Defense Security Service
Office of the Designated
Approving Authority

Industrial Security Field Operations (ISFO)
Process Manual
for the
Certification and Accreditation
of
Classified Systems under the
National Industrial Security Program
Operating Manual (NISPOM)

Revision 3
June 2011

Title Page

Document Name:	Industrial Security Field Operations (ISFO) Process Manual for the Certification and Accreditation Of Classified Systems under the National Industrial Security Program Operating Manual (NISPOM) and NIST 800-53
Publication Date:	March, 2006
Revision Date:	June, 2011
Document Owner:	Defense Security Service (DSS) Industrial Security Field Operations (ISFO) Office of the Designated Approving Authority (ODAA)
Point of Contact:	Questions regarding the process or the figures provided should be directed to the Office of the Designated Approving Authority at ODAA@dss.mil. Defense Security Service Office of the Designated Approving Authority Russell-Knox Building 27130 Telegraph Road Quantico, VA 22134 www.dss.mil

Table of Contents

1 Preface 1
2 Introduction 2
3 Purpose 2
4 Introduction of NIST 800-53 Controls 2
5 SECURITY CONTROLS 4
5.1 MANAGEMENT CONTROLS 4
5.1.1 SECURITY PLANNING (PL) 4
5.1.1.1 Roles and Responsibilities 4
5.1.1.1.1 Office of the Designated Approving Authority (ODAA) 5
5.1.1.1.2 Information System Security Professional (ISSP) 5
5.1.1.1.3 Information Systems Security Manager (ISSM) 5
5.1.1.1.4 ISSMs for Multiple Facility Organizations (MFO) 6
5.1.1.1.5 Information System Security Officer (ISSO) 7
5.1.1.1.6 Network ISSO 7
5.1.1.1.7 Users of Information Systems (IS) 8
5.1.1.2 Information System (IS) Types 13
5.1.1.2.1 Multiuser Standalone (MUSA) 13
5.1.1.2.2 Local Area Networks (LAN) 14
5.1.1.2.3 Interconnected System/Wide Area Network (WAN) 14
5.1.1.2.4 Virtualization 15
5.1.1.2.5 Special Categories 15
5.1.1.2.5.1 Single-User, Standalone Systems (SUSA) 15
5.1.1.2.5.2 Periods Processing 16
5.1.1.2.5.3 Pure Servers 17
5.1.1.2.5.4 Test Equipment 17
5.1.1.2.5.5 Special Purpose, Tactical, Embedded Systems 17
5.1.1.2.5.6 Copiers 19
5.1.2 SECURITY ASSESSMENT AND AUTHORIZATION (CA) 20
5.1.2.1 Types of Security Plans 20
5.1.2.1.1 System Security Plan (SSP) 21
5.1.2.1.2 Master System Security Plan (MSSP) 21
5.1.2.2 Information System Connections 36
5.1.2.2.1 Network Security Plans (NSP) 36
5.1.2.2.1.1 Memorandum of Understanding (MOU)/Interconnected Systems Agreement (ISA) 53
5.1.2.2.1.1.1 MOU Requirements 53
5.1.2.2.1.1.2 MOU Content 54
5.1.2.2.1.1.3 MOU Sample 55
5.1.2.2.1.2 Defense Information Systems Network (DISN) Connections 59
5.1.2.2.2 International System Security Plans 60
5.1.2.3 Types of Networks 63

5.1.2.3.1 Unified Networks 63
5.1.2.3.2 Interconnected Networks 63
5.1.2.3.3 Network Security Plans (NSP) 63
5.1.2.4 Plan of Action & Milestone (POA&M) 64
5.1.2.4.1 Plan of Action and Milestone Template (POA&M) 66
5.1.3 CONFIGURATION MANAGEMENT (CM) 68
5.1.3.1 Configuration Management Process 69
5.1.4 PROGRAM MANAGEMENT (PM) 70
5.1.5 RISK ASSESSMENT (RA) 71
5.1.5.1 Risk Assessment Requirements 71
5.1.5.2 Enhanced Controls 72
5.1.6 SYSTEM AND SERVICES ACQUISITION (SA) 73
5.1.6.1 Certification and Accreditation (C&A) 73
5.1.6.1.1 C&A Life Cycle 73
5.1.6.1.2 C&A Process 75
5.1.6.1.2.1 Certification 76
5.1.6.1.2.2 Review 76
5.1.6.1.2.3 Accreditation 78
5.1.6.1.2.4 Verification 78
5.1.6.2 Software Protections 84
5.2 OPERATIONAL CONTROLS 86
5.2.1 AWARENESS AND TRAINING (AT) 86
5.2.1.1 Security Education 86
5.2.1.2 Cleared Contractor Training 87
5.2.2 CONTINGENCY PLANNING (CP) 88
5.2.2.1 Contingency Planning 89
5.2.2.2 System Recovery and Assurances 89
5.2.3 INCIDENT RESPONSE (IR) 90
5.2.3.1 Classified Spills 90
5.2.3.1.1 Incident Response Plan 91
5.2.3.1.2 Sanitizing and Declassifying 92
5.2.3.1.3 Classified Spill Cleanup Procedures 92
5.2.3.1.4 Wiping Utility 92
5.2.3.1.5 DSS-Approved Classified Spill Cleanup Plan 94
5.2.3.1.6 Contamination Cleanup Procedures 96
5.2.4 MAINTENANCE (MA) 115
5.2.4.1 Maintenance 115
5.2.4.2 Cleared Maintenance Personnel 115
5.2.4.3 Uncleared (or Lower-Cleared) Maintenance Personnel 116
5.2.4.4 Remote Maintenance 116
5.2.5 MEDIA PROTECTION (MP) 117
5.2.5.1 Media Protection 117
5.2.5.2 Hardware Marking 119

5.2.5.3 Trusted Download 119
5.2.5.3.1 Trusted Download Procedures 120
5.2.5.3.1.1 DSS Authorized File Type/Formats 124
5.2.5.3.1.2 DSS File Transfer Procedures 125
5.2.5.3.1.3 DSS Authorized Procedure (Windows-Based) 127
5.2.5.3.1.4 DSS Authorized Procedure (Unix) 131
5.2.5.3.1.5 Alternate Trusted Download Risk Acceptance Letter (RAL) Example 135
5.2.5.4 Mobile Systems 136
5.2.5.4.1 Mobile Processing Procedures 140
5.2.5.5 Clearing and Sanitization 150
5.2.5.5.1 Clearing 150
5.2.5.5.2 Sanitizing 150
5.2.5.5.3 Magnetic Tape 150
5.2.5.5.4 Organization Destruction Options 151
5.2.5.5.5 DSS Clearing and Sanitization Matrix 153
5.2.6 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE) 158
5.2.6.1 Physical Security (8-308, 5-306, 5-308, 6-104) 158
5.2.6.2 Hardware and Software Protection 159
5.2.6.3 Protected Distribution System (PDS) 159
5.2.6.4 Emergency Procedures (5-104) 167
5.2.6.5 TEMPEST (11-100) 167
5.2.7 PERSONNEL SECURITY (PS) 168
5.2.7.1 Personnel Security Clearance Verification 169
5.2.7.2 Personnel Sanctions 169
5.2.8 SYSTEM AND INFORMATION INTEGRITY (SI) 170
5.2.8.1 Flaw Remediation 170
5.2.8.2 Unclassified Software Review 171
5.2.8.3 Antivirus 171
5.3 TECHNICAL CONTROLS 172
5.3.1 ACCESS CONTROL (AC) 172
5.3.1.1 Access Control 174
5.3.1.2 Separation of Function 174
5.3.1.3 Logon Banner 174
5.3.1.4 Session Controls 175
5.3.1.4.1 Successive Login Attempt Controls 175
5.3.1.4.2 User Inactivity 176
5.3.1.4.3 Logon Notification (PL-2/PL-3) 176
5.3.1.5 USB Devices and Ports 176
5.3.1.6 Radio Frequency ID (RFID) Tags 176
5.3.1.7 Secure Wireless LANs (S-WLAN) 177
5.3.1.8 Foreign Ownership, Control & Influence (FOCI) 177
5.3.2 AUDIT AND ACCOUNTABILITY (AU) 186

5.3.2.1 Audit Requirements 187
5.3.2.2 Security Seals 188
5.3.3 IDENTIFICATION AND AUTHENTICATION (IA) 189
5.3.3.1 Identification and Authentication Management 190
5.3.3.2 Generic or Group Accounts (8-505) 190
5.3.3.3 Password Policy 191
5.3.3.4 BIOS Password 191
5.3.4 SYSTEM AND COMMUNICATIONS PROTECTION (SC) 192
5.3.4.1 Data Transmission Protection 193
5.3.4.2 Network Management and Protections 193
5.3.4.2.1 Controlled Interfaces 194
5.3.4.3 Classified Voice over IP (VOIP)/Video Teleconferencing (VTC) 195
5.3.4.4 Thin Client Systems 197
5.3.4.5 Masking/Coding/Disassociation 197
6 System Security Plan Submission Process 199
6.1 Variances 206
7 Defense Industrial Base Cyber Security Accreditation Process (DIBNET) 211
8 Reference List 214
9 Glossary 215

Figures

Figure 1 Flow Diagram for Self-Certification Under an MSSP 27
Figure 2 NSP Accreditation Process Diagram 43
Figure 3 Overall Network Security Profile 46
Figure 4 NSP Architecture Diagram Example 48
Figure 5 Network Host Security Profile 49
Figure 6 Network Node Security Profile Form 51
Figure 7 Flow Diagram For Initial (M)SSP 83
Figure 8 Flow Diagram for a Reaccreditation and Re-evaluation 84
Figure 9 Main Cleansing Process Checklist 99
Figure 10 Microsoft Exchange Server Cleansing Checklist 100
Figure 11 Novell GroupWise Server Cleansing Checklist 105
Figure 12 Desktop Client Workstation Cleansing Checklist 110
Figure 13 Process for Clearing a Blackberry 111
Figure 14 Trusted Download Authorization Form 133
Figure 15 Trusted Download Record 134
Figure 16 Authorized Alternate Site Locations 140
Figure 17 Authorized Sites for Mobile Processing 142
Figure 18 System Component Information Form 143
Figure 19 Matrix for Degaussing Media 151
Figure 20 FOCI Process Flowchart 181
Figure 21 Accreditation Boundaries 195

Figure 22 Tunneling 196

Tables

Table 1 Roles and Responsibilities..... 9
Table 2 Table for Self-Certification 33
Table 3 MSSP IS Tracking Form 35
Table 4 DSS Authorized File Type/Formats 124
Table 5 Clearing and Sanitization Matrix 154
Table 6 Subject Line Requirements for Plan Submissions 201

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 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, the process manual is designed to provide a full spectrum resource to newly appointed contractor Information Systems Security Managers (ISSM) and well seasoned Information Systems Security Officers (ISSO).

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. This process manual is not directive in nature, but adherence to the standards in this process manual by NISP contractors is recommended in order for DSS to be able to expeditiously issue Interim Approvals to Operate (IATO) and Approvals to Operate (ATO).

The Risk Management Framework (RMF) for this process manual has been aligned with the Committee on National Security Systems Instruction (CNSSI) 1253 High-Impact confidentiality security objective. In producing the CNSSI 1253 High-Impact baseline set of controls, the following is assumed: all users have all required clearances, formal access approvals, and the need-to-know (NTK) for all information on the information system (IS).

This process manual will be updated twice a year and may be requested on the DSS web site. Therefore, it is the responsibility of all those involved in the C&A process to stay abreast of the current Industrial Security Field Operations (ISFO) Process Manual so that consistency is maintained and an understanding of the current processes is being followed.

This process manual is not intended, does not, and may not 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.

Implementation of the ISFO Process Manual is effective September 12, 2011 for new plans, or plans that require reaccreditation due to a security relevant change. Current accreditations will be valid until expiration.

2 Introduction

The Director, DSS is responsible for C&A oversight of cleared NISP contractors' IS. 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.

3 Purpose

The ODAA was created in the autumn of 2005. Aligned with this new ODAA standup were efforts to provide cleared contractors with greater efficiency and flexibility within the C&A process. The result was the centralization of the DSS C&A process and clarification of numerous C&A concepts.

The formation of this single, centralized body and changes in several fundamental DSS C&A concepts necessitated a number of changes in the way System Security Plans (SSP) and Master System Security Plans (MSSP) are submitted for approval. As such, this process manual was created and revised to clearly explain the changes that have been made, as well as clarify all steps of the C&A process for the cleared contractor's classified IS.

As the office of the ODAA matures, it has been determined that numerous opportunities exist that could significantly enhance the C&A process through establishing standards and clarification. For these reasons it was determined that a detailed process manual would be appropriate. This process manual will identify the personnel roles and responsibilities involved in the C&A process, description of typical IS encountered, and clarification of the C&A process itself.

4 Introduction of NIST 800-53 Controls

Included in this version of the process manual are the National Institute of Standards and Technology (NIST) 800-53 controls, based on NIST Special Publication 800-53 Revision 3, dated August 2009. NIST 800-53 controls are mapped to the corresponding NISPOM reference and are addressed by the stated NISPOM reference.

Below is an example of the NIST 800-53 controls included in each section, and how they are mapped to the NISPOM.

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	**CNTL NO.**	**CONTROL NAME**	**NISPOM Reference**	**PM location Para heading**	**Protection Levels Confidentiality**
MANAGEMENT		**Planning**			
* not addressed **not contractually imposed	PL-1	Security Planning Policy and Procedures	8-101	Roles and Responsibilities	1
	PL-2	System Security Plan	8-610	Information System Types	1,2,3
	PL-2 (1)	System Security Plan Control Enhancement		Information System Types	
	PL-2 (2)	System Security Plan Control Enhancement		Information System Types	
	PL-4	Rules of Behavior	8-609	Roles and Responsibilities	1,2,3

Column 1 displays the family which the controls fall under. Column 2 displays the NIST 800-53 control number. In addition, the parenthesized numbers indicate the control enhancements that are required. Some control enhancements are only required for specific Protection Levels (PL). Column 3 displays the NIST 800-53 control name. Column 4 displays the mapping of NIST 800-53 controls to the NISPOM. Column 5 indicates the process manual paragraph heading in which the NIST control applies. And column 6 displays the PL.

5 SECURITY CONTROLS

The documentation of the C&A process is divided into three categories:

- Management Controls
- Operational Controls
- Technical Controls

5.1 MANAGEMENT CONTROLS

5.1.1 SECURITY PLANNING (PL)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	**CNTL NO.**	**CONTROL NAME**	**NISPOM Reference**	**PM location Para heading**	**Protection Levels Confidentiality**
MANAGEMENT		**Planning**			
* not addressed **not contractually imposed	PL-1	Security Planning Policy and Procedures	8-101	Roles and Responsibilities	1
	PL-2	System Security Plan	8-610	Information System Types	1,2,3
	PL-2 (1)	System Security Plan Control Enhancement		Information System Types	
	PL-2 (2)	System Security Plan Control Enhancement		Information System Types	
	PL-4	Rules of Behavior	8-609	Roles and Responsibilities	1,2,3
	PL-5	Privacy Impact Assessment		*	
	PL-6	Security-Related Activity Planning		*	

5.1.1.1 Roles and Responsibilities

The ODAA is delegated the responsibility for carrying out the DSS C&A mission for cleared contractor IS under the NISP. ODAA C&A oversight is comprised of reviewing the (M)SSPs and supporting documentation, performing onsite validations and inspections to verify system controls are in place and operating as intended, providing advice and assistance to DSS and cleared contractors, and promulgating guidance and policy interpretation. The ODAA is the sole accrediting authority of contractor classified systems under the NISP. The ODAA oversees the C&A of contractor classified systems to verify it is consistent with national computer security information assurance policy and

performed in an efficient and effective manner. The ODAA also checks to see that systems maintain their accreditation security posture throughout their life cycle by conducting onsite validations and annual reviews.

The ODAA process includes DSS Field Operations staff known as Industrial Security Representatives (IS Reps). The ODAA has established a formal in-house C&A training program (Certified C&A Reviewer) so that IS Reps formally obtain training in the ODAA processes.

5.1.1.1.1 Office of the Designated Approving Authority (ODAA)

The ODAA is delegated the responsibility for the DSS mission for cleared contractor IS C&A oversight. ODAA C&A oversight is comprised of reviewing the (Master) System Security Plan ((M)SSP) and supporting documentation, performing onsite validations and inspections to verify system controls, providing advice and assistance to DSS and cleared contractors, and promulgating guidance and policy interpretation. The ODAA is the sole accrediting authority of industry classified systems.

5.1.1.1.2 Information System Security Professional (ISSP)

The primary role of the ISSP is technical in nature. The ISSP will evaluate, certify, and inspect all IS technical features and safeguards for all IS. Additionally, the ISSP will review the (M)SSPs to determine if the physical, 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 inspections to verify that the protection measures as certified by the ISSM have been implemented on the IS.

Contractor Personnel

5.1.1.1.3 Information Systems Security Manager (ISSM)

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

ISSM training includes both technical and policy aspects. If the ISSM is not technically competent to securely configure the systems under their purview, there must be a local Information Systems Security Officer (ISSO) that can configure and manage the systems to verify system security controls are in place and operating. During onsite validation visits and security reviews, 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 and local ISSO. If it is determined during an IS certification visit or security review 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 on the "IS Certification Report," or as a security review finding and may be cause for not approving an accreditation or withdrawing an 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 (if workload requires it) 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 must 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.

5.1.1.1.4 ISSMs for Multiple Facility Organizations (MFO)

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. Per ISL 2007-01, Article #4, the ISSM who has been granted self-certification authority for like systems under approved Master System Security Plans (MSSP) may self-certify systems for those facilities where he or she has been designated as the ISSM. 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 (Note: DSS will consider exceptions to this reasonable distance criterion on a case by case basis. Such requests must specify how the ISSM will carry out oversight and other responsibilities from afar). DSS considers approximately one to two hours driving time between locations as a reasonable distance.

- The aggregate complexity of the collective facilities is such that only one ISSM is required.

- The ISSM is trained to a level commensurate with the overall complexity of all facilities.

- Each facility has at least one appointed ISSO who has been assigned the duties identified in NISPOM paragraph 8-104.

- 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.

5.1.1.1.5 Information System Security Officer (ISSO)

The ISSO (NISPOM 8-104) is appointed by the ISSM when the contractor has multiple accredited IS, is 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 be able to configure and manage the security configuration of the systems under their purview.

5.1.1.1.6 Network ISSO

In many cases there are requirements for cleared contractors to communicate and share information with each other in support of a large contract (or multiple contracts). In order for contractors to exchange classified information they must verify that each site (node) has an accredited system to join this interconnected system/wide area network (WAN). A network security plan (NSP) must be in place before any classified information can be exchanged. Within each NSP, a Network ISSO must be identified to manage the connection process of each node that is joined to the WAN. Generally, the prime contractor is considered the host. The host contractor will appoint an individual located at the host site as the Network ISSO. The duties of a Network ISSO 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.

- Serve as focal point for the network and the connecting node ISSMs, to include collecting network security profiles.

- Generate and maintain approvals for the NSP and, if applicable, the Memorandum of Understanding (MOU).

- Verify all systems on the network have an accredited plan.

- Ensure proper network security procedures are developed and implemented.

- Perform or oversee weekly reviews of the system 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 to DSS to 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.

5.1.1.1.7 Users of Information Systems (IS)

NISPOM paragraph 8-105 identifies two types of IS users, privileged and general. From a security standpoint, this is the most basic user structure. Depending on the complexity and number of accredited IS at the contractor facility, users can have multiple roles. Each role has separate and unique requirements that are vital to successful IS operations. The ISSP, IS Rep, and ISSM, will review the various user roles and responsibilities.

Table 1 Roles and Responsibilities

Participant(s)	Responsibilities
Defense Security Service	
HQ Office of the Designated Approving Authority (ODAA)	• Accreditation authority for contractor IS processing classified information. • Approval signatory on all SSPs • Approval signatory on all Master SSPs (MSSPs) • Approval signatory on all Network Security Plans (NSPs) • Approval signatory on all MOUs/MOAs
Regional Designated Approving Authority (RDAA)	• Supervises Team Leaders • Subject matter expert on information systems • Coordinates with field on C&A issues • DAA responsibilities and authority within their region • Oversees and manages status of IT security at contractor facilities within region and is cleared contractor's primary point of contact for C&A issues • Reports to the Regional Director
Information Systems Security Professional (ISSP)	• Subject matter expert in information systems • Reviews (M)SSPs • Notifies the DAA on system compliance • Performs certification, validation, and annual reviews on IS • First level of inquiry of cleared contractors issues and questions
Regional Director (RD)	• Directs the FOCs • Verifies adequate IS Rep support to the C&A process
Field Office Chief (FOC)	• Directs the IS Reps in certification support and annual reviews
Industrial Security Representative (IS Rep)	• Primary DSS POC for Industry • Performs validation and annual reviews on certain IS (if qualified) • Notifies the FOC and DAA on IS compliance • Reviews (M)SSPs as needed (if qualified) • Coordinates with 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 in support of contractors and IS under the NISP • Spot-checks (M)SSPs as needed

Industry	
Contractor Management	• Verifies that the ISSM is granted access and trained to a level commensurate with the complexity of the contractor's IS and the level of classified information processed • Publishes and promulgates an IS security policy addressing the classified processing environment • Are Key Management Personnel (KMP).
Information Systems Security Manager (ISSM)	• Employee appointed by management with oversight responsibility for the development, implementation, and evaluation of the IS security program • Develops (M)SSPs which comply with the NISPOM • Verifies IS are configured in accordance with security requirements and the (M)SSPs • Informs DSS of security relevant changes to accredited systems • In an MFO, can have oversight of the IS security program of multiple contractors subject to the following conditions: →Travel time by car between locations must be within a reasonable distance. Approximately one to two hours is considered reasonable unless approved on a case-by-case basis →Complexity of any one cleared entity or all cleared entities is such that only one ISSM is required →ISSM is trained to a level commensurate with the overall complexity of all IS →Each contractor has an appointed ISSO • Must have access and need-to-know for all information processed on all accredited IS. In large contractor facilities, the ISSM may supervise hundreds of ISSOs; in small contractor facilities, the company owner may also be the ISSM and the general user of the accredited IS • 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 an alternate ISSM to act with full authority in the absence of the primary ISSM or simultaneously if work load requires it. However, the primary ISSM is still responsible • For very large contractors, may appoint subordinate ISSMs but the responsibility and accountability rests with the primary ISSM
Information Systems Security Officer (ISSO)	• Supports the ISSM in their efforts to implement security requirements as mandated by the NISPOM • May directly participate in the C&A process • Appointed by the ISSM 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 • ISSOs must have access and need-to-know, and formal access approvals for all information processed on accredited IS under his or her cognizance • ISSO must be local with the systems they manage
Network 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, to include collecting network security profiles • Generates and maintains approvals for the Network Security Plan (NSP) and the Memorandum of Understanding (MOU), if applicable • Verifies all systems on the network have an accredited plan • Assures proper network security procedures are developed and implemented • Conducts weekly reviews of the system to verify that only connections that are accredited and exhibited on the topology diagram are connecting to the system • Evaluates the impact of system and network changes and applies for re-approvals as needed • Reports anomalies or violations to DSS and any other accrediting authorities with nodes on the network
Escort	• Assigned by the ISSM or ISSO to verify that visitor and maintenance engineer access to the IS is consistent with the purpose of the visit • Must have access and need-to-know, and formal access approvals for the IS in which he or she is acting as escort • Must monitor maintenance activities and record them in the maintenance log
General User	• Inputs or modifies information on an IS • Authorized by the ISSM or ISSO to process classified information on an accredited IS • Must have access and need-to-know, and formal access approvals appropriate to the protection level PL of the IS to be accessed • 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 access and need-to-know and formal access approvals for all information processed on accredited IS to

	which he or she has access • Must have working knowledge of system functions, security policies, technical security safeguards, and operational security measures • Number of privileged users must be limited to the minimum needed to manage the accredited IS • Must have unique ID to track activity • Subordinate to the ISSM or ISSO on all matters related to IS security
System/Network Administrator	• Privileged user with operational responsibility for the accredited IS(s) • Usually assigned to large, multiuser IS or contractor facilities with interconnected IS
System Analyst	• Privileged user with software responsibility for the accredited IS(s) • Reports to the system/network administrator but coordinates with the ISSM or ISSO on all security-related matters
System Operator	• Privileged user responsible for the daily operations of the IS • Usually the general user on standalone machines and/or workstations • Usually responsible for IS upgrading/downgrading and audit and media sanitizing on accredited IS under his or her cognizance • Might act as an escort to individuals who are not authorized access to classified information or maintenance personnel and coordinate all security matters with the ISSM or ISSO
Maintenance Engineer	• Person who performs maintenance or diagnostics on the accredited IS(s) • Must be a U.S. citizen; eligibility for access not required but preferred • If authorized access to classified information an escort is not required, provided need-to-know controls are implemented. A technically knowledgeable escort who is authorized to have access should remain in the area to verify that security procedures are followed • If not authorized access, must be escorted. Can have keyboard access provided monitoring is performed, but cannot initiate or terminate the IS and must use a separate, unclassified copy of the operating system labeled "UNCLASSIFIED – FOR MAINTENANCE ONLY"
Facility Security Officer (FSO)	• Supports the ISSM in their efforts to implement security requirements as mandated by the NISPOM

5.1.1.2 Information System (IS) Types

There are many IS types and system configurations that operate within cleared contractor facilities. However, the three predominant IS types are the Multiuser Standalone (MUSA), the Local Area Network (LAN) and the Wide Area Network (WAN). Single User Standalone systems (SUSA) will be separately addressed under a separate section of the process manual.

5.1.1.2.1 Multiuser Standalone (MUSA)

Approximately half the plans submitted to ODAA consist of the MUSA. The physical security parameters within the (M)SSPs vary between closed areas and various configurations of restricted areas. 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) shall consider the systems as such in determining the protection level and the resulting security requirements. ODAA further defines 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. 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. With a SUSA, there is only one user that is held accountable, therefore, technical security features are not required to be enabled. Because of the vast differences between the technical security requirements of the MUSA and SUSA forethought should be given in considering 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
Physical security:
- Closed area
- Restricted area

Operating system must be NISPOM compliant, or have a risk acceptance letter (RAL) from the GCA

5.1.1.2.2 Local Area Networks (LAN)

A Local Area Network (LAN) consists of two or more IS connected together in close proximity for the purpose of sharing information. Similar to the MUSA, almost half the plans submitted to ODAA consist of LANs. The physical security parameters within the (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 generally reside in closed areas. A LAN can be as simple as two laptops connected together 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

Operating system must be NISPOM compliant, or have a risk acceptance letter (RAL)
Peer-to-peer
Client-server/Active Directory

5.1.1.2.3 Interconnected System/Wide Area Network (WAN)

Interconnected System/Wide Area Network (WAN) is a computer network that covers a broad area (i.e., 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) 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.

5.1.1.2.4 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 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 shall document the use and purpose of the virtual machine within the (M)SSP.

5.1.1.2.5 Special Categories

(NISPOM 8-500) The requirements of NISPOM Chapter 8 are written for the general-purpose or office automation system and personal computer. Including security requirements for components such as weapons or tactical systems, test stands, simulators, or embedded components (NISPOM 8-504) that can be integral elements of a larger IS would be almost impossible. To apply the general requirements of Chapter 8 in these instances may result in unnecessary costs and adversely impact operations (Article #34, Industrial Security Letter (ISL) 2007-01). The following are examples of special categories:

- SUSA
- Period Processing
- Pure Server
- Test Equipment

5.1.1.2.5.1 Single-User, Standalone Systems (SUSA)

NISPOM Chapter 8 (8-501) distinguishes between standalone, single-user and standalone, multiuser 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, clearing of memory is all that is required when changing between classification levels, information sensitivity, or users.

Extensive technical protection measures are normally inappropriate and inordinately expensive for single-user, stand-alone systems. The CSA can approve administrative and

environmental protection measures for such systems, in lieu of technical ones. Systems that have one user at a time, but have a total of more than one user with no sanitization between users, are multiuser systems, and the CSA shall consider the systems as such in determining the protection level and the resulting security requirements. Systems that have one user at a time, are sanitized between users and periods of different classification/sensitivity, are periods processing systems.

Manual logs have been authorized for single-user standalones, however, DSS encourages the use of automated audit trails whenever possible.

5.1.1.2.5.2 Periods Processing

A. 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.

   (NISPOM 8-502a) One advantage to periods processing is that an IS 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 or IS Rep will verify with the ISSM that the different processing times are established for the different classification, sensitivity of information, or users.

   If an IS 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.

B. Sanitization After Use: NISPOM paragraphs 8-301 and 8-502(b) require IS resources and media to be sanitized before and after periods of processing, and prior to releasing from classified information controls or for re-use at a lower classification level. Only clearing is required if the IS is not being "released" (e.g., not physically protected at the higher level) to users with a lower access levels or accredited at the TOP SECRET level.

C. Sanitization between Periods: NISPOM paragraph 8-502(c) requires the IS to be sanitized between different processing sessions. Only clearing is required if the IS is not being "released" (e.g., not physically protected at the higher level) to users with a lower access level or accredited at the TOP SECRET level.

D. Separate media for each period.

E. Audit: When the IS being used for periods processing is not capable of automated logging, manual logging is required.

F. During the validation process and on security reviews, the IS Rep or ISSP 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.

5.1.1.2.5.3 Pure Servers

(NISPOM 8-503) This category of specialized systems does not fit the protection level criteria, as does the general-purpose or office automation system. As an example, a pure server does not have users in the traditional sense, but has clients. The only users on a pure server are privileged users that maintain the device. More and more, software maintenance of pure servers is being performed remotely. No longer does the system or network support staff have to be physically located at the pure server to perform maintenance. Instead, the support staff logs into the device remotely. This requires I&A mechanisms, auditing, and access controls. Each pure server is different, serves a specialized purpose, and has to be reviewed by the ISSP before a determination is made as to what, if any, technical security features are required.

5.1.1.2.5.4 Test Equipment

Test equipment with non-volatile memory that is going to process or retain classified information requires accreditation. When drafting an (M)SSP for test equipment, the generic NISPOM Section (8-500) will be referenced. 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.

5.1.1.2.5.5 Special Purpose, Tactical, Embedded Systems

Chapter 8 identifies these types of systems as "special category," and allows for protection measures and safeguards to be implemented on a case-by-case basis. Special purpose/tactical equipment is designated as such by the GCA/customer. Written designation by GCA/customer to be included with (M)SSP. If the entire system is special

purpose/tactical no (M)SSP is required, just a Standard Operating Procedures (SOP) with the letter from the GCA/customer.

A. 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 (ISL 2007-01, #40).

B. A simple tactical/embedded/special purpose system may, in some instances be evaluated by the IS Rep. Examples of a simple system are guidance sets where the contractor will utilize destruction or will send the unit to the government customer or test equipment with volatile memory. A complex tactical/embedded/special purpose system may need an ISSP evaluation. Examples of a complex system are test equipment with non-volatile memory, or large manufacturing equipment that processes classified information. The IS Rep will always coordinate with the ISSP when the equipment contains non-volatile memory. For special purpose systems not part of a larger system the facility needs to explain the need to the GCA and get RAL to include GCA security guidance since the system won't meet NISPOM requirements. The facility needs to retain the documentation for security inspections, but ODAA will not accredit the system or component. The GCA letter would be documentation to identify the system as special purpose.

C. 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 published clearing and sanitization procedures for their equipment, e.g., Agilent's Security and Memory document often meet the requirements for sanitization, as the memory that contains the user accessible or configurable data is battery-backed RAM. In situations where the user accessible or configurable data is contained in EEPROM or Flash EPROM, the published procedures will only be considered the manufacturer's recommended procedure and the additional requirements of the matrix apply. The ISSP must verify the procedures and determine if further process is required to clear or sanitize the equipment, to include ensuring all test equipment registers are cleared and sanitized.

D. 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.

5.1.1.2.5.6 Copiers

Newer multifunction copiers are basically a PC, printer and scanner put together in a specialized case. They can have non-volatile memory, hard drives, an operating system and networking capability. Some even utilize RFID technology. Copiers with any of these features must be accredited under NISPOM Chapter 8. While very similar to a special purpose system since many NISPOM requirements can't be applied, an SSP needs to be submitted. Attention needs to be applied to their maintenance, clearing and sanitization, etc. NISPOM Chapter 5, Section 6 still applies 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 through 5-603 apply.

5.1.2 SECURITY ASSESSMENT AND AUTHORIZATION (CA)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	**CNTL NO.**	**CONTROL NAME**	**NISPOM Reference**	**PM location Para heading**	**Protection Levels Confidentiality**
MANAGEMENT		**Security Assessments and Authorization**			
* not addressed **not contractually imposed	CA-1	Security Assessment and Authorization Policy	8-200, 8-610	addressed at PL-1 (Roles and Responsibilities)	1,2,3
	CA-2	Security Assessments	8-200, 8-614, 8-500	Types of Security Plans	1,2,3
	CA-2 (1)	Security Assessments Control Enhancement		*	
	CA-2 (2)	Security Assessments Control Enhancement		**	
	CA-3	Information System Connections	8-700	Network Security Plans (NSP)s/MOUs/SCPs	1
	CA-3 (2)	Information System Connections Control Enhancement		Network Security Plans (NSP)s/MOUs/SCPs	
	CA-5	Plan of Action and Milestones	8-610	Plans of Action & Milestones (POA&M)	1,2,3
	CA-6	Security Authorization	8-202	addressed at control SA-2	1
	CA-7	Continuous Monitoring	8-202, 8-614	addressed at control SA-2	1,2,3
	CA-7 (1)	Continuous Monitoring Control Enhancement		addressed at control SA-2	
	CA-7 (2)	Continuous Monitoring Control Enhancement		**	

5.1.2.1 Types of Security Plans

Plans submitted to DSS must be based upon the DSS-provided plan templates in order to accommodate timely reviews. The templates can be requested from the DSS web site. Once completed the plans should be kept from public disclosure as best possible since they can provide to adversaries an insight to how classified information is being protected. There are three types of plans that can be submitted to the ODAA:

1. System Security Plan (SSP)
2. Master System Security Plan (MSSP)
3. Network Security Plans (NSP)

5.1.2.1.1 System Security Plan (SSP)

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 (Security Controls, Management Controls, System and Services Acquisition (SA), C&A Process). The submission format is outlined in the System Security Plan Submission Process section.

The ISSM shall make the SSP accessible to authorized personnel.

5.1.2.1.2 Master System Security Plan (MSSP)

The term "Master" indicates the authorization to add IS to an approved plan by an ISSM. The ISSM may add IS to the MSSP once ODAA has determined the ISSM has the requisite knowledge and skills to manage multiple IS under one master plan. Upon determination the ISSM has met those requirements, self-certification authority will be granted. 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"
- Self-certification
- Managing added IS
- ISL 2007-01 Extract

The concept of the MSSP allows two or more information systems (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, 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 (granted that 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 operating at PL 1 or 2.

Included at the end of this section is the ISL 2007-01 Article #14 extract relating to MSSP/self-certification for ease of reference.

The use of an MSSP is highly encouraged to further expedite the timely 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.

Once the RDAA grants approval of an MSSP, an IATO will 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 and not the contractor's copy. The ISSP/C&A Reviewer for the facility will validate the IS represented in the MSSP and approved in the IATO within 180 days. Only in exceptional circumstances will a second IATO be granted. After a successful certification, the RDAA will send an ATO to the ISSM that identifies the system, system type(s), operating system(s), operations, and operating environment that the ISSM is approved to self-certify. New systems that meet the requirements of the MSSP and CSA accredited system as defined in the MSSP and specified in the ATO shall 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 MSSP.

When the ISSM wishes to add new operating systems or configurations not addressed in an approved MSSP, the ISSM must submit the approved MSSP for reference and the new IS profile to be considered for accreditation by following procedures in System Security Plan Submission Process.

Once the submitted plan is received by the ODAA database administrator, it will be assigned to the responsible ODAA reviewer for review and onsite validation. The C&A process identified in Security Assessment and Authorization (CA), Certification and Accreditation (C&A) still applies. 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. The RDAA will issue an IATO for the new IS profile once a favorable review is completed. While the MSSP will not need to be re-approved, the ISSP/C&A Reviewer must certify the new IS profile within 180 days. Only in exceptional circumstances will a second IATO be granted. 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 shall be retained with the approved copy of the MSSP.

The ISSM must update/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/C&A Reviewer at least 30 days 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/C&A Reviewer to determine submission frequency of self-certified IS and any other required notifications for the addition of self-certified systems to be submitted to the ODAA mailbox. Unless directed otherwise by ISSP/C&A Reviewer, every self-certified IS profile must be forwarded immediately upon completion of the self-certification to the ODAA mailbox to ensure contractor systems and ODAA database match. The listing provided at the end of this section will also be used to reconcile all existing IS at the facility.

(8-202g(4)): IS certified under an MSSP remain certified until the MSSP is changed or 3 years have elapsed since the IS was certified. This means each IS Profile added to the initial DSS accredited MSSP IS has its own 3 year expiration from the date it was self-certified. If the IS that was initially accredited by DSS is disestablished, the ISSM will resubmit the MSSP with an IS Profile that is an appropriate substitution of the initially accredited IS. It is recommended that a self-certified IS that has been reviewed by an ISSP/C&A Reviewer during an annual inspection be submitted as an appropriate substitute. DSS will sign an ATO indicating the new IS Profile that is to be identified for similar ISs that operate in equivalent environments.

If either the levels of concern or protection level described in the MSSP change, the MSSP shall be re-accredited by the CSA and all IS certified under the MSSP shall be re-certified by the ISSM in coordination with the CSA. A POA&M may be used so that all self-certified IS do not incur the same expiration date when re-certified. The MSSP Tracking Form at the end of this section will be used to manage the additions of self-certified IS.

If there are no security relevant changes, the three-year reaccreditation may be based on an e-mail from the ISSM to ODAA stating that there have been no security relevant changes to the MSSP. Existing MSSPs which are not written in the format described here will need to be submitted using this format when they need to be resubmitted for the three-year reaccreditation.

If either the levels of concern or protection level change for any IS covered by in the MSSP, the MSSP must be revised and reaccredited by the ODAA and all IS certified under the MSSP shall be re-certified by the ISSM in coordination with the ISSP/C&A Reviewer before the changes are implemented. Any IS that can no longer be covered by the MSSP due to those changes will be either rolled into an existing MSSP that matches the security requirements or will be covered by a new plan.

If a security relevant change occurs to only one system under an MSSP (e.g. upgrade an OS from Win2000 to XP), only that system needs to be re-certified (when the change occurs) before the MSSP is re-issued with the addition of the new system.

General Guidelines for MSSPs and Self-Certification

Self-Certification Requirements

The need for Self-Certification shall be reviewed on an annual basis. The following are requirements in order for an ISSM to obtain self-certification authority.

1) Successful completion the NISPOM Chapter 8 Requirements for Industry Course and its final exam.

2) The facility must have a Satisfactory rating from the previous DSS annual review. Or if the contractor received a lower rating, findings are not resulting from the facility's IS program.

3) A written recommendation from contractor management recommending the facility's ISSM to be granted self-certification authority.

The following are how an ISSM can have its self-certification authority rescinded:

1) A written recommendation from contractor management recommending the facility's ISSM self-certification authority be rescinded.

2) Two or more serious IS-related findings at the most recent annual review.

The following are general guidelines on writing MSSPs and self-certifying systems under an approved MSSP by an ISSM.

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. IS that have caveated information, i.e. 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.

An IS profile under an 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.

Master plans will not be written for any system requiring a variance or waiver. Only those systems that are NISPOM compliant (i.e., an IS that meets all NISPOM requirements) may be self-certified.

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.

The following are some standard MSSP submissions:

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 is granted in the MSSP Approval to Operate (ATO), and is only authorized as long as the ATO is valid. The ISSP/C&A Reviewer must specifically request that self-certification not be granted. There must be specific justification that the ISSM is not technically competent, does not have adequate experience or has violated trust in the past.

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.

Self-certification is only authorized for systems that are fully compliant and meet all NISPOM 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, multiuser 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/C&A Reviewer to get clarification.

When a system is self-certified, the following documentation MUST be included with the self-certification packet maintained with the IS, as well as being sent to ODAA@dss.mil:

- 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.

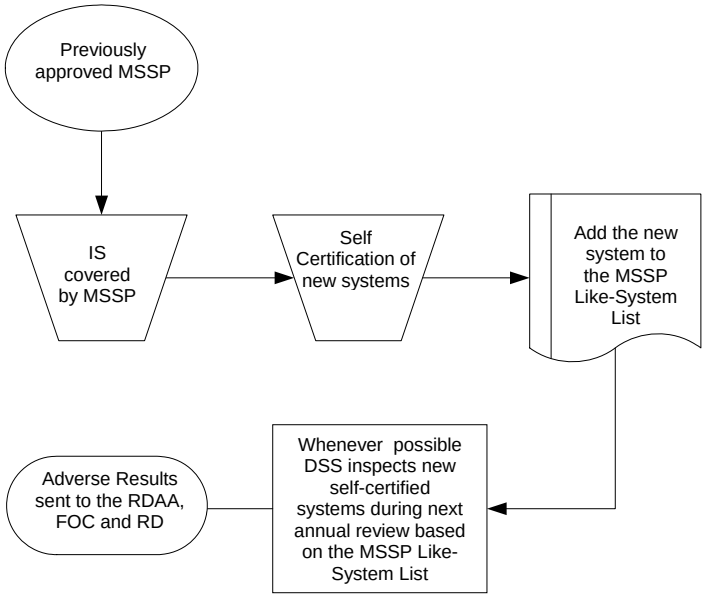
- The complete IS profile and supporting documents
  1) Certification test results.
  2) A signed statement by the ISSM that security features; including access controls and configuration management are implemented and operational. This is often included as part of the statement of self-certification.
  3) Any documentation uniquely identifying the self-certified system, i.e. location information, system administrator (SA) or ISSO information, network diagrams, hardware list and software list, etc.

  The facility **MUST** have the proper documentation for the self-certified system. The ISSM can not simply state that the system was self-certified.

- A list must be kept for all systems and all self-certified systems must be identified. This list must be given to the ISSP/C&A Reviewer when each IS 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/C&A Reviewer.

Figure 1 Flow Diagram for Self-Certification Under an MSSP



Limitations on Self-Certification of Similar Systems

The ISSM cannot self-certify systems that require variances. See examples below and required documentation and procedures.

- SIPRNET

An ISSM cannot self-certify a SIPRNET node, but can self-certify a system on the node providing all self-certification requirements are met.

- Interconnected Systems/WANs

1. An ISSM cannot self-certify a WAN.

2. An ISSM can self-certify a WAN node providing all self-certification requirements are met.

3. An ISSM can self-certify a new system on the WAN node providing all self-certification requirements are met.

4. To add a self-certified node to an existing WAN, the node ISSM must submit the following 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.
  1) Certification test results.
  2) 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.
  3) Any documentation uniquely identifying the self-certified system, i.e. location information, system administrator (SA) or ISSO information, network diagrams, hardware list and software list, etc.

5. The WAN host must request approval of additional nodes by resubmitting an updated NSP for approval.

6. 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 operating with a protection measure variance. This includes but is not limited to legacy operating systems, alternate trusted download procedures, or audit variances. The following rules apply to self-certification of system requiring a variance.

- Systems with audit variances

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

NOTE: The approval letters will be system specific and will expire when the associated MSSP or IS profile expires, unless rescinded.

NOTE: A separate system plan for a specific system may include the audit variance procedures in the plan narrative as well as the IS profile and will be approved at the time the security plan is accredited.

- 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
- Detailed procedures and file types applicable under the alternate procedures
- 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

Once approved, the procedures, the RAL and 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.

NOTE: 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. Additionally, the CSA recommends that a comprehensive list of all test equipment to include manufacturer, nomenclature, model, type and amount of memory, and clearing and sanitization procedures for each piece of equipment in use at the facility be developed. 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.

NOTE: 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 will occur three years from the issuance date of the ATO. 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 Figure 8 Flow Diagram for a Reaccreditation and Re-evaluation.

If there are significant changes, the plan must be resubmitted like a new request using the appropriate procedure. 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 90 days to expiration to allow 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.

ISL 2007-1 #4. (8-101(b), 8-103) In a multiple facility organization (MFO), can an ISSM who has been granted self-certification authority self-certify systems across the MFO structure?

Answer: The ISSM who has been granted self-certification authority for like systems under approved Master System Security Plans (MSSP) may self-certify systems for those facilities where he or she has been designated as the ISSM. 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 (Note: DSS will consider exceptions to this "reasonable distance" criteria on a case by case basis. Such requests must specify how the ISSM will carry out oversight and other responsibilities from afar).
- The aggregate complexity of the collective facilities is such that only one ISSM is required.
- The ISSM is trained to a level commensurate with the overall complexity of all facilities.
- Each facility has at least one appointed Information System Security Officer (ISSO) who has been assigned the duties identified in paragraph 8-104.

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.

ISL 2007-1 #12. (8-202(g)) Can one MSSP cover multiple cleared facilities?

Answer: No. While many elements of an MSSP may be the same (for similar IS), each MSSP must be tailored to the unique circumstances of each cleared facility.

ISL 2007-1 #13. (8-202(g)) Can one MSSP be written that covers all IS within the contractor's facility that operate at PL 1 and PL 2?

Answer: No. NISPOM paragraph 8-202(g) states that the IS covered by a single MSSP must have equivalent operational environments, and PL1 and PL2 are distinct operational environments.

ISL 2007-1 #14. (8-201, 8-202) What are the parameters for self-certification by a contractor?

The certification and accreditation processes are discussed in NISPOM paragraphs 8-201 and 8-202, respectively. The following discussion is an effort to make clear how DSS applies these terms.

Certification is the attestation by a contractor that comprehensive technical and non-technical system security controls are established and operating in conformity to a specified set of NISPOM security requirements. Certification of an IS is performed by the contractor in order to achieve accreditation from the Government.

Accreditation is the official governmental action performed by the DSS ODAA to permit an IS to operate at an acceptable risk level within a specified environment. Accreditation is issued after the contractor provides a certification that security controls are in place and operating as intended. All IS certifications shall be reviewed and IS accredited to operate by DSS (ODAA).

The following table provides parameters governing self-certification by industry under a DSS-approved MSSP.

Table 2 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 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 IS 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 the 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.

ISL 2007-1 #15. (8-202(g)(3)) NISPOM paragraph 8-202(g)(3) requires the ISSM to certify additional IS under an MSSP but does not require notification to DSS. Should DSS be notified?

Answer: Yes. It's imperative that DSS have up-to-date knowledge and awareness of all accredited IS processing classified information. At a minimum, the contractor shall provide an updated list of IS self-certified under an MSSP to the IS Rep and ISSP on a quarterly basis. If the IS Rep or ISSP determines that more frequent notification is necessary because of volume or complexity or to address specific security concerns, the IS Rep or ISSP can request more frequent notification.

Table 3 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					

5.1.2.2 Information System Connections

5.1.2.2.1 Network Security Plans (NSP)

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 reviewer 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 accredited as an information system. Utilizing an NSP for a WAN enables us to add new connections or nodes to the system without requiring the existing nodes to be reaccredited.

NSPs are submitted to DSS for review and accreditation in the same manner as a (M)SSP.

NSP Content

The responsibility for creating, gaining accreditation for, 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 IS is connecting to a WAN accredited by another government entity or DAA. This type of connection also requires an MOU or MOA signed by both DAAs. MOAs/MOUs are covered in detail in the Security Assessment and Authorization (CA), Types of Security Plans, Memorandum of Understanding section.

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

1) ODAA Unique ID and IS name.
2) Facility addresses.
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 with an accompanying 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 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 identification and authentication (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 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:

1) All personnel will be briefed on the use of the WAN and will be knowledgeable of the NSP security requirements.
2) 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.
3) 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 ISSMs to support contractually related work or programs.
2) One ISSM is designated "host" node and assumes role of "Network ISSO" for the WAN.
3) Host node ISSM or "Network ISSO" prepares the NSP.
   a. Collects signed participant data sheets and local accreditation letters from all node ISSMs.
   b. Provide e-mail addresses in the package for all node ISSMs.
   c. Ensures encryption devices are in place at all nodes. Note: Some nodes may need to get reaccredited locally when adding the encryptor and WAN connection to the profile.
   d. 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.
   e. Completes the NSP document and diagram, etc. Attaches MOU (if required), accreditation letters and signed participant data sheets for each node.
   f. Assigns an ODAA Unique Identifier to the NSP.
   g. 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.
   h. 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.
   a. If the NSP includes components/devices not accredited under an associated profile (rare), the ISSP will schedule a visit to validate these components.
   b. There may be cases where an NSP is granted an IATO, but typically, an NSP is issued an ATO when all documentation is correct.
   c. 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 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 DAA.

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.

Example 1: 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) to 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 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.

Example 2: 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 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.

Example 3: 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.

Example 4: 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

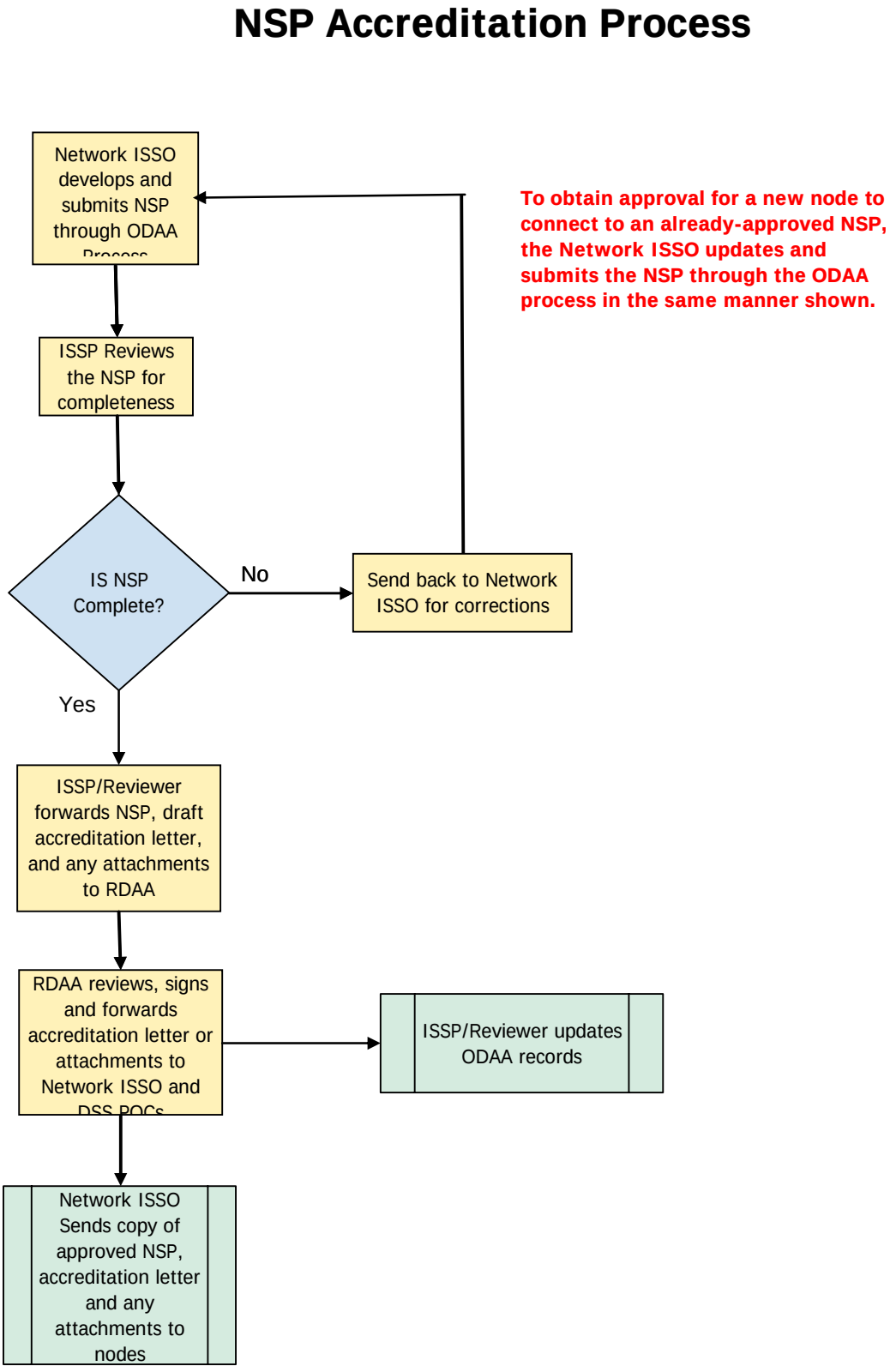
1) Host node ISSM or "Network ISSO" updates the NSP.
   a. Collects signed participant data sheets and local accreditation letters from the new node ISSM(s). Verifies all existing nodes' participant data is current and requests updated information as needed.
   b. Provides e-mail addresses for all node ISSMs.
   c. Ensures encryption devices are in place at new nodes. Note: Some nodes may need to get reaccredited locally when adding the encryptor and WAN connection to their profile.
   d. 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.
   e. 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.
   f. 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 include all required documentation is included.
   a. 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).
   b. 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.
   a. RDAA will sign and send the signed ATO for the NSP back to the Network ISSO.
   b. The Network ISSO will update all nodes with a copy of the ATO and updated NSP along with any new or modified MOUs.

The figure that follows 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.

Figure 2 NSP Accreditation Process Diagram



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.

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 system 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.

Figure 3 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: 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

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 shall 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.

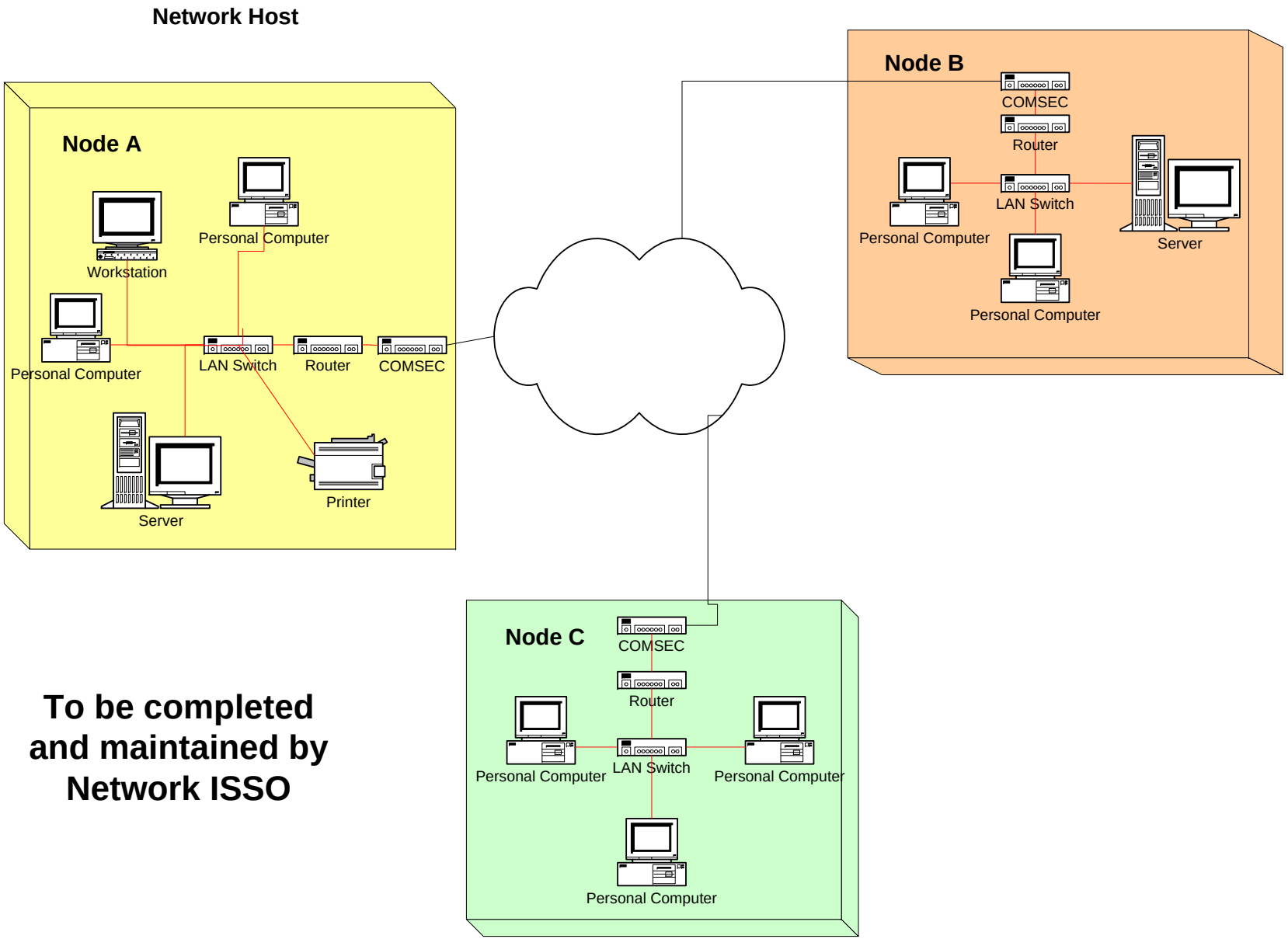
Data Transmission Records

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, which ever 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:



To be completed and maintained by Network ISSO

Figure 4 NSP Architecture Diagram Example

Figure 5 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:			

Network Host Security Profile (To be completed by Network Host)	Network Identifier:	Network Host Facility:
Date:	Facility Address:	CAGE Code :

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 ☐ * FG ☐ 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: 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 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 verification of requisite clearance via a Visitor Authorization Letter (VAL) or other method of clearance verification (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:

Figure 6 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:			

Network Node Security Profile (To be completed by each Network Node)	Node Identifier:	Contractor facility name:
Date:	Facility Address:	CAGE Code :

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: 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

☐ 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 verification of requisite clearance via a Visitor Authorization Letter (VAL) or other method of clearance verification (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: Date:

5.1.2.2.1.1 Memorandum of Understanding (MOU)/Interconnected Systems Agreement (ISA)

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

An MOU *is not* required for contractor to contractor connections if DSS is the DAA for both. If the contractor wants an MOU, that is between the contractors involved. The host contractor may also be a signer if the program office and the contractor desire. 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 connections. If the GCA wants to use that format, it can be allowed, however, DSS must require some additions to meet NISPOM requirements.

All MOU/MOAs (Memorandum of Acceptance) will be sent to ODAA Headquarters for signature. Any MOU/MOAs with signatories of General Officer rank/equivalent or above will be signed by the Director, Industrial Security Program, DSS. All signatories below the general/equivalent grades will be signed by the Deputy Director, ODAA. ODAA requires a minimum of 30 days to properly staff the MOUs for signature. MOU's require re-accomplishing prior to the three-year reaccreditation.

For the purposes of this manual, MOU and MOA can be used interchangeably. We will refer to the document as an MOU throughout. We will focus on information system MOUs only. MOUs created for other purposes (e.g. sharing a space or closed area) are not addressed in this manual.

An approved template or sample MOU document follows. Using this document to create an MOU will reduce time required for review and processing by DSS.

5.1.2.2.1.1.1 MOU Requirements

When IS accredited by different DAAs are to be interconnected, an MOU is required to be completed and signed by the DAAs for the systems involved. MOUs are created to describe the security responsibilities and other information as agreed upon by two or more designated approving authorities or DAAs.

While contractor-to-contractor system interconnections do not require an MOU when DSS is the DAA for all systems involved, an NSP should be used to document security responsibilities for all parties.

The MOU must be completed and approved by all parties before the connection will be authorized by DSS. Under most circumstances, the contractor(s) needing the MOU will create the document and forward to the DAAs for review. After the MOU content has been agreed to, the GCA or user agency (UA) should sign the MOU first. The MOU is then sent to the responsible DSS IS Rep or ISSP who will route it through ODAA for final signature.

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

5.1.2.2.1.1.2 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 ISSO and responsibilities
- High-level description of and usage of the network
- Contract or program name
- Name and location of facilities involved
- 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)
- 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, 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
- 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 needed, a new MOU should be 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.

5.1.2.2.1.1.3 MOU Sample

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 system (IS) security requirements for approval purposes and supplements (**Company Name**) approved system 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**) IS is located at (**address**).

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

Name Title Phone

The following (**User Agency**) 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 IS 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 shall be at the **(classification level)** level.

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

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

The Network ISSO (**Network ISSO Name**) at (host--**Company and User Agency Name**) will 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:

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

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

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

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

e. 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 shall 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**) shall 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	(**User Agency**)
_____	_____
(**Name of DAA**) Title Designated Approval Authority	(Name of User Agency Official and Rank) Title Designated Approval Authority

5.1.2.2.1.2 Defense Information Systems Network (DISN) Connections

In addition to satisfying the requirements of the NISPOM, several other requirements are imposed when connecting to government networks. The following are examples of DISN networks with associated procedures to connect:

- Secret Internet Protocol Router Network (SIPRNet)
- DISN Leading Edge Services (LES) - TBD in future revisions
- Defense Research and Engineering Network (DREN)/S-DREN - TBD in future revisions
- Missile Defense Agency Classified Network (MDACNet) - TBD in future revisions

SIPRNET Plan Review and Accreditation Process

SIPRNet guidance has been removed from this process manual. All SIPRNet guidance has been moved to the DSS web site (www.dss.mil).

5.1.2.2.2 International System Security Plans

In certain instances, contractors may elect to transmit and receive classified data to a foreign customer via voice or fax via a secure communications link. 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 a Program Security Instruction (PSI) approved by the Office of the Deputy Under Secretary of Defense – Technology Security Policy and National Disclosure Policy before transmission of data can take place. The ODAA is concerned with two documents that make up the Program Security Instruction; the System Certification and Accreditation (C&A) package and the Secure Communication Plan (SCP).

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 stand alone until the SCP is approved. Once the SCP is approved the SSP must be submitted for reaccreditation as an International Wide Area Network (WAN) because of the security relevant change.

Secure Communications Plan (SCP):

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

Insofar as the need for international secured communications has increased, and the connections themselves have become more complex, the ODAA has adopted a more expanded role in this process. The following paragraphs will define roles and responsibilities for how the ODAA and the International Program Branch (IPB) will interact when DSS headquarters receives a request to accredit a secure link between nations.

Request from U.S. contractors

1. The initial request will be directed to the ODAA.
2. ODAA will record receipt of the request.
3. ODAA will conduct a critical review to determine whether the package is complete. If the documentation is deficient, the package will be returned to sender with comments. A 30 day suspense will be maintained by ODAA.
4. If the request is complete, copies will be transmitted to National Security Agency (NSA), Office of the Deputy Under Secretary of Defense – Technology Security Policy and National Disclosure Policy, and the foreign government's national security authority for action. A "complete" package is defined as containing a request that indicates that the IS is in process of being accredited and the encryption devices are clearly identified.
5. The transmission to the foreign government described in #4 above will be performed by the Chief, IPB.
6. If questions are received from the foreign government, they will be forwarded to ODAA for resolution via IPB. When the ATO is received from the foreign government the ODAA will advise the U.S. parties that the secured connection has been approved and can be made functional.

Requests by foreign governments

1. Foreign governments will be advised that requests to establish secure links require an SCP be sent to the IPB.
2. IPB will transmit the initial request to the ODAA.
3. ODAA will record receipt of the request and conduct an initial critical review to determine whether the request is complete. If the documentation is deficient, the request will be returned via IPB to sender with questions and comments. A 60 day suspense will be maintained by ODAA/IPB.
4. If the request is complete, copies will be transmitted by the ODAA to NSA, Office of the Deputy Under Secretary of Defense – Technology Security Policy and National Disclosure Policy and the appropriate DSS field office(s) for action.
5. The DSS field personnel will work with their contractors to assure the U.S. systems are certified and accredited. If the connection involves establishment of secured networks among U.S. contractors, ODAA will assure the appropriate Memorandum of Understandings (MOUs) are executed.
6. See "ODAA" below.

Requests by U.S. program office

1. When IPB receives a request from a U.S. program office to facilitate a secure connection involving a U.S. cleared facility, IPB will confirm that the PSI contains provisions for secured communications. Upon determination that such provisions

exist, IPB will transfer the request to the foreign government's national security authority and to the ODAA.

2. ODAA will record receipt of the request and conduct an initial critical review to determine whether the request is viable. If the documentation is deficient, the request will be returned, via IPB, to sender with questions and comments. A 60 day suspense will be maintained by ODAA/IPB.
3. If the request is complete, copies will be transmitted to NSA and the appropriate DSS field office(s) for action.
4. The DSS field personnel will work with their contractors to assure the U.S. systems are certified and accredited. If the connection involves establishment of secured links to the program office and or U.S. contractors, ODAA will assure the appropriate MOUs are executed.
5. See "ODAA" Below.

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 ***must*** specify the entities that are approved to connect and that the international connection is authorized. The ODAA will then notify the IPB 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.

5.1.2.3 Types of Networks

5.1.2.3.1 Unified Networks

A unified network applies when all DAA 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 usually only one security policy. For those Unified WANs, 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 ODAA reviewers will review the SSP for unified networks like any other SSP.

5.1.2.3.2 Interconnected Networks

An interconnected network applies when there are a number of separately accredited nodes on a network. These can 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 configured. 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.

5.1.2.3.3 Network Security Plans (NSP)

An 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 purpose of this requirement is fourfold.

1. It allows for more accurate tracking of WANs by providing an ODAA Unique Identifier (UID) to the WAN separate from any UID assigned to one of the nodes.

2. Independently documenting the WAN allows for a more thorough understanding of the WAN. Providing separate detailed documentation focusing on the WAN as a whole eliminates the need to read multiple node SSPs which may or may not contain a complete WAN description or configuration.

3. By requiring an NSP for every WAN, it becomes easier to add additional nodes by minimizing any required changes to the original nodes' security plan. Essentially, DSS has built the flexibility needed to support the often inevitable expansion of many WANs into the accreditation process.

4. It is in accordance with NISPOM paragraph 8-700(c) "An interconnected network also requires accreditation as a unit." To meet this requirement, an NSP is written to document interconnections between two or more separately accredited information systems. In addition to systems accredited by different designated approving authorities (DAAs), these requirements apply when interconnecting two or more separately accredited systems managed by a single ISSM at the same facility, campus, or Commercial and Government Entity **(**CAGE) code and/or same DAA.

5.1.2.4 Plan of Action & Milestone (POA&M)

The primary purpose of the POA&M is to assist the contractor in obtaining accreditation as soon as possible. It facilitates an agreement between the contractor and DSS stating which items from the Baseline Technical Security Configurations cannot be met and why, and/or cannot be met immediately but can be met eventually, resulting in the contractor obtaining an IATO in a much shorter timeframe. The POA&M applies to initial (M)SSP submissions, as well as existing accredited systems that require accreditation under the new DSS Configuration Baseline (i.e. when they become due for re-accreditation after three years). The GCA must approve non-compliant settings due to program compatibility or contract requirements. Non-compliance with Baseline Technical Security Configurations resulting from operating system limitations or capabilities will not require GCA approval.

When a system has to be re-submitted with the new baseline (three year re-accreditation or other security-relevant change) or for a new system:

- Use a POA&M if the Baseline Technical Security Configurations are not yet fully implemented, to include the timeline for implementation.

- 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 (365 days because no more than two IATOs can be issued, 180 days each).

- If the POA&M and the (M)SSP are acceptable, ODAA will issue an IATO for the system.

- After all items in the POA&M have been completed, and the ISSP/C&A Reviewer has successfully conducted an onsite validation, ODAA will issue an ATO to include self-certification (MSSP only).

- The ISSM can now self-certify the similar systems in the same environment with the new baseline standards based on that POA&M (MSSP only).

For those (older) (M)SSPs that have a large number of profiles all expiring at the same time, the POA&M can be used to "spread out" the accreditation dates, hence helping to spread out the workload for the ISSM over a period of time.

