Defense Security Service

Office of the Designated Approving Authority (ODAA)
Process Guide
For
Certification and Accreditation
Of
Classified Systems under the
National Industrial Security Program
Operating Manual (NISPOM)

Revised May, 2008

Revision 2008.1

Title Page

Document Name: ODAA Process Guide for C&A of Classified Systems under NISPOM

Publication Date: March, 2006

Revision Date: May, 2008

Document Owner: Defense Security Service (DSS)
Industrial Security Program (ISP)
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
1340 Braddock Place
Alexandria, VA 22314-1651

Table of Contents

Figures

Tables

Preface

The Defense Security Service (DSS), Office of he Designated Approving Authority (ODAA), has been delegated the responsibility for providing Certification & Accreditation (C&A) oversight of National Industrial Security Program (NISP) contractor systems that process classified information. This process guide is for DSS staff and NISP contractors involved that require C&A oversight from DSS. In addition, the process guide is designed to provide a full spectrum resource to DSS staff and to newly appointed contractor Information System Security Managers (ISSM) and well seasoned ISSO's.

Specifically, the intent of this process guide is to explain process standards, interpretation standards, technical configuration standards, and system security plan standard templates. This guide is intended to be followed by DSS staff. Adherence to the standards in this process guide by NISP contractors is recommended in order for DSS to be able to issue of Interim Approvals to Operate (IATO) and Approvals to Operate (ATO) proceeding expeditiously.

This process guide will be updated bi-annually with the next revision planned for December 2008. Therefore, it is the responsibility upon all those involved in the C&A process to stay abreast of the current ODAA Process Guide so that consistency is maintained and an understanding of the current processes is being followed.

This process guide 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.

1.0 Introduction

The Director, DSS is responsible for C&A oversight of cleared NISP contractors' Information Systems (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 National Industrial Security Program (NISP), the Director, Industrial Security for DSS is the delegated DAA for NISP contractors and has further delegated those responsibilities to the Deputy Director, Office of the Designated Approving Authority (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.

1.1 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 guide was created and revised to clearly explain the changes that have been made as well as clarify all the steps of the C&A process for the cleared contractor's classified information systems.

This Process Guide can be viewed from several perspectives:

- ODAA Staff Perspective
- DSS Field Operations Staff Perspective
- Government Contractor (ISSM) Perspective
- Training/Mentoring Perspective

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 guide would be appropriate. This Process Guide 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.

1.2 Roles and Responsibilities

The ODAA is delegated the responsibility for carrying out the DSS C&A mission for cleared contractor IS. ODAA C&A oversight is comprised of reviewing the 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. The ODAA oversees the C&A of contractor classified systems to see if 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 on-site validations and annual inspection reviews.

In addition to those required by NISPOM, the Appendix A is a list of key participants and their responsibilities in the ODAA process. 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.

The following sections will use the term "ISSP/C&A Reviewer" to identify the use of an ISSP or C&A Reviewer as they become involved in the ODAA Process.

1.3 Training

The ODAA will provide training through several venues and multiple elements within DSS. For example:

ODAA:

1. ODAA Headquarters has a:

    - Technical Standards & Training Development element that is established to identify the training needs of ODAA personnel. These training requirements will contain tiered levels so that the needs of the Industrial Security Reps are also met (to include the Qualified C&A Reviewer). Once identified, these training requirements get forwarded to the DSS Academy (DSSA) so that a curriculum can be established and infused into other established formal training sessions or provided separately under a seminar type format.

    - Quality Assurance element that continually reviews established processes and procedures to verify they are efficient, effective and are applied consistently throughout DSS and in particular the ODAA regions. These reviews include the ISSPs mentor program and the IS Rep C&A Reviewer program.

2. ODAA ISSPs provide training on several fronts. They provide training to:

    - Other ISSPs through the ODAA Mentor Program (See Appendix B).

- IS Reps through the C&A Reviewer Process (See Appendix B).
- DSSA as Adjunct Faculty Instructors
- Cleared contractors in support of the NISP. Training can be in the form of:
    - workshops,
    - conferences,
    - seminars, and
    - individually through Advice and Assist visits.

Note: (1) ISSPs must contact and obtain from their respective supervisor approval before committing to discuss availability/participation in contractor-related conferences, seminars, workshops, etc.

Note (2) ISSPs will coordinate any information systems presentations to contractors with their RDAAs to verify that the information they will present is both accurate and in accordance with current policy guidance. Additionally, ISSPs must coordinate with the DSS Public Affairs Office on all presentations outside DSS (see current guidelines).

Note (3) ISSPs must provide to the Deputy Director ODAA and their respective RDAA within 24 hours of such external meeting a trip report that describes the following:

- Date and name of event.
- Purpose and location of event.
- Significant issues or discussions that arose at the event.

DSSA: Provides a multitude of training classes that benefit ODAA, Field Operations and cleared contractors. Please visit the DSS website for a list of available courses.

1.4 Information System (IS) Types

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

1.4.1 Multi-user Standalone (MUSA)

Approximately half the plans submitted to ODAA consist of the MUSA. The physical security parameters within the SSPs vary between closed areas and various configurations of restricted areas. 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 multi-user 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 information systems. 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 a system security plan 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

1.4.2 Local Area Networks (LAN)

A Local Area Network 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 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 Wide Area Networks (WANs), include their much higher data transfer rates, smaller geographic range, and lack of a need for leased telecommunication lines.

General characteristics of LAN:

- Two or more computers
- Connection devices
  - Hubs
  - Switches
  - Routers
- Physