPRNet are required to implement certain enhanced security measures (i.e., Security Technical Implementation Guide (STIG) and CTO) as a result of an Approval To Connect (ATC) or the Memorandum of Agreement (MOA) with DISA. Communication Tasking Order (CTO) 07-13 and DoD CIO Memo dated September, 2012 documents the DoD Warning Banner used for IS connected to the DISN. The DoD, at their discretion, may change the warning banner without advanced notice. NISP contractors with approved DISN SIPRNet connection will utilize the DoD Warning Banner on the SIPRNet system as follows.

DoD SIPRNet Warning Banner

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Use this banner for desktops, laptops, and other devices accommodating banners of 1300 characters. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating “OK.”

6.3 Session Controls

6.3.1 Successive Login Attempt Controls

Repeated unsuccessful login 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 three unsuccessful attempts. The account will remain locked for at least 60 minutes or must be unlocked by an administrator. Additionally, the system will grant system entry only in accordance with the conditions associated with the authenticated user’s profile. If no explicit entry conditions are defined, the default (deny all) will prohibit all remote activities, such as remote logons and anonymous file access.

For PL-2 and PL-3 systems, the system will be configured to support multiple logon sessions for each user ID or account, the IS will provide a protected capability to control the number of logon sessions for each user ID, account, or specific port of entry. The IS default will be a single logon session.

6.3.2 User Inactivity

If technically feasible, the IS will detect an interval of user inactivity, such as no keyboard entries, and will disable/lock any future user activity until the user re-establishes the correct identity with a valid authenticator. The inactivity time period and restart requirements will not be more than 15 minutes. The IS will provide a session lock mechanism, when activated on a device with a display screen, places an unclassified viewable pattern onto the associated display, hiding what was previously visible on the screen such as a screen saver.

6.3.3 Logon Notification (PL-2/PL-3 only)

The operating system should have the capability to provide the notification of the date and time of the user's last logon; the location of the user (as can best be determined) at last logon; and the number of unsuccessful logon attempts using this user ID since the last successful logon. This notice will require positive action by the user to remove the notice from the screen.

6.4 USB Devices and Ports

USB ports are not required to be disabled physically or by the BIOS. External storage devices that connect to the USB port(s) are allowed but must be controlled. All data storage devices must be marked with the highest classification level of the data saved to the device and stored in approved containers. External media must be destroyed at the end of their usable life until a DoD approved sanitization method is available. If required (i.e., Top Secret), USB memory devices must be inventoried, accounted for, and documentation made available during security reviews. Locking or write-protecting unused USB ports is recommended to the extent practical to minimize threats related to USB storage devices. Refer to Section 9.2 for additional guidance.

6.5 Radio Frequency ID Tags

Vulnerabilities associated with the use of Radio Frequency ID (RFID) should be considered when there is a TEMPEST or Emission Security (EMSEC) requirement in the DD254 or contract. The use of RFID to store classified information is not approved. Equipment with RFID capabilities (e.g., printers) that are connected to accredited systems processing classified information must be documented in the SSP. See the DISA Wireless STIG Version 6, Release 1, Paragraph 3.5.1 for more information.

6.6 Secure Wireless LANs

The use of Secure Wireless LANs (S-WLAN) technology with classified information must be in accordance with the latest version of the DISA Wireless STIG. S-WLAN networks cannot be self-certified and cannot be issued an IATO.

6.7 Audit and Accountability

6.7.1 Audit Requirements

Auditing and monitoring requirements apply to all auditable devices on the accredited system. System components (e.g. Operating systems, firewalls, routers, intrusion detection devices, etc.) should be monitored and reviewed for anomalies through the use of audit trails. Contractors' auditing and monitoring policies and procedures will include efforts to detect activity indicative of insider threat behavior, along with reporting procedures to the FSO and ITSO. The policies and procedures will include how to properly protect, interpret, store and limit access to user activity monitoring methods and results to authorized personnel.

Audit records will be maintained and reviewed from the date of IS accreditation until withdrawal of accreditation. At all times, a minimum of 12 months audit trails are required to be available for review.

Audit records will include the following:

- 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)
- Successful and unsuccessful logins and logoffs
- Unsuccessful accesses to security-relevant objects and directories
- Changes to user authenticators
- The blocking or blacklisting of a user ID, terminal, or access port
- Denial of Access from an excessive number of unsuccessful login attempts

Audit records will be protected against unauthorized access, modification, or deletion and will be retained for 12 months, or from the date of accreditation, whichever is less. The IS will be configured to automatically create and maintain an audit trail or log to record security-relevant activities of the IS. The information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.

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.

- User briefing statements
- Additions, deletions, reconfiguration, and repair actions to accredited hardware
- Installation, modification or testing of operating system and security related software
- Actions take to sanitize IS components
- The placement and destruction of security seals

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.

ISSMs may choose to install and use audit reduction tools on larger or high-traffic systems. Audit reduction tools are considered security relevant and must be evaluated by the ISSP. Raw audit trails should be retained for the system to provide data for analysis in the event of an inquiry or investigation into an IS related event.

Guidelines for reviewing automated audit records:

- Verify that the automated audit functions are performing properly and there are no time periods during which audit data is missing
- Review all failed logins. Question multiple failed login attempts and account lockouts
- 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
- Question login sessions that occur at unusual times (e.g., 2:00am) or sessions that are left open for long periods of time
- Scrutinize direct logins to generic or group accounts. Verify they are within the guidelines specified in the (M)SSP
- If applicable, verify accesses to privileged group/generic accounts were made from authorized user IDs
- 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

6.7.2 Weekly Audit Reviews – Definition

System audit trails will be analyzed and reviewed at least weekly. "At least weekly" means once per calendar week. Setting different days for audit analysis can be useful in breaking up established patterns of analysis by the ISSM/ISSO. However, certain patterns should be highly discouraged.

6.8 Security Seals

Approved tamper-proof, pre-numbered seals should be used on hardware components anytime the hardware may be subject to access by uncleared personnel (e.g., used for periods-processing, in restricted areas, mobile systems, printers or relocation).

6.9 Identification and Authentication

6.9.1 Identification and Authentication Management

Logon authentication will be implemented on all ISs. Each user of an IS will be assigned a unique identifier, commonly referred to as a 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.

The following are requirements for identification and authentication management:

- User IDs will be established after the user’s clearance and need-to-know has been validated and they are required to have received an IS briefing from the ISSM/ISSO regarding there is security responsibilities
- The ISSM/ISSO or delegated privileged user may establish the initial password, relay the same to the user, and the user will 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
- Active user IDs will 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
- 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
- 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
- Individual authenticators will not be shared with anyone
- Access to authentication data will be restricted to authorized personnel through the use of encryption or file access controls, or both

For PL-2 systems, the ISSM will ensure access to the IS by privileged users who either reside outside of the IS's perimeter or whose communications traverse data links that are outside the IS's perimeter will require the use of strong authentication such as an I&A technique that is resistant to replay attacks.

6.9.2 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. Generic group accounts (e.g., Guest, Field, Nobody, etc.) will be deleted or disabled.

On rare occasions group accounts may be permitted where required by the contract, deliverable configuration, or when otherwise necessary. The ISSM should document the need for a group account in the security plan. Individuals utilizing group account logons must be documented in a manual log (or other approved method) to ensure individual user accountability.

6.9.3 Password Policy

The following are requirements for all passwords:

- Passwords will be protected at the highest classification level and most restrictive classification category of information to which they permit access.
- Passwords will be changed at least every 60 days
- Passwords will be changed when compromised
- Passwords will not be displayed to the screen when input
- Passwords will contain a minimum number of characters, as defined in the baseline standards for each OS, alpha/numeric upper/lower case and special characters

For PL-2 systems, in those instances where the means of authentication is user-specified passwords, the ISSM may employ (with the approval of the CSA) automated tools to validate that the passwords are sufficiently strong to resist cracking and other attacks intended to discover the user's password.

6.9.4 BIOS Password

The BIOS must be protected with a password which must meet the length and complexity requirements stated above to the extent supported by the particular BIOS firmware. Waivers, exceptions, or variances are not required in cases where the BIOS cannot support the password length requirement. However, a waiver must be requested if the system's BIOS cannot be password protected for operational reasons. BIOS passwords are not deemed user authenticators and need not be changed every 60 days.

6.10 System and Communications Protection

6.10.1 Data Transmission Protection

Protection measures are required whenever classified information is to be transmitted outside the boundaries of the controlled IS area.

The ISSM will ensure data transmissions will be protected by one of the methods below:

- Information distributed only within an approved closed area
- National Security Agency (NSA) approved Type 1 encryption device (e.g., KIV-7M, KIV-7HS, KG-175, etc.)
- A Protected Distribution System (PDS) compliant with NSTISSI 7003.

When changes to transmission protections are required, the ISSM will be notified. The ISSM will ensure the (M)SSP is updated and DSS re-accreditation occurs as necessary. All changes to communication interfaces will be performed by authorized personnel and documented.

6.10.2 Protected Distribution Systems

PDS require approval prior to installation of conduit and subsequent cabling/wiring. The process and procedures to install PDS per NSTISSI 7003 follows, as well as a sample plan to expedite the approval process.

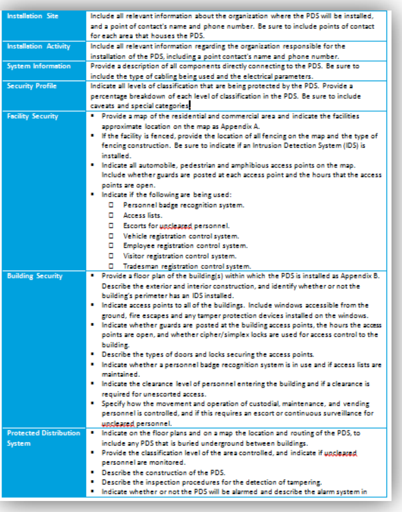
Classified information must be protected whenever it is transmitted through areas or components where unauthorized individuals may have unescorted physical or uncontrolled electronic access to the information or communications media.

The contractor must use National Security Agency (NSA) Type 1 encryption devices when transmitting classified information outside its facility and either NSA Type 1 devices or a PDS when transmitting classified information within its facility. The policy requirements for a PDS are contained in National Security Telecommunications and Information Systems Security Instruction (NSTISSI), Number 7003, which is posted on the ODAA web site. NSTISSI 7003 states that each contractor must be evaluated on its own risks and vulnerabilities based upon factors such as location, depth of security, environment, access controls, and personnel security. The remaining risk is then compared against an installation and inspection requirements matrix.

The PDS may be constructed from hardened metal conduit, or PVC, and the matrix of the NSTISSI 7003 explains when each should be used.

The IS Rep and/or ISSP should be involved in the early stages of PDS design and throughout installation. In many cases, however, the IS Rep is not asked to review the PDS until after it has been completed. The PDS must be approved prior to use after installation. Ensuring the IS Rep and/or ISSP review the PDS during installation avoids unnecessarily spending money on a PDS that does not meet NSTISSI 7003 standards or a PDS that cannot be visually inspected for approval after completion.

Example
Protected Distribution System Approval Request



Installation Site	Include all relevant information about the organization where the PDS will be installed, and a point of contact's name and phone number. Be sure to include points of contact for each area that houses the PDS.
Installation Activity	Include all relevant information regarding the organization responsible for the installation of the PDS, including a point contact's name and phone number.
System Information	Provide a description of all components directly connecting to the PDS. Be sure to include the type of cabling being used and the electrical parameters.
Security Profile	Indicate all levels of classification that are being protected by the PDS. Provide a percentage breakdown of each level of classification in the PDS. Be sure to include caveats and special categories.
Facility Security	▪ Provide a map of the residential and commercial area and indicate the facilities approximate location on the map as Appendix A. ▪ If the facility is fenced, provide the location of all fencing on the map and the type of fencing construction. Be sure to indicate if an Intrusion Detection System (IDS) is installed. ▪ Indicate all automobile, pedestrian and amphibious access points on the map. Include whether guards are posted at each access point and the hours that the access points are open. ▪ Indicate if the following are being used: □ Personnel badge recognition system. □ Access lists. □ Escorts for uncleared personnel. □ Vehicle registration control system. □ Employee registration control system. □ Visitor registration control system. □ Tradesman registration control system.
Building Security	▪ Provide a floor plan of the building(s) within which the PDS is installed as Appendix B. Describe the exterior and interior construction, and identify whether or not the building's perimeter has an IDS installed. ▪ Indicate access points to all of the buildings. Include windows accessible from the ground, fire escapes and any tamper protection devices installed on the windows. ▪ Indicate whether guards are posted at the building access points, the hours the access points are open, and whether cipher/simplex locks are used for access control to the building. ▪ Describe the types of doors and locks securing the access points. ▪ Indicate whether a personnel badge recognition system is in use and if access lists are maintained. ▪ Indicate the clearance level of personnel entering the building and if a clearance is required for unescorted access. ▪ Specify how the movement and operation of custodial, maintenance, and vending personnel is controlled, and if this requires an escort or continuous surveillance for uncleared personnel.
Protected Distribution System	▪ Indicate on the floor plans and on a map the location and routing of the PDS, to include any PDS that is buried underground between buildings. ▪ Provide the classification level of the area controlled, and indicate if uncleared personnel are monitored. ▪ Describe the construction of the PDS. ▪ Describe the inspection procedures for the detection of tampering. ▪ Indicate whether or not the PDS will be alarmed and describe the alarm system in

An example of a Protected Distribution System Approval Request (14.1.31) is located in the Reference Materials, page 141.

The most common mistake contractors make during PDS installation is hiding the PDS run either above a false ceiling or between walls or columns where inspection is impossible. When the PDS is installed above a false ceiling or under a raised floor, the contractor must alarm the surrounding area, alarm the PDS*, or install clear ceiling tiles. The clear tiles must cover the entire length of the run. Installation in walls and/or columns is more difficult. In order to permit the IS Rep to see the installation work and verify that it is correct, the preferred option is for the IS Rep to be on hand after the conduit is installed, but before the wall, column, or trench is closed. Photos taken during PDS installation should be retained to provide a record for later review and to substantiate the installation. If none of these options is possible, the wall, column, or trench must be opened for inspection. PDS is used for the transmission of classified information; unclassified lines cannot be in the same PDS as classified lines.

The Forward of the NSTISSI 7003 states that NSTISSI 7003 "provides guidance for protection of wire line and optical fiber PDS to transmit unencrypted classified National Security Information (NSI)." The document is referencing classified wire lines and fiber optic. NSTISSI ANNEX B, PDS Installation Guidance, Paragraph 5a, General, states “more than one classification level may use components of a single protected distribution system." This is guidance for allowing different classification levels in the same PDS, but does not apply to unclassified lines. Within a closed or restricted area, physical security safeguards must be used to prevent or detect unauthorized modification to the transmission lines and cabling. Personnel and physical security mechanisms and inspections usually accomplish this before each classified processing session. If tampering is suspected, the ISSM should be notified immediately, and processing classified information will be discontinued until the reason for the tampering is determined and all security issues are resolved.

The PDS should be included on the topology diagram in associated information systems security plans. During security reviews, ISSPs will verify transmission procedures and controls established at approval are maintained.

Reminder

There are no UL standards for installing alarms on a PDS. Normally, alarm companies used for Closed Area intrusion detection systems (alarms) can be employed to alarm a PDS run. The ability for the alarm to detect an attempted intrusion will be demonstrated during the approval process of the PDS.

6.10.3 Network Management and Protections

In areas where both classified and unclassified systems reside, it is a good practice to clearly mark or color code classified lines to prevent inadvertent connections to unclassified systems. Where feasible, network devices such as routers, switches, and patch panels reside within physically separate restricted access communications closets within the Closed Area to which only authorized network management personnel are permitted access. When feasible, unclassified and classified network devices within the communications closets can be mounted in physically separate racks. Network devices such as routers and switches have password protections enabled to assure only authorized network management personnel are permitted access to set or change configurations.

6.10.4 Controlled Interfaces

This section serves to clarify the requirements from the NISPOM Chapter 8, Section 7, interconnected systems.

- Controlled interfaces can range from a simple router with an access control list (ACL) implemented, to firewalls, intrusion detection systems (IDS) and intrusion prevention systems (IPS), up to a high assurance guard (HAG) used as a cross-domain solution. Selecting a device to implement is dependent upon the security requirements of the networks involved
- Two interconnected networks of the same classification and protection level that merely need to restrict users from one network from accessing all or specific services on the other network can use a router with an ACL implemented that restricts by IP addresses, ports and protocols
- The CI will be implemented so that all possible failures will result in no loss of confidentiality or unacceptable exposure to loss of integrity or availability

Reminder

Auditing must be performed on firewalls and IDS at least weekly along with the remainder of the information systems. MOUs associated with interconnected systems may have additional information and/or requirements documented within them. Any suspected intrusion attempts must be investigated and reported to the ISSP and IS Rep promptly.

6.11 Classified Voice over Internet Protocol/Video Teleconferencing

Classified Voice over Internet Protocol (VoIP) and video teleconferencing (VTC) applications present considerable cost savings when utilized over existing networks. Whether including in a new network, piggy-backing on an existing network, or tunneling through a network of lower classification, they do present unique vulnerabilities.

A VoIP phone is basically a "dumb terminal". Any configuration on the phone should be limited to the System Administrator/ISSO. Referencing 14.1.32, in the case of the VoIP phone on LAN B it needs to be added to the SSP for LAN B in the network description and configuration diagram, but does not need to be included in the hardware list. An VoIP phone added at a later time doesn't constitute a security relevant change so the system will not need reaccreditation.

Example
WAN Accreditation Boundaries

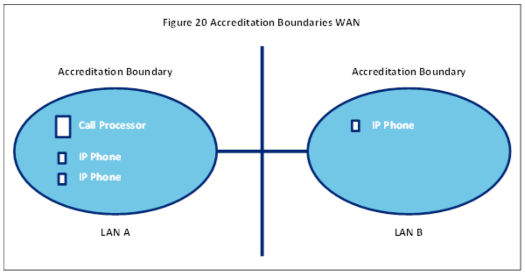


Figure 20 Accreditation Boundaries WAN

WAN Accreditation Boundaries is located in the Reference Materials (14.1.32), page 142.

Call Processor (Call Manager) must have NISPOM Chapter 8 implemented to the extent possible (e.g., auditing may not be possible). At a minimum, configuration should be limited to the System Administrator/ISSO. Referencing 14.1.32, in the case of the Call Processor and IP Phones located on LAN A, they need to be included in the SSP for LAN A in the network description and configuration diagram, and the call processor needs to be included in the hardware list.

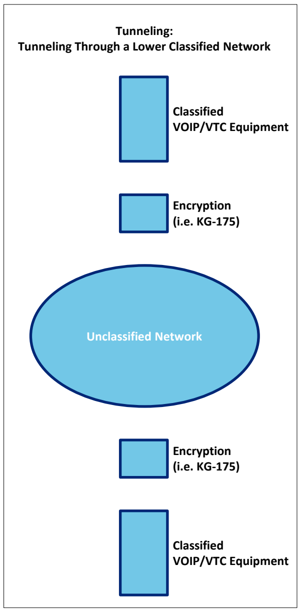
For more detailed security issues related to VoIP and VTC see the DISA VTC and VoIP STIGs at http://iase.disa.mil/stigs/stig/index.html.

Minimum Requirements for Use of VoIP/VTC on Classified Contractor LANs/WANs

- Normal I&A should be implemented on all servers, firewalls, encryption devices, and computers associated with the system to the extent they can be configured
- Implement Access Control Lists so that only valid IP addresses for VoIP/VTC components can be reached, denying all others
- From the Call Processor, perform a PING and TRACERT to non-VoIP/VTC IP address, which should fail

Since Contractor WANs are small a community of interest networks, firewalls may not be required; however, if the WAN is a part of a larger GCA WAN a firewall will be required.

Example
Tunneling


Tunneling:
Tunneling Through a Lower Classified Network
Classified VOIP/VTC Equipment
Encryption (i.e. KG-175)
Unclassified Network
Encryption (i.e. KG-175)
Classified VOIP/VTC Equipment

Tunneling is located in the Reference Materials (14.1.33), page 143.

6.12 Thin Client Systems

Thin client systems operate in a client-server network and depend on the central server for processing activities, focusing on conveying user input and output between the thin client terminal and the central server. In contrast, a thick or fat client does as much processing as possible and passes only data for communications and storage to the server.

Many thin client devices run only web browsers or remote desktop software, meaning that all significant processing occurs on the server. However, recent devices marketed as thin clients can run complete operating systems such as Debian Linux, qualifying them as diskless nodes or hybrid clients. Some thin clients are also called "access terminals." Consequently, the term "thin client", in terms of hardware, has come to encompass any device marketed as, or used as, a thin client in the original definition (actual capabilities are much greater). The term is also sometimes used in an even broader sense which includes diskless nodes.

Classified thin client systems require the same physical protection as any other information systems. They need to be configured to meet NISPOM Chapter 8 requirements to the degree possible.

6.13 Virtualization

NISPOM Chapter 8 (Section 3) describes the protection requirements that are common to all IS. For systems that employ virtualization, there may be one or more virtual systems on one or more redundant sets of hardware. Every IS that is capable of technical protection measures must be accredited for use and must meet ODAA standards, to include virtual systems. Each OS used in a virtual environment must be listed within the (M)SSP. The ISSM will document the use and purpose of the virtual machine within the (M)SSP.

6.14 Masking/Coding/Disassociation

Masking, Coding & Disassociation are risky processes that industry sometimes utilizes to conceal or camouflage classified information. If this practice is occurring without user agency knowledge, the contractor must take action to ensure that no classified information has been disclosed, and seek DSS ISSP formal approval. The ISSP will draft an approval letter for RDAA signature and include it in an e-mail to the RDAA with an explanation. If the user agency concurs, but has not given the contractor written acceptance of this practice, along with their agreement to accept the risk, they must do so. It is acceptable for a subcontractor to have a copy of the letter from the user agency to the prime contractor for the contract.

Disassociation and coding have been used in the traveling wave tube industry. This has been carried over to the information systems industry, especially in testing environments, and is sometimes referred to as masking. By using disassociation procedures, classified information pertaining to the frequency range, bandwidth, etc., is encoded or camouflaged to conceal the association between commercial items and items procured for defense application.

Masking, Coding, & Disassociation are no substitution for secure procedures when processing classified information. These methods will not be used to replace security procedures for visual control of test equipment that have capabilities to retain and display classified information.

When Masking or Blanking is used to camouflage information, the display of the test equipment is usually blanked out or masked out with unrelated data displayed. In order to ensure that the data is not recallable for display once blanked or masked, user must follow the test equipment manufacture procedure for disabling data display and its recall function. In the case of multiple recall capabilities, overwrite the display data with random settings or save the resettled values to multiple memory location. Any saved displayed data is considered classified. Sanitization procedures from the manufacture and NISPOM procedure must be followed if the test equipment is to be declassified for calibration or unclassified work. Note that putting a physical cover over the display is not masking and does not release the user from physical security during classified processing.

Coding is a method of disassociation so that information can be used without disclosing the actual value. A set of representative values is given in the classified document with associated classified values (e.g., F0 = 500MHz or P0 = 200mW). The contractor should do the testing with actual classified values; however, the display on the test equipment would display only the code value F0, for example. Blanking occurs where the actual classified value (or frequency) is entered into test source equipment (most likely a signal generator) and its display blanked, the test of the component in classified mode is tested and results displayed on an analyzer with the coded values shown or plotted on a printer. Using this method does not allow the contractor to have uncleared personnel to perform testing. The inherent issues are that the values being used may be reverse engineered if the ranges of values are deduced from the components being built. Other issues may include derived compilation of multiple unclassified tests which resulted in classified information. For example, a shipping document that included a test range specification with a set of values with a set of test results of coded values. In other instances where visual control cannot be maintained the contractor is required to assert some temporary visual control in conjunction with disassociation.

7.0 Variances

The following sections are elements of an SSP or "variances" that have deviated from standard security practices and were allowed by DSS in the past.

Applicability of Login Authentication (NISPOM 8-303(c))

In some cases, it may not be possible to use IS security controls as logon authenticators. DSS encourages IS logon authenticators to be employed to the maximum extent possible as a common IS security control standard and practice. GCA concurrence is required any time technical logon and authentication controls are not utilized.

In cases where IS logon authenticator controls cannot be implemented, physical security controls and personnel security controls may suffice. An acceptable personnel security control is an area access control list or an equipment authorization list. This type of authentication in conjunction with user identification (e.g., picture identification) for standalone workstations or a small LAN can provide alternate means for controlling authentication and access to an IS. An example of an IS that would fall into this category would be a contract deliverable that consists of a suite of systems that would be at a facility for approximately six months for possible upgrades then shipped out to the government customer. There would be no long-term users involved; therefore, user/access lists would be appropriate in this case as long as appropriate physical controls are in place and validated to verify physical access to the information systems is not compromised. However, these exceptions or deviations from preferred methods of authentication and access controls do not relieve the contractor from the requirement for auditing. DSS NISPOM and/or OSD policy requires that systems that are capable of automatically creating and maintaining an audit trail or record must do so even if the contractor chooses to not have automated I&A. The automated audit trails must still be enabled.

Marking Hard Drives

When hard drives are affixed to the internal chassis of a desktop computer, the external housing for the system should be properly marked. It is not necessary to remove the drive for the purpose of marking only. When a drive is removed from a classified system, the drive is required to be marked appropriately in accordance with the NISPOM.

Audit Variances for Holiday Shutdowns

On occasions when a facility plans to stop all work for an extended period of time such as holiday shutdowns an auditing variance may be requested from DSS. The variance will require that physical security measures are identified that will preclude user access to accredited information systems during the shutdown period. Examples of acceptable physical security measures include the closed areas being locked and checked regularly, roving security guards, alarms, etc. The facility should request the variance several weeks in advance. The request should describe physical security measures planned. The request should be routed through the IS Rep and ISSP to RDAA.

Deviations from Automated Auditing

NISPOM 8-602(a)(3) requires audit trail analysis on at least a weekly basis. This does not necessarily mean that the hard drives need to be pulled from a safe to inspect the security logs. The use of seals and supplemental logs such as a safe log can be used to supplant the typical security logs for review. These procedures must be documented in the accredited (M)SSP.

For systems that are used infrequently throughout a typical year (once every month or two), the ISSM may include a variance/special procedure in the profile when submitting for accreditation. The special procedure will specify how the drive is secured and how the ISSM will know if it has been used. Weekly audit trail analysis will include a check of the safe log, seal on anti-stat bag, etc.

If the SSP/IS profile submitted for accreditation indicates only that the system's audit trails are analyzed weekly (i.e., there is no special procedure/variance in the plan), the ISSM is required to do the audit trail analysis weekly as stated in the accredited SSP.

If a system has not been used in 90 days or longer, the ISSM should consider disestablishing the system and then re-establish it when needed.

Legacy (non-compliant) Operating Systems

Legacy operating systems are those systems that are no longer receiving support from the vendor. ODAA approves legacy operating systems on a case-by-case basis with the understanding that they will be updated to compliant operating systems within a three year review cycle, that should be annotated in a POA&M. In those cases where a legacy system cannot be upgraded due to incompatibilities with program requirements, or the manufacturing process, ODAA will make allowances if the GCA determines the legacy operating system is required.

A mature program or old manufacturing process should not require approval of additional legacy systems. Any growth in the program should be accomplished by use of compliant operating systems. An ISSM may be allowed to install replacement legacy systems. Self-certification will not be granted under an MSSP to allow creation of new legacy (non-compliant) systems.

The government customer must provide a letter signed by the Contracting Officer, the Contracting Officer's Representative, the Contracting Officer's Technical Representative, or the Government Program Manager stating that there is a contractual requirement to operate the system in its current configuration. The system cannot be used for classified processing until approval is granted by the CSA. The signed customer letter is provided along with the system documentation when requesting accreditation. These systems will operate under a separate plan that is specific to each system.

The customer letter must identify the following information:

- System UID
- Operating System
- Operating environment
- NISPOM requirement(s) that cannot be met and how the requirement is mitigated

Once approved, the signed customer letter must be retained as an attachment in the IS profile as security relevant documentation for the specific system.

Reminder

IS profiles for legacy systems should be grouped into one SSP, but it will not provide for self-certification which is allowed for in a MSSP. The format would be the same as covered above for MSSPs.

Unified Networks can use a standard SSP format

Initial accreditation	A unified network applies when all DAAs concur that there will be a single security policy for the entire WAN. For WANs where all the nodes are accredited by DSS, there is only one security policy. For those unified WANs, the RDAA of the host network will accredit the network. If self-certification is not required, the network can have an SSP for a unified network that outlines all the requirements contained in NISPOM paragraph 8-610. The ODAA Reviewers will review the SSP for unified networks like any other SSP.

The following procedures apply to Unified Networks:

- The host contractor will prepare an SSP for a unified network and include specific information for each node on the network. This may mean the nodes are identical systems where one hardware list is appropriate. The nodes may have different equipment; thus a system profile for each node may be appropriate. Because there is one security plan, and each node is described in it, a separate Network SSP or Network Security Profile is not required. Additionally, the SSP for a unified network must include a provision that the host must be notified before any changes are made to the system
- The host contractor will provide the SSP for a unified network to the ODAA for review and approval
- The ODAA will review the plan and provide the accreditation action as described in the C&A procedures
- The ISSP will perform an onsite validation of the host system
- The ISSP for each connecting node will take the provided documentation and perform an onsite validation that the system is as described in the documentation and that all features as outlined in the plan are compliant and fully functional. This should be accomplished within 60 days
- Following onsite validations for the host and all connecting nodes, the ODAA will issue a final accreditation letters. An IATO will not be granted for unified networks

Reaccreditation Procedures for reaccreditation are similar to accreditation procedures.

During the security review, the ISSP will determine if changes were made to the WAN that require reaccreditation.

DSS will not approve unified networks where another government agency has control of the contractor computer systems located within contractor facilities. Unified networks with other government agencies must clearly define the demarcation point in the MOA.

8.0 Enhanced Controls

Enhanced controls are those controls that exceed NISPOM requirements. Situations that require enhanced controls are based on contractual requirements, requirements by a GCA sponsored circuit connection (SIPRNet, SDREN, DISN-LES, etc.), or an endorsement by management. The ISSP will evaluate, certify, and assess all IS technical features and safeguards, as documented in the (M)SSP, at contractor facilities in accordance with the NISPOM and its baseline technical security guidance. All enhanced controls will be noted within the (M)SSP and/or the IS Profile. Once an IS is accredited, any changes to reflect enhanced controls will be evaluated by the ISSM as reaccreditation may be necessary due to a possible security relevant change.

9.0 Systems/Networks with Enhanced Controls or Processes

9.1 SIPRNet

9.1.1 SIPRNet Systems

DSS and DISA have agreed on a MOA that defines their roles, responsibilities, and relationships for contractor classified information systems connecting to the Secret Internet Protocol Router Network (SIPRNet). As a result of the MOA, NISP contractors with DoD CIO approval to connect to the SIPRNet are required to implement enhanced security measures beyond the NISPOM. Failure to implement the enhanced security measures may add an additional level of risk deemed unacceptable by the DAA. This results in disconnection of the network by a withdrawal or termination of an accreditation.

Examples of required enhanced security controls/procedures include:

- DSS Communication Tasking Order (CTO) 10-133 Data Transfer Procedures, CTO 08-008a – DoD SIPRNet Warning Banner, CTO 08-005 – Scanning, CTO 09-002 – Disable Auto Run or other applicable TASKORDs
- Host Based Security System (HBSS)
- Vulnerability Management System (VMS)
- Application of applicable Security Technical Implementation Guides (STIGs) (e.g., Network Infrastructure, operating system STIGs or others as required). The (M) SSP IS hardware and software baselines will dictate which STIGs are applicable
- Ensure alignment with an accredited Computer Network Defense Service Provider (CNDSP). A MOU/A or security contract/agreement between the sponsor and CNDS provider is also required per DoD CIO
- SIPRNet PKI tokens
- Obtain account on DISA SIPRNet Global Information Grid (GIG) Interconnection Approval Process System (SGS)
- Register circuit information and submit packages to DISA CAO

NISP contractors will coordinate with the sponsor of the SIPRNet connection to obtain guidance, procedures and any related IA tools for implementing the enhanced controls (e.g., STIGs, Vulnerability Scanning/Retina, VMS and HBSS). The enhanced security controls will be implemented prior to requesting certification and accreditation from DSS and fully documented in the (M) SSP.

9.1.2 Command Cyber Readiness Inspections

In accordance with CJCSI 6211.02D any IS connected to the SIPRNet is subject to an annual Command Cyber Readiness Inspection (CCRI). The CCRI teams evaluate enclave and network security, perform network-based vulnerability scans, and assess compliance with applicable policies. Failure to comply with the inspection process or failure to receive a passing score may prompt disconnection of the contractor sponsored DISN SIPRNet connection and require a subsequent re-inspection to ensure compliance. The CCRIs are typically scheduled in advance and notifications are sent from DISA FSO to circuit sponsors approximately 120 days prior to an inspection. However, CYBERCOM can conduct CCRIs on short notice at their discretion. In preparation for a CYBERCOM scheduled compliance inspection it is recommended that sponsors and their contractors conduct pre-CCRI assessments well in advance. Sponsors are advised to check with their aligned CNDSP for possible pre-CCRI support.

9.1.3 NISP SIPRNet Circuit Acquisition Process

The NISP SIPRNet Circuit Acquisition Process (NSCAP), formerly called DSS SCAP was developed to provide a step-by-step guidance for cleared contractors and their sponsors to ensure a successful connection to the SIPRNet. The document describes the roles and responsibilities for sponsors, cleared contractors, DISA and DSS. The NSCAP also provides a process flow chart, helpful links, contact information as well as required accreditation documentation to be submitted to ODAA and DISA Classified Connection Approval Office (CAO).

To obtain the latest version of the NSCAP visit http://www.dss.mil/isp/odaa/request.html#sip.

The following table outlines the Non-DoD SIPRNet Checklist:

As part of the ODAA submission include the following documentation	▪ Non-DoD DISN Connection Validation (or revalidation) letter endorsed by government sponsor, DISA SIPRNet Management Office, and the Service/Agency validation official ▪ DoD CIO connection approval letter ▪ Completed SIPRNet Connection Questionnaire (SCQ) for RDAA signature ▪ Consent To Monitor (CTM) memorandum with government's sponsor signature ▪ Statement of Residual Risk (SRR) with contractor signature ▪ Evaluated Assurance Level (EAL) certificates validating at least current EAL-4 firewall and EAL-2 IDS (http://www.niap-ccevs.org/vpl) ▪ Copy of MOU/A or contract signed by Computer Network Defense Service Provider (CNDSP) and sponsor (the MOU/A must be funded/resourced) ▪ Risk Acceptance Letter(s) (if applicable) ▪ Unclassified Plan of Action & Milestone(s) (if applicable)
Per DSS DISA MOA and CJCSI 6211.02D, ensure compliance with enhanced security controls (applicable DoD controls or equivalent) required for connection to the Defense Information Systems Network (DISN) SIPRNet	▪ DoD Warning Banner – (See section 5.3.1.3 of ODAA PM) ▪ Utilization of applicable Secure Technical Implementation Guides (STIG) (Network Infrastructure, HBSS, Operating System, Traditional) ▪ Request and obtain a Vulnerability Management System (VMS) account ▪ Ensure Host Based Security System (HBSS) is aligned per DISA provided guidance below and FRAGO 13 ▪ Compliance with DSS CTO 10-333 guidance ▪ Maintain compliance with any applicable CYBERCOM directives to include but not limited to the following: CTO 08-005, CTO 09-002, CTO 08-008a, CTO 10-133, and FRAGO 13

Below are helpful links to Resources, Training, and Support:

Topic	Links
Resources	▪ http://iase.disa.mil/stigs/stig_viewing_guidance.html (STIG Viewer) ▪ http://iase.disa.mil/stigs/gold_disk/index.html (NIPR): Due to PKI requirement, may require sponsor assistance to provide certain STIGs ▪ https://vms.disa.smil.mil (SIPR): requires appropriately filled out dd2875 ▪ VMS Help Desk Phone number: (405)739-5600 // 1-800-490-1643 or email: disa.tinker.esd.mbx.okc-service-desk@mail.mil . ▪ http://iase.disa.smil.mil (SIPR): training, STIGs, and other checklists ▪ https://www.cybercom.smil.mil (SIPR): Contains CYBERCOM orders/directives ▪ https://patches.csd.disa.smil.mil/default.aspx (SIPR): DOD patch server where Microsoft, and other vendor patches can be accessed ▪ https://giap.disa.smil.mil/ (SIPR) DISA SGS ▪ http://www.disa.mil/Services/Network-Services/DISN-Connection-Process/Getting-Started/SIPRNet/SIPRNet-NonDod-New (NIPR): connection process tool ▪ DISA Approved Products List (APL) - https://aplits.disa.mil/processAPList.do (PKI)
DISA FSO Training Opportunities:	▪ Online training: http://iase.disa.mil/eta/online-catalog.html ▪ Classroom training (may require sponsors assistance for attendance) https://powhatan.iiie.disa.mil/classroom_training/index.html (*PKI) ▪ VMS online training: https://vmscbt.disa.mil/curriculum/1.html
HBSS Support for Contractors	▪ https://www.intelink.gov/wiki/HBSS

The DoD/DISA HBSS license and vendor support covers cleared defense contractors for SIPRNet only. It is the responsibility of the sponsoring authority, as the owner of the DoD information contained within a CDC system, to align the computer network defense posture within the sponsor's existing enterprise CND architecture. CDCs in need of HBSS coverage should direct questions about deploying and operating HBSS to the sponsoring authority.

SIPRNet PKI Token Implementation

Contractors should contact the sponsoring organization to obtain a SIPRNet token. The sponsor is required to fill out form DD2842 and submit it to a registration authority for their organization. The contact information for the major CC/S/A's can be found on the Contact Us portion of DISA's website at http://iase.disa.mil/pki-pke/contact.html.

9.2 Defense Industrial Base Cyber Security Accreditation Process (DIBNet)

Several additional items are referenced throughout this section and are received by the participating contractor upon acceptance into the DIB CS/IA program through a program framework agreement:

- Users Guide to Configure and Process IS
- DIB CS/IA Reporting-System-C&A-Handbook-8-2009.pdf

By following the procedures outlined below, the cleared defense contractor (CDC) will increase the possibility of acquiring accreditation for the Defense Industrial Base Cyber Security Accreditation Process (DIBNet) information systems (IS) in a timely manner.

1. Configure the computer in accordance with requirements of the DD-254, framework agreement and DIB CS/IA program office, gain accreditation; and forward the accreditation to the DIBNet-S WAN program office.
2. Complete the appropriate SSP and IS profile documentation. The ISSM will need to ensure the plan accurately reflects the protective measures for the IS within a specific environment. Do not forget to sign the certification statement. The IS Rep and/or ISSP will serve as points of contact for any help you require during this process. The security plan and DD-254 to support justification should be submitted after the encryption card/NSA Type-1 device has been received. By submitting the package, you are triggering the mechanism that allows ODAA to schedule the onsite validation upon after completing a successful review of the SSP. Submitting the accreditation package without all the required components in place will result in rescheduling the system validation and may cause delays in the connection process. "DIB" should be included on the subject line for all DIB CS/IA system e-mail submissions. Please refer to the Systems Security Plan Submission Process, Table 14.1.14 Subject Line Requirements for Plan Submissions.
3. The ISSM will need to forward the ATO to the DIBNet-S WAN program office to gain approval for the new node to connect.

In addition to the standard configuration, the following additional configurations are needed to address the persistent malware threats identified with the use of USB thumb drives and the connection to sensitive data. The use of USB storage devices will be disabled for the system.

The following section describes two methods that can be used to prevent users from connecting to a USB storage device.

USB Storage Device Is Not Already Installed on the Computer	USB Storage Device Is Already Installed on the Computer
If a USB storage device is not already installed on the computer, assign the user or the group Deny permissions to the following files: ▪ %SystemRoot%\Inf\Usbstor.pnf ▪ %SystemRoot%\Inf\Usbstor.inf **When you do so, users cannot install a USB storage device on the computer. To assign a user or group Deny permissions to the Usbstor.pnf and Usbstor.inf files, follow these steps:** 1. Start Windows Explorer, and then locate the %SystemRoot%\Inf folder 2. Right-click the Usbstor.pnf file, and then click Properties 3. Click the Security tab 4. In the Group or user names list, click the user or group that you want to set Deny permissions for 5. In the Permissions for UserName or GroupName list, click to select the Deny check box next to Full Control, and then click OK. Note In addition, add the System account to the Deny list 6. Right-click the Usbstor.inf file, and then click Properties 7. Click the Security tab 8. In the Group or user names list, click the user or group that you want to set Deny permissions for 9. In the Permissions for UserName or GroupName list, click to select the Deny check box next to Full Control, and then click OK	**Warning** – Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall your operating system. **If a USB storage device is already installed on the computer, set the Start value in the following registry key to 4:** ▪ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor **When you do so, the USB storage device does not work when the user connects the device to the computer. To set the Start value, follow these steps:** 1. Click Start, and then click Run 2. In the Open box, type regedit, and then click OK 3. Locate, and then click the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor 4. In the right pane, double-click Start 5. In the Value data box, type 4, click Hexadecimal (if it is not already selected), and then click OK 6. Quit Registry Editor

9.3 International Systems Security Plans

In certain instances, contractors may elect to transmit and receive classified data to a foreign customer via voice, fax, secure communications link or network. These situations are unique as a system accreditation package is only one part of the documentation required for the systems approval to communicate with the foreign system. Systems that connect to a foreign system must have an approved Security Communication Plan (SCP). If the SCP is not approved within a Program Security Instruction or another document, the International SSP can double as the SCP and will be forwarded to the appropriate International stakeholders for concurrence before DSS can accredit the system. Please include export authorization with all submissions.

Certification and Accreditation Package

All SSPs must be submitted to the ODAA Headquarters for review and approval. The SSP may receive an accreditation to process Foreign Government Information (FGI) as a standalone until the SCP is approved. Once the SCP is approved the SSP must be submitted for reaccreditation as an International WAN because of the security relevant change.

Secure Communications Plan

Background

Requests to establish international secure communications links between U.S. cleared contractors and foreign governments or foreign cleared defense contractors can originate from one of three sources.

These sources are:

- The U.S. cleared facility
- The foreign government
- A U.S. program office managing a multinational development or production program such as the Joint Strike Fighter

ODAA

When ODAA receives all the necessary documentation from the field, NSA and OSD, they will forward the information to the field office. The field office will then notify the contractor that all of the approvals have been received and prompt the contractor to submit their SSP (whether it is under an IATO or an ATO) for reaccreditation as an International WAN as a security relevant change. Once the ODAA receives this request they will issue a new accreditation letter giving the contractor the authority to initiate the international connection. The accreditation letter should specify the entities that are approved to connect and that the international connection is authorized. The ODAA will then notify the DSS International Policy Office that it should advise the foreign government in writing that the link has been accredited by the United States. The ODAA will then store the approved SCP and the approval documentation.

10.0 NIST 800-53 Control Mapping

NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations was released on April 30, 2013* and is a comprehensive list of recommended security controls and control enhancements to address the risk of threat on DoD Information Systems processing classified information. The security and privacy controls are meant to provide a level of security necessary to preventing the advance persistent threat (e.g., mobile computing, insider threat and cyber-attacks).

Below is a general overview of the family names in which the controls fall under.

SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Refer to http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf for a more comprehensive list of the entire catalog of security controls.

11.0 Reference

DoD 5220.22-M National Industrial Security Program Operating Manual (2006). Washington DC: Department of Defense.

12.0 Acronyms List

ACL	Access Control List
AI	Administrative Inquiry
ATC	Approval to Connect
ATO	Approval to Operate
CI	Counterintelligence
C&A	Certification and Accreditation
CAC	Common Access Card
CAGE	Commercial And Government Entity
CAN	Campus Area Network
CCRI	Command Cyber Readiness Inspection
CM	Configuration Management
CNA	Computer Network Attack
CND	Computer Network Defense
CNDSP	Computer Network Defense Service Provider
COR	Contracting Officer Representative
CSA	Cognizant Security Authority
CTO	Communication Tasking Orders
CYBERCOM	U.S. Cyber Command
DAA	Designated Approving Authority
DCO	Device Configuration Overlay
DIB CS/IA	Defense Industrial Base Cyber Security / Information Assurance
DIBNET-S	Defense Industrial Base Network - Secret
DISN - LES	Defense Information System Network - Leading Edge Services
DSS	Defense Security Service
EPL	Evaluated Product Listing
FCL	Facility (Security) Clearance
FGI	Foreign Government Information
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOC	Field Office Chief
FRAGO	Fragmentary Orders
FSO	Facility Security Officer
GCA	Government Contracting Authority
GFE	Government Furnished Equipment
GIG	Global Information Grid
HAG	High Assurance Guard
HBSS	Host Based Security System
HDD	Hard Disk Drive
HPA	Host Protected Area
I&A	Identification and Authentication
IA	Information Assurance
IATO	Interim Approval to Operate
IAW	In Accordance With
IDS	Intrusion Detection System
IP	Internet Protocol
IS	Information Systems
ISA	Interconnection Security Agreement
ISSM	Information Systems Security Manager

ISSO	Information Systems Security Officer
ISSP	Information Systems Security Professional
LAN	Local Area Network
MAN	Metropolitan Area Network
MFO	Multiple Facility Organization
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MSSP	Master Systems Security Plan
MUSA	Multiple User Stand-Alone
NATO	North Atlantic Treaty Program
NISP	National Industrial Security Program
NIST	National Institute of Standards and Technology
NSP	Network Security Plan
NSCAP	NISP SIPRNet Circuit Acquisition Process
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
ODAA	Office of the Designated Approving Authority
ODM	Operational Directive Messages
OGC	DSS Office of the General Council
PAN	Personal Area Network
PDF	Portable Document Format
PDS	Protected Distribution System
PKI	Public-Key Infrastructure
PL	Protection Level
POA&M	Plan of Action and Milestones
POC	Point of Contact
RAL	Risk Acceptance Letter
RD	Regional Director
RDAA	Regional Designated Approval Authority
RFID	Radio Frequency ID
SA	System Administrator
SAR	Situational Awareness Reports
SCQ	SIPRNet Connection Questionnaire
SDREN	Secure Defense Research and Engineering Network
SGS	SIPRNet Global Information Grid (GIG) Interconnection Approval Process System
SIPRNET	Secret Internet Router Protocol Network
SSP	Systems Security Plan
STE	Secure Terminal Equipment
STIG	Security Technical Implementation Guide
SUSA	Single User Stand-Alone
S-WLAN	Secure Wireless Local Area Networks
TEMPEST	Transient Electromagnetic Pulse Emanation Standard
UL	Underwriters Laboratories
USB	Universal Serial Bus
VAL	Visit Authorization Letter
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
VTC	Video Teleconference
WAN	Wide Area Network
WARNORD	Warning Orders

13.0 Glossary

Accreditation	Formal declaration by the DAA that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Accreditation Boundary	The delineation of all systems which are accredited under a specified security plan. The accreditation boundary can be disguised from separately accredited information resources that are interconnected or with which information is exchanged
Approval to Connect	Formal approval granted by a WAN DAA allowing the connection of a node to a WAN.
Approval to Operate	Approval granted by a DAA for an IS to process classified information.
Assurance	Measure of confidence that the security features, practices, procedures and architecture of an IT system accurately mediates and enforces the security policy.
Automated Information Systems	An assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information and textual material.
Automated Information Systems Security	All security safeguards needed to provide an acceptable level of protection for Automated Information Systems and the classified data processed.
Certification	Comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements.
Classified Contract	Any contract that requires or will require access to classified information by a contractor or his or her employees in the performance of the contract. (A contract may be a classified contract even though the contract document is not classified.) The requirements prescribed for a “classified contract” also are applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other GCA program or project which requires access to classified information by a contractor.
Classified Information	Official information that has been determined, pursuant to Executive Order 12958 or any predecessor order, to require protection against unauthorized disclosure in the interest of national security and which has been so designated. The term includes National Security Information (NSI), Restricted Data (RD), and Formerly Restricted Data (FRD).
Coercivity	Coercivity, also called the coercive field or coercive force, of a ferromagnetic material is the intensity of the applied magnetic field required to reduce the magnetization of that material to zero after the magnetization of the sample has been driven to saturation.
Cognizant Security Agency	The office or offices delegated by the Head of a CSA to administer industrial security in a contractor's facility on behalf of the CSA.
Command Cyber Readiness Inspection	A review of an IS connected to the SIPRNet to evaluate enclave and network security, perform network-based vulnerability scans, and assess compliance with applicable policies.
Commercial and Government Entity	Standardized method of identifying a given facility at a specific location.
Common Access Card	Standard ID card for active duty members of the Uniformed Services, Selected Reserve, DoD civilian employees, and eligible contractor personnel.
Company	A generic and comprehensive term which may include sole proprietorships, individuals, partnerships, corporations, societies, associations, and organizations usually established and operating to commonly prosecute a commercial, industrial or other legitimate business, enterprise, or undertaking.
Computer Network Attack	Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Computer Network Defense	Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.
Confidential	This designation will be applied to information or material the unauthorized disclosure of which could be reasonably expected to damage national security.
Contracting Officer Representative	Individual who is designated and authorized in writing by the contracting officer to perform specific technical or administrative functions on contracts or orders.
Contractor	Any industrial, educational, commercial, or other entity that has been granted an FCL by a CSA.
Denial	When a Systems Security plan has been accepted and reviewed by an ISSP and is not granted an Interim Approval to Operation (IATO) due to errors/omissions.
Defense Industrial Base Cyber Security / Information Assurance	DoD program open to industry partners for reporting intrusion attempts to their unclassified systems. (DIB CS/IA)
Defense Industrial Base Network - Secret	Network that hosts the connection enable the DIB CS/IA program reporting.
Defense Security Service	Supports national security and the warfighter, secures the nation's technological base, and oversees the protection of US and foreign classified information in the hands of industry
Department of Defense	The Office of the Secretary of Defense (OSD) (including all boards, councils, staffs, and commands), DoD agencies, and the Departments of Army, Navy, and Air Force (including all of their activities).
Designated Approving Authority	Official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk.
Document	Any recorded information, regardless of its physical form or characteristics, including, without limitation, written or printed matter, tapes, charts, maps, paintings, drawing, engravings, sketches, working notes and papers; reproductions of such things by any means or process; and sound, voice, magnetic, or electronic recordings in any form.
Environment	Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an IT system.
Executive Order 12829	The NISP was established by Executive Order 12829, 6 January 1993, "National Industrial Security Program" for the protection of information classified pursuant to Executive Order 12356, April 2, 1982, "National Security Information," or its successor or predecessor orders and the Atomic Energy Act of 1954, as amended.
Facility	A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined herein.) For purposes of industrial security, the term does not include Government installations.
Facility (Security) Clearance	An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).
Federal Information Processing Standard	Set of standards that describe document processing, encryption algorithms and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies.
Federal Information Security Management Act	US legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats.
Field Office Chief	Responsible for managing the DSS Mission across an assigned are of responsibility. IS Reps report to the Field Office Chief.
Formal Access Approval	Formal Access Approval is the documented approval by a data owner to allow access to a particular category of information. It can be linked to any caveated information such as compartmented, NATO, REL TO, Critical Nuclear Weapon Design Information, COMSEC or Crypto variable information, FRD, etc.
Government	An element of an agency designated by the agency head and delegated broad

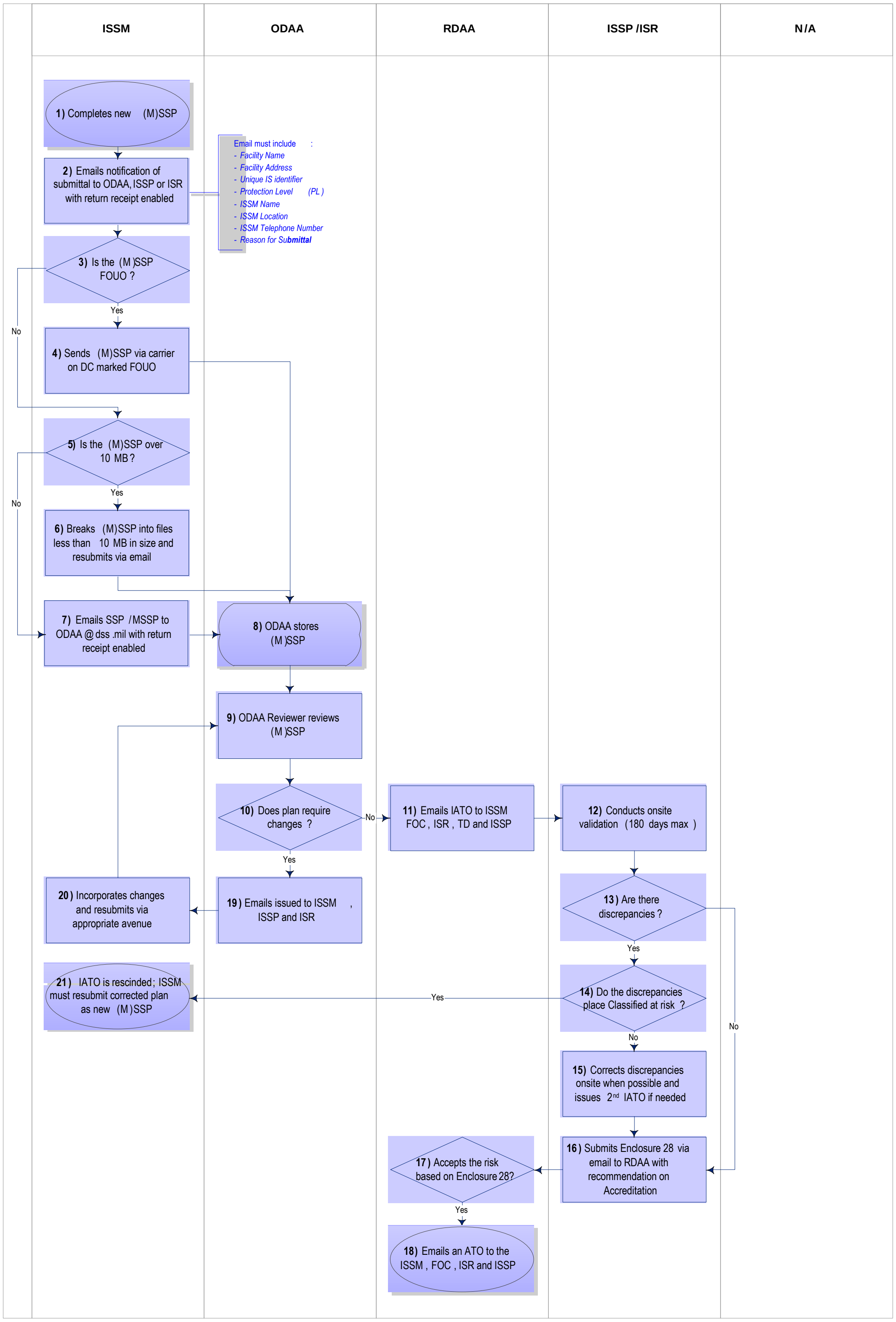
Contracting Activity	authority regarding acquisition functions.
Government Furnished Equipment	Property that is acquired directly by the government and then made available to the contractor for use
Host	The individual who takes ultimate responsibility for preparation and maintenance of accreditation documentation (NSP) for the WAN. Usually the ISSM for one of the nodes, the Host also determines the requirements that must be met before connection to the WAN is permitted.
Industrial Security	That portion of information security which is concerned with the protection of classified information in the custody of U.S. industry.
Information Assurance	Steps involved in protecting information systems, like computer systems and networks
Information Security	The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by executive order.
Information Systems	Any telecommunication or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of voice or data, and includes software, firmware and hardware.
Information Systems Security Manager	The contractor employee responsible for the implementation of Automated Information Systems security, and operational compliance with the documented security measures and controls, at the contractor facility.
Information Systems Security Officer	The ISSO(s) (NISPOM 8-104) is appointed by the ISSM when the facility has multiple accredited ISs, is in a multiple facility organization in which the ISSM has oversight responsibility for multiple facilities, or when the technical complexity of the facility's IS program warrants the appointment. The name and phone number of the ISSO(s) must be identified in the SSP(s). During an IS certification visit the IS Rep or ISSP will determine what duties and responsibilities have been delegated to the ISSO and verify the ISSO understands them. During a Security Review, the IS Rep or ISSP will review those duties and responsibilities and verify the ISSO is carrying them out.
Information Systems Security Professional	Evaluates, certifies, and inspects all IS technical features and safeguards for all IS within their area of responsibility.
Interconnection Security Agreement	Contract between telecommunication organizations for interconnecting their networks and exchanging telecommunication traffic.
Interim Approval to Connect	Temporary approval granted by a WAN DAA allowing the connection of a node to WAN.
Interim Approval to Operate	Temporary approval granted by a DAA for an IS to process classified information.
Internet Protocol	Connectionless protocol used in packet-switched layer networks, such as Ethernet.
Local Area Network	Computer network within a small geographical area such as a home, school, computer laboratory, office building or group of buildings.
Master Systems Security Plan	The term "Master" indicates the authorization to add IS to an approved plan by an ISSM.
Memorandum of Agreement	The purpose of an MOU/MOA/ISA is to adjudicate the differences in requirements of different DAAs and to establish roles and responsibilities. The terms MOU , MOA and ISA can be used interchangeably.
Memorandum of Understanding	An MOU between DSS and the Government Contracting Authority (GCA) is required for all government to contractor connections to include connections over STU III, STE, and Secure Data Devices.
Multiple Facility Organization	A legal entity (single proprietorship, partnership, association, trust, or corporation) that is composed of two or more facilities.
Multiple User Stand-Alone	Systems that have one user at a time, but have a total of more than one user with no sanitization between users, as Multiuser systems.
National Institute of	Organization that promulgates national level standards, including those designed to

Standards and Technology	protect IS
Network	An IS term meaning a network composed of a communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include ISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices.
Network Security Plan	Document(s) submitted by the WAN owner to the WAN DAA that describes the security features and requirements of the WAN.
Node	Any device or collection of devices accredited under a single Systems Security plan connected to a WAN. Physical Security The measures used to provide physical protection of resources against deliberate and accidental threats.
Office of the Designated Approving Authority	Delegated the responsibility for the DSS mission for cleared contractor IS certification and accreditation oversight.
Plan of Action and Milestones	Facilitates an agreement between the contractor and DSS identifying items from the baseline configuration requirements cannot be met and the reasons. The POA&M documents deficiencies that can be corrected and defines a timeline for resolving the issues.
Protected Distribution System	Secure conduit for protecting classified lines, transmitting data outside of a controlled area.
Protection Level	The protection level of an Information System (IS) is determined by the relationship between two parameters: first, the clearance levels, formal access approvals, and need-to-know of users; and second, the level of concern based on the classification of the data on a particular system. The protection level translates into a set of requirements contained in Chapter 8-402 (tables 4, 5, 6, and 7) of the NISPOM that must be implemented in the resulting system.
Radio Frequency ID	Technologies that use wireless communication between an object (also known as a tag) and an interrogating device (also known as a reader), for the purposes of automatically tracking and identifying of such objects.
Reaccreditation	An action taken by DSS when security relevant changes are made to an approved (M)SSP.
Reevaluation	An action taken by DSS 3 years from the date of the ATO for a (M)SSP.
Regional Designated Approval Authority	Delegated the responsibility for accreditation of cleared contractor classified information systems within their region.
Regional Director	Responsible for all aspects of operations within the region.
Rejection	When a Systems Security plan submission to ODAA is not in accordance with the DSS Process Manual and is not accepted for review.
Risk	A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact.
Risk Acceptance Letter	Letter from the Government Contracting Authority (GCA) accepting the level of risk when an information system cannot be configured to meet requirements of the NISPOM based on customer defined requirements.
Risk Assessment	Process of analyzing threats to, and vulnerabilities of, an IT system, and the potential impact that the loss of information or capabilities of a system would have on national security. The resulting analysis is used as a basis for identifying appropriate and effective measures.
Risk Management	Process concerned with the identification, measurement, control, and minimization of security risks in IT systems to a level commensurate with the value of the assets protected.
SECRET	The designation that will be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

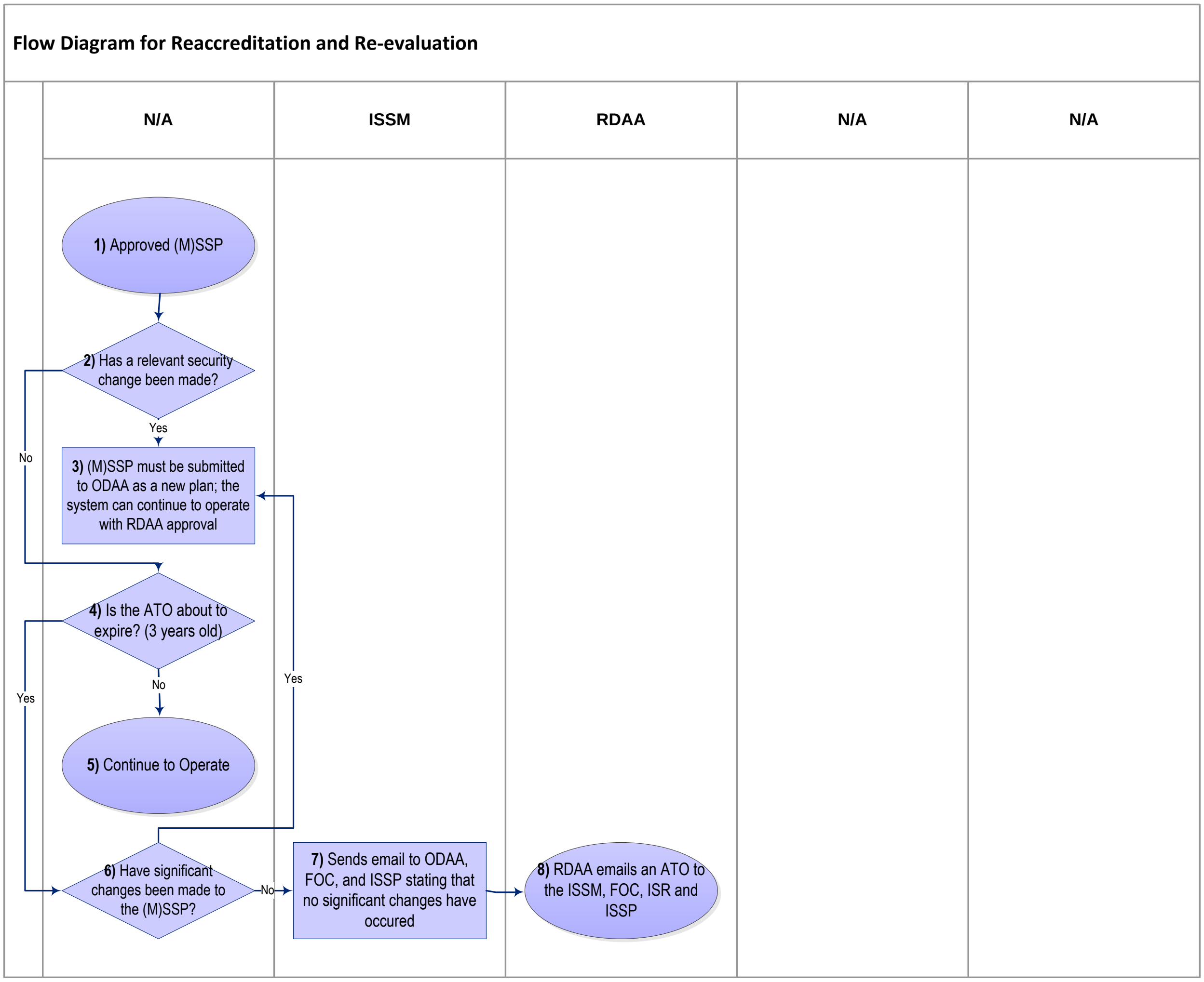
Secret Internet Protocol Router Network	Worldwide SECRET level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry.
Secure Terminal Equipment	Piece of equipment utilized to enable encrypted/secure voice and/or data communication.
Security Cognizance	The Government office assigned the responsibility for acting for CSAs in the discharge of industrial security responsibilities described in the NISPOM.
Security-Relevant Change	A security-relevant change to a system is any change affecting the availability, integrity, authentication, confidentiality, or non-repudiation of an IS or its environment. Examples would include changes to the Identification and Authentication, Auditing, Malicious Code Detection, Sanitization, Operating System, Firewall, Router Tables and Intrusion Detection Systems (IDS) of a system, or any changes to its location or operating environment.
Security Requirement	Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.
Single User Stand-Alone	Systems assigned to single user and are without network connectivity.
Systems Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
TOP SECRET	The designation that will be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
Telecommunications Electronics Material Protected from Emanating Spurious Transmissions	The protection of sensitive information being compromised from electronic equipment producing emanations.
Universal Serial Bus	Common interface that enables communication between devices and a host controller such as a personal computer (PC).
User	Person or process authorized to access an IT system.
User Code	Software that allows a user to modify data or functions of an IS. Determining if an IS has user code may be a matter of degree, but as an example, if an IS only has a button that performs a single function when pressed, the system is considered to have no user code on it. If the user can input classified information and save it to the IS then the IS certainly has user code.
Validation	The process of determining compliance of the evolving IT system specification, design, or code with the security requirements and approach agreed on by the users, acquisition authority, and the DAA.
Video Teleconference	Technology that facilitates the communication and interaction of two or more users through a combination of high-quality audio and video over Internet Protocol (IP) networks.
Virtual Private Network	A private network that is built over a public infrastructure.
Voice Over Internet Protocol	Technology used for delivering different kinds of data from a source to a destination using IP (Internet Protocol).
Wide Area Network	Any two systems interconnected as defined by NISPOM 8-700 c.

14.0 Reference Materials

14.1.1 Flow Diagram: Initial (M)SSP


ISSM
ODAA
RDAA
ISSP /ISR
N/A
1) Completes new (M)SSP
2) Emails notification of submittal to ODAA, ISSP or ISR with return receipt enabled
Email must include :
- Facility Name
- Facility Address
- Unique IS identifier
- Protection Level (PL)
- ISSM Name
- ISSM Location
- ISSM Telephone Number
- Reason for Submittal
3) Is the (M)SSP FOUO ?
Yes
No
4) Sends (M)SSP via carrier on DC marked FOUO
5) Is the (M)SSP over 10 MB?
Yes
No
6) Breaks (M)SSP into files less than 10 MB in size and resubmits via email
7) Emails SSP /MSSP to ODAA@dss.mil with return receipt enabled
8) ODAA stores (M)SSP
9) ODAA Reviewer reviews (M)SSP
10) Does plan require changes ?
No
Yes
11) Emails IATO to ISSM FOC, ISR, TD and ISSP
12) Conducts onsite validation (180 days max)
13) Are there discrepancies ?
Yes
No
19) Emails issued to ISSM , ISSP and ISR
20) Incorporates changes and resubmits via appropriate avenue
14) Do the discrepancies place Classified at risk ?
Yes
No
21) IATO is rescinded; ISSM must resubmit corrected plan as new (M)SSP
15) Corrects discrepancies onsite when possible and issues 2nd IATO if needed
16) Submits Enclosure 28 via email to RDAA with recommendation on Accreditation
17) Accepts the risk based on Enclosure 28?
Yes
18) Emails an ATO to the ISSM, FOC, ISR and ISSP

14.1.2 Flow Diagram: Reaccreditation and Re-evaluation


Flow Diagram for Reaccreditation and Re-evaluation
N/A
ISSM
RDAA
N/A
N/A
1) Approved (M)SSP
2) Has a relevant security change been made?
Yes
No
3) (M)SSP must be submitted to ODAA as a new plan; the system can continue to operate with RDAA approval
4) Is the ATO about to expire? (3 years old)
No
Yes
Yes
5) Continue to Operate
6) Have significant changes been made to the (M)SSP?
No
7) Sends email to ODAA, FOC, and ISSP stating that no significant changes have occured
8) RDAA emails an ATO to the ISSM, FOC, ISR and ISSP

14.1.3 Example ODAA Disestablishment Letter

ABC Company

August 13, 2012

IS Rep Name
Defense Security Service
Capital Field Office
123 Somewhere Road
Alexandria, VA 22314

Subject: Disestablishment of Captial-12345-20080310-00003-00123

IS Rep Name,

Please take the necessary steps to disestablish the Information System (IS) which had been designated as Information System Profile 123 (Capital-12345-20080310-00003-00123) known as ACME. This system is no longer needed to perform classified processing. All IS hardware has been properly sanitized IAW approved procedures. All available records will be kept on file for a period of twelve (12) months or one security assessment cycle.

If you have any questions regarding this matter, please contact me at (212) 555-4567.

Sincerely,
ISSM Name,
Information Systems Security Manager
ABC Company
101 Anywhere Street
Alexandria, VA 22314

CC: Frank Smith, ISSP

14.1.4 Plan of Action and Milestones Template

Defense Security Service
Certification and Accreditation
Plan of Action and Milestones Template (POA&M)

Company Name	CAGE Code	DSS UID	ISSM	ISSM PHONE NUMBER

Item Number	Non-Compliance	C/I*	Mitigation Plans and Adjustments	Milestone Date Based on Risk Level	ISSM/FSO Approval	Status (Open/Closed)	DSS Approval Date and Determination (Open/Close)	Risk Level Low/Medium/ High

C/I – Enter "C" if non-compliance issue was identified during the C&A process. Enter "I" if non-compliance issue was identified during assessment.

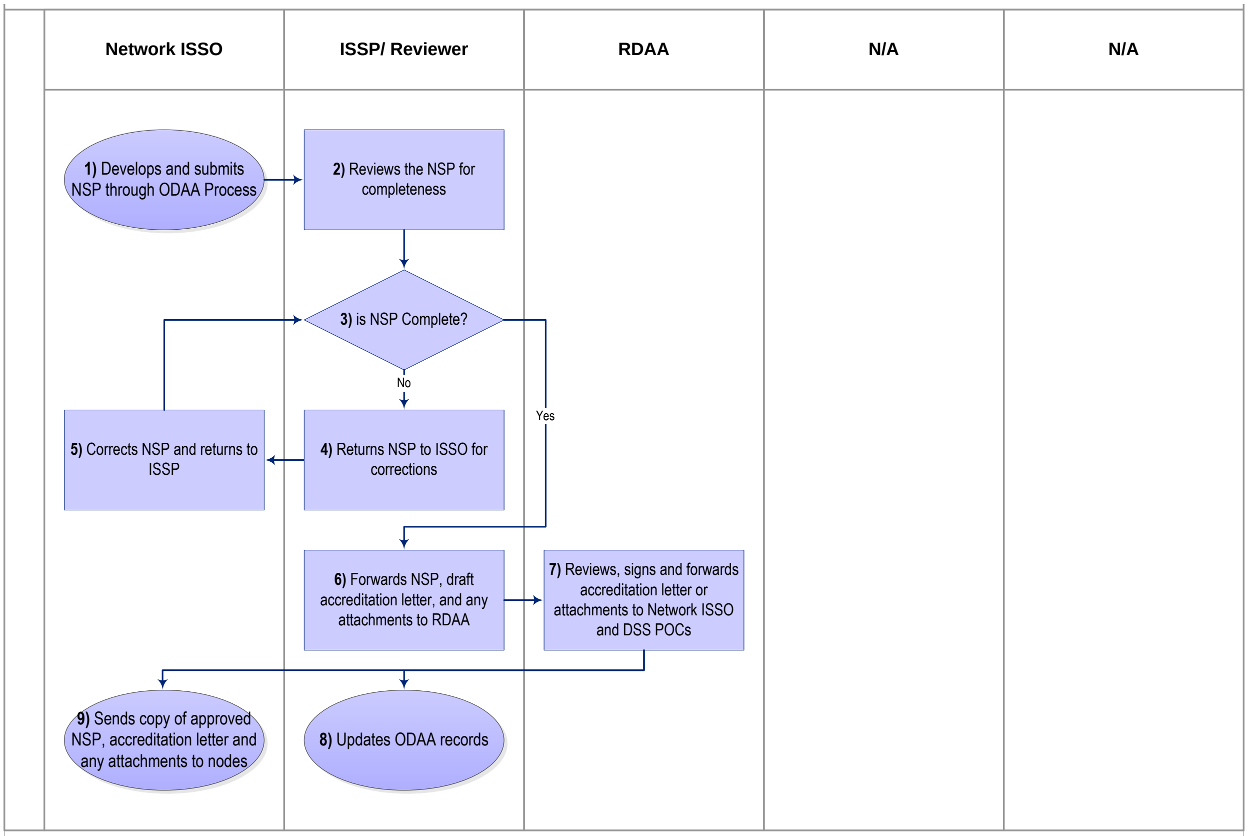
Milestone dates will be determined on a High/Medium/Low scale. High = 90 days, Medium = 180 days, Low = 365 days. The criteria for these elements are listed on the following page.

Plan of Action and Milestones Template (POA&M) Guidance

- The POA&M applies to initial (M)SSP submissions, as well as existing accredited systems that require accreditation under the new DSS Configuration Baseline.
- Milestone dates will be determined on a High/Medium/Low scale. High = 90 days, Medium = 180 days, Low = 365 days. Risk level settings will be vetted against each configuration setting and the NIST risk-factor (action item).
  - High Impact Code. The absence or incorrect implementation of the IA control may have a severe or catastrophic effect on system operations, management, or information sharing. Exploitation of the weakness may result in the destruction of information resources and/or the complete loss of mission capability. High impact codes will be assessed on a case-by-case basis. If approved, system must be compliant within 90 days.
  - Medium Impact Code. The absence or incorrect implementation of the IA control may have a serious adverse effect on system operations, management, or information sharing. Exploitation of the weakness may result in loss of information resources and/or the significant degradation of mission capability. Must be compliant within 180 days.
  - Low Impact Code. The absence or incorrect implementation of the IA control may have a limited adverse effect on system operations, management, or information sharing. Exploitation of the weakness may result in temporary loss of information resources and/or limit the effectiveness of mission capability. Must be compliant within 365 days.
- Items under Status are considered closed when validated by DSS.
- Self-certified systems – All new systems will require a new master and are required to be compliant with the new settings. To add a new workstation to an existing system by self-certification, it must be configured IAW the enhanced requirements. They may either update the entire IS at that time, or this may push them into a POA&M whereby they plan migration of the entire IS to the new settings.

- GCA must approve non-compliant settings due to program compatibility or contract requirements. Non-compliance with baseline configuration settings resulting from operating system limitations or capabilities will not require GCA approval.
- Documentation must reflect which items cannot be met, as well as why it cannot be met.
- All non-compliant issues that come up during an assessment that are not corrected on the spot must be put in the POA&M. This will ensure a formal date for resolution which can be tracked through completion.

14.1.5 NSP Accreditation Process Diagram


Network ISSO
ISSP/ Reviewer
RDAA
N/A
N/A
1) Develops and submits NSP through ODAA Process
2) Reviews the NSP for completeness
3) is NSP Complete?
No
Yes
4) Returns NSP to ISSO for corrections
5) Corrects NSP and returns to ISSP
6) Forwards NSP, draft accreditation letter, and any attachments to RDAA
7) Reviews, signs and forwards accreditation letter or attachments to Network ISSO and DSS POCs
8) Updates ODAA records
9) Sends copy of approved NSP, accreditation letter and any attachments to nodes

*To obtain approval for a new node to connect to an already approved NSP, the Network ISSO updates and submits the NSP through the ODAA process in the same manner shown

14.1.6 Overall Network Security Profile

Overall Network Security Profile (To be completed by host activity)		Network Identifier:	Network Host Facility:
Date:	Revision #:	Facility Address:	CAGE Code:

Protection, Sensitivity Level, and User Information

Network Protection Level: □ PL1 □ PL2 □ PL3 □ PL4
Highest classification level of data:
□ CONFIDENTIAL □ SECRET □ TOP SECRET
Category(s): □ NONE □ COMSEC* □ RD* □ FRD* □ FGI*
□ Other, Specify:
Formal access approvals: No Yes.
If yes, indicate □ NATO** □ CNWDI* □ CRYPTO*

Minimum clearance level of user:
□ CONFIDENTIAL
□ Interim SECRET
□ SECRET
□ Interim TOP SECRET
□ TOP SECRET

Need-to-Know Methodology for Network

Check all that apply
□ Router IP Filters
□ Configuration disks for NES with accounts on each machine.
□ Other: Specify:

Periods Processing: If used, IS Upgrade/Downgrade procedures shall include steps to ensure network configurations are appropriately changed between processing sessions.
□ Entire network utilizes periods processing
□ Individual nodes as indicated in their Network Security Profile utilize periods processing while the network host does not.

Network ISSO Responsibilities

1. Focal point for the network and the connecting node Information Systems Security Managers (ISSMs) to include collecting and distributing Network Security Profiles for all nodes.
2. Generate and maintain approvals for the Network Security Profile, and if applicable, MOUs.
3. Perform and oversee weekly reviews of the network in order to determine that only connections that are accredited and exhibited on the topology diagram are connected to the WAN.
4. Assure proper network security procedures are developed and implemented, and monitor the Network Security Plan for compliance.
5. Evaluate the impact of IS and network changes and apply for reaccreditation of the Network Security Plan if necessary. Reaccreditation is required if a new physical site is added.
6. Recommend that DSS rescind the NSP if necessary, and report any anomalies to DSS or accrediting authority.

* Final SECRET Government Issued PCL is required for access
** Interim SECRET Government Issued PCL is adequate for access based upon current OSD issued waiver

Overall Network Security Profile (To be completed by host activity)	Network Identifier:	Network Host Facility:

Network Connection Rules

1. The interconnection between remote ISs will be controlled by National Security Agency (NSA) endorsed Type 1 encryption devices
2. Clearance levels, contractual relationship with need-to-know and Formal Access Approval determinations at all locations must be established prior to connecting to the wide area network.
3. All ISs on the network are required to have an accredited System Security Plan (SSP).
4. The ISSM at each site will maintain current Visit Authorization Letters for all remote users of their ISs.
5. Passwords will be provided by a classification level appropriate secure means.
6. Users must be knowledgeable of the Network Security Plan requirements for which they are responsible.
7. Each connecting site's ISSM shall coordinate any changes to the network with the Network ISSO and shall gain approval by the appropriate cognizant security officials in advance.
8. The Network ISSO and connecting sites will report immediately any security-related incident to the appropriate local cognizant security official.

Data Transmission Records

1. All nodes of the classified network have a contractual relationship.
2. The above information is recorded once and updated upon change in contract status.
3. Records shall be retained for 2 years from the termination of the contract or when the connection is no longer required, whichever is sooner.

Signature

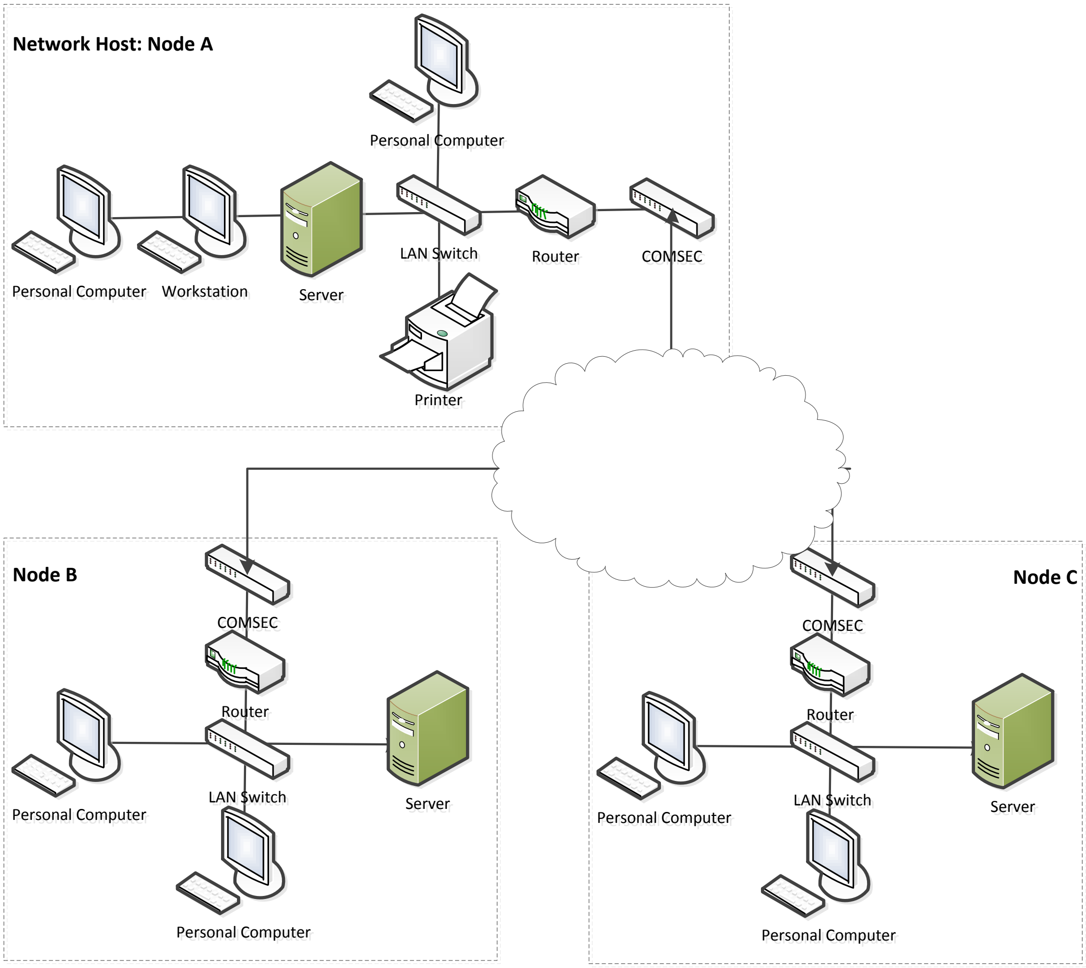
By signing, I hereby certify that there are no additional connections to the wide area network other than those identified in this NSP.

Network ISSO Signature:

Date:

14.1.7 NSP Architecture Diagram Example

NSP Architecture Diagram Example



*To be completed and maintained by the Network ISSO

14.1.8 Network Host Security Profile

Network Host Security Profile (To be completed by Network Host)	Network Identifier:	Network Host Facility:

Date:	Facility Address:	CAGE Code:

IS Contact Information

Network DAA: Phone Number:	Network ISSP: Phone Number:	Network ISSO: Phone Number:	ISSM: Phone Number:

Contracts Supported (Contract Numbers):

Describe role in supporting the above contract(s):

Reason for network participation □ Access other nodes □ Other nodes access your node

This node is accessible by (check/describe all that apply): □ O/S Login □ Other:
Specify all nodes accessing your node:

If applicable, describe procedures for remote users to gain access to your site:

Description of local systems/network:

□ Terminal Node (no backside connections) □ Backside connections, separately accredited WAN:

IS Protection, Sensitivity Level, and User Information

Accredited Protection Level: □ PL1 □ PL2 □ PL3 □ PL4 Highest classification level of IS data: □ CONFIDENTIAL □ SECRET □ TOP SECRET Category(s):□ NONE □ COMSEC* □ RD* □ FRD* □ FGI* □ Other Specify: Formal access approvals: □ No □ Yes If yes, Indicate: □ NATO* □ CNWDI* □ CRYPTO*	Highest classification level of data TRANSMITTED: □ CONFIDENTIAL □ SECRET □ TOP SECRET Category(s): □ NONE □ COMSEC* □ RD* □ FRD* □ FGI* □ Other Specify: Formal access approvals: □ No □ Yes If yes, indicate: □ NATO* □ CNWDI* □ CRYPTO*

Minimum clearance level of users: □ CONFIDENTIAL □ Interim SECRET □ SECRET □ Interim TOP SECRET
□ TOP SECRET

Network Data Transmission Protections

Network Host Security Profile (To be completed by Network Host)	Network Identifier:	Network Host Facility:

Date:	Facility Address:	CAGE Code:

Type 1 NSA Encryption Devices(s):

Need-to-Know Methodology for Network

□ Router IP Filters
□ Configuration disks for NES with accounts on each machine.
□ Other: Specify

Periods Processing: If used, IS Upgrade/Downgrade procedures shall include steps to ensure network configurations are appropriately changed between processing sessions.
□ This node will utilize periods processing

Network ISSO Responsibilities

1. Coordinate changes to the network with all nodes, including providing NSP updates as changes occur.
2. If applicable, develop a process for remote users to gain access to your site. The process must include validation of requisite clearance via a Visit Authorization Letter (VAL) or other method of clearance validation (JPAS), and a security method for providing passwords to remote users.
3. Establish a process so that audit trails associated with the network are reviewed on a weekly basis.
4. Report any security incidents or violations to the Network ISSO.
5. Report and obtain approval by cognizant DAAs when any changes are made to the wide area network configuration including the updating of the NSP, and distribution of the approved NSP to all nodes.

By signing, I hereby certify that there are no additional connections to the host node other than as described in this host node profile.

Network ISSO Signature:	Date:

14.1.9 Network Node Security Profile Form

Network Node Security Profile **(To be completed by each Network Node)**	Node Identifier:	Contractor facility name:	
Date:	Facility Address:	CAGE Code:	
Contact Information & Description of Network Participation			
Network DAA: Phone Number:	Network ISSP: Phone Number:	Network ISSO: Phone Number:	Node ISSM: Phone Number:
Contracts Supported (Contract Numbers):			
Describe role in supporting the above contract(s):			
Reason for network participation □ Access other nodes □ Other nodes access your node.			
This nodes is accessible by (check/describe all that apply): □ O/S Login □ Other: Specify all nodes accessing your node:			
If applicable, describe procedures for remote users to gain access to your site:			
Description of local systems/network:			
□ Terminal Node (no additional/backside connections): □ Separately Accredited WAN:			
IS Protection, Sensitivity Level, and User Information			
Accredited Protection Level: □ PL1 □ PL2 □ PL3 □ PL4 Highest classification level of IS data: □ CONFIDENTIAL □ SECRET □ TOP SECRET Category(s): □ NONE □ COMSEC* □ RD* □ FRD* □ FGI* □ Other, Specify: Formal access approvals: □ No □ Yes. If yes, Indicate: □ NATO* □ CNWDI* □ CRYPTO*	Highest classification level of data TRANSMITTED: □ CONFIDENTIAL □ SECRET □ TOP SECRET Category(s): □ NONE □ COMSEC* □ RD* □ FRD* □ FGI* □ Other, Specify: Formal access approvals: □ No □ Yes. If yes, indicate: □ NATO* □ CNWDI* □ CRYPTO*		
Minimum clearance level of users: □ CONFIDENTIAL □ Interim SECRET □ SECRET □ Interim TOP SECRET □ TOP SECRET			
Network Data Transmission Protections			
Type 1 NSA Encryption Device(s):			
Need-to-Know Methodology for Network			

Network Node Security Profile (To be completed by each Network Node)	Node Identifier:	Contractor facility name:
Date:	Facility Address:	CAGE Code:
□ Router IP Filters □ Configuration disks for NES with accounts on each machine. □ Other, Specify:		Periods Processing: If used, IS Upgrade/Downgrade procedures shall include steps to ensure network configurations are appropriately changed between processing sessions. □ This node will utilize periods processing

ISSM Responsibilities for Connection to WAN

1. Notify the Network ISSO of all proposed external connections or system changes that will affect the security of the wide area network.
2. If applicable develop a process for remote users to gain access to your site. The process must include validation of requisite clearance via a Visit Authorization Letter (VAL) or other method of clearance validation (JPAS), and a secure method for providing passwords to remote users.
3. Brief personnel on the use of the wide area network.
4. Establish a process so that audit trails associated with the network are reviewed on a weekly basis.
5. Report any security incidents or violations to the Network ISSO.
6. Report and obtain approval by cognizant DAAs when any changes are made to the wide area network configuration including the updating of the NSP, and distribution of the approved NSP to all nodes.
7. Provide the Node Security Profile and signed DSS accreditation letter to the Network ISSO, including all subsequent revisions

By signing, I hereby certify that there are no additional connections to this node other than as described in this node security profile.

Node ISSM Signature:	Date:

14.1.10 Memorandum of Understanding Template

Note to Template User: This must be appropriately modified for the situation. If connection is between several nodes, please list all node information where appropriate.

MEMORANDUM OF UNDERSTANDING
Between
(Name of User Agency)
and
Defense Security Service

References: (a) NISPOM, Chapter 8
(b) (GCA Regulation)

This Memorandum of Understanding (MOU) between (User Agency) and the Defense Security Service (DSS), Designated Approval Authority for (Company Name), is for the purpose of establishing a secure communications link between (User Agency) and (Company Name) for the electronic transfer of classified information. Each of the undersigned agrees to and understands the procedures that will be in effect and adhered to. It is also understood that this MOU summarizes the information systems (IS) security requirements for approval purposes and supplements (Company Name) approved Systems Security plan (SSP).

1. Contract Information
This MOU describes the classified network arrangement between (Company Name) and (User Agency) in support of the (Name of Program). The (Name of Program) is a (brief description of program) sponsored by (User Agency). The contract number is (Contract Number). The prime contractor is (Name of Prime Contractor), whose CAGE Code is (CAGE Code Number).

At (User Agency) direction, (Company or User Agency Name) is establishing a remote access capability to the (Name of Classified Computer System); with a remote access IS located at (List User Agency or Company, as appropriate). (Note to Template User: Please word this paragraph so that it is obvious who will be the host, if applicable, and who will be the remote site(s)). This capability will allow (Company or User Agency, as appropriate) personnel to access the (List Name of Classified IS) as remote users. The (User Agency) Information System is located at (address).

The following (DSS) key points of contact are identified:

Name______________________ Title________________________ Phone (____) ______ - _________

The following (User Agency) key points of contact are identified:

Name______________________ Title________________________ Phone (____) ______ - _________

The following (Company) key points of contact are identified:

Name______________________ Title________________________ Phone (____) ______ - _________

2. Description
(Company or User Agency Name) operates the (List Names of Classified System) IS at Protection Level X (#), whereby all users have the clearance and need to know for all information on the system. The highest level of classification of the Information System is (Level of Classification). All personnel with access to the (Name of Classified System) will be briefed for (Give name of specific briefing, e.g., COMSEC).

(Describe connection. An example follows): The (Company or User Agency Name) IS will be connected to the (Name of Classified System at different enclave (if needed)) at (Company or User Agency Name at different enclave (if needed)), by a communication circuit for the transfer of data. The circuit will be protected at each end by an NSA Type 1 encryption device, to provide encryption of the circuit. Operational key for the NSA Type 1 encryption will be at the (classification level) level.

Any further network security requirements are detailed in the attached network security plan.

3. Network Information Systems Security Officer (Network ISSO) Responsibilities

The Network ISSO (Network ISSO Name) at (host--Company and User Agency Name) are required to have the following responsibilities. He or she will brief operator personnel involved with use of the communications link on network operating procedures and their responsibilities for safeguarding classified information in accordance with the requirements of paragraph 5-100 of the National Industrial Security Program Operating Manual (NISPOM) and associated Department of Defense interpretive guidance. The IS Security Officer at (List Names of other User Agency or Company Site) will conduct an equivalent briefing for network responsible personnel.

The Network ISSO at (Company and User Agency Name) and the IS Security Officer at (Name of other site(s)) will indoctrinate system operators and support personnel concerning:

- The need for sound security practices for protecting information handled by their respective IS, including all input, storage, and output products.

- The specific security requirements associated with their respective IS as they relate to Protection Level X (#) and operator access requirements.

- The security reporting requirements and procedures in the event of a system malfunction or other security incident occurs.

- What constitutes an unauthorized action as it relates to system usage.

- Their responsibility to report any known or suspected security violations.

It is the responsibility of each individual operator to understand and comply with all required procedures for using the (Name of Classified System at Company Site), as described in the SSP which is approved by the Defense Security Service (DSS).

The system user will report all instances of any security violations to the ISSM (or Network ISSO if located at company) at (Company Name). In addition, the User Agency IS Security Officer (or Network ISSO if located at User Agency) will report any security violations to the system.

4. Interconnect Procedures

The communication link at (Host Site Name) will be available 24 hours per day. The operating system at the host IS automatically records all operators logging in and out. When logged in, the operators at (Contractor or User Agency Name) will be able to access the system for the transfer of classified data.

All signers agree there are no further connections on this network to DISN networks, including the SIPRNet.

Each interconnected site must maintain a current and valid accreditation in accordance with Department of Defense policy.

When the communications link between (User Agency) and (Company Name) is no longer required, communications between sites will be disabled by removing the remote users from the “system password file” and physically disabling the encrypted link from the router, if applicable.

5. Approval

The secure communication link between (User Agency) and (Company Name) will not be initialized until approval of these procedures by all DAAs is indicated below. This agreement will remain in effect for three years from the date of the signatures below, unless specifically terminated by either DAA. This MOU becomes effective upon signatures of all parties. Additionally, the user agency will notify DSS in writing of cancellation of the MOU.

Defense Security Service

____

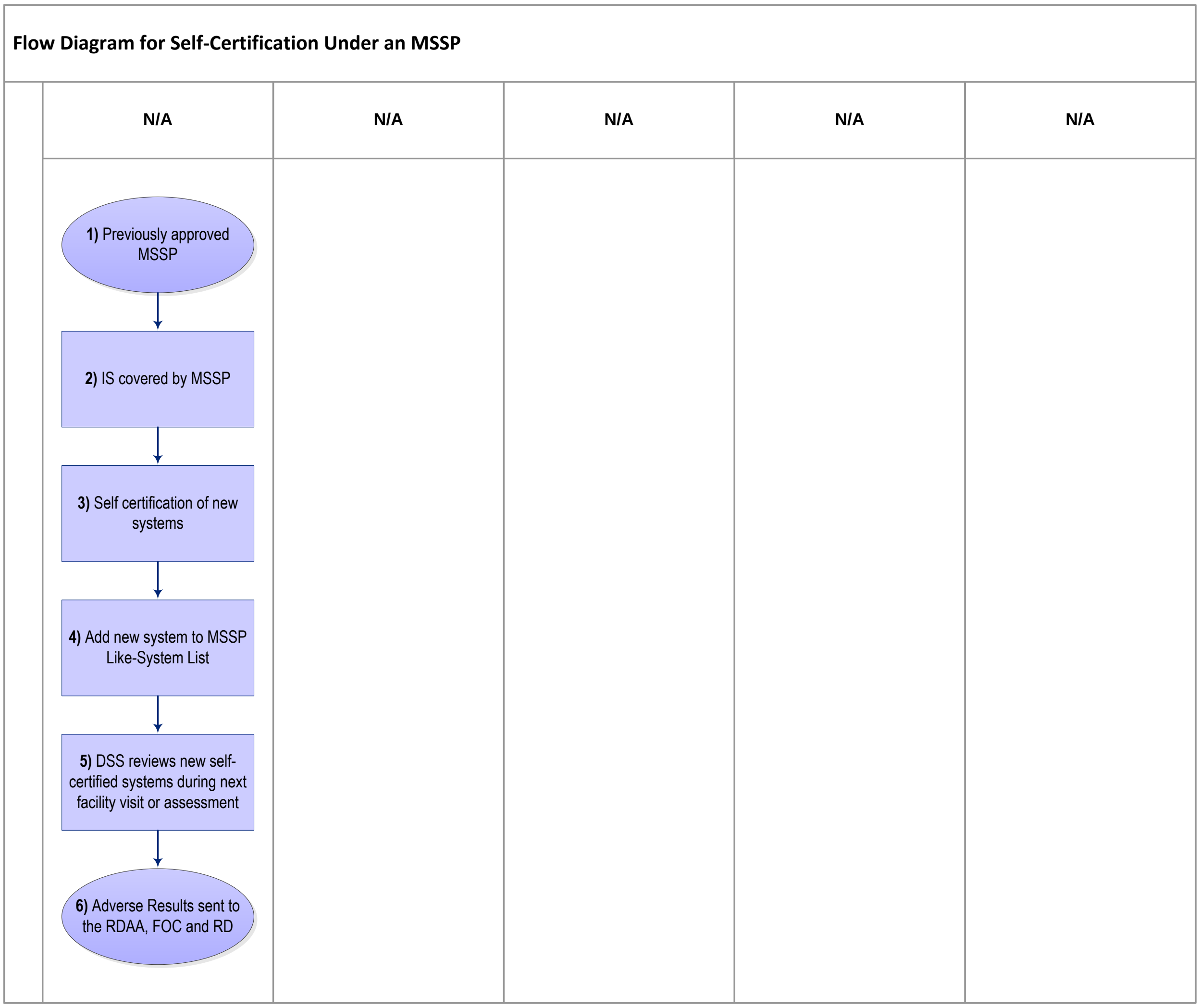
(Randall Riley)
Assistant Deputy Director
Office of the Designated Approving Authority

(User Agency)

____

(Name of User Agency Official)
Designated Approving Authority

14.1.11 Flow Diagram for Self-Certification under an MSSP


Flow Diagram for Self-Certification Under an MSSP
N/A
N/A
N/A
N/A
N/A
1) Previously approved MSSP
2) IS covered by MSSP
3) Self certification of new systems
4) Add new system to MSSP Like-System List
5) DSS reviews new self-certified systems during next facility visit or assessment
6) Adverse Results sent to the RDAA, FOC and RD

14.1.12 Table for Self-Certification

(Most common parameters)

	Protection Level (PL) (NOTE: 1)	Level of Concern (NOTE: 2)	Physical (NOTE: 3)	Operating Systems (OS) (NOTE: 4)	System Type (NOTE: 5)	Trusted Downloading Procedures (NOTE: 6)	Periods Processing (NOTE: 7)	Mobile Systems/ Alt Site (NOTE: 8)	Test Equipment (NOTE: 9)
Required to be considered “similar”	■	■	■	■	■	■	■	■	■

NOTE: 1 – MSSP can consist of systems at PL-1 or PL-2, but not both.

NOTE: 2 – Level of Concern (NISPOM 8-401) must be the same. This refers to the classification levels of information (TOP SECRET, SECRET and CONFIDENTIAL).

NOTE: 3 – Physical. This pertains to the physical security environment (most notably restricted areas and closed areas). Be mindful that there are many scenarios that could describe a restricted area, therefore, if the scenarios are not similar, the IS will not be self-certified. In this case a reaccreditation of the MSSP would be required to include the additional scenario. There are hybrids (i.e. A LAN that encompasses closed and restricted areas) but are generally the exception rather than the rule.

NOTE: 4 – Only approved OS can be used for subsequent self-certified systems. Any OS version changes may not be self-certified if the new version changes an approved existing security configuration. For clarification please check with the ODAA for determination.

NOTE: 5 – System type generally refers to system architecture: For example, multiuser standalones (MUSA) or LANs. It can also refer to how an information system is used. A Windows 2003 server can be used as a domain controller (which controls half the (I&A) "handshake" and requires all technical security features to be enabled) or as a file server (which can be recognized as a pure server in some instances which doesn't require all technical security features to be enabled).

NOTE: 6 – Trusted downloading procedures. Only DSS approved procedures can be considered for self-certification.

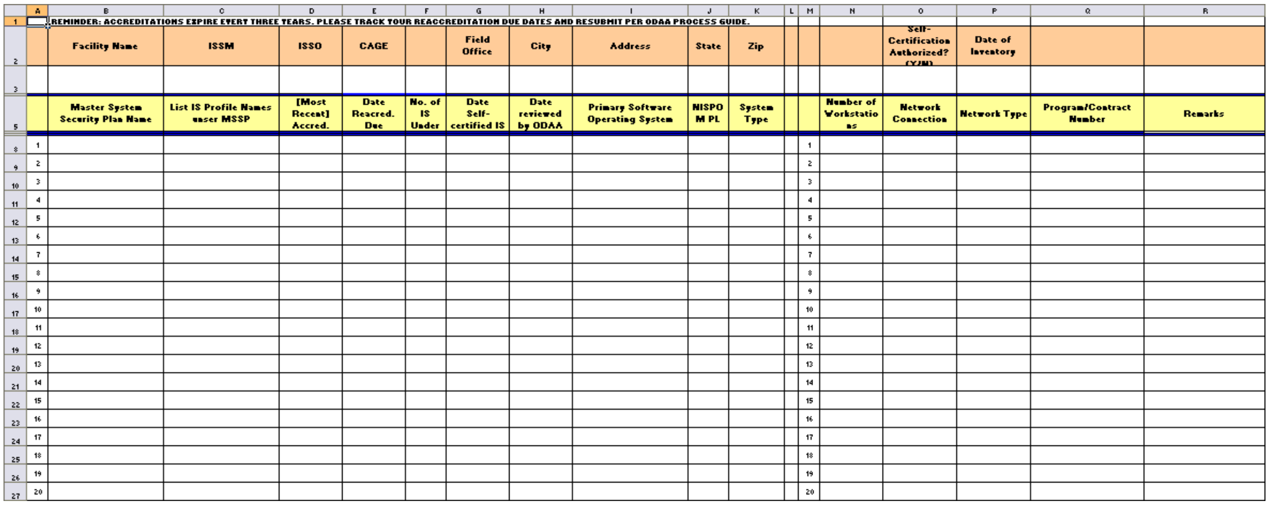
NOTE: 7 – Periods processing (NISPOM 8-502). Periods processing provides the capability to either have more than one user or group of users (sequentially) on a single-user IS who do not have the same need-to-know or who are authorized to access different levels of information; or use an IS at more than one protection level (sequentially).

NOTE: 8 – Mobile systems. Procedures for identifying, managing and protecting mobile systems must be similar for DSS to consider approving self-certification.

NOTE: 9 – Test equipment can only be self-certified if it is the same make and model as another device that has been previously accredited by DSS.

NOTE: 10 - At a minimum, the contractor will provide an updated list of IS self-certified under the MSSP to the IS Rep and ISSP on a quarterly basis. If DSS determines that more frequent notification is necessary because of volume or complexity or to address specific security concerns, they can request more frequent notification.

14.1.13 MSSP IS Tracking Form



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1		REMINDER: ACCREDITATIONS EXPIRE EVERY THREE YEARS. PLEASE TRACK YOUR REACCREDITATION DUE DATES AND RESUBMIT PER ODAA PROCESS GUIDE.																
2		Facility Name	ISSM	ISSO	CAGE		Field Office	City	Address	State	Zip				Self-Certification Authorized? (Y/N)	Date of Inventory		
3																		
5		Master System Security Plan Name	List IS Profile Names unser MSSP	[Most Recent] Accred.	Date Reacred. Due	No. of IS Under	Date Self-certified IS	Date reviewed by ODAA	Primary Software Operating System	NISPOM PL	System Type			Number of Workstations	Network Connection	Network Type	Program/Contract Number	Remarks
8	1												1					
9	2												2					
10	3												3					
11	4												4					
12	5												5					
13	6												6					
14	7												7					
15	8												8					
16	9												9					
17	10												10					
18	11												11					
19	12												12					
20	13												13					
21	14												14					
22	15												15					
23	16												16					
24	17												17					
25	18												18					
26	19												19					
27	20												20					

										Self-Certification Authorized? (Y/N)	Date of Inventory		
Facility Name	ISSM	ISSO	CAGE	Field Office	City	Address	State	Zip			Network Type	Program/ Contract Member	Remarks

14.1.14 Table of Subject Line Requirements for Plan Submissions

Region	PLAN Unique Identifier			IS # Identifier	Variables
	XXXXX-YYYYMMDD-XXXXX				
Capital	Cage Code(1)	YYYYMMDD(2)	XXXXX(3)	XXXXX(4)	See Variables
Northern					
Southern					
Western					

Unique Identifiers	
(1)	Use the facility's 5 character CAGE Code
(2)	Use the date on the SSP or MSSP
(3)	Use a number from 00001 - 99999. Each plan must use a unique number
(4)	Use a number from 00001 - 99999. Each plan must use a unique number NSP will use 00000 MSSPs with multiple profiles will use XXXXX
Variables	
MSSP	Use MSSP when the plan is a Master Systems Security Plan
SSP	Use SSP when the plan is a Systems Security Plan
REV	Use Rev when the plan has been resubmitted after the contractor has made revisions as required by the ODAA
SIPR	Use when the IS seeking accreditation has a connection to the SIPRNet
TERM	Use when the information system is no longer used for classified processing
INT	Use INT for SSPs with International connections
NSP	Use NSP for Network Security Plans (IS # Identifier will use 00000)
DIB	Use DIB for DIBCS Systems Security Plans

Examples

- Capital SSP #5 for CAGE code 12345 dated Oct 30, 2005 protecting IS#2. It is a SIPRNet plan submitted with revisions.
  - Capital 12345-20051030-00005-00002 -SIPR – REV

- Western MSSP #10 for CAGE code ABCDE dated July 14, 2004 protecting IS#1
  - Western ABCDE-20040714-00010-00001 – MSSP

- Western MSSP #7 for CAGE code 11223 dated April 22, 2006 protecting multiple IS (#5 and #6)
  - Western 11223-20060422-00007-XXXXX – MSSP

- Standard SSP #13 from the Northern region from CAGE code 10101, dated Nov. 18, 2005 protecting IS#10
  - Northern 10101-20051118-00013-00010 – SSP

- NSP #9 from the Southern region from CAGE code 98765, dated Jan 9, 2003
  - Southern 98765-20030109-00009-00000 – NSP

14.1.15 E-mail to ODAA Mailbox Template and Sample

Below is a template for submitting a request to ODAA via e-mail. Each field has the available options; please delete the options that do not apply.

From: (Recipient address)
To: ODAA@dss.mil; ISSP
CC: IS Rep

Subject: ODAA Submission - UID (Use UID format from Table 15.1.14)
Attachment: (Attached Plan and Associated files)

ODAA Submission Information

Tracking ID: xxxxx-xxxxxxxx-xxxxx-xxxxx (Format CAGE Code (5 digit code) – Original date of the plan yyyymmdd-unique 5 digit code – unique 5 digit IS Profile Code)

Date of Systems Security Plan:
Receipt Date: (e-mail date)
Type of Plan: (SSP, MSSP, NSP, SIPR, DIB)
Protection Level: (PL 1, PL 2, PL 3,)
Classification: (High (TOP SECRET), Medium (SECRET), Basic (CONFIDENTIAL))
System Type: (LAN, WAN, Standalone Multiuser, Standalone Single-User)
Area Type: (Closed, Restricted, Both)
IS Profiles: (list the IS profile descriptions associated with the plan)
1.
2.

- IS Rep Name:
- ISSP Name:
- ISSM Name:
  - Phone:
  - Address:
  - E-mail:

Purpose of Submission: (Select the appropriate purpose for this request)

- Initial Request of Certification and Accreditation
- Reaccreditation request
- Added IS to an existing Master plan
- Submitting updated plan to include required corrections
- Submitting updated plan due to system changes and requesting security review
- Submitting updated plan with no security relevant change (for informational purposes only)
- Submitting as self-certified system by ISSM)

Additional Information/Comments:

In FY 2014, DSS will be transitioning from receiving security plans via email and the mail to receiving plans via the ODAA Business Management System (OBMS). OBMS will automate the submittal, review and approval process. Additional information can be found at www.dss.mil.

This is an example of a request of an initial Certification and Accreditation of an MSSP.

From: (Recipient address)
To: ODAA@dss.mil; ISSP
CC: IS Rep

Subject: ODAA Submission - Capital – 12345-20080310-00001-00001
Attachment: 12345-20080310-00001-00001.zip

ODAA Submission Information

Tracking ID: 12345-20080310-00001-00001

Date of Systems Security Plan: March 10, 2008
Receipt Date (e-mail date): 03/11/2008
Type of Plan: SSP
Protection Level: PL 1
Classification: Medium (SECRET)
System Type: LAN
Area Type: Both
IS Profiles: (list the IS profile descriptions associated with the plan)

1. 00001

- IS Rep Name: Tom Jones
- ISSP Name: Francis Smith
- ISSM Name: Jane Doe
  - Phone: (212)555-4567
  - Address: 101 Anywhere St
  - Alexandria, VA, 12345
  - E-mail: Jane.Doe@ABC.com

Purpose of Submission: (Select the appropriate purpose for this request)

- Initial Request of Certification and Accreditation

Additional Information/ Comments: N/A

14.1.16 Clearing and Sanitization Matrix

Media	Clear					Sanitize																
Magnetic Tape																						
Type I	a						b										l					
Type II	a						b										l					
Type III	a						b										l					
Magnetic Disk																						
Bernoulli	a	c					b										l					
Floppy	a	c					b										l					
Non-Removable Rigid Disk		c				a			d								l					
Removable Rigid Disk	a	c				a			d								l					
Optical Disk																						
Read Many, Write Many		c															l					
Read Only																	l	m				
Write Once, Read Many (Worm)																	l	m				
Memory																						
Dynamic Random Access Memory (DRAM)		c	g					c					g				l					
Electronically Alterable Programmable Read Only Memory (EAPROM)				h											i		l					
Electronically Erasable PROM (EEPROM)				h							f						l					
Erasable Programmable ROM (EPROM)					j			**c**								**k**	l					**k then c**
Flash EPROM (FEPROM)				h				**c**						**h**			l					**h then c**
Programmable ROM (PROM)		c															l					
Magnetic Bubble Memory		c				a		c									l					
Magnetic Core Memory		c				a			d								l					
Magnetic Plated Wire		c						**c**			**e**						l					**c and e**
Magnetic Resistive Memory		c															l					
Non-volatile RAM (NOVRAM)		c						c									l					
Read Only Memory (ROM)																	l					
Synchronous DRAM (SDRAM)		c	g					c					g				l					
Static Random Access Memory (SRAM)		c	g					c					g				l					
Other Media																						
Video Tape																	l					
Film																	l					
Equipment																						
Monitor			g																		p	
Impact Printer			g										**g**							**o**		**o then g**
Laser Printer			g										**g**						**n**			**n then g**

INSTRUCTIONS FOR READING THE MATRIX:

A letter in black in the above table indicates the procedure is a complete, single option. For example, to sanitize EEPROM: Perform either procedure f or l (refer to indices below) and the media/memory is completely sanitized. Letters in bold indicate the procedures must be combined for a complete sanitization. For example, to sanitize a Laser Printer: n must be performed, followed by g.

NOTE: When a combination of two procedures is required, the far right hand column indicates the order of the procedures (e.g., o then g).

MATRIX INDEX:

a. Degauss with Type I, II, or III degausser.
b. Degauss with same Type (I, II, or III) degausser.
c. Overwrite all addressable locations with a single character utilizing an approved overwrite utility.
d. For spills only, overwrite with a pattern, and then its complement, and finally with another unclassified pattern (e.g., “00110101” followed by “11001010” and then followed by “10010111” [considered three cycles]). Sanitization is not complete until three cycles are successfully completed. Once complete, verify a sample. If any part could not be written to the disk, the disk must be destroyed or degaussed. This option does not apply to disks used on a system accredited for classified processing.
e. Each overwrite must reside in memory for a period longer than the classified data resided.
f. Overwrite all locations with a random pattern, then with binary zeros, and finally with binary ones utilizing an approved overwrite utility.
g. Remove all power to include battery power.
h. Perform a full chip erase as per manufacturer’s data sheets.
i. Perform h above, then c above, a total of three times.
j. Perform an ultraviolet erase according to manufacturer’s recommendation.
k. Perform j above, but increase time by a factor of three.
l. Destruction (see below.)
m. Destruction required only if classified information is contained.
n. Run 1 page (font test acceptable) when print cycle not completed (e.g., paper jam or power failure). Dispose of output as unclassified if visual examination does not reveal any classified information.
o. Ribbons must be destroyed. Platens must be cleaned.
p. Inspect and/or test screen surface for evidence of burn-in information. If present, screen must be destroyed.

14.1.17 Main Cleansing Process Checklist

Date: ________________

Incident Title: ____

Check Box	Step ID	Step Description	Step Owner
□	A1	Notification received by ISSM. This checklist is initiated by the ISSM. Initial contact should include all known e-mail message information.	
□	A2	Identify all initial recipients of the contaminated e-mail.	
□	A3	For each individual, identify the locations of their Client Workstation.	
□	A4	Dispatch a team to secure these Client Workstations within an approved, Classified storage location. Include these Client machines on the list for Client Cleansing. Name(s) of individuals assigned to secure these machines: __________________________________ __________________________________ __________________________________ __________________________________	
□	A5	Identify the extent of network servers affected by the contaminated e-mail.	
□	A6	Initiate the appropriate ‘Cleansing Check Lists’ (GroupWise, Exchange, Desktop Clients) and perform computer equipment cleansing as necessary.	
□	A7	Perform ‘Exchange Server Cleansing’ sub-process(s) as necessary. Responsible Authority:	
□	A8	Perform ‘GroupWise Cleansing’ sub-process(s) as necessary. Responsible Authority: __________________________________	
□	A9	Perform ‘Desktop Client Cleansing’ sub-process(s) as necessary. Responsible Authority: __________________________________	
□	A10	Complete and report to DSS.	

Cleansing Completion Date: ______________________________

Signature of Validator:

Print Name: ____

Signature: ____

14.1.18 Microsoft Exchange Server Cleansing Checklist

Date: _______________

Incident Title: ____

Exchange Server Name: ____

Check Box	Step ID	Step Description	Step Owner
□	B1	Identify, secure, and lock-up all affected Exchange Server back-up tapes.	
□	B2	Interview each individual who received the contaminated e-mail message. Inform each individual: ▪ That they are to cease all e-mail activities until further notice. ▪ Under NO circumstances should the contaminated e-mail be deleted. The original e-mail (sender and recipient) is required so that “Message Tracking” can be performed by the Exchange Administrator to document the scope of the compromise. Message Tracking allows an Exchange Administrator to determine the path an e-mail has traveled, and ascertain if it is necessary to cleanse more than a single Exchange Server. If it is discovered that the contaminated e-mail has left the company e-mail System, and/or crossed an internet boundary, additional cleansing of all recipient e-mail systems may be required. The ISSM should be notified immediately if Message Tracking indicates a contaminated e-mail has left the company network.	
□	B3	Determine if the contaminated e-mail was contained within the ‘Domain of Responsibility’ (your system). Was the e-mail message released outside of the ‘Domain of Responsibility’ (your System) (Y/N)? ____________. ▪ If ‘Yes’ proceed to step B5 ▪ If ‘No’ proceed to step B4	
□	B4	If e-mail message has been released outside of the ‘Domain of Responsibility’ (your system), notify ISSM. Continue with step B5.	
□	B5	Disable all affected User’s Exchange mailbox access. 1. Start/Programs/Microsoft Exchange/Active Directory Users and Computers. 2. Right click on domain and select ‘Find’. 3. Enter affected user’s name in the Name field and select ‘Find Now’. 4. Open Properties of the user object and select ‘Exchange Advanced’ tab. 5. Click on the ‘Mailbox Rights’ button. 6. Highlight the user’s account and enter a check in all the ‘Deny’ check boxes. 7. Click the ADD button. 8. Select the name of the Exchange Administrator who will sanitize the contaminated users’ mailbox. 9. Grant Admin full mailbox permissions to each contaminated mailbox and check all boxes EXCEPT “Associated External Account”	

		for this admin account. 10. Click 'Apply' and 'OK'.	
□	B6	Have any of the Users 'forwarded' the contaminated e-mail to other individuals? Yes / No: _______________. The Exchange Administrator must use " Message Tracking" to: ▪ Determine the path in which a contaminated e-mail has traveled so that all compromised Exchange servers can be targeted for cleansing. ▪ Determine all recipients of the contaminated e-mail so that each contaminated Mail Box can be cleansed. ▪ Determined if ISSM must be notified in the event the e-mail has contaminated an e-mail server outside of the company computer network. If 'Yes' to B6, perform Steps B7 and B8 to add these 'second tier' Users to the 'Client Cleansing' process list. If "Message Tracking" indicates that an outside e-mail system may be contaminated, ISSM must be informed immediately. If 'No' to B6, perform Step B9.	
□	B7	Add these additional Users to the 'Client Cleansing Process' list. ___________________________________	
□	B8	Dispatch a team to secure these Client Workstations within an approved, Classified storage location. Include these Client machines on the list for Client Cleansing. Name(s) of individuals assigned to secure these machines: ___________________________________ ___________________________________	
□	B9	Open the individual's mailbox with an Exchange Administrator account. Delete the message from the Inbox and/or Sent Items.	
□	B10	Empty the deleted items folder.	
□	B11	Go to Deleted Item Recovery and delete the message again.	
□	B12	Identify if the User saves and/or backs up e-mail messages to other locations. ▪ Archives: Location of *.pst and/or *.ost files – local or server. ▪ Back-ups: Local hard drive, network drive, zip drive, floppy drive.	
□	B13	As necessary, perform the following activities: ▪ External Media: Identify, secure, and lock-up all external media (floppy and zip). ▪ Local Drive Storage: Ensure that the Desktop Client machine has been identified for 'Client Cleansing'. ▪ Network Storage: Ensure that affected server(s) has been included for server cleansing sub-process(s) (GroupWise and/or Exchange).	

		Provide comments that clarify the actions taken at this step. ____________________________________ ____________________________________ ____________________________________ Continue with Step B12.	
□	B14	Confirm that “Database Zeroing” is enabled on the Exchange Server you are cleansing. (This setting is/should be enabled for all Exchange Servers). To verify “Database Zeroing” has been enabled: ▪ Start/Programs/Microsoft Exchange/System Manager/Administrative Groups/ Servers/ <Mail Server Computer Name>/ Storage Group that contains the contaminated Mail Box(es) ▪ Right click on the Storage Group (i.e., “SG1”) and click properties. ▪ On the “General” tab check “Zero out deleted database pages.”	
□	B15	Backup the e-mail servers involved to delete the transaction logs. Since transaction logs may be shared between several Mail-Box Stores. A Full exchange backup of the entire exchange server is recommended. If using Veritas Netbackup to perform the Exchange Server backups, the following Microsoft Event ID#’s can be found in the EVENT VIEWER’s APPLICATION logs ▪ Start Backup = MS Event ID# 220 ▪ Stop Backup = MS Event ID# 221,223 (224) If Backup of the Exchange Server is spooled to : ▪ TAPE media, then these backup TAPES must also be identified and secured with TAPE media in Step “B1”. ▪ DISK media, then all DISKS used for the Exchange Server backup must be zeroed with a DSS-approved disk cleansing utility. ▪ TAPE & DISK media, then both steps “B15-1” & “B15-2” must be performed.	
□	B16	Save the servers log files to verify that zeroing has been done. Print out the log files that indicate that zeroing was done on the storage group that was in question, along with the mailbox databases. The “EVENT VIEWER” “APPLICATION LOG” contains the Database zeroing entries. The Microsoft event ID numbers for Exchange 2000 SP2 / W2K-SP2 / Exchange 2007 Database Zeroing are as follows: ▪ Start Zeroing = MS Event ID# 706, 712, 718 ▪ Finished Zeroing = MS Event ID# 707, 713, 722 Save the Application entire application log from the MS Event Viewer and note the times in which Database Zeroing Started and Stopped. This log will be submitted to the FSO as proof that the Exchange Server has been sanitized.	
□	B17	Re-activate each User’s Mailbox on the server. ▪ Start/Programs/Microsoft Exchange/Active Directory Users and	

		Computers. ▪ Right click on domain and select ‘Find’. ▪ Enter affected user’s name in Name field and select ‘Find Now’. ▪ Open Properties of the user object and select ‘Exchange Advanced’ tab. ▪ Click on the ‘Mailbox Rights’ button. ▪ Highlight the user’s account and uncheck all the ‘Deny’ check boxes. ▪ Remove the Exchange Admin account that was added in step “B5”. ▪ Click ‘Apply’ and ‘OK’.	
□	B18	Verify that each Users Mail Account is working.	
□	B19	Inform each User that their Exchange Mail account has been cleansed.	
□	B20	Complete and verify Exchange server Cleansing Checklist.	
□	B21	Ensure all printed material and backup tapes have been turned over to security.	

Exchange Server Cleansing Completion Date: ______________________________.

Signature of Validator:

Print Name: ____.

Signature: ____.

14.1.19 Novell GroupWise Server Cleansing Checklist

Date: ________________.

Incident Title: ____.

GroupWise Server Name: ____.

Check Box	Step ID	Step Description	Step Owner
□	C1	Identify, secure, and lock-up all affected GroupWise Server back-up tapes.	
□	C2	Interview each individual who received the contaminated e-mail message.	
□	C3	Determine if the contaminated e-mail was contained within the 'Domain of Responsibility' (your system). Was the e-mail message released outside of the 'Domain of Responsibility (your system) (Y/N)? _____________. ▪ If 'Yes' proceed to step C5, ▪ If 'No' proceed to step C4	
□	C4	If e-mail message has been released outside of the 'Domain of Responsibility' (your system), notify the ISSM and the cognizant Security Manager. Continue with step C5.	
□	C5	Disable all affected Users GroupWise mail accounts. 1. Run NWADMN32. 2. From the GroupWise View or NDS View, locate Users in question – click for detail window. 3. Click on 'GroupWise Account' tab. 4. Select 'Disable Logins' box then OK.	
□	C6	Have any of the Users 'forwarded' the contaminated e-mail to other individuals? Yes / No: ______________. 1. Run NWADMN32 2. From the GroupWise View or NDS View, locate Users in question – click for detail window. 3. Click on 'GroupWise Account' tab. 4. Change Users password for accessing e-mail account. 5. Run 'grpwise.exe /@u-?'. 6. Login as User with new password. 7. Open 'Sent Items' to view all e-mail that was recently sent or forwarded on to determine if further action is required. If 'Yes' to C6, perform Steps C7 and C8 to add these 'second tier' Users to the 'Client Cleansing' process list. If 'No' to Step C6, perform Step C9	
□	C7	Add these additional Users to the 'Client Cleansing Process' list.	
□	C8	Dispatch a team to secure these Client Workstations within an approved, Classified storage location. Include these Client machines on	

		the list for Client Cleansing. Name(s) of individuals assigned to secure these machines: ___________________________ ___________________________	
□	C9	Identify if the User saves and/or backs up e-mail messages to other locations. ▪ Archives: GroupWise archiving schema – local or server. ▪ Back-ups: Local hard drive, network drive, zip drive, floppy drive.	
□	C10	As necessary, perform the following activities: External Media: Identify, secure, and lock-up all external media (floppy and zip). Local Drive Storage: Ensure that the Desktop Client machine has been identified for 'Client Cleansing'. Network Storage: Ensure that affected server(s) has been included for server cleansing sub-process(s) (GroupWise and/or Exchange). Provide comments that clarify the actions taken at this step. ___________________________ ___________________________ ___________________________ Continue with Step C11.	
□	C11	As a GroupWise Administrator, locate the contaminated e-mail message. 1. Use Novell's stand-alone version of 'GWCHK32.EXE' to locate and delete the contaminated message. Place this program on your local hard drive. 2. Determine the exact 'Subject' line of the e-mail. 3. Create a text file called "itempurg" without double quotes or file extension. Place this file in the directory where GWCHK32.EXE will be run from. 4. Edit the text file and put the EXACT subject line in the file. For example: If the subject line reads: "RE Important Message From: Jane Doe" or "FWD: Important Message From: Jane Doe," make sure the "RE" or "FWD" or whatever else is also included in the text file. − When you enter the text of the subject into the itempurg file, we have seen some users that did not have mail deleted unless we copied and pasted the subject. It was not enough to type it in. 5. Map a drive to the location of the GroupWise Post Office: \\server\volume\PODir\ 6. Launch the GWCHK32.EXE program. 7. Configure GWCHECK with the following options: − Database Type = Post Office − Database Path = [Path where the wphost.db resides] − Post Office Name = [name of the NDS object for the post	

		office] – Object Type = Post Office – Action = Analyze/Fix Databases with Contents check and Fix problems selected – Databases = User 8. Click the 'Run' button. 9. If the check was successful, the log file (located in the directory where GWCHECK is run from) will have lines for each user infected which will say something like the following: – 259 ITEM_RECORD check – Item matches subject "Important message from:" – Item 259 purged successfully Additional Information can be found at http://support.novell.com. TID # 10052682 contains these procedures under the section named 'HOW TO REMOVE BAD MESSAGES FROM THE MESSAGE STORE'.	
□	C12	Using a DSS-approved wiping utility, completely delete the contaminated e-mail.	
□	C13	Re-activate each Users Mail Account on the GroupWise server.	
□	C14	Verify that each Users Mail Account is working.	
□	C15	Inform each User that their GroupWise Mail account has been cleansed.	
□	C16	Complete and verify GroupWise server Cleansing Checklist.	

GroupWise Server Cleansing Completion Date: ________________________________.

Signature of Validator:

Print Name: ____.

Signature: ____.

14.1.20 Desktop Client Workstation Cleansing Checklist

Date: ________________

Incident Title: ____

Desktop Client ID: ____

Check Box	Step ID	Step Description	Step Owner
□	D1	Verify that the Desktop Client machine has been secured in an approved classified storage location.	
□	D2	Use an administrative tool to search the hard drive for applicable data bit strings. Include temp files, hidden files, and protected files.	
□	D3	When a match on 'data strings' is found, coordinate with the ISSM to determine if the data is within scope for cleansing.	
□	D4	If the 'data string' match is determined to be 'out of scope', leave file as is.	
□	D5	If the 'data string' match is determined to be 'In Scope', delete the file from the hard drive. Also delete contents of Temp directories. On Windows systems delete file from Recycle Bin.	
□	D6	Cleans the Users Outlook archive file(s) (*.pst and *.ost). Delete the Re-cycle bin.	
□	D7	Using a DSS-approved wiping utility, 'wipe' all free space from the Client hard drive.	
□	D8	Execute the de-fragmentation utility of the Client hard drive.	
□	D9	Complete and verify Desktop Client Cleansing checklist.	
□	D10	After approval of the FSO return the Client Desktop machine to its appropriate working location.	

Desktop Client Cleansing Completion Date: ______________________________

Signature of Validator:

Print Name: ____

Signature: ____

14.1.21 Process for Clearing a Blackberry

The process is recommended for use by Industry when a Blackberry must be cleared as a result of a security incident involving contamination of the unclassified device by receipt of emails classified as SECRET and below. Contamination above SECRET (i.e., TOP SECRET, Sensitive Compartmented Information (SCI), Special Access Programs (SAP), etc.) requires confiscation and destruction of the Blackberry.

Throughout the procedure, Industry will be responsible for the process as a whole, and will provide response to Government personnel as required. This procedure details the Contractor's responsibility in the over-all cleanup process as it relates to the erasing of Blackberry devices. The Government Contracting Activity (GCA) as the data owner may specify other methods or procedures to be used in lieu of this one.

The following procedures do not sanitize BlackBerrys and are not to be used for sanitizing the device for turn-in or release outside DoD or DoD Cleared Contractor control. These procedures are approved only for data spillage involving information classified as SECRET and below. TOP SECRET, SECRET Restricted Data, and SCI/SAP contaminations require the Blackberry be confiscated and destroyed by the cognizant security official. Additionally, if the Blackberry software is below version 5.x, the Blackberry must be destroyed.

All contaminations and Blackberry devices cleared utilizing this procedure must be documented as required by NISPOM paragraphs 1-303 and 1-304. Also, the user responsible, serial number of the device, and dates of occurrence must be recorded and maintained for a minimum of two years after the device is destroyed.

There are a number of ways to clear Blackberry devices that have become contaminated with classified information, as follows:

Clearing Process 1	1. Open the Blackberry Desktop Manager and double click on the <Application Loader>. 2. When the application loader is opened, click <Next> to continue. 3. At the <Application Loader Wizard – Selecting Options> screen, click <Next> to continue. 4. At the <Completing Application Loader> screen, click on <Advanced> to continue. 5. At the <Handheld Data Preservation> screen, check <Erase all application data> to erase all data on the Blackberry device. If prompted, choose to not backup data files. Click <Next> to continue. 6. At the <Application Data Backup> screen, select the <Do not automatically backup and restore the handheld application data during the loading process> option. When this option is selected it will erase all handheld data. Click <Next> to continue. 7. The <Completing the Application Loader Wizard> screen will have a warning that all application data will be erased. Click <Finish> to erase the data. 8. After the erasing process, confirmation should show that <Your handheld's software has been updated successfully>. Click <Close> to complete. All application will be erased from the Blackberry. This also forces password expiration and clears any initial screen messages that the user set up previously. However, the calendar, tasks and notes, etc. (except e-mail messages) will resynchronize with Outlook and be placed back on the Blackberry after the completion of this process.
Clearing Process 2 **Erase Data and Disable Handheld Command**	The Erase Data and Disable Handheld command is sent wirelessly to a Blackberry device, erasing all of the device data and disabling the device so it can no longer be used on the Blackberry Enterprise Server. When this command is sent, it should be verified by the sender that the command was received successfully.

	1. The Blackberry device must be turned on and in an area of coverage to receive the command. If the device is turned off or out of coverage, the command is queued on the Blackberry Enterprise Server until the device is turned on or returns to an area of coverage. NOTE: To be able to view and verify the success of the command, the Blackberry Policy Service (POLC) logging level must be set to 4. 2. Sending the Erase Data and Disable Handheld Command − 1. Open Blackberry Manager. − 2. Go to the User List tab. − 3. In the IT Admin section, click <Erase Data and Disable Handheld> in the list of IT commands. A dialog box appears, stating that all data will be erased if the user proceeds. − 4. Select <Proceed>. Determining the Success of the Command ▪ To verify when the Erase Data and Disable Handheld command was sent and received, review the POLC log file (located by default in the Blackberry Enterprise Server directory, in subfolder Logs/<date>. ▪ [40000] (10/03 13:00:52):{0x974}{username@domain.com,PIN=XXXXXXXX, UserID=1}SCS::PollDBQueueNewRequests - Queuing KILL_DEVICE_REQUEST request ▪ The above line indicates when the command was first sent and that the command is being queued for the user. ▪ [40000] (10/03 13:01:15) :{0x960} {username@domain.com, PIN=XXXXXXXX, UserId=1}RequestHandler::HandleITADMINDataCommand - ITPolicy Success Ack for the command KILL_HANDHELD_COMMAND - Processing packet, Tag=23980295 ▪ The above line indicates when the Blackberry device received the command and that it sent a confirmation of the receipt. ▪ NOTE: To search using a string in the log file, search for ITPolicy Success Ack for the command KILL_HANDHELD_COMMAND. Once it is located, verify the user associated with the command. Search for this string when the Blackberry device does not meet the requirements to receive the command when it is first sent.
Clearing Process 3 **Erase all the Data and Applications on the Blackberry Device**	The following procedures will delete either all data, or all data and applications on the device. The choice can be made to either erase all the data or all the data and applications on the Blackberry device. To erase all the data: 1. Select the <Wipe Handheld> option. 2. Type an incorrect password ten times. 3. Use Application Loader to erase all data. 4. Use Backup and Restore to clear the device databases. To erase all the data and applications: 1. Connect the device to the computer running Desktop Manager. 2. In Desktop Manager, double-click the <Application Loader> icon. 3. In the Application Loader Wizard window, click <Next>. 4. On the Device Security Password screen, type an incorrect password and click <Next>. 5. Perform this step ten times. 6. Click <Close>.

	Without software, the device is unresponsive. It displays device error 507. To re-install the device software, open the Application Loader and select the software and applications to install.
Clearing Process 4 **Wipe Handheld Option**	To erase all the data on the Blackberry device, complete the following steps. This option is available with Blackberry device software 3.8 and later. 1. In the device options, click <Security>. 2. Click the track wheel and select <Wipe Handheld>. 3. Click <Continue>. 4. Type <blackberry>. All the data on the Blackberry device is erased. Use Backup and Restore to Clear the Databases. To clear the databases on a Blackberry device: 1. Connect the device to the computer running Desktop Manager. 2. In Desktop Manager, double-click the <Backup and Restore> icon, then click <Advanced>. 3. Press and hold the Shift key while selecting all the databases in the Handheld Databases list box. 4. Click <Clear>. 5. Click <Ok> on the Warning window. All databases on the Blackberry device are erased. 6. Click <Close> until the Desktop Manager is displayed.

14.1.22 Trusted Download Authorization Form

Printed Name:	Job Function or Title:

Manager Request

I request the above named individual be authorized to perform Trusted Downloads. I understand this access requires training to perform Trusted Downloads, a process for generating unclassified or lower classified media from a classified system. I understand this process involves both knowledge of classification issues and attention to detail in reviewing information and following the process for performing a download. I also understand that transferring information from a classified environment to an unclassified environment increases the risk of compromising classified information and will instruct authorized employees under my supervision to perform these actions only when absolutely necessary.

Printed Name:

Signature:	Date:

Acceptance of Responsibility

I have attended a Trusted Download training class and understand both the risks associated with performing a Trusted Download and the mechanisms associated with the Trusted Download process. I understand that all media generated from a classified system must be labeled and handled at the highest level of data on the system unless a Trusted Download Procedure is performed. I understand it is my responsibility to perform this process as outlined in the Trusted Download Procedure.

Signature:	Date:

ISSM or ISSO Authorization

I certify that the individual identified above has been briefed in the vulnerabilities associated with transferring unclassified or lower classified information from an accredited Information System (i.e., trusted download). Additionally, he/she has demonstrated extensive knowledge of all appropriate security classification guide(s) and authorized procedures associated with the information downloaded.

Authorized File Formats: ASCII/Text, HTM/HTML, JPEG, BMP, GIF
Specify:

Printed Name:

Signature:	Date:

14.1.23 Trusted Download Record

Date	Person	File Type	File Description

14.1.24 Alternate Trusted Download Risk Acceptance Letter (RAL) Example

(Government letterhead)

[GCA/Data Owner Name]
[Address]

SUBJECT: Acceptance of Risk to Classified Information

TO: [Contractor]

Reference National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M, Chapter 8, February 28, 2006 (http://www.dss.mil).

Paragraphs 8-302a, 8-305, 8-306b, 8-309, 8-310a,b 8-401, 8-610a(1)c; permit the transfer of unclassified or lower classified information from an Information System (IS) accredited by the Defense Security Service (DSS). DSS has identified certain file formats and procedures that are authorized for this transfer. However, the particular file format/procedure is not robust enough for the type or amount of information that we require.

Working in combination with a DSS Information Systems Security Professional (ISSP), an alternative to the DSS procedure for [file format(s)] has been developed. It is understood that this alternative procedure, though considered safe, increases the risk of compromise to classified information. In order to use this alternative procedure, DSS requires that the additional risk be identified to, and accepted by, the GCA or data owner.

The alternative procedure is attached for your review. If you agree with the alternative procedure and paragraph 5, please sign and return to the above address. If you have any questions, I may be reached at the number below.

It is understood that there is an inherent risk associated with the transferring of unclassified or lower classified information from a DSS accredited IS to unclassified or lower classified media. The undersigned concurs that a trusted download is necessary for [contractor name] to adequately perform work on our behalf and we accept the Alternate Procedures falls well within the governments standards for acceptable risk.

____
Signature
Customer/sponsor or data owner

____
Printed Name Phone #

14.1.25 Table of DSS Authorized File Type/Formats

Format Type	Explanation	Common File Extension(s)
ASCII	ASCII formatted information is essentially raw text just like the words you are reading now. Many applications have the ability to export data in ASCII or text format. Program source code, batch files, macros and scripts are straight text and stored as ASCII files. ASCII files may be read with any standard text editor.	.txt .dat .c .for .fil .asc .bat *(NOTE: This is not an all-inclusive list. If a file cannot be read with a standard text editor, try changing the extension to .txt. If the file still cannot be read with a text editor, it is most likely not an ASCII file.)*
Hypertext Markup Language	The document format used on the World Wide Web. Web pages are built with HTML tags (codes) embedded in the text. HTML defines the page layout, fonts and graphic elements as well as the hypertext links to other documents on the Web.	.html .htm
JPEG	Joint Photographic Experts Group (pronounced jay-peg) An ISO/ITU standard for compressing still images that is very popular due to its high compression capability.	.jpg
BMP	A Windows and OS/2 bitmapped graphics file format. It is the Windows native bitmap format. Every Windows application has access to the BMP software routines in Windows that support it.	.bmp
Graphics Interchange Format	A popular bitmapped graphics file format developed by CompuServe.	.gif

NOTE: Executable programs may not be transferred. The source code (ASCII text) may be reviewed/transferred to a lower level IS then re-compiled into executable code.

14.1.26 Mobile System Relocation Form

CONTRACTOR LETTERHEAD
(To be used when releasing IS to government activity or test site.)

(DATE)

FROM: (ISSM)
TO: (Name of government site ISSO and address)

SUBJECT: Relocation of DSS Accredited Information System (name or number of IS) from (company name) to (user agency site or test-site).

On (accreditation date) the Defense Security Service (DSS) accredited under the National Industrial Security Program Operating Manual (NISPOM) information system (IS) (name or number of IS) located at (company name) to process classified information at the (level of classified information) level. A copy of the accreditation letter is attached for your review.

(Company name) has a requirement in conjunction with (contract number) with (name of GCA) to relocate the above to (name of government site or test site) in order to process classified information for (purpose). During the period when this will be resident at (name of government site, test site, or installation, etc.) your activity must assume cognizance for the security of the system. Any movement of an accredited IS outside of the DSS-approved area changes the original intent of DSS' accreditation. As you are aware, different risks and vulnerabilities are associated with moving an IS, to include, for example, different threats to the IS or classified information, different physical security factors and different user need-to-know concerns.

Prior to the above system being relocated to your site, an authorized official of (name of site) must sign this letter and return it to the address provided. Your authorized official's signature will represent your organization's formal concurrence to accept security cognizance for the above-specified IS while it will be located at your site and under your jurisdiction. (Name of contractor) anticipates the IS (or closed area) will be removed from (name of site), and consequently your jurisdiction, by (provide approximate time of removal and location to which the system will be subsequently relocated).

If you have questions or would like to discuss this, please contact (company POC) at (telephone number) or by e-mail at (e-mail).

Sincerely,

(ISSM's Name)
(Title/Company)
Attachments: DSS Accreditation Letter
Dated (Date)
Copy to: (Cognizant DSS ISR)
CONCURRENCE:
____
(Name/Title of Authorized Official)

14.1.27 Authorized Alternate Site Locations

Alternate Site	Point of Contact
A. Location Operating Environment □ Restricted Area □ Closed Area	Contact Name Phone: Phone: Fax: Cell: E-mail:
B. Location Operating Environment □ Restricted Area □ Closed Area	Contact Name Phone: Phone: Fax: Cell: E-mail:

14.1.28 Authorized Sites for Mobile Processing

Mobile site Information	Point of Contact
A. [Facility] Type of Site: □ Contractor □ Government	Contact Name Phone: Phone: Fax: Cell: E-mail: Shipping Method and Instructions:
B. [Facility] Type of Site: □ Contractor □ Government	Contact Name Phone: Phone: Fax: Cell: E-mail: Shipping Method and Instructions:
C. [Facility] Type of Site: □ Contractor □ Government	Contact Name Phone: Phone: Fax: Cell: E-mail: Shipping Method and Instructions:

14.1.29 System Component Information Form

[Facility Information]	**System/Component Information**	**System Identification**

To relocate a system approved for Mobile Processing, this form must be completed and submitted by the Information System Security Manager (ISSM) the local DSS Industrial Security Representative (IS Rep) prior to Shipment. The owning ISSM must coordinate the movement through the local IS Rep anytime the system is relocated. The ISSM must receive concurrence from the gaining ISSM/GCA in writing prior to shipment accepting responsibility for the system or components being relocated.

Program:	Contract Number:

Owning Facility Contact Information

ISSO	Telephone	Fax	E-mail
Alternate ISSO	Telephone	Fax	E-mail
ISSM	Telephone	Fax	E-mail

Relocation Site Information

□ Government Site	□ Contractor Site	Gaining Facility Name:

Address	City	State	Zip Code

Specific Processing Location (Bldg/Room)	Cage Code

Security Office Point of Contact (FSO/GCA/ISSM)	Telephone	Fax	E-mail

DSS ISR Name	Telephone
Program Point of Contact	Telephone

Duration of Visit – Date from:	Date to:	Shipping Date (mm/dd/yy)

Authorization to process at the relocation site

The following documentation is provided authorizing classified processing at the relocation site.

	Yes	No	Comment
Contractual Relationship	□	□	
Technical Instruction	□	□	
Statement of Work	□	□	
Provisions within Special Instructions	□	□	
Other	□	□	

Relocation Site Activities

Will the equipment be moving from the contractor facility to a government location?	□ Yes	□ No
If so, how will the equipment be handled? Will the equipment leave possession of the contractor?		
Does the equipment return to the contractor facility when not in use?	□ Yes	□ No

System Connection Requirements

If the relocation site is another contractor facility, will the system be connected to the gaining facility's network?	☐ Yes	☐ No
If so, is the connection authorized and approved by DSS? Provide details of approved connection, to include MOU.		
Will the system be connected to the gaining facility's network (if government site)?	☐ Yes	☐ No

Privileged User Information /Relocation Site ISSO			
Users Identified Below have been Briefed/Trained and are Responsible for Conducting Weekly Audits and Antivirus Updates			
Relocation Site ISSO Name	**Privileged Account**	**Briefing/Training Date**	**Briefed by Name**
Relocation Site Alternate ISSO Name	**Privileged Account**	**Briefing/Training Date**	**Briefed by Name**

IS System or List of Components being Moved to the Relocation **Site**					
Quantity	Make/Model	Serial Number	Memory	Non-volatile?	Method of Sanitization

14.1.30 Mobility Plan Sample

For the Movement of Classified Information Systems (IS)

Facility
Address
City, State Zip Code

Date of Mobility Plan
Revision Number

A. Introduction
This plan outlines the procedures for the transporting of classified IS equipment between [Facility], and various sites as listed in the Mobile Processing Plan attached to the IS Profile.

B. Description of Equipment
Equipment consists of computers, components and test equipment to be used in support of field tests, flight test, customer reviews and meetings. See IS Profile for list of equipment.

C. Identification of Participating Government and Contractor Representatives

[Facility]
Name of ISSM
Address
Contact information

Local Defense Security Service Representative
Name of IS Representative
Address
Contact information

D. Shipping and Transportation
Movement of the equipment will originate from [Facility]. Equipment will be transported to various sites listed in the Mobile Processing Procedures attached to the IS Profile. The ISSM will notify the DSS Representative prior to shipping the system to/from any off-site location. All equipment will be shipped either as classified at system approval level or downgraded to an unclassified state, security seals affixed. All remaining classified components will be properly shipped or hand carried.

E. Notification of Transportation
The ISSM will be notified of the upcoming shipment as early as possible.
The following information must be provided:
-Program name
-Classification
-Will the shipment contain hazardous material? If so, provide MSDS sheet or IHC letter from customer
-Size and weight of equipment
-Who owns the equipment, is it GFE?

F. Hand Carry (Courier)
You are reminded that hand carry (courier) is only done in emergency situations. When couriers are to be used, the program must justify why a hand carry must occur rather than utilizing approved classified mailing or shipping capabilities. This must be authorized by the Security Manager. Each courier must be identified by name, title, payroll number, as well as the name of the program being supported. Flight

itinerary and vehicle rental information must be furnished. Couriers must be cleared at the appropriate level and be thoroughly briefed on their security responsibilities. Each courier will be issued a "Courier Authorization" and will be provided emergency telephone numbers.

G. Responsibilities of Receiving Facility

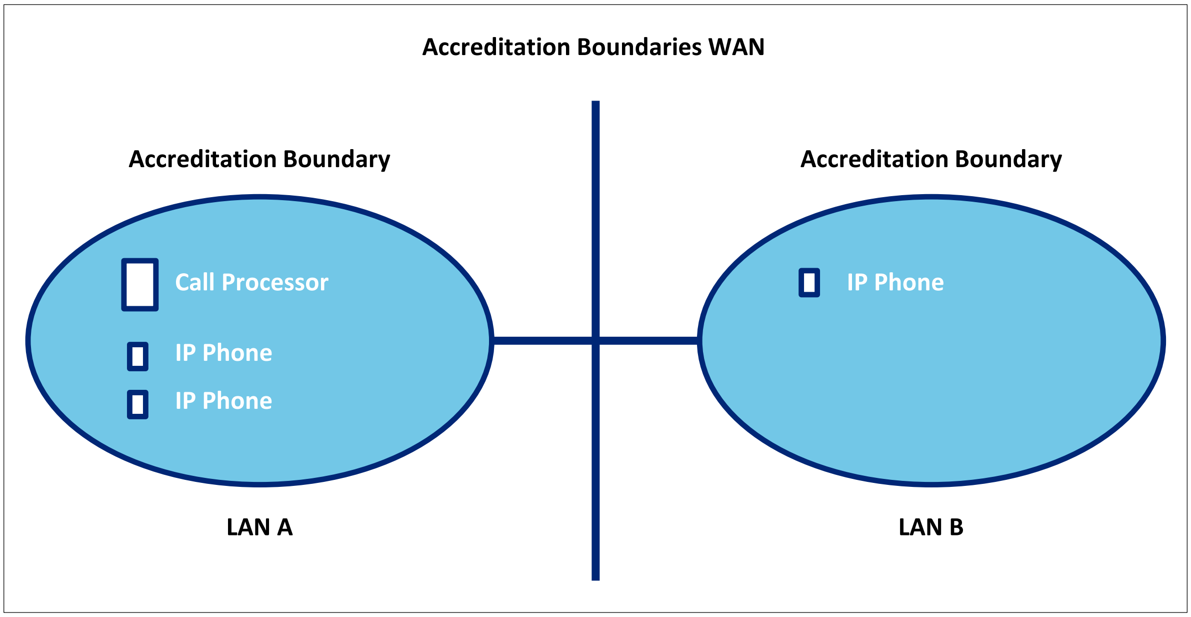
- The recipient organization must notify the dispatching organization and [Facility] Security of any security relevant problems that occur.
- The recipient organization must notify the dispatching organization and [Facility] Security of any discrepancies in the documentation or equipment.

14.1.31 Protected Distribution System Approval Request

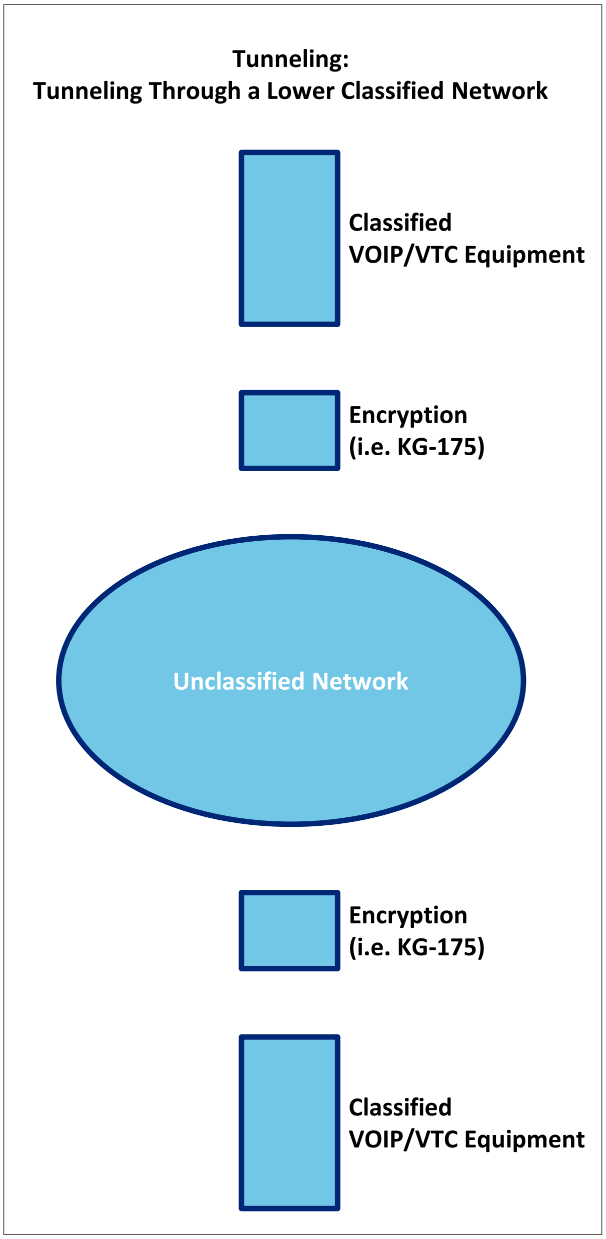
All requests for PDS approval will include all of the following information:

Installation Site	Include all relevant information about the organization where the PDS will be installed, and a point of contact's name and phone number. Be sure to include points of contact for each area that houses the PDS.
Installation Activity	Include all relevant information regarding the organization responsible for the installation of the PDS, including a point contact's name and phone number.
System Information	Provide a description of all components directly connecting to the PDS. Be sure to include the type of cabling being used and the electrical parameters.
Security Profile	Indicate all levels of classification that are being protected by the PDS. Provide a percentage breakdown of each level of classification in the PDS. Be sure to include caveats and special categories.
Facility Security	▪ Provide a map of the residential and commercial area and indicate the facilities approximate location on the map as Appendix A. ▪ If the facility is fenced, provide the location of all fencing on the map and the type of fencing construction. Be sure to indicate if an Intrusion Detection System (IDS) is installed. ▪ Indicate all automobile, pedestrian and amphibious access points on the map. Include whether guards are posted at each access point and the hours that the access points are open. ▪ Indicate if the following are being used: □ Personnel badge recognition system. □ Access lists. □ Escorts for uncleared personnel. □ Vehicle registration control system. □ Employee registration control system. □ Visitor registration control system. □ Tradesman registration control system.
Building Security	▪ Provide a floor plan of the building(s) within which the PDS is installed as Appendix B. Describe the exterior and interior construction, and identify whether or not the building's perimeter has an IDS installed. ▪ Indicate access points to all of the buildings. Include windows accessible from the ground, fire escapes and any tamper protection devices installed on the windows. ▪ Indicate whether guards are posted at the building access points, the hours the access points are open, and whether cipher/simplex locks are used for access control to the building. ▪ Describe the types of doors and locks securing the access points. ▪ Indicate whether a personnel badge recognition system is in use and if access lists are maintained. ▪ Indicate the clearance level of personnel entering the building and if a clearance is required for unescorted access. ▪ Specify how the movement and operation of custodial, maintenance, and vending personnel is controlled, and if this requires an escort or continuous surveillance for uncleared personnel.
Protected Distribution System	▪ Indicate on the floor plans and on a map the location and routing of the PDS, to include any PDS that is buried underground between buildings. ▪ Provide the classification level of the area controlled, and indicate if uncleared personnel are monitored. ▪ Describe the construction of the PDS. ▪ Describe the inspection procedures for the detection of tampering. ▪ Indicate whether or not the PDS will be alarmed; describe the alarm system in detail.

14.1.32 WAN Accreditation Boundaries



14.1.33 Tunneling



This is the end of the document.