5.1.2.4.1 Plan of Action and Milestone Template (POA&M)

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

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

* 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 Milestone Template (POAM) Guidance

- The POA&M apply to initial (M)SSP submissions, as well as existing accredited systems that require accreditation under the new DSS Configuration Baseline.
  *C/I – Enter C if non-compliance issue was identified during the C&A process. Enter I if non-compliance issue was identified during inspection. Milestone date for non-compliance issues should completed within **XX** days.
- 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 information assurance (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 will have 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 inspection that are not corrected on the spot must be put in the POA&M. This will make a formal, trackable date for resolution.

5.1.3 CONFIGURATION MANAGEMENT (CM)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	**CNTL NO.**	**CONTROL NAME**	**NISPOM Reference**	**PM location Para heading**	**Protection Levels Confidentiality**
MANAGEMENT		**Configuration Management**			
* not addressed **not contractually imposed	CM-1	Configuration Management Policy and Procedures	8-311, 8-610	Configuration Management Process	1,2,3
	CM-2	Baseline Configuration	8-311, 8-610	Configuration Management Process	1,2,3
	CM-2 (1)	Baseline Configuration Control Enhancement		Configuration Management Process	
	CM-2 (2)	Baseline Configuration Control Enhancement		Configuration Management Process	
	CM-2 (3)	Baseline Configuration Control Enhancement		Configuration Management Process	
	CM-2 (4)	Baseline Configuration Control Enhancement		Configuration Management Process	
	CM-2 (5)	Baseline Configuration Control Enhancement		Configuration Management Process	
	CM-2 (6)	Baseline Configuration Control Enhancement		*	
	CM-3	Configuration Change Control	8-103, 8-104 ,8-311, 8-610	addressed at control PL-1 (ISSM/ISSO)	1,2,3
	CM-3 (1)	Configuration Change Control Control Enhancement		*	
	CM-3 (2)	Configuration Change Control Control Enhancement		*	
	CM-4	Security Impact Analysis	8-103, 8-104 ,8-311, 8-610	addressed at control PL-1 (ISSM/ISSO)	1,2,3
	CM-4 (1)	Security Impact Analysis Control Enhancement		addressed at control PL-1 (ISSM/ISSO)	
	CM-5	Access Restrictions for Change	8-311, 8-610, ISL 2007_01 #32	Addressed at control SI-2 Flaw Remediation	1,2,3
	CM-5 (1)	Access Restrictions for Change Control Enhancement		*	
	CM-5 (2)	Access Restrictions for Change Control Enhancement		addressed at control PL-1 (ISSM/ISSO)	

5.1.3.1 Configuration Management Process

The configuration management (CM) process ensures that the protection features are implemented and maintained in the system. 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 IS profile(s) to include hardware, software, procedures, reports and audit records. In cases where change impacts upon previously accredited procedures, reaccreditation by DSS will be required prior to implementation. The hardware and software lists will show the current baseline. The CM program will be periodically verified during a contractor self-inspection to ensure it is working effectively and that changes outside the CM process are not permitted. Verification will be accomplished by a physical audit of the hardware and software currently in use on the IS against the hardware and software baselines listed in the accredited (M)SSP.

5.1.4 PROGRAM MANAGEMENT (PM)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	**CNTL NO.**	**CONTROL NAME**	**NISPOM Reference**	**PM location Para heading**	**Protection Levels Confidentiality**
Management		**Program Management**			
* not addressed **not contractually imposed	PM-1	Information Security Program Plan		*	
	PM-2	Senior Information Security Officer		*	
	PM-3	Information Security Resources		*	
	PM-4	Plan of Action and Milestones Process		*	
	PM-5	Information System Inventory		*	
	PM-6	Information Security Measures of Performance		*	
	PM-7	Enterprise Architecture		*	
	PM-8	Critical Infrastructure Plan		*	
	PM-9	Risk Management Strategy		*	
	PM-10	Security Authorization Process		*	
	PM-11	Mission/Business Process Definition		*	

5.1.5 RISK ASSESSMENT (RA)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	CNTL NO.	CONTROL NAME	NISPOM Reference	PM location Para heading	Protection Levels Confidentiality
Management		Risk Assessment			
* not addressed **not contractually imposed	RA-1	Risk Assessment Policy and Procedures	8-610	Risk Assessment Requirements	1,2,3
	RA-2	Security Categorization	8-402	Protection Levels	
	RA-3	Risk Assessment	8-402	Risk Assessment Requirements	
	RA-5	Vulnerability Scanning	8-614	Risk Assessment Requirements	1,2,3
	RA-5 (1)	Vulnerability Scanning Control Enhancement		*	
	RA-5 (2)	Vulnerability Scanning Control Enhancement		*	
	RA-5 (3)	Vulnerability Scanning Control Enhancement		*	
	RA-5 (4)	Vulnerability Scanning Control Enhancement		*	
	RA-5 (5)	Vulnerability Scanning Control Enhancement		*	
	RA-5 (7)	Vulnerability Scanning Control Enhancement		*	

5.1.5.1 Risk Assessment Requirements

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

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.

DSS has developed NISP tools which are intended for use by government contractors to assess compliance with NISPOM technical requirements for Windows NT, 2000, XP and 2003. The NISP tool provides configuration guidance as well as the capability to scan Windows operating systems for NISPOM compliance. Although NISP Tools can help

reveal security issues, they should not be used as a substitute for a full site security test and evaluation or other similar means of identifying security weaknesses.

See ODAA NISP Tool under Awareness and Training for more information.

5.1.5.2 Enhanced Controls

Enhanced controls are controls that are above and beyond the NISPOM. Situations that require enhanced controls are a contractual requirement, requirement by a GCA sponsored circuit connection (SIPRNet, SDREN, DISN-LES, etc.), or an endorsement by management. The DSS ISSP will evaluate, certify, and inspect all IS technical features and safeguards at contractor facilities in accordance with the NISPOM and its baseline technical security guidance. All enhanced controls shall be noted within the (M)SSP and/or the IS Profile. Once an IS has its accreditation any changes to reflect enhanced controls shall be evaluated by the ISSM as reaccreditation may be necessary because of a possible security relevant change.

5.1.6 SYSTEM AND SERVICES ACQUISITION (SA)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	**CNTL NO.**	**CONTROL NAME**	**NISPOM Reference**	**PM location Para heading**	**Protection Levels Confidentiality**
Management		**System and Services Acquisition**			
* not addressed **not contractually imposed	SA-1	System and Services Acquisition Policy and Procedures		*	
	SA-3	Life Cycle Support	8-200	Certification and Accreditation (C & A)	
	SA-5 SA-5 (1) SA-5 (2) SA-5 (3)	Information System Documentation Information System Documentation Control Enhancement Information System Documentation Control Enhancement Information System Documentation Control Enhancement	8-610	addressed at CA-2 (SSPs) addressed at CA-2 (SSPs) addressed at CA-2 (SSPs) addressed at CA-2 (SSPs)	1,2,3
	SA-6 SA-6 (1)	Software Usage Restrictions Software Usage Restrictions Control Enhancement	8-302,8-613	Software Protections *	1,2,3
	SA-7	User Installed Software	8-302,8-202	Software Protections	
	SA-8	Security Engineering Principles	8-311	Software Protections	
	SA-9	External Information System Services		*	
	SA-10	Developer Configuration Management	8-613	addressed at control CM-5	
	SA-11	Developer Security Testing		*	

5.1.6.1 Certification and Accreditation (C&A)

5.1.6.1.1 C&A Life Cycle

C&A is a continuous process designed to validate that systems processing classified information meet the requirements for accreditation, and that the systems continue to maintain the accredited security posture throughout their system life cycle from system inception to termination. The following outlines the C&A life cycle from the submission of an (M)SSP to the issuance of an accreditation letter or ATO and finally the termination of the IS for classified use.

As a general guideline, an IS processing classified information must be accredited if it has storage media or programmable or writeable non-volatile memory. Test equipment with non-volatile memory that is going to process or retain classified information requires accreditation. If any amount of classified information is intentionally input into a system

that has non-volatile memory, the system must be accredited. If a system does not process or retain classified information, it does not require accreditation; however, procedures explaining how classified information is protected should be determined during security reviews and subsequently documented. A personal computer with only volatile memory requires accreditation since it has some type of media involved. Equipment with only volatile memory but no media does not require accreditation.

Typical C&A life cycle of a cleared contractor's IS:

- 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/ISLs.

- An ODAA reviewer reviews the plan and makes the following recommendation:

  1. Accept the plan requiring no corrective action

  2. Accept the plan requiring some corrective action

  3. Reject the plan (Note: in this case the life cycle restarts)

- The ODAA Regional Designated Approving Authority (RDAA) signs an Interim Approval to Operate (IATO) to allow the cleared contractor to begin classified processing.

- During the period identified in the IATO, an onsite validation will take place by a representative of ODAA to determine if the protective security measures noted in the SSP match the actual technical and physical settings of the IS. Note: Only the RDAA can waive an onsite validation.

- At this point the ISSP/C&A Reviewer will make the following recommendation:

  1. Issue an Approval To Operate (ATO) for final accreditation

  2. Issue an ATO once the ISSM has made minor administrative on-the-spot changes

  3. Reschedule another onsite validation once corrective action has been made

- In some cases, the ODAA Reviewer can conduct on onsite validation immediately after reviewing the plan and may recommend an ATO without recommending an IATO.

- The ODAA RDAA signs an ATO for final accreditation.

- If there are security-relevant changes/modifications to the (M)SSP, the life cycle will start over again

- Once classified processing is no longer required, the ISSM will notify the local ISSP/C&A Reviewer.

    - The ISSP/C&A Reviewer will validate that the IS has been effectively declassified and forward the recommendation to terminate the accreditation.

    - RDAA will issue a termination letter to the ISSM.

5.1.6.1.2 C&A Process

The 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/C&A Reviewer. A system cannot process classified information without an accreditation. If an accreditation expires or is withdrawn the ISSM must stop processing classified information immediately. 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 applicable Office of the Secretary of Defense (OSD) policy, 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.

5.1.6.1.2.1 Certification

Contractor:

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/ISLs.

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

The ISSM's certification process must outline inspection and test procedures used to demonstrate compliance with the security requirements associated with the Protection Level (PL) assigned to the IS. The certification test shall 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 signatures 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.

This electronic format can be a:

1. Digital certificate

2. An inserted signature (e.g., a .bmp) to a document then saved as a .pdf

3. An ink signature that has been scanned and saved as a .pdf

See System Security Plan Submission Process for instructions to submit (M)SSPs to ODAA.

5.1.6.1.2.2 Review

ODAA reviewers (ISSPs/C&A Reviewers/Headquarters staff) are responsible for the (M)SSPs under their purview for the purposes of review, verification and inspections. The reviewer shall conduct a desktop review of the system's (M)SSP to verify compliance with NISPOM Chapter 8 requirements.

The ODAA reviewer makes the following recommendation:

1. Accept the plan requiring no corrective action.

2. Accept the plan requiring some corrective action.

3. Reject the plan.

Examples of a reason to deny an IATO:

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

Once the security plan has been revised in accordance with the provided review comments, the ISSM should forward the revision to ODAA@dss.mil. The ISSM must copy the ISSP and ODAA C&A Reviewer (if different from the ISSP), and IS Rep on the revised submission.

The ISSM will be given two opportunities for resubmission. If after the second resubmission (or third submission) the plan is still rejected, the plan will be archived, and appropriate corporate management will be notified (note: in this case the life cycle restarts).

The reviewer will establish a tickler system to notify the ISSM by e-mail that corrective action is still outstanding. If the ISSM has not resubmitted a corrected plan after three consecutive months of notification by the reviewer, the plan will be archived and the life cycle restarts. This is not to be construed as a reminder system for the ISSM. It is intended to give the opportunity to resubmit within reasonable timeframes else the plans will be removed from the ODAA database. It is still the responsibility of the ISSM to monitor his/her certification actions.

Note: In some cases (schedules permitting), the ODAA reviewer may be able to conduct on onsite validation immediately after reviewing the plan and may recommend an ATO without recommending an IATO.

5.1.6.1.2.3 Accreditation

Interim Approval to Operate (IATO)

Once the security plan has been reviewed and found to be NISPOM compliant, the Regional Designated Approving Authority (RDAA) will review the recommendations of the reviewer. If appropriate, the RDAA will sign an Interim Approval to Operate (IATO) and e-mail it to the ISSM (with a copy to the ISSP, ODAA reviewer (if different from the ISSP), FOC and IS Rep) with the Comments Form (if applicable) to allow the cleared contractor to begin classified processing. In some cases the RDAA may issue an IATO pending ISSM resolution of plan review comments. However, the comments must be resolved during the IATO period and prior to the issuance of an Approval to Operate (ATO). The IATO will indicate to the ISSP that the system is ready for onsite verification.

An IATO is a temporary approval. If a system has an IATO and the ISSM needs to make changes, the changes can be made to the system and (M)SSP during the IATO phase without reissuing another IATO. The ODAA must be contacted prior to implementing the changes. ***NOTE*****:** *The (M)SSP and all changes will be frozen one week before the ISSP conducts the onsite validation to ensure the system matches the (M)SSP when inspected. Additionally, IATOs will not be issued to systems with SIPRNET connectivity or if they are part of the DIBNet program*.

IATOs may be granted up to 180 days with an option for the RDAA to extend the interim for an additional 180 days. The IATO period shall not exceed 1 year. Approved protection measures shall be in place and functioning during the interim period of approval. **NOTE:** *The ISSM is required to forward all outstanding documentation to ODAA* ***60 days prior to the expiration of the IATO.*** *Failure to do so could result in lapse of accreditation and system operation stoppage. The C&A life cycle will also restart. Documentation supporting initial accreditations should be forwarded to ODAA 60 days prior to the facilities anticipated completion timelines.*

5.1.6.1.2.4 Verification

During the period identified in the IATO, an onsite verification will take place by an ISSP or authorized IS Rep to determine if the protective security measures noted in the (M)SSP match the actual technical and physical settings of the IS. This representative may not be the reviewer of record for that plan.

The ISSP, Field Office Chief (FOC) and IS Rep will coordinate to conduct that visit. Prior to the onsite verification, the ISSP/C&A Reviewer (if not the original plan reviewer) will conduct a cursory review of the plan to get familiarized with the system and to identify any issues that may have been overlooked by the plan reviewer. If

anything is identified, the ISSP/C&A Reviewer will contact the plan reviewer to resolve the discrepancy prior to the onsite visit.

During the onsite verification any discrepancies between the plan and actual system configuration should be corrected on the spot by the ISSM either through modification of the system or by correcting the plan.

After the onsite validation, the ISSP/C&A Reviewer will make the following recommendation:

1. Issue an Approval To Operate (ATO) for final accreditation.

2. Issue an ATO once the ISSM has made minor administrative on-the-spot changes.

3. If major discrepancies were discovered during the onsite verification, it may be necessary to schedule a second validation of the IS prior to accreditation being granted.

If the discrepancies reveal a significant difference between the system's configuration and the approved plan, which places classified information at risk of compromise, the ISSP/C&A Reviewer should notify the RDAA and the FOC with an appropriate explanation. The IATO may be rescinded by the RDAA (after coordination with the Deputy Director, ODAA, the Regional Director and the Deputy Director, Field Operations) until the corrections are made. The corrected plan will then be resubmitted and processed as a new system request. The exception to this is "nonexistent" systems. ODAA will not consider certifying systems that are not yet in place. The plan will be rejected and the ISSM will be required to resubmit.

If the discrepancies do not place classified information at risk, the IATO may be extended until the corrections are made, based on a request forwarded to the RDAA by the reviewer. The ISSM must initiate the request and must include a clear plan of action and milestone (POA&M) created by the ISSM detailing the actions and timetable for correction of the discrepancies. The contractor's failure to provide a POA&M may result in a denial of the IATO extension request.

Approval to Operate (ATO)

IS can only be approved to process classified information in two ways.

1. DSS accredits the IS

2. The IS is added to an MSSP after the ISSM has been granted authorization to self-certify similar IS (see Security Assessment and Authorization (CA), Types of Security Plans, Master System Security Plan (MSSP)).

The RDAA may grant a full ATO for up to three years. During this period it is mandatory for the ISSM to notify the appropriate DSS representative of any security relevant modifications to the system. All security relevant changes will be reviewed by ODAA for a reaccreditation determination.

The term "Master" is associated with the self-certification authority granted to an ISSM. When an MSSP is accredited, the date of the ATO letter starts the three-year cycle. Each IS Profile that uses the MSSP as the document to provide the protective measures for that IS will have its own ATO date. This date will be established in one of three ways:

1. Date an ATO for the MSSP and IS Profiles under it when submitted is signed based on an onsite validation

2. Date an ATO for the IS Profile is signed based on an onsite validation (i.e. when adding an IS Profile to an already accredited MSSP)

3. Date the IS was self-certified by an authorized ISSM

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 resubmit to ODAA@dss.mil with a copy to the ISSP, and IS Rep. The documentation shall be reviewed to determine if reaccreditation is required. If reaccreditation is required the accreditation life cycle will start over again at which time the RDAA may grant an IATO during the review/verification period. Examples of a security relevant change would be when a sniffer (LANAlyser) is added to a network; when a new OS is added; or any change in the protection level.

Re-evaluation will occur three years from the issuance date of the ATO. If there are no proposed changes, re-evaluations 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. See Figure 7 Flow Diagram for Initial (M)SSP.

If there are significant proposed changes, the (M)SSP or IS profile must be resubmitted like a new request using the appropriate procedures above and the life cycle restarts. 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 ensure that plans submitted for reaccreditation with changes are submitted with enough time to permit ODAA to conduct a review and verification of the plan and system components. A minimum of 90 days prior to expiration is expected to ensure other

operational commitments are met. If the accreditation expires during the review time, the ISSM must stop processing classified information until the plan is approved. The RDAA may grant an IATO the system during the review/verification period.

Revocation of an IATO or ATO

If the ODAA, in coordination with other Industrial Security Program (ISP) offices, determines that conditions exist that place classified information at risk, or if there is gross noncompliance with the approved (M)SSP, an IATO or ATO can be revoked. Prior to revocation, the RDAA will coordinate with the Deputy Director, ODAA, Deputy Director, Industrial Security Field Operations, the Regional Director (RD), IS Rep and the FOC. If an IATO or ATO is revoked, the ISSM will be notified via e-mail by the RDAA with a copy to the RD, ISSP and FOC. This e-mail will clearly state all security issues that must be resolved. Processing on the IS must cease immediately upon notification by the ODAA. If there is a disagreement between the Deputy Director, ODAA and Deputy Director, Field Operations, the issue will be raised to the Deputy Director, ISP.

Changes to an IS may not require the revocation of the IATO. An IATO is a temporary approval. If a system has an IATO and the ISSM needs to make changes, the changes can be made to the (M)SSP without reissuing another IATO if ODAA is contacted prior to the changes. However, the (M)SSP and all changes will be frozen one week before the ISSP conducts the onsite validation so that the system matches the (M)SSP when inspected.

Reaccreditation of an IS after a Revocation

Before an (M)SSP can be reaccredited after a revocation, the cleared facility 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.

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

When an IS has come to the end of its usefulness 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 submits a letter signed by the ISSM to the ISSP and IS Rep, to include the UID for the system, reason for disestablishment, and the disposition of the hard drive(s) and media. The ISSP/C&A Reviewer will validate that the IS has been effectively declassified in accordance with the (M)SSP and forward the recommendation to terminate the accreditation to the RDAA.

Figure 7 Flow Diagram For Initial (M)SSP

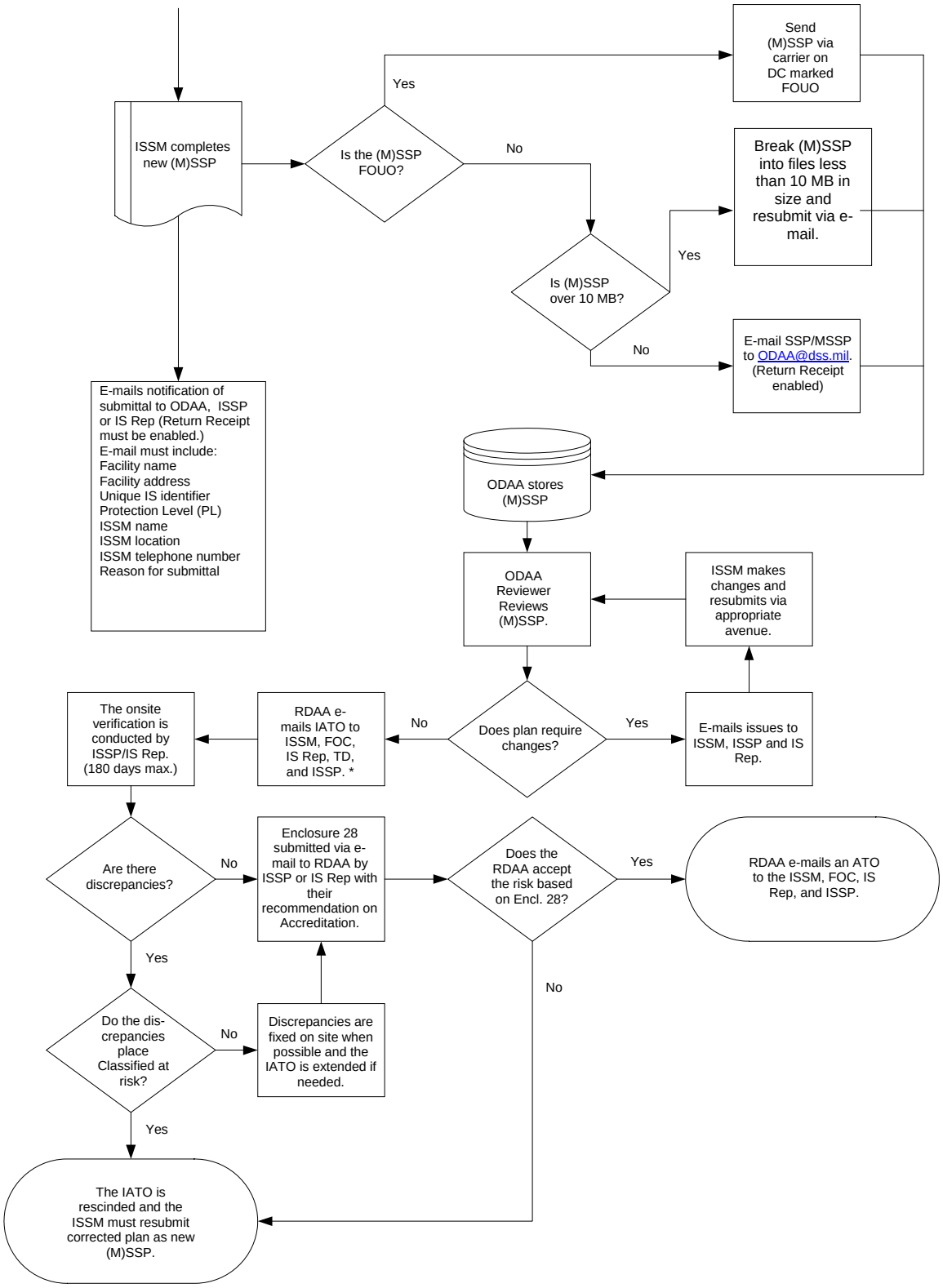
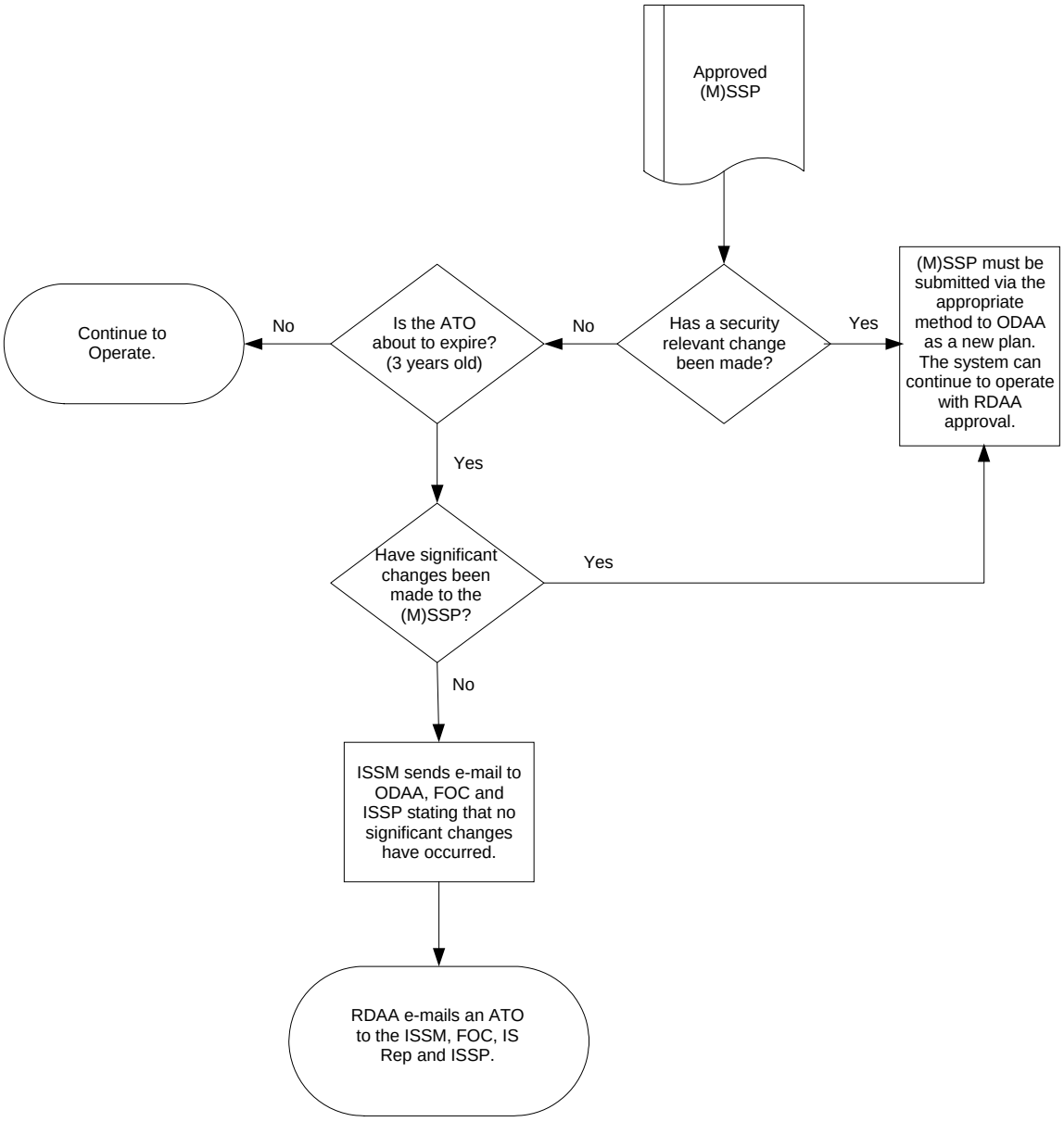


Figure 8 Flow Diagram for a Reaccreditation and Re-evaluation



5.1.6.2 Software Protections

Software from unknown or questionable sources will not be used on an 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 be loaded from media that is write-protected. Software will be screened and/or tested for malicious code or logic.

(ISL 2007-01 #18) Unclassified software that will eventually be used during classified processing periods must either be developed by cleared, knowledgeable personnel or reviewed and/or tested by cleared, knowledgeable personnel. This includes operating system, virus detection and software sanitization software. The best method to safeguard is to develop the software on the classified system. If developing the software in an unclassified environment 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. Software disconnects are not permitted on ISs that process at the TOP SECRET level.

5.2 OPERATIONAL CONTROLS

5.2.1 AWARENESS AND TRAINING (AT)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	**CNTL NO.**	**CONTROL NAME**	**NISPOM Reference**	**PM location Para heading**	**Protection Levels Confidentiality**
Operational		**Awareness and Training**			
* not addressed **not contractually imposed	AT-1	Security Awareness and Training Policy and Procedures	8-101	Security Education	
	AT-2 AT-2 (1)	Security Awareness Security Awareness Control Enhancement	8-101	Security Education *	
	AT-3	Security Training	8-101,8-103, 8-104	Cleared Contractor Training	
	AT-4	Security Training Records	8-103,8-104	Security Education	

5.2.1.1 Security Education

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

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

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

5.2.1.2 Cleared Contractor Training

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

1. The Center for Development of Security Excellence (CDSE)
2. ODAA staff
3. Contractor seminars, workshops, conferences, etc
4. 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 can be more readily 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 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 are highly encouraged and are designed to strengthen IS security controls, protection of classified data, and accountable system access controls. Also, the technical configuration standards are designed in concert with (M)SSP templates. Any deviation from these configuration standards will require DSS further 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.

- ODAA NISP Tool – this tool is designed to assist cleared contractors and DSS staff in ensuring technical configurations are set and provide a level of evidence that system security controls are in place. This tool is also designed in conjunction with the (M)SSP template and Baseline Technical Security Configurations. Specifically, this analysis tool evaluates the operating systems to identify vulnerabilities and non-compliant settings.

5.2.2 CONTINGENCY PLANNING (CP)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	CNTL NO.	CONTROL NAME	NISPOM Reference	PM location Para heading	Protection Levels Confidentiality
Operational		Contingency Planning			
* not addressed **not contractually imposed	CP-1	Contingency Planning Policy and Procedures	8-603	Contingency Planning **	
	CP-2	Contingency Plan	8-614	Contingency Planning **	
	CP-2 (1)	Contingency Plan Enhanced Control		**	
	CP-2 (2)	Contingency Plan Enhanced Control		**	
	CP-2 (3)	Contingency Plan Enhanced Control		**	
	CP-3	Contingency Training	8-615	Contingency Planning **	
	CP-3 (1)	Contingency Training Enhanced Control		**	
	CP-3 (2)	Contingency Training Enhanced Control		**	
	CP-3 (3)	Contingency Training Enhanced Control		**	
	CP-4	Contingency Plan Testing and Exercises	8-615	Contingency Planning **	
	CP-4 (1)	Contingency Plan Testing and Exercises Enhanced Control		**	
	CP-4 (2)	Contingency Plan Testing and Exercises Enhanced Control		**	
	CP-4 (3)	Contingency Plan Testing and Exercises Enhanced Control		**	
	CP-6	Alternate Storage Site	8-603	Contingency Planning **	
	CP-6 (1)	Alternate Storage Site Enhanced Control		**	
	CP-6 (2)	Alternate Storage Site Enhanced Control		**	
	CP-6 (3)	Alternate Storage Site Enhanced Control		**	
	CP-7	Alternate Processing Site	8-603	Contingency Planning **	
	CP-7 (5)	Alternate Processing Site Enhanced Control		**	
	CP-8	Telecommunications Services	8-615	Contingency Planning **	
	CP-8 (1)	Telecommunications Services Enhanced Control		**	
	CP-8 (2)	Telecommunications Services Enhanced Control		**	
	CP-8 (3)	Telecommunications Services Enhanced Control		**	
	CP-8 (4)	Telecommunications Services Enhanced Control		**	
	CP-9	Information System Backup	8-603,8-612	System Recovery and Assurances	
	CP-9 (1)	Information System Backup Enhanced Control		System Recovery and Assurances	
	CP-9 (2)	Information System Backup Enhanced Control		System Recover and Assurances	
	CP-9 (3)	Information System Backup Enhanced Control		System Recovery and Assurances	
	CP-10	Information System Recovery and Reconstitution	8-613	System Recovery and Assurances	1,2,3
	CP-10 (1)	Information System Recovery and Reconstitution Enhanced Control		*	

	CP-10 (2)	Information System Recovery and Reconstitution Enhanced Control		**	
	CP-10 (3)	Information System Recovery and Reconstitution Enhanced Control		System Recover and Assurances	

5.2.2.1 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.

5.2.2.2 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 (in IS profile) will be completed by the ISSM verifying 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.

5.2.3 INCIDENT RESPONSE (IR)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	**CNTL NO.**	**CONTROL NAME**	**NISPOM Reference**	**PM location Para heading**	**Protection Levels Confidentiality**
Operational		**Incident Response**			
* not addressed **not contractually imposed	IR-1	Incident Response Policy and Procedures	8-101, 8-103	Classified Spills	
	IR-2	Incident Response Training	8-103, 8-104	addressed at AT-1 (Security Education)	
	IR-2 (1)	Incident Response Training Control Enhancement		*	
	IR-2 (2)	Incident Response Training Control Enhancement		*	
	IR-3	Incident Response Testing and Exercises		*	
	IR-3 (1)	Incident Response Testing and Exercises Control Enhancement		*	
	IR-4	Incident Handling	1-303, 4-218, ISL 2006-02 #5	Classified Spills	
	IR-5	Incident Monitoring	1-303, 4-218, ISL 2006-02 #5	Classified Spills	
	IR-5 (1)	Incident Monitoring Control Enhancement		*	
	IR-6	Incident Reporting	1-303, 4-218, ISL 2006-02 #5	Classified Spills	
	IR-6 (1)	Incident Reporting Control Enhancement		*	
	IR-7	Incident Response Assistance		*	
	IR-7 (1)	Incident Response Assistance Control Enhancement		*	
	IR-8	Incident Response Plan	8-103, 1-302	Incident Response Plan	

GCA/Customer is the data owner and contractor should GCA/Customer procedures/guidance. If GCA/Customer does not provide procedures/guidance then procedures/guidance contained in this process manual should be followed if the GCA/Customer concurs.

5.2.3.1 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 for the facility concerned.

5.2.3.1.1 Incident Response Plan

The contractor shall 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 shall be distributed to appropriate incident response personnel. The incident response plan shall be reviewed and revised when appropriate to ensure accuracy to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

Note: wiping (overwriting) can be used for the cleanup of spills, but can no longer be used for sanitization of disks used with systems accredited to process classified.
Note: The tracking of hard drives involved in a spill cleanup is no longer required.

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, *Information Assurance (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.

5.2.3.1.2 Sanitizing and Declassifying

Sanitizing removes information from media to render the information unrecoverable by technical means (e.g., you cannot recover it in a laboratory environment). 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 and declassification.

5.2.3.1.3 Classified Spill Cleanup Procedures

The following procedures apply to all cleared facilities, on both accredited and non-accredited systems. These procedures will be used to cleanup spills at SECRET and below. TOP SECRET spills 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 System Security Managers (ISSM), Information System 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 DSSA Chapter 8 course.

5.2.3.1.4 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:

1. If wiping whole disks, it must be able to wipe the entire drive (i.e. partition tables, user data, operating systems and boot records).

2. If wiping whole disks, it must be able to wipe Device Configuration Overlay (DCO) hidden sectors if ATA-6 disks are being used.

3. If wiping whole disks, it must be able to wipe a Host Protected Area (HPA).

4. 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.

5. 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.

6. 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, 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.

5.2.3.1.5 DSS-Approved Classified Spill Cleanup Plan

Purpose

This document describes a procedure for cleanup of information systems (IS) 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 Office of the Designated Approving Authority (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 non-cleared company or individual that does not fall under the NISPOM (i.e. to a Yahoo user, or to a non-cleared 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.

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 Responsibilities

The local FSO for the facility where the contamination is first reported will act as the incident lead. The FSO will:

- Notify applicable Government agencies of the security incident. **NOTE: 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. (ISL 2006-02 #5)**
- 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 responsibilities

- Assess the extent of contamination and plan cleanup actions with the local ISSM.

- Conduct cleanup of contaminated systems and any peripherals using cleared personnel.

- 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.

5.2.3.1.6 Contamination Cleanup Procedures

Coordination

Communications: Employees or security managers who report the discovery of classified information on unclassified 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 local FSO for the facility where the contamination is first reported 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 shall promptly submit an initial report of the incident unless notified by the CSA. The initial report shall be distributed via secure channels (STE, secure fax, cleared network, etc.). If secure channels are not available the initial report shall not include location and/or classification of the spill.

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

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

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

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.

Figure 9 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 Verification:

Print Name:

_____.

Signature:

_____.

Figure 10 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. For details go to sub-process E.	
☐	B2	Interview each individual who received the contaminated e-mail message. Inform each individual: a. a: That they are to cease all e-mail activities until further notice. b. b: 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.	

Check Box	Step ID	Step Description	Step Owner
☐	B5	Disable all affected User's Exchange mailbox access. a. Start/Programs/Microsoft Exchange/Active Directory Users and Computers. b. Right click on domain and select 'Find'. c. Enter affected user's name in the Name field and select 'Find Now'. d. Open Properties of the user object and select 'Exchange Advanced' tab. e. Click on the 'Mailbox Rights' button. f. Highlight the user's account and enter a check in all the 'Deny' check boxes. g. Click the ADD button. h. Select the name of the Exchange Administrator who will sanitize the contaminated users' mailbox. i. Grant Admin full mailbox permissions to each contaminated mailbox and check all boxes EXCEPT "Associated External Account" for this admin account. j. 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: a. Determine the path in which a contaminated e-mail has traveled so that all compromised Exchange servers can be targeted for cleansing. b. Determine all recipients of the contaminated e-mail so that each contaminated Mail Box can be cleansed. c. 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. _____ _____ _____	

Check Box	Step ID	Step Description	Step Owner
☐	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.	

Check Box	Step ID	Step Description	Step Owner
☐	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: a. Start/Programs/Microsoft Exchange/System Manager/Administrative Groups/ Servers/ <Mail Server Computer Name>/ Storage Group that contains the contaminated Mail Box(es) b. Right click on the Storage Group (i.e.: "SG1") and click properties. c. 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 a. Start Backup = MS Event ID# 220 b. Stop Backup = MS Event ID# 221,223 (224) If Backup of the Exchange Server is spooled to : 1. TAPE media, then these backup TAPES must also be identified and secured with TAPE media in Step "B1". 2. DISK media, then all DISKS used for the Exchange Server backup must be zeroed with an DSS-approved disk cleansing utility. 3. 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: a. Start Zeroing = MS Event ID# 706, 712, 718 b. 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.	

Check Box	Step ID	Step Description	Step Owner
☐	B17	Re-activate each User's Mailbox on the server. a. Start/Programs/Microsoft Exchange/Active Directory Users and Computers. b. Right click on domain and select 'Find'. c. Enter affected user's name in Name field and select 'Find Now'. d. Open Properties of the user object and select 'Exchange Advanced' tab. e. Click on the 'Mailbox Rights' button. f. Highlight the user's account and uncheck all the 'Deny' check boxes. g. Remove the Exchange Admin account that was added in step "B5". h. 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.	
☐	B20	Ensure all printed material and backup tapes have been turned over to security	

Exchange Server Cleansing Completion Date: _____.

Signature of Verification:

Print Name:

_____.

Signature:

_____.

Figure 11 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. a. Run NWADMN32. b. From the GroupWise View or NDS View, locate Users in question – click for detail window. c. Click on 'GroupWise Account' tab. d. Select 'Disable Logins' box then OK.	

Check Box	Step ID	Step Description	Step Owner
☐	C6	Have any of the Users 'forwarded' the contaminated e-mail to other individuals? Yes / No: _____. a. Run NWADMN32 b. From the GroupWise View or NDS View, locate Users in question – click for detail window. c. Click on 'GroupWise Account' tab. d. Change Users password for accessing e-mail account. e. Run 'grpwise.exe /@u-?'. e. Login as User with new password. f. 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.	

Check Box	Step ID	Step Description	Step Owner
☐	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.	

Check Box	Step ID	Step Description	Step Owner
☐	C11	As a GroupWise Administrator, locate the contaminated e-mail message. a. Use Novell's stand-alone version of 'GWCHK32.EXE' to locate and delete the contaminated message. Place this program on your local hard drive. b. Determine the exact 'Subject' line of the e-mail. c. 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. d. Edit the text file and put the EXACT subject line in the file. For example: If the subject line reads: "RE Important Message From: John Doe" or "FWD: Important Message From: John 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. e. Map a drive to the location of the GroupWise Post Office: \\server\volume\PODir\ f. Launch the GWCHK32.EXE program. g. 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 h. Click the 'Run' button. i. 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.	

Check Box	Step ID	Step Description	Step Owner
☐	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 Verification:

Print Name:

_____.

Signature:

_____.

Figure 12 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 Verification:

Print Name:

_____.

Signature:

_____.

Figure 13 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.

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.

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.

5.2.4 MAINTENANCE (MA)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	CNTL NO.	CONTROL NAME	NISPOM Reference	PM location Para heading	Protection Levels Confidentiality
Operational		**Maintenance**			
* not addressed **not contractually imposed	MA-1	System Maintenance Policy and Procedures	8-304	Maintenance	
	MA-2	Controlled Maintenance	8-304	Maintenance	
	MA-2 (1)	Controlled Maintenance Control Enhancement		Maintenance	
	MA-2 (2)	Controlled Maintenance Control Enhancement		*	
	MA-3	Maintenance Tools	8-304	Maintenance	
	MA-3 (1)	Maintenance Tools Control Enhancement		Maintenance	
	MA-3 (2)	Maintenance Tools Control Enhancement		Maintenance	
	MA-3 (3)	Maintenance Tools Control Enhancement		*	
	MA-4	Non-Local Maintenance		Remote Maintenance	
	MA-4 (3)	Non-Local Maintenance Control Enhancement		Remote Maintenance	
	MA-5	Maintenance Personnel	8-304	Maintenance	
	MA-5 (1)	Maintenance Personnel Control Enhancement		Maintenance	
	MA-5 (2)	Maintenance Personnel Control Enhancement		Maintenance	

5.2.4.1 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 shall be checked for malicious code before the media is connected to the system.

5.2.4.2 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.

5.2.4.3 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 IS. Special attention should be given to portable units containing memory and/or have retention capabilities. These devices may require accreditation by DSS. Prior to admittance of any uncleared maintenance personnel, the area will be inspected to verify that no classified material is remaining within visual access. Prior to maintenance, the IS will be downgraded and all non-volatile data storage media will be removed or physically disconnected and secured. The separate, "UNCLASSIFIED – FOR MAINTENANCE ONLY", copy of the operating system and diagnostic routines will be loaded. If it is not feasible to clear the IS or if clearance will impede maintenance activities, the following procedures will be followed: The technically knowledgeable escort will log into their account. If possible, the escort will remain in control of the keyboard and take instructions from the maintenance person on activities to perform. If the uncleared person is given keyboard access the escort will monitor all input and output to the IS (i.e. keystroke monitoring) to ensure only system files are accessed and no user files are viewed.

5.2.4.4 Remote Maintenance

Remote maintenance procedures (when required) shall be developed by the ISSM and approved by the CSA before implementation. All other options shall 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 shall be described in the (M)SSP.

5.2.5 MEDIA PROTECTION (MP)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	**CNTL NO.**	**CONTROL NAME**	**NISPOM Reference**	**PM location Para heading**	**Protection Levels Confidentiality**
Operational		**Media Protection**			
* not addressed **not contractually imposed	MP-1	Media Protection Policy and Procedures	8-306, 8-309	Media Protection	1,2,3
	MP-2	Media Access	8-310	Media Protection	1,2,3
	MP-2 (1)	Media Access Control Enhancement		*	
	MP-3	Media Marking	8-306, 8-310	Media Protection and Trusted Downloading	
	MP-4	Media Storage	8-308	addressed at PE-1 (Hardware and Software Protections)	
	MP-4 (1)	Media Storage Control Enhancement		addressed at PE-1 (Hardware and Software Protections)	
	MP-5	Media Transport	8-605	Mobile Processing Procedures	1,2,3
	MP-5 (2)	Media Transport Control Enhancement		Mobile Processing Procedures	
	MP-5 (3)	Media Transport Control Enhancement		Mobile Processing Procedures	
	MP-5 (4)	Media Transport Control Enhancement		addressed at PE-4 (PDS)	
	MP-6	Media Sanitization and Disposal	8-301,8-608	Clearance and Sanitization	1,2,3
	MP-6 (1)	Media Sanitization and Disposal Control Enhancement		Clearance and Sanitization	
	MP-6 (2)	Media Sanitization and Disposal Control Enhancement		Clearance and Sanitization	
	MP-6 (3)	Media Sanitization and Disposal Control Enhancement		Clearance and Sanitization	
	MP-6 (5)	Media Sanitization and Disposal Control Enhancement		Clearance and Sanitization	
	MP-6 (6)	Media Sanitization and Disposal Control Enhancement		Clearance and Sanitization	

5.2.5.1 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 any media which fits any of the following descriptions:

1) Media containing classified data
2) Media that was or is mounted without write-protection enabled on a classified IS This is most often media that has been specifically designated for the storage of classified information.

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

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 (i.e. once per day) 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 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. 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 shall 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.

5.2.5.2 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, shall 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 media shall also be marked.

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

5.2.5.3 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 System (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 NISPOM Chapter 8 do not support more than one classification and/or sensitivity level of information. Simply stated, the IS cannot recognize or distinguish information based on content. All information residing or processed on a PL 1, 2 or 3 IS are handled/treated at the classification/sensitivity level for which the IS is accredited. ODAA approved trusted download procedures follow 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.

5.2.5.3.1 Trusted Download Procedures

Scope

The February 2006 NISPOM Chapter 8 requirements for trusted download shall 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)
- The applicable DSS standard file type/formats and file transfer procedures documented in the IS (M)SSP
- Where authorized on the DD-254 or as a contract line item, alternate detailed procedures included in the IS SSP which constitutes an acknowledgement and acceptance of additional risk from the government customer/data owner.

NISPOM Requirements for Trusted Downloading

The following Chapter 8 requirements apply to trusted downloading:

8-310a. Human-Readable Output Review. An appropriate sensitivity and classification review shall 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 shall be verified by a comprehensive review (in human-readable form) of all data on the media including embedded text (e.g., 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) based on Security Classification Guide(s), restriction(s).

Acceptance of Risk. Alternative 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 shall 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 shall be created by a "Knowledgeable User" following the DSS "File Transfer Procedure" as defined in the IS's (M)SSP.

Knowledgeable User. An IS user (general or privileged) who is considered a data matter expert with extensive knowledge of all appropriate security classification guide(s), and who can perform the "Comprehensive Review". The User shall be trained by the Information System Security Manager (ISSM) or Information System Security Officer (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 System (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. For the most part every application, 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 system. 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 (note: does not include MAC X O/S)
- 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.

5.2.5.3.1.1 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 (i.e., 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:

Table 4 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'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**

*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.

5.2.5.3.1.2 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. What's important to remember about these or any alternate procedure is that the contractor 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:

1. The file types/formats and transfer procedures must be certified by DSS and documented in the SSP.

2. Target media must be factory fresh.

3. A comprehensive review must be performed so as to ascertain the sensitivity and classification level of the data.

4. Classified path/file embedded links and/or classified path/file name(s) are not used for source or target file(s).

5. The compilation of all files on the target media does not cause an increased classification level due to "Aggregation".

6. File(s) are transferred using a known, authorized utility or command.

7. The target media is verified to contain only intended source file(s).

8. File(s) are verified on target media to contain the correct sensitivity of information and/or level of unclassified or lower classified information.

9. The appropriate security classification label is applied to the target media.

10. 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.

5.2.5.3.1.3 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 (i.e. .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. is examined. 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, but some items will not apply:

PowerPoint:

   a. 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.

   b. 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).

   c. For each slide, click on **Edit**, then **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.

d. 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.

   a. Spreadsheet and database files must be exported as an ASCII text file(s).

   b. 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.

   c. 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.

   a. 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. Internet Explorer or Netscape 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.

   b. 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).

   c. 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**.

   d. Review remaining ASCII files not viewable with NotePad with MS Word:

      (1) 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.

      (2) 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**.

(3) 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.

(4) 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. Note: If a document has multiple sections, each section may have different Headers and Footers.

(5) 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.

(6) 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.

(7) 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. Note: Embedded objects may be opened and saved separately prior to deletion. Each separately saved object is subject to this procedure prior to transfer.

(8) 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**.

e. 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.

5.2.5.3.1.4 DSS Authorized Procedure (Unix)

Note: These procedures should be tailored for the local environment. In particular, the Unix commands listed herein are for illustration only and must be modified to account for the Unix 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."

    a. For text files use software that displays the entire contents of the file. (EG: Hex editor) Any unintelligible data is assumed to be classified at the accredited IS level.

    b. 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).

    c. 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.

        (1) 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.

        (2) 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.

(3) In the case of binary database files, export the data to ASCII text format, then review and downgrade the text file for media migration.

(4) 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.

Figure 14 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:

Figure 15 Trusted Download Record

Date	Person	File Type	File Description

5.2.5.3.1.5 Alternate Trusted Download Risk Acceptance Letter (RAL) Example

(Government letterhead)

[GCA/Data Owner Name]
[Address]

SUBJECT: Acceptance of Risk to Classified Information

TO: *[Contractor]*

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

2. 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.

3. Working in combination with a DSS Information System 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.

4. 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.

5. 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.

_____
Customer/sponsor or data owner Signature

_____ ( ) -
Printed Name Phone #

5.2.5.4 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. DSS has determined that for periods greater than 120 days the facility at which classified processing is being conducted will submit an (M)SSP so that DSS can conduct that appropriate risk management evaluation based on that facility.

Definition

A mobile system is system that is accredited by the CSA or self-certified by the ISSM under an MSSP to process classified information at one location, and temporarily relocate 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. NOTE: When relocated, systems that are connected to another system require an NSP.

Types of Mobile Systems

There are two categories of mobile systems; systems that are relocated to other contractor sites, or 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 be on 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 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 should follow self-certification procedures (if any)

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.

DSS Form Letter 16

The DSS Form Letter 16 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 Letter 16 will be valid for the life of the contract or system accreditation, whichever is less. The owning ISSM must provide a separate Letter 16 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, contractor sites, or relocated within the facility to conduct briefings, presentations, data analysis, or tests. 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.

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:

- Identify the system.
- List relocation site(s) and type of site (i.e. Government or Contractor).
- 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).
- How the equipment, dedicated software, and all classified information are to be transported and safeguarded.
- 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.
- 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.

- Before the accredited IS 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.
- 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).
- The FSO or ISSM must provide the receiving location with a copy of the SSP and the IS Accreditation Letter. The ISSM of record (i.e., ISSM of facility where the IS was accredited) must provide any training and/or briefings necessary to the receiving ISSM.
- 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

- The contractor will provide the applicable government sites with a copy of the approved SSP, DSS IS Accreditation Letter, and a DSS Form Letter 16 acknowledging relocation of the IS to a particular government site if the system is to remain overnight or longer.
- 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.
- An approved MOU must be provided if the DSS accredited system will connect to a government accredited system.

NOTE: All documentation must be retained for auditing purposes.

Documentation

- 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 (i.e., 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.

5.2.5.4.1 Mobile Processing Procedures

[IS Number]

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.

Figure 16 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:

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 shall notify DSS no later then 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:

1) Designate, in writing to the DSS Representative who will be responsible for the system at the relocation site.
2) Maintain a complete copy of the system documentation to accompany equipment.
3) Update the system maintenance log to reflect movement to and from the facility.
4) Brief users accompanying the system on their responsibilities to include:
   a) Maintaining the audit records of the system (automated or paper).
   b) Responsibilities for maintaining the integrity of the security seals (if equipment is in an unclassified area).
   c) Make certain that the equipment is properly downgraded (if not in an approved closed area at system approval level with appropriate need-to-know).
   d) Establishing a process so that media (paper and magnetic) is properly reviewed and labeled.
   e) Ensuring that the weekly audit (review) is performed and annotated on the review record.
   f) Bringing any discrepancies to the attention of the ISSO.
   g) Responsibility that all records are returned with the system.
5) 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.
6) 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.

Figure 17 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:

Figure 18 System Component Information Form

System Identification

System/Component Information

[Facility Information]

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: (mm/dd/yy)	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

Mobility Plan
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 shall 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 then 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

1. The recipient organization must notify the dispatching organization and **[Facility]** Security of any security relevant problems that occur.

2. The recipient organization must notify the dispatching organization and **[Facility]** Security of any discrepancies in the documentation or equipment.

Letter 16 – Letter Acknowledging Relocation of IS By Government Activity/Site (Sample)

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).

1. 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.

2. (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.

3. 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).

4. 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)

5.2.5.5 Clearing and Sanitization

5.2.5.5.1 Clearing

NISPOM 8-301(a) refers to a procedure by which classified information is removed in such a manner that known non-laboratory attacks (i.e., 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 to have access to classified information are present (NISPOM paragraph 8-304(b)(3). 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. Once cleared, personnel with a lower access level can use the equipment provided that the SSP describes how the equipment will remain safeguarded during these times.

5.2.5.5.2 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. Sanitization of memory and media is required if a system is being "released" to users with access level lower than the accreditation level.

5.2.5.5.3 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).

Note: The terms "Type I-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.

Figure 19 Matrix for Degaussing Media

If the Degausser is:	Then the Coercivity levels are:	It will sanitize or clear the following media:			
		Type I	Type II	Type IIA	Type III
Type I	0-350 Oe	S	C	C	C
Type II	351-750 Oe	S	S	C	C
Type II Extended Range	751-1000 Oe	S	S	S	C
Type III	1001-1700 Oe and above	S	S	S	S

S – Media is considered sanitized and can be declassified.
C – Media is only considered cleared and retains its original classification.

The destruction of optical media, compact disc (CD), and DVD media present unique destruction issues. There are three basic types of CD and DVD media (e.g., CD-ROM, CD-R, CD-RW) and two categories, types that are recordable (i.e., 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.

5.2.5.5.4 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:

1. 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.

2. 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 then fill out a Contractors Approval Form (provided by NSA) and follow the instructions provided by the destruction engineers at NSA.

3. Destruction by the organization – If the organization does not meet the criteria of option 1 or 2, the organization must destroy the materials. The Contract Manager should call the NSA Media Destruction Customer Service Center at (301) 688-6672 to obtain information on approved media destruction equipment or information on approved and licensed destruction sites.

4. Destruction by other organization – An organization can send the materials to another approved organization with an NSA approved method for destruction.

5.2.5.5.5 DSS Clearing and Sanitization Matrix

(Updated March 21, 2008)

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.

Table 5 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																					
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					
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.

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 System Security Plan (SSP) and reviewed/approved in connection with the information system certification and accreditation process. The following summary information is provided for organizations in updating system 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 Information Systems (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.

5.2.6 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	CNTL NO.	CONTROL NAME	NISPOM Reference	PM location Para heading	Protection Levels Confidentiality
Operational		Physical and Environmental Protection			
* not addressed **not contractually imposed	PE-1	Physical and Environmental Protection Policy and Procedures	8-308	Physical Security	1,2,3
	PE-2	Physical Access Authorizations	8-308, 5-306, 5-308, 6-104	Physical Security	1,2,3
	PE-2 (3)	Physical Access Authorizations Control Enhancement	ISL 2007-01, #1	Physical Security	
	PE-3	Physical Access Control	5-300, 6-104	Physical Security	
	PE-3 (1)	Physical Access Control - Control Enhancement	ISL 2007-01, #1	Physical Security	
	PE-3 (2)	Physical Access Control - Control Enhancement		Physical Security	
	PE-3 (3)	Physical Access Control - Control Enhancement		Physical Security	
	PE-4	Access Control for Transmission Medium	8-605	addressed at CA-3 (Information Systems Connections) and PDS	1,2,3
	PE-5	Access Control for Output Devices	8-310	addressed at MP-3 (Media Protection and Trusted Downloading	
	PE-6	Monitoring Physical Access	5-300	Physical Security	
	PE-6 (2)	Monitoring Physical Access Control Enhancement		Physical Security	
	PE-7	Visitor Control	8-307, 6-104	Physical Security	
	PE-7 (1)	Visitor Control Control Enhancement		Physical Security	3

5.2.6.1 Physical Security (8-308, 5-306, 5-308, 6-104)

Safeguards shall 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 shall 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.

Closed Areas are required for ISs that have non-removable media and/or will remain in a classified mode while unattended. All personnel granted unescorted access to an IS Closed Area will have an appropriate security clearance and need-to-know for the area (i.e. Visit Authorization Letter (VAL)). The contractor shall 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 shall 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.

5.2.6.2 Hardware and Software Protection

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 (i.e. store in a closed area).

5.2.6.3 Protected Distribution System (PDS)

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.

(NISPOM 8-605) 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 IS Rep will verify that the contractor uses National Security Agency (NSA) Type 1 encryption devices when transmitting classified information outside its facility and either NSA Type 1 devices or a Protected Distribution System (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 or ISSP must be involved in the early stages of PDS design and 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 installation. This avoids those instances where money would have been unnecessarily spent on a PDS that does not meet NSTISSI 7003 and would require re-engineering in order to be approved.

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, 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 install, but before the wall or column is closed. When this is not possible, an alternative is for the ISSM to witness the installation and provide verification that it was correct. The ISSM may use photos of the installation to provide a record for review and to help substantiate the verification. If none of these options is possible, the wall or column must be opened for inspection. The IS Rep will *not* approve a PDS installation if classified information is at risk of being compromised. The IS Rep will validate and or verify that the PDS is used for the transmission of classified information; unclassified wire lines cannot be in the same PDS as classified wire 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. Fiber optic is no exception. 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 wire 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 user or ISSO must notify the ISSM immediately, and processing classified information will be discontinued until the reason for the tampering is determined and all security issues are resolved. PDS will be incorporated into the SSP accreditation.

During security reviews, ISSPs and authorized C&A Reviewers will validate and or verify transmission procedures established at certification are maintained.

Note: There are no UL standards for alarming a PDS, but the alarm companies used for alarming a Closed Areas can be used 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.

Defense Security Service

Protected Distribution System Installation Plan

Submitted by:

Robert Smith
Company
100 Company Rd
Suite 100
City, State Zip code

PDS Security Plan Revision Log			
By signing the PDS Security Plan Revision log I certify that all information contained within this document is accurate.			
Revision	**Description of Baseline Change**	**ISSM Signature / Certification**	**Submittal & Approval Dates**

DAA PDS Approval

The Defense Security Service has reviewed this Protected Distribution System Installation Plan and has determined that it meets the criteria of the National Industrial Security Program operating Manual (NISPOM) dated February 28, 2006; and NSTISSI7003, Protected Distribution system (PDS), dated 13 December 1996.

Accordingly, we hereby grant approval to Company Name, Location for this Protected Distribution System Installation Plan, including self-certification of additional Protected Distribution Systems having similar construction. Re-approval is required if there is a change affecting the security posture of the facility.

This is my formal declaration that Company Name, Location has properly implemented the Protected Distribution System and that a satisfactory level of security is present. It is the responsibility of the Information Systems Security Manager (ISSM) to make certain that any changes in configuration, threat, environment, or other modification is analyzed to determine its impact and to take appropriate action, including notification of the DAA, in order to maintain a level of security consistent with the requirements of this approval.

In accordance with paragraph 1-206(a) of the NISPOM, DSS will conduct periodic onsite technical reviews of the facility Protected Distribution systems to validate and or verify that safeguards identified in this plan are adequate for the protection of classified information.

_____

IS Rep Signature
Defense Security Service
Industrial Security Field Office _____
Date

Protected Distribution System Approval Request

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

1.0 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.

2.0 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.

3.0 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.

4.0 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.

5.0 Facility Security:

5.1 Provide a map of the residential and commercial area and indicate the facilities approximate location on the map as Appendix A.

5.2 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.

5.3 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.

5.4 – 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.

6.0 Building Security:

6.1 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.

6.2 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.

6.3 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.

6.4 Describe the types of doors and locks securing the access points.

6.5 Indicate whether a personnel badge recognition system is in use and if access lists are maintained.

6.6 Indicate the clearance level of personnel entering the building and if a clearance is required for unescorted access.

6.7 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.

7.0 Protected Distribution System:

7.1 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.

7.2 Provide the classification level of the area controlled, and indicate if uncleared personnel are monitored.

7.3 Describe the construction of the PDS.

7.4 Describe the inspection procedures for the detection of tampering.

7.5 Indicate whether or not the PDS will be alarmed and describe the alarm system in detail.

5.2.6.4 Emergency Procedures (5-104)

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

5.2.6.5 TEMPEST (11-100)

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:

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

5.2.7 PERSONNEL SECURITY (PS)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	**CNTL NO.**	**CONTROL NAME**	**NISPOM Reference**	**PM location Para heading**	**Protection Levels Confidentiality**
Operational		**Personnel Security**			
* not addressed **not contractually imposed	PS-1	Personnel Security Policy and Procedures	8-307	Personnel Security Clearance Verification	
	PS-2	Position Categorization	8-307	addressed at PL-4 (Roles and Responsibilities)	
	PS-3	Personnel Screening	8-103, 8-104, 8-307	Personnel Security Clearance Verification	
	PS-3 (1)	Personnel Screening Control Enhancement		Personnel Security Clearance Verification	
	PS-3 (2)	Personnel Screening Control Enhancement		Personnel Security Clearance Verification	
	PS-4	Personnel Termination	8-303, 5-309	Personnel Security Clearance Verification	
	PS-5	Personnel Transfer	8-303, 5-309	Personnel Security Clearance Verification	
	PS-6	Access Agreements	8-103, 8-104	Personnel Security Clearance Verification	
	PS-6 (1)	Access Agreements Control Enhancement		Personnel Security Clearance Verification	
	PS-6 (2)	Access Agreements Control Enhancement		Personnel Security Clearance Verification	
	PS-7	Third-Party Personnel Security	8-304	addressed at MA-5 (Maintenance Personnel)	
	PS-8	Personnel Sanctions	1-304	Personnel Sanctions	

5.2.7.1 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 IS.

5.2.7.2 Personnel Sanctions

(1-304) Contractor management shall establish and enforce sanctions on personnel failing to comply with the established information security policies and procedures.

5.2.8 SYSTEM AND INFORMATION INTEGRITY (SI)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	**CNTL NO.**	**CONTROL NAME**	**NISPOM Reference**	**PM location Para heading**	**Protection Levels Confidentiality**
Operational		**System and Information Integrity**			
* not addressed **not contractually imposed	SI-1	System and Information Integrity Policy and Procedures	8-101	addressed at CM-1 (Configuration Management Process)	
	SI-2	Flaw Remediation	8-610, ISL 2007-01 #17, #18 & #32	Flaw Remediation	
	SI-2 (1)	Flaw Remediation Control Enhancement		*	
	SI-2 (2)	Flaw Remediation Control Enhancement		*	
	SI-3	Malicious Code Protection	8-305	Antivirus	
	SI-3 (1)	Malicious Code Protection Control Enhancement		*	
	SI-3 (2)	Malicious Code Protection Control Enhancement		*	
	SI-3 (3)	Malicious Code Protection Control Enhancement		Antivirus	
	SI-4	Information System Monitoring Tools and Techniques	8-602	addressed at control CA-3 (Firewall and IDS)	
	SI-4 (4)	Information System Monitoring Tools and Techniques Control Enhancement		addressed at control CA-3 (Firewall and IDS)	
	SI-4 (10)	Information System Monitoring Tools and Techniques Control Enhancement		addressed at control CA-3 (Information Systems Connections)	

5.2.8.1 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 system error handling, are also addressed expeditiously. Maintaining security compliance (e.g., patching, service packs, hotfixes) do not require reaccreditation as these are maintenance items and shall be documented as such (i.e., Maintenance, Operating System & Security Software Change Log entries).

5.2.8.2 Unclassified Software Review

An unclassified software review and/or testing encompass provides two options for examination of unclassified software prior to its introduction into the IS and use for classified processing. The contractor may choose either a review or testing of the unclassified software. An unclassified software review must be a line-by-line source code review. Unclassified software testing must include a verification of all functionality for security-relevant items (e.g., includes security relevant software such as all OS software on an IS where Identification and Authentication (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 either be developed by cleared, knowledgeable personnel or reviewed and/or tested by cleared, knowledgeable personnel. The review and/or testing is done to provide reasonable assurance that security vulnerabilities do not exist.

5.2.8.3 Antivirus

Software for the detection of malicious code must be implemented. 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 for viruses and malicious code before being introduced on an IS. Additionally, the ISSM shall ensure that the IS prevents non-privileged users from circumventing malicious code protection capabilities.

5.3 TECHNICAL CONTROLS

5.3.1 ACCESS CONTROL (AC)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	**CNTL NO.**	**CONTROL NAME**	**NISPOM Reference**	**PM location Para heading**	**Protection Levels Confidentiality**
TECHNICAL		**Access Control**			
* not addressed	AC-1	Access Control Policy and Procedures	8-101, 8-606	Access Control	1,2,3
	AC-2	Account Management	8-606	addressed at control IA-1 (Identification and Authentication Management)	1,2,3
**not contractually imposed	AC-2 (1)	Account Management Control Enhancement		*	
	AC-2 (2)	Account Management Control Enhancement		*	
	AC-2 (3)	Account Management Control Enhancement		address at control IA-1 (Identification and Authentication Management)	
	AC-2 (4)	Account Management Control Enhancement		addressed at AU-2 (Audit Requirements)	
	AC-2 (7)	Account Management Control Enhancement		addressed at PL-1 (Users of IS)	
	AC-3	Access Enforcement	8-606	Access Control	
	AC-3 (3)	Access Enforcement Control Enhancement		Access Control	3
	AC-3 (4)	Access Enforcement Control Enhancement		Access Control	2
	AC-4	Information Flow Enforcement		*	
	AC-5	Separation of Duties	8-611	Separation of Function	3
	AC-6	Least Privilege	8-303	addressed at control IA-1 (Identification and Authentication Management)	1,2,3
	AC-6 (1)	Least Privilege Control Enhancement		address at control IA-1 (Identification and Authentication Management)	
	AC-6 (2)	Least Privilege Control Enhancement		addressed at PL-1 (Roles and Responsibilities)	
	AC-6 (5)	Least Privilege Control Enhancement		Access Control	
	AC-7	Unsuccessful Login Attempts	8-609	Successive Logon Attempts	1,2,3
	AC-7 (1)	Unsuccessful Login Attempts Control Enhancement		Session Controls	
	AC-8	System Use Notification	8-609	DoD Warning Banner	1,2,3

AC-9 AC-9 (1)	Previous Logon (Access) Notification Previous Logon (Access) Notification Control Enhancement	8-609	Session Controls Session Controls	2,3
AC-10	Concurrent Session Control	8-609	Session Controls	2,3
AC-11 AC-11 (1)	Session Lock Session Lock Control Enhancement	8-609, ISL 2007-01 #48	User Inactivity User Inactivity	1,2,3
AC-14 AC-14 (1)	Permitted Actions without Identification or Authentication Permitted Actions without Identification or Authentication Control Enhancement	8-501	addressed at control PL-1 (SUSA) addressed at control PL-1 (SUSA)	
AC-16 AC-16 (4)	Security Attributes Security Attributes Control Enhancement	8-306	addressed at control MP-3 (Marking) *	
AC-17 AC-17 (1) AC-17 (2) AC-17 (3) AC-17 (4) AC-17 (5) AC-17 (6) AC-17 (7) AC-17 (8)	Remote Access Remote Access Control Enhancement Remote Access Control Enhancement Remote Access Control Enhancement Remote Access Control Enhancement Remote Access Control Enhancement Remote Access Control Enhancement Remote Access Control Enhancement Remote Access Control Enhancement		* * * * * * * * *	
AC-18 AC-18 (1) AC-18 (2) AC-18 (3) AC-18 (4) AC-18 (5)	Wireless Access Restrictions Wireless Access Restrictions Control Enhancement Wireless Access Restrictions Control Enhancement Wireless Access Restrictions Control Enhancement Wireless Access Restrictions Control Enhancement Wireless Access Restrictions Control Enhancement	8-311	Secure Wireless LANs (S-WLAN) Secure Wireless LANs (S-WLAN) Secure Wireless LANs (S-WLAN) Secure Wireless LANs (S-WLAN) Secure Wireless LANs (S-WLAN) Radio Frequency ID (RFID) Tags	
AC-19 AC-19 (1) AC-19 (2) AC-19 (3) AC-19 (4)	Access Control for Mobile Devices Access Control for Mobile Devices Control Enhancement Access Control for Mobile Devices Control Enhancement Access Control for Mobile Devices Control Enhancement Access Control for Mobile Devices Control Enhancement	8-610	USB Devices and Ports USB Devices and Ports USB Devices and Ports USB Devices and Ports addressed at control MP-1 (Media Protection)	1,2,3
AC-20 AC-20 (1)	Use of External Information Systems Use of External Information Systems Control Enhancement	8-700	addressed at control CA-3 (Information Systems Connections) addressed at control CA-3	

	AC-20 (2)	Use of External Information Systems Control Enhancement		(Information Systems Connections) *	
	AC-22	Publicly Accessible Content		*	

5.3.1.1 Access Control

The ISSM ensures the IS stores and preserves the integrity of the sensitivity of all information internal to the IS. IS entry is based upon users having an account (i.e. User Profile) on each system to which they require access. Users' initial logins must include the entry of both their unique User ID and password. It shall always be required that each and every user authenticate into the IS using a unique User ID and password. For Generic or Group accounts, see 5.3.3.2 Generic or Group Accounts. 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 shall 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 shall 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.

5.3.1.2 Separation of Function

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

5.3.1.3 Logon Banner

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 DoD Warning Banner follows.

DoD 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.

5.3.1.4 Session Controls

5.3.1.4.1 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 shall 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) shall prohibit all remote activities, such as remote logons and anonymous file access.

For PL-2 and PL-3 systems, the system shall be configured to support multiple logon sessions for each user ID or account, the IS shall provide a protected capability to control

the number of logon sessions for each user ID, account, or specific port of entry. The IS default shall be a single logon session.

5.3.1.4.2 User Inactivity

If technically feasible, the IS shall detect an interval of user inactivity, such as no keyboard entries, and shall 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 shall 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 (i.e. screen saver).

5.3.1.4.3 Logon Notification (PL-2/PL-3)

If the operating system provides the capability, the user shall be notified upon successful logon 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 shall require positive action by the user to remove the notice from the screen.

5.3.1.5 USB Devices and Ports

USB ports not required should be disabled physically or by the BIOS. USB memory devices are allowed but must be accounted for and controlled. They must be marked with the highest classification stored on them, and stored in approved containers. They must be destroyed at the end of their usable life since they cannot be sanitized. They must be inventoried and accounted for, and the documentation made available during security reviews.

5.3.1.6 Radio Frequency ID (RFID) Tags

Vulnerabilities associated with the use of 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 (i.e. printers) that are connected to accredited systems processing classified information must be documented in the SSP. See the Defense Information Systems Agency (DISA) Wireless Security Technical Implementation Guide (STIG) Version 6, Release 1, Paragraph 3.5.1 for more information.

5.3.1.7 Secure Wireless LANs (S-WLAN)

The use of S-WLAN technology with classified information must be in accordance with the latest version of the Defense Information Systems Agency (DISA) Wireless Security Technical Implementation Guide (STIG). S-WLAN networks cannot be self-certified and cannot be issued an IATO.

5.3.1.8 Foreign Ownership, Control & Influence (FOCI)

The NISPOM establishes policy concerning the initial or continued eligibility for access to classified information by U.S. companies with foreign involvement; provides criteria for determining whether U.S. companies are under FOCI; prescribes responsibilities in FOCI matters; and outlines security measures that may negate or mitigate FOCI-related security risks to an acceptable level. DSS is responsible for determining if contractors are owned, controlled or influenced by one or more foreign persons or entities. If they are, DSS must evaluate the associated risks and risk-reduction plans presented by the affected contractor to determine the contractor's eligibility for access or continuing access to classified information.

ODAA assists the FOCI Branch in adjudicating the mitigated risk for Information Systems located in Facilities with Foreign involvement. The FOCI Branch is ultimately responsible for approving the Contractor's POA&M for mitigating the risk. The FOCI action officer has the responsibility for coordinating the complete FOCI adjudication package. FOCI adjudication coordination includes HQ FOCI Branch, ODAA, CI, FOC, and IS Rep. Examples of items included with the FOCI mitigation package could include:

- Security Control Agreement (SCA)
- Special Security Agreement (SSA)
- National Interest Determination (NID)
- Security Points of Contacts (name and numbers)
- IT staff controlling US controlled technologies (name, number, location/address)
- IS Configuration Diagrams
- IS Concept of Operations/System Description
- Standard Form 328, Certificate of Foreign Interest

ODAA staff will receive requests for assistance from the FOCI Branch action officer. The FOCI action officer is responsible for ensuring the ODAA staff has the appropriate information to assess the IS operating environment (CSA, SSA, Concepts of Operation, IS Configuration Diagrams, etc).

The following are general guidelines for accessing the contractor FOCI mitigation strategies:

The ODAA reviewer must:

- Determine if adequate documentation is provided to assess the system and verify that acceptable security measures are proposed to protect Sensitive but Unclassified (SBU) data that are required to be protected by the U.S. Government.
- Identify what resource(s) must be protected from the Foreign partners
- Review the proposed solution outline in the network description and configuration diagram.
- Determine if, as is required, all system physical access is located in U.S. controlled space and if all remote connections must be controlled.
- Verify that a U.S. citizen is responsible for controlling authorized users, user requests and restricting the IS.
    - Firewall configuration, monitoring and maintenance
    - Strong authentication preferred (two-factor)
    - Separate domain for sensitive but unclassified servers
- Check if there is separation of duties for Firewall/System Administrator for the foreign entity and U.S. contractor under FOCI.
- Check if there is data encryption at the desktop/laptop level.
- Verify that the U.S. cleared contractor and the foreign owner are using separate unclassified e-mail servers. If a shared e-mail server exists, a procedure should be in place to mitigate the risk of inadvertently sending e-mail to a Foreign partner.
- Provide recommendation response to FOCI action officer as soon as possible, no more than five working days after receiving the request for review and all necessary information.

Please refer to Security Assessment and Authorization (CA), Types of Security Plans, International System Security Plans section for information pertaining to Classified Information Systems with Foreign Interest.

ODAA Mitigation Process for Cleared Facilities under Foreign, Ownership, Control or Influence (FOCI)

The ODAA assists the FOCI Branch in adjudicating the mitigated risk for Information Systems for companies cleared under the auspices of a FOCI mitigation agreement. Reference: NISPOM 2-307.

Procedures to submit new and revised FOCI package to ODAA:

- The Electronic Communication Plan (ECP) and Technology Control Plan (TCP) are components of the FOCI mitigation package.
- The contractor must submit the FOCI package in accordance with procedures established by the FOCI Branch. Refer to the DSS website for guidance at www.dss.mil.
- The FOCI Action Officer will assign an ODAA Unique Identifier (UID) to the package and will forward the package to ODAA via e-mail at ODAA@dss.mil. HQ ODAA will forward a copy of the submittal e-mail to the RDAA, FOC, IS Rep and ISSP.
    - The ODAA UID consists of Region Cage Code-Date-0000X-ECP.
    - Temporary cage code will be used for facilities where a cage code has not been assigned.
    - FOCI Action Officer will notify ODAA when a temporary cage code has been updated to a permanent cage code for the facility.
- ODAA HQ assigns plan to an ODAA Reviewer/ISSP.
- The ODAA Reviewer/ISSP will forward comments or questions for plans needing corrective action back to the FOCI Action Officer with an information copy sent to the IS Rep and FOC.
    - If there is a need for corrective action, the reviewer will use the standard ODAA comments form to communicate necessary changes.
    - Reviewer will forward a recommendation of acceptance, if applicable, to respective RDAA for concurrence
- RDAA will send the ODAA mitigation acceptance to the FOCI Action Officer with an information copy to the ISR, ISS and FOC.
- The FOCI Action Officer will forward information back to the Contractor.

FOCI Information System Mitigation Validation:

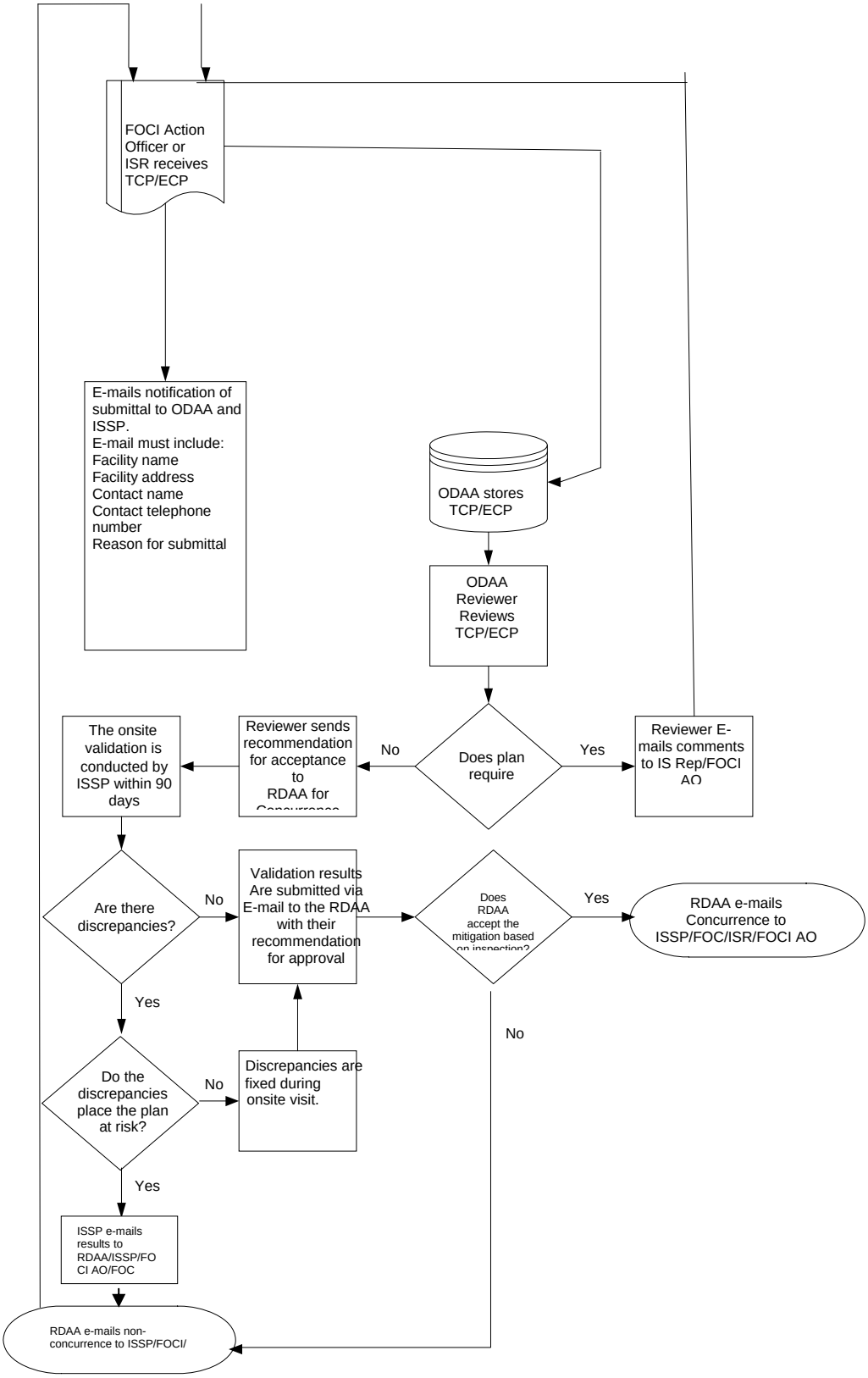
- ISSP will conduct the onsite validation within 90 days after the applicable parties sign the mitigation agreement.
- ISSP will report discrepancies found during the onsite validation to the RDAA, IS Rep and FOCI Action Officer.
- If the plan mitigates risks to an acceptable level, the ISSP will submit the validation results to the RDAA with the recommendation for concurrence.

- If the RDAA concurs, the RDAA will forward concurrence to the FOCI Action Officer, FOC and IS Rep.
- If the plan does not mitigate risks to an acceptable level, the ISSP will submit the validation results to the RDAA with the recommendation for non-concurrence.
- RDAA e-mails the non-concurrence to the IS Rep, FOC and FOCI Action Officer.
- If the onsite validation determines that the risk is not mitigated to an acceptable level, DSS will need to determine what impact the visit outcome has on the facility clearance.

FOCI Information System Mitigation Acceptance

- ISSP submits validation to RDAA with their recommendation for acceptance.
- RDAA e-mails the concurrence for the ECP to the ISSP, FOC, IS Rep and FOCI Action Officer.
- The FOCI Action Officer will forward information back to the Contractor.

Figure 20 FOCI Process Flowchart



The ECP must include the following information:

- Detailed network description to include explicitly what data/information will be shared and what resources will be protected from foreign access.
- Listing of all privileged/super users with citizenship and area of responsibility.
- Physical and logical location of all the information that requires protection from the FOCI.
- Address
  - Access control
  - Access Management
  - Separation of Duties
  - Session Control
  - Remote Access
  - Audit and Accountability Policy
  - Protection of Audit Information
  - Rules of Behavior for Firewalls and Routers
  - Export Control Procedures (include e-mail review)
  - Awareness and Training
  - Incident Response
  - Physical and Environmental Protection
  - Contingency Planning and Operation
  - Configuration Management
  - Maintenance
- Other Items
  - Flow of information/data
  - Type of information (data, e-mail, etc.)
  - Audit points (servers, routers, firewall)
  - The Contractor must limit the number of access points to the information system to effectively monitor inbound and outbound network traffic
  - The Contractor must minimize the number of connections
  - The Contractor must implement a managed interface (boundary protection device such as a firewall) to support any external communications
  - The Information System must deny network traffic by default and allow network traffic by exception
  - The Contractor must employ tools and techniques to monitor events on the shared data and restricted data to detect attacks, and identify unauthorized use of the system.

The following are fundamental guidelines and examples for the ECP reviewer/ISSP:

- ODAA reviewer must ensure adequate documentation is provided to assess the system and ensure acceptable security measures are proposed to protect the controlled information.

- Identify what information/resource(s) are shared with the foreign owner(s).
- Identify what resource(s) must be protected from the foreign owner(s).
- Review the proposed solution outline in the network description and configuration diagram.
- System physical access must be located in U.S. controlled space and all remote connections must be controlled.
- Ensure a U.S. citizen is responsible for controlling authorized users, user requests and administering the IS.
- ECP must include:

  - Firewall configuration
  - Monitoring
  - Maintenance
  - Separate domain for controlled information (example: export controlled and unclassified data relating to a classified contract)

- Separation of duties required:

  - U. S. contractor must employ all Information Technology (IT) personnel
  - Foreign owner must employ separate IT personnel

- A separate e-mail server is preferred for the Contractor. The U.S. company must manage its own e-mail services.
- ODAA will provide recommendation response to FOCI action officer ASAP, no later than thirty (30) working days after receipt of the package.

Example questions and answers for consideration:

The questions and answers below should be used as a guide and not as the sole reasoning for the mitigation strategy. The reviewer is responsible for assessing all submitted risk mitigation proposals and seeking advice with their assigned RDAA if required. The RDAA is responsible for coordinating further action to the ODAA Headquarters staff if warranted.

- Is a firewall in place and configured to deny external access to controlled information (export controlled or unclassified information relating to a classified contract)?

	RECOMMENDATION
YES	Use of a firewall properly configured to deny access from external sources is an acceptable step towards mitigating foreign control or influence.
NO	If there is no firewall or the firewall is configured to allow external access to the internal LAN, then there is a potential for foreign control or influence of the company's unclassified network and information.

- Is remote administration of any server allowed?

	RECOMMENDATION
YES	If the LAN is configured to allow for remote administration, especially from higher headquarters, then there is a potential for Foreign Control or Influence of the company's unclassified network and information.
NO	A LAN that is properly configured which does not allow remote administration is an acceptable step towards mitigating foreign control or influence.

- Is the e-mail server located or controlled by Foreign Parent?

	RECOMMENDATION
YES	If the e-mail server is located in a remote location or at a Foreign owned higher headquarters, then there is a potential for Foreign Control or Influence of the company's network and information.
NO	A local e-mail server which does not allow remote administration is an acceptable step towards mitigating foreign control or influence.

- Are any of the business systems (HR/Benefits, Etc.) hosted at a remote location or at a Foreign Parent?

	RECOMMENDATION
YES	If business systems are located in a remote location or at a Foreign Parent, then there is a potential for Foreign Control or Influence of the company's unclassified network and information. Review mitigation strategy closely. Confirm whether there is a logical disconnection separating controlled resources (export controlled and unclassified information relating to a classified contract) by Domains
NO	A local business system which does not allow remote administration or access to users not directly associated with the local facility is an acceptable step towards mitigating foreign control or influence.

- Are there any trusted relationships between the local facility LAN and any external facilities or with a foreign owned higher headquarters?

	RECOMMENDATION
YES	If trusted relationships exist between the local LAN and systems at a remote location or at a foreign owned higher headquarters, then there is a potential for Foreign Control or Influence of the company's unclassified network and information.
NO	A local business system which does not allow trusted relationships with external systems is an acceptable step towards mitigating foreign control or influence.

- Do they allow VPN?

	RECOMMENDATION
YES	If VPNs exist which provide connections from a remote location or at a foreign owned higher headquarters, then there is a potential for Foreign Control or Influence of the company's unclassified network and information. Review mitigation strategy closely. Confirm whether there is a logical disconnection separating resources by Domains
NO	A LAN which does not allow remote administration or access to users not directly associated with the local facility is an acceptable step towards mitigating foreign control or influence.

- Do they allow thin client terminal services access from remote locations?

	RECOMMENDATION
YES	If thin client terminal services exist which provide connections from a remote location or at a foreign owned higher headquarters, then there is a potential for Foreign Control or Influence of the company's unclassified network and information.
NO	A LAN which does not allow remote administration or access to users not directly associated with the local facility is an acceptable step towards mitigating foreign control or influence.

- Do personnel at a foreign owned higher headquarters have local LAN accounts?

	RECOMMENDATION
YES	If personnel from remote locations or from a foreign owned higher headquarters are allowed accounts on the local network, then there is a potential for Foreign Control or Influence of the company's unclassified network and information. Review mitigation strategy closely. Confirm whether there is a logical disconnection separating resources by Domains.
NO	Limiting network accounts only to people directly employed at the local facility is an acceptable step towards mitigating foreign control or influence.

5.3.2 AUDIT AND ACCOUNTABILITY (AU)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	**CNTL NO.**	**CONTROL NAME**	**NISPOM Reference**	**PM location Para heading**	**Protection Levels Confidentiality**
Technical		**Audit and Accountability**			
* not addressed **not contractually imposed	AU-1	Audit and Accountability Policy and Procedures	8-602	Audit Requirements	1,2,3
	AU-2	Auditable Events	8-602	Audit Requirements	1,2,3
	AU-2 (3)	Auditable Events Control Enhancement		*	
	AU-2 (4)	Auditable Events Control Enhancement		Audit Requirements	
	AU-3	Content of Audit Records	8-602	Audit Requirements	1,2,3
	AU-3 (1)	Content of Audit Records Control Enhancement		Audit Requirements	
	AU-3 (2)	Content of Audit Records Control Enhancement		*	
	AU-4	Audit Storage Capacity	8-602	Audit Requirements	1,2,3
	AU-5	Response to Audit Processing Failures	8-602	Audit Requirements	1,2,3
	AU-5 (4)	Response to Audit Processing Failures Control Enhancement		*	
	AU-6	Audit, Analysis and Reporting	8-602	Audit Requirements	1,2,3
	AU-6 (1)	Audit, Analysis and Reporting Control Enhancement		*	
	AU-6 (8)	Audit, Analysis and Reporting Control Enhancement		*	
	AU-7	Audit Reduction and Report Generation		*	
	AU-7 (1)	Audit Reduction and Report Generation Control Enhancement		*	
	AU-8	Time Stamps	8-602	Audit Requirements	1,2,3
	AU-9	Protection of Audit Information	8-602	Audit Requirements	1
	AU-9 (2)	Protection of Audit Information Control Enhancement		Audit Requirements	
	AU-9 (4)	Protection of Audit Information Control Enhancement		Audit Requirements	
	AU-10	Non-repudiation		*	
	AU-11	Audit Record Retention	8-602	Audit Requirements	1,2,3
	AU-12	Audit Generation	8-602	Audit Requirements	1,2,3

5.3.2.1 Audit Requirements

Audit records will be maintained and reviewed from the date of IS accreditation until withdrawal of accreditation. Audit records shall include the following:

1. Enough information to determine the action involved, the date and time of the action, the system on which the action occurred, the system entity that initiated or completed the action, and the resources involved (if applicable).
2. Successful and unsuccessful logins and logoffs.
3. Unsuccessful accesses to security-relevant objects and directories.
4. Changes to user authenticators.
5. The blocking or blacklisting of a user ID, terminal, or access port.
6. Denial of Access from an excessive number of unsuccessful 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 shall 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.

1. User briefing statements.
2. Additions, deletions, reconfiguration, and repair actions to accredited hardware.
3. Installation, modification or testing of operating system and security related software.
4. Actions take to sanitize IS components.
5. 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. Below are guidelines for reviewing automated audit records:

1. Verify that the automated audit functions are performing properly and there are no time periods during which audit data is missing.
2. Review all failed logins. Question multiple failed login attempts and account lockouts.
3. Review a sampling of successful logins to ensure those persons were actually present and using their account during the recorded time periods. For example, if you are aware of someone being on travel or on vacation during the week, verify his or her account was not accessed.
4. Question login sessions that occur at unusual times (e.g., 2:00am) or sessions that are left open for long periods of time (e.g., over 24 hours).

5. Scrutinize direct logins to generic or group accounts. Verify they are within the guidelines specified in the (M)SSP.
6. If applicable, verify accesses to privileged group/generic accounts were made from authorized user IDs.
7. Depending on the available audit mechanism, failed attempts to access objects may be all inclusive rather than limited to security-relevant objects. Attempt to focus your review on identifying any user ID that consistently has failed access attempts to privileged system files.

5.3.2.2 Security Seals

Approved tamper-proof, pre-numbered seals should be used on hardware components (to include monitors and keyboards) anytime the hardware may be subject to access by uncleared personnel (i.e. used for periods-processing, or relocation).

5.3.3 IDENTIFICATION AND AUTHENTICATION (IA)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	**CNTL NO.**	**CONTROL NAME**	**NISPOM Reference**	**PM location Para heading**	**Protection Levels Confidentiality**
Technical		**Identification and Authentication**			
* not addressed **not contractually imposed	IA-1	Identification and Authentication Policy and Procedures	8-607	Identification and Authentication management	1,2,3
	IA-2	User Identification and Authentication (Organizational Users) Control Enhancement	8-607	Identification and Authentication management	1,2,3
	IA-2 (1)	User Identification and Authentication (Organizational Users) Control Enhancement		Identification and Authentication management	
	IA-2 (2)	User Identification and Authentication (Organizational Users) Control Enhancement		Identification and Authentication management	
	IA-2 (3)	User Identification and Authentication (Organizational Users) Control Enhancement		Identification and Authentication management	
	IA-2 (4)	User Identification and Authentication (Organizational Users) Control Enhancement		Identification and Authentication management	
	IA-2 (5)	User Identification and Authentication (Organizational Users) Control Enhancement		Generic or Group Accounts *	1,2,3
	IA-2 (6)	User Identification and Authentication (Organizational Users) Control Enhancement			
	IA-2 (8)	User Identification and Authentication (Organizational Users) Control Enhancement		Identification and Authentication management	2
	IA-2 (9)	User Identification and Authentication (Organizational Users) Control Enhancement		*	
	IA-3	Device Identification and Authentication	8-607	Identification and Authentication management	1,2,3
	IA-4	Identifier Management	8-607	Identification and Authentication management	1,2,3
	IA-4 (4)	Identifier Management Control Enhancement		*	
	IA-5	Authenticator Management	8-607	Password Policy	1,2,3
	IA-5 (1)	Authenticator Management Control Enhancement		Password Policy	
	IA-5 (4)	Authenticator Management Control Enhancement		Password Policy	2,3
	IA-5 (6)	Authenticator Management Control Enhancement		Password Policy	
	IA-5 (7)	Authenticator Management Control Enhancement		Identification and Authentication management	

	IA-6	Authenticator Feedback	8-607	Password Policy	1,2,3
	IA-7	Cryptographic Module Authentication		*	
	IA-8	Identification and Authentication (Non-Organizational Users)		*	

5.3.3.1 Identification and Authentication Management

Logon authentication shall 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:

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

For PL-2 systems, the ISSM shall 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 shall require the use of strong authentication (i.e., an I&A technique that is resistant to replay attacks.)

5.3.3.2 Generic or Group Accounts (8-505)

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. All generic or group accounts (i.e., GUEST, FIELD, NOBODY, etc.) will be deleted or disabled, with the following exceptions only: Although extremely rare, generic or group accounts may be permitted where required by software or otherwise necessitated for work to be accomplished. A statement certifying this must be provided in writing by the ISSM and receive the approval of the CSA. When generic or group accounts are used for logon, manual logs (or other methods) should be utilized to assure individual accountability.

5.3.3.3 Password Policy

The following are requirements for all passwords:

1. Passwords shall be protected at the highest classification level and most restrictive classification category of information to which they permit access.
2. Passwords shall contain a minimum of fourteen (14) alpha/numeric upper/lower case and special characters.
3. Passwords shall be changed at least every 60 days.
4. Passwords shall be changed when compromised.
5. Passwords shall not be displayed to the screen when input.

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.

5.3.3.4 BIOS Password

The BIOS must be protected with a password which must meet the length and complexity requirements stated above. A waiver is not required if a system's BIOS password cannot be configured to meet the NISPOM requirements. 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.

5.3.4 SYSTEM AND COMMUNICATIONS PROTECTION (SC)

The following section applies to these NIST 800-53 controls:

	NIST 800-53r3		ISFO Process Manual v3		
FAMILY	**CNTL NO.**	**CONTROL NAME**	**NISPOM Reference**	**PM location Para heading**	**Protection Levels Confidentiality**
Technical		**System and Communications Protection**			
* not addressed **not contractually imposed	SC-1	System and Communications Protection Policy and Procedures	8-101, 8-605	Data Transmission Protection	1,2,3
	SC-2	Application Partitioning		*	
	SC-3	Security Function Isolation		*	
	SC-4	Information In Shared Resources	8-609	addressed at control AC-11 (Session Controls)	2,3
	SC-4 (1)	Information In Shared Resources Control Enhancement		*	
	SC-7	Boundary Protection	8-701	addressed at control CA-3 (Controlled Interfaces)	
	SC-7 (1)	Boundary Protection Control Enhancement		*	
	SC-7 (2)	Boundary Protection Control Enhancement		*	
	SC-7 (3)	Boundary Protection Control Enhancement		*	
	SC-7 (4)	Boundary Protection Control Enhancement		addressed at control CA-3 (Controlled Interfaces)	
	SC-7 (5)	Boundary Protection Control Enhancement		address at control CA-3 (Controlled Interfaces)	
	SC-7 (6)	Boundary Protection Control Enhancement		*	
	SC-7 (7)	Boundary Protection Control Enhancement		*	
	SC-7 (8)	Boundary Protection Control Enhancement		*	
	SC-7 (12)	Boundary Protection Control Enhancement		*	
	SC-7 (18)	Boundary Protection Control Enhancement		*	
	SC-9	Transmission Confidentiality	8-605	Data Transmission Protection	1,2,3
	SC-9 (1)	Transmission Confidentiality Control Enhancement		Data Transmission Protection	
	SC-9 (2)	Transmission Confidentiality Control Enhancement		*	
	SC-10	Network Disconnect	8-609	addressed at control AC-11 (Session Controls)	1,2,3
	SC-12	Cryptographic Key Establishment and Management		*	
	SC-13	Use of Cryptography	9-400	Data Transmission Protection	

	SC-13 (2)	Use of Cryptography Control Enhancement		*	
	SC-15	Collaborative Computing Devices		*	
	SC-16	Transmission of Security Attributes	8-700	Network Management and Protections	
	SC-17	Public Key Infrastructure Certificates	8-616	*	
	SC-19	Voice Over Internet Protocol	8-700	Classified VOIP/VTC	
	SC-22	Architecture and Provisioning for Name/Address Resolution Service		*	
	SC-24	Fail In Known State	8-702	addressed at control CA-3 (Controlled Interfaces)	
	SC-25	Thin Nodes	8-613	Thin Clients	
	SC-28 SC-28 (1)	Protection of Information at Rest Protection of Information at Rest Control Enhancement	8-604	addressed at control PE-1 (Physical Security) addressed at control PE-1 (Physical Security)	
	SC-32	Information System Partitioning		*	

5.3.4.1 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:

1) Information distributed only within an area approved for open shelf or bin storage of the information (i.e., closed area)

2) National Security Agency (NSA) approved Type 1 encryption device (i.e. KIV-7M, KIV-7HS, KG-175, etc.).

3) A Protected Distribution System (PDS) compliant with NSTISSI 7003 (see control PE-4).

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.

5.3.4.2 Network Management and Protections

In areas where both classified and unclassified systems reside, classified lines are clearly marked or color coded to prevent inadvertent connections to unclassified computer

systems. When 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 are within 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. Network devices have password protections enabled to assure only authorized persons are permitted access to set or change configurations.

5.3.4.2.1 Controlled Interfaces

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

2) 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. What device to implement depends upon the security requirements of the networks involved. Examples are provided below.

3) 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.

4) Networks that process information at different classification levels or at different compartments of information require the use of a cross-domain solution meeting the DISA Global Information Assurance Program (GIAP) Cross Domain Solutions (CDS) Program requirements, which replaced the SABI connections process. For more information on DISA's CDS requirements, go to http://iase.disa.mil/index2.html or directly to CDS at http://iase.disa.mil/cds/index.html.

5) SIPRNet require that all SIPRNet sites be configured with a firewall and intrusion detection system (IDS). Requirements for the firewall/IDS selection and configuration are found in the DISA Security Technical Implementation Guide (STIG) for Network Infrastructure Ver7 Rel 1 dated 25 Oct 2007 at: http://iase.disa.mil/stigs/stig/network_stig_v7r1_20071025.pdf , and DISA Enclave STIG, Ver4, Rel 2, dated 10 March 2008 at: http://iase.disa.mil/stigs/stig/enclave_stigv4r2.pdf . The Network Infrastructure STIG calls for a firewall evaluated and validated by the National Information Assurance Partnership (NIAP) at EAL- 4; and an IDS that is equivalent to the established U.S. Protection Profile identified by the red PP on the NIAP webpage. For questions

relating to approved boundary devices please contact the SIPRNet CCAO at 703-882-1455.

6) Note that auditing must be performed on firewalls and IDS at least weekly, and any suspected intrusion attempts investigated and reported to the ISSP and IS Rep.

The CI shall be implemented so that all possible failures shall result in no loss of confidentiality or unacceptable exposure to loss of integrity or availability.

5.3.4.3 Classified Voice over IP (VOIP)/Video Teleconferencing (VTC)

Classified VOIP and VTC applications present considerable cost savings when utilized over existing networks. Whether including in a new network, piggy-backing an existing network, or tunneling through a network of lower classification, they do present unique vulnerabilities.

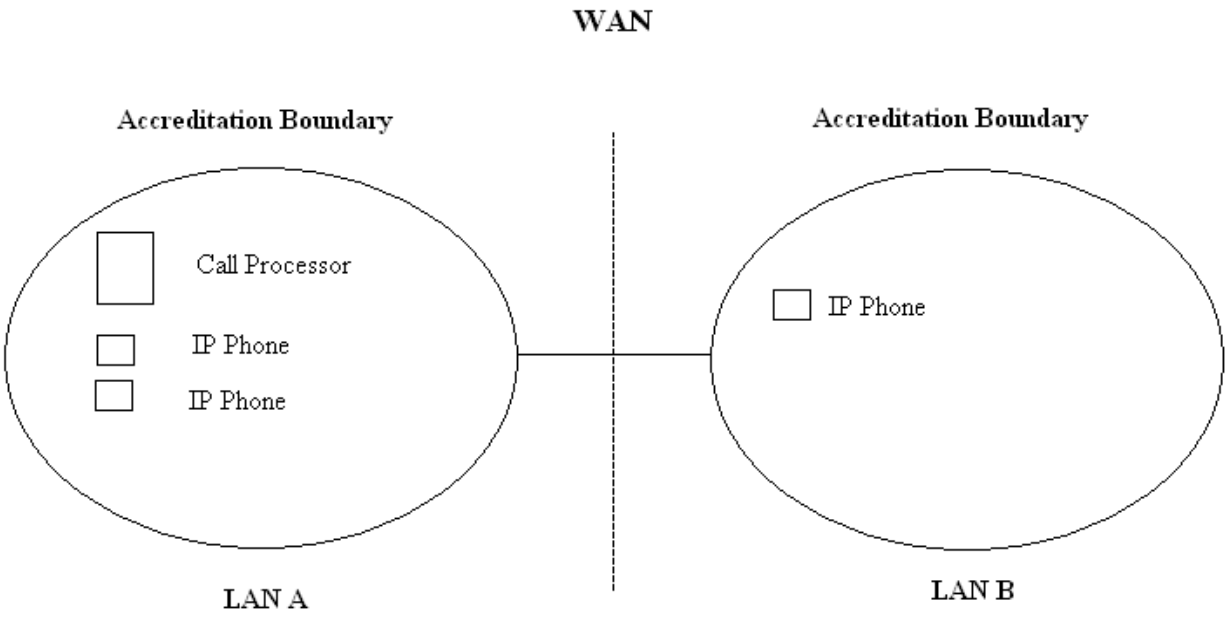


Figure 21 Accreditation Boundaries

An IP Phone is basically a "dumb terminal". Any configuration on the phone should be limited to the System Administrator/ISSO. Referencing Figure 21, in the case of the IP 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 IP Phone added at a later time doesn't constitute a security relevant change so the system will not need reaccreditation.

Call Processor (Call Manager) must have NISPOM Chapter 8 implemented to the extent possible (i.e. auditing may not be possible). At a minimum, configuration should be

limited to the System Administrator/ISSO. Referencing Figure 21, 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 Security Technical Implementation Guides (STIGs) at http://iase.disa.mil/stigs/stig/index.html.

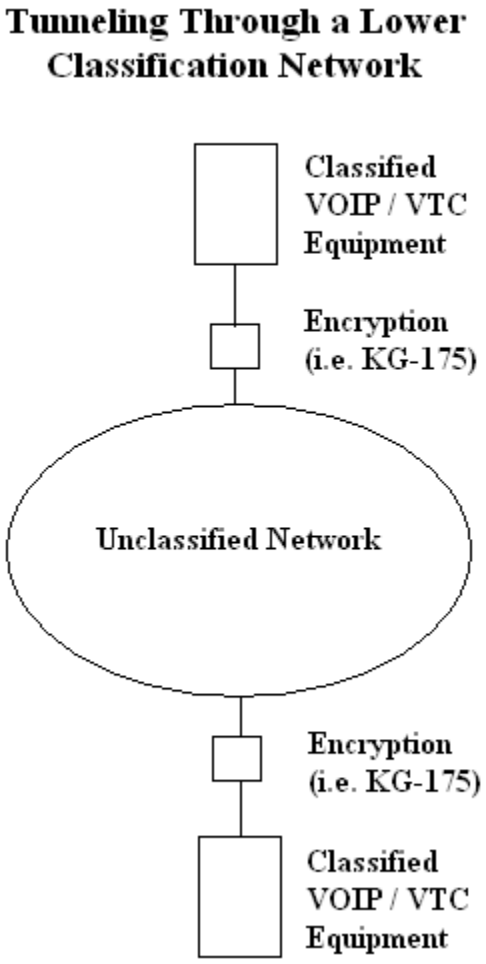


Figure 22 Tunneling

- 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. See the Security Assessment and Authorization (CA), Types of Networks, Network Security Plans, Controlled Interfaces section of this Process Manual.

5.3.4.4 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 – even if its 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 system. They need to be configured to meet NISPOM Chapter 8 requirements to the degree possible.

5.3.4.5 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 often also 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. These methods shall 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 of information are 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 would 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 can not be maintained the contractor is required to assert some temporary visual control in conjunction with disassociation.

6 System Security Plan Submission Process

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 table 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.

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

The **second method** of submittal for (M)SSPs marked FOUO:

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 Information Systems Security Professional (ISSP) and Industrial Security Representative (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, Field Office Chief (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. This can occur in one of two ways:

1. ODAA conducts an onsite verification to validate the IS can be protected by the existing (M)SSP. ODAA will then accredit the system.

2. The ISSM, if authorized to self-certify certain systems, will add the IS Profile to the accredited/established MSSP.

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 (i.e. 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.

Table 6 Subject Line Requirements for Plan Submissions

Region	**PLAN Unique Identifier**			**IS # Identifier**	**Variables**
	XXXXX-YYYYMMDD-XXXXX				
Capital	CageCode[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 shall use 00000 MSSPs with multiple profiles shall use XXXXX
Variables	
MSSP	Use MSSP when the plan is a Master System 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 IS is no longer used for classified processing
INT	Use INT for SSPs with International connections
NSP	Use NSP for Network Security Plans (IS # Identifier shall use 00000)
DIB	Use DIB for DIBCS System Security Plans

Examples

1) 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

2) Western MSSP #10 for cage code ABCDE dated July 14, 2004 protecting IS#1

Western ABCDE-20040714-00010-00001 –MSSP

3) Western MSSP #7 for cage code 11223 dated April 22, 2006 protecting multiple IS (#5 and #6)

Western 11223-20060422-00007-XXXXX –MSSP

4) Standard SSP #13 from the Northern region from cage code 10101, dated Nov. 18, 2005 protecting IS#10

Northern 10101-20051118-00013-00010

5) NSP #9 from the Southern region from cage code 98765, dated Jan 9, 2003

Western 98765-20030109-00009-00000 –NSP

Sample E-mail to ODAA Mailbox

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. Below this template 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 - UID (Use UID format from Table E-1)

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 System 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.

3.

4.

5.

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:

Example ODAA Submission E-mail

From: John.Doe@abc.com

To: ODAA@dss.mil; Frank.Smith@dss.mil

CC: Tom.Jones@dss.mil

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 System 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: Frank Smith

ISSM Name: John Doe

Phone: (212)555-4567

Address: 101 Anywhere St
Alexandria, VA, 22314

E-mail: John.Doe@ABC.com

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

Initial Request of Certification and Accreditation

Additional Information/ Comments: N/A

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 have not been identified in the e-mail as well, there could be potentially significant delays 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.

6.1 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 (i.e., historically under certain situations DSS has allowed certain system types such as standalone workstations or small LANs) 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 IS 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.

Receipt and Dispatch:

The requirement to maintain receipt and dispatch records for SECRET and CONFIDENTIAL information has been eliminated.

Audit Variances for Holiday Shutdowns:

On those occasions when a facility plans to stop all work for an extended period of time (e.g. 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 so that no users have access to the accredited information systems. The request should be routed through the IS Rep and ISSP to ODAA.

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 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 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 is not used over in over 90 days, the ISSM should decertify the system and then re-establish it when needed.

Legacy (non-compliant) Operating Systems:

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. 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.

NOTE: 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:

A. 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:

1. 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.

2. The host contractor will provide the SSP for a unified network to the ODAA for review and approval.

3. The ODAA will review the plan and provide the accreditation action as described in the C&A procedures.

4. The ISSP will perform an onsite verification of the host system.

5. The ISSP/C&A Reviewer for each connecting node will take the provided documentation and perform an onsite verification 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.

6. Following onsite verifications for the host and all connecting nodes, the ODAA will issue a final accreditation letters. An IATO will not be granted for unified networks.

B. Reaccreditation: Procedures for reaccreditation will be very similar to accreditation procedures.

C. 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.

7 Defense Industrial Base Cyber Security Accreditation Process (DIBNET)

By following the procedures outlined below, the cleared defense contractor (CDC) will increase the possibility of acquiring accreditation for the DIB information system (IS) in a timely manner.

Several additional items are referenced throughout this section and are received by the participating contractor upon acceptance into the DIBNET program:

- Users Guide to Configure and Process IS
- DIBCS-Reporting-System-C&A-Handbook-8-2009.pdf
- DIBCS-SSP
- DIBCS-IS-PROFILE
- ODAA NISP Tool

Note: Although the "Users Guide to Configure and Process IS" discusses the issuance of an Interim Authority to Operate (IATO), because of the WAN connection to a government IS in this instance, an IATO will not be issued. An onsite validation will be conducted prior to issuance of an ATO.

1. Configure the computer to NISPOM Chapter 8 requirements. Follow the directions in "Attachment one – CONFIGURE SYSTEM" for the both the automated portion and subsequent manual configuration steps.

2. Analyze the operating system (using the ODAA NISP Tool) to ensure compliance with NISPOM Chapter 8. Please review the ODAA NISP Tool Users Guide prior to running the tool. Run the NISP Reporting Tool and include the report in the accreditation submission package to ODAA.

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 Department of Defense Cyber Crime Center (DC3) data, the use of USB storage devices will be disabled.

The ability to use tiny USB memory sticks to download and walk away with relatively large amounts of data has already made the ubiquitous devices a potent security threat in the computing environment. Now, the emergence of USB flash drives that can store and automatically run applications straight off the device poses even more threat. The recommendation is to disable the USB storage device. 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

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:

- Start Windows Explorer, and then locate the %SystemRoot%\Inf folder
- Right-click the **Usbstor.pnf** file, and then click **Properties**
- Click the **Security** tab
- In the **Group or user names** list, click the user or group that you want to set Deny permissions for
- 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
- Right-click the **Usbstor.inf** file, and then click **Properties**
- Click the **Security** tab
- In the **Group or user names** list, click the user or group that you want to set Deny permissions for
- In the **Permissions for *UserName or GroupName*** list, click to select the **Deny** check box next to **Full Control**, and then click **OK**

USB Storage Device Is Already Installed on the Computer

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:
- Click **Start**, and then click **Run**
- In the **Open** box, type **regedit**, and then click **OK**
- Locate, and then click the following registry key:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor
- In the right pane, double-click **Start**
- In the **Value data** box, type **4**, click **Hexadecimal** (if it is not already selected), and then click **OK**
- Quit Registry Editor

3. Complete the SSP and IS profile in attachments two and three. Please note that although these are tailored templates, you, as the ISSM, will need to ensure the plan accurately reflects the protective measures for your IS within your specific facility. Do not forget to sign the certification statement. IS Rep and ISSP will serve as points of contact for any help you require during this process. Submission should only occur after a SCIP/HAIPE encryption card/NSA Type-1 device has been received. By submitting the package, you are triggering the mechanism that allows the ODAA representative to schedule the onsite validation upon successful review of your SSP. Submitting the accreditation package without all the required components requires reallocation of resources that could ultimately cause considerable delays in the connection process. The addition of "DIB" must be included on the subject line for all DIBNET e-mail submissions. Please refer to the System Security Plan Submission Process, Table 6 Subject Line Requirements for Plan Submissions.

4. Within 30 days, you should receive feedback from DSS concerning the SSP. If the SSP was accepted, ODAA personnel will schedule an onsite validation. If the onsite visit is successful, an ATO will be issued within five working days. If it was not successful, DSS will provide constructive feedback regarding the changes your plan requires. Your ability to utilize your DIBCS reporting system occurs at the end of this certification and accreditation process.

5. Once an ATO is received, the ISSM needs to forward it to DCISE@dc3.mil. The ATO will be the source document authorizing DC3 to connect you to their network.

8 Reference List

DoD Industry White Paper (March 2005). Information System Security, SSP Accreditation Process Requires "Re-Invention" and Major Improvement

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

Industrial Security Letter ISL 2007-01 (October 2007). Alexandria VA: Department of Defense, Defense Security Service, Industrial Security Program Office

Central Florida Industrial Security Awareness Council (2004, March). Florida Association of Information Systems Security Representatives (FAISSR) Network Security Plan extract. Retrieved February 20, 2008 from http://fiswg.research.ucf.edu/

9 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 illustrated via a network diagram or described via a hardware listing or system description.
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 System	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 System 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 bee so designated. The term includes National Security Information (NSI), Restricted Data (RD), and Formerly Restricted Data (FRD).
Cognizant Security Agency (CSA)	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.
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.
Confidential	This designation shall be applied to information or material the unauthorized disclosure of which could be reasonably expected to damage national security.
Contractor	Any industrial, educational, commercial, or other entity that has been granted an FCL by a CSA.
Denial	When a system security plan has been accepted and reviewed by an ISSP/C&A Reviewer and is not granted an Interim Approval to Operation (IATO) due to errors/omissions.
Department of Defense (DoD)	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 (DAA)	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 (FCL)	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).
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 Cryptovariable information, FRD, etc.
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.
Government Contracting Activity(GCA)	An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.
Industrial Security	That portion of information security which is concerned with the protection of classified information in the custody of U.S. industry.
Information Security (INFOSEC)	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 System	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 System Security Manager (ISSM)	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 System Security Officer (ISSO)	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.
Interim Approval to Connect	Temporary approval granted by a WAN DAA allowing the connection of a node to said WAN.
Interim Approval to Operate	Temporary approval granted by a DAA for an IS to process classified information.
Multiple Facility Organization	A legal entity (single proprietorship, partnership, association, trust, or corporation) that is composed of two or more facilities.
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 system security plan connected to a WAN.
Physical Security	The measures used to provide physical protection of resources against deliberate and accidental threats.
Protection Level (PL)	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.
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.
Rejection	When a system security plan submission to the ODAA is not in accordance with the ISFO 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 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 shall 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.
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.
TOP SECRET	The designation that shall 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.
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 IS 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.
Verification	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.
Wide Area Network (WAN)	Any two systems interconnected as defined by NISPOM 8-700 c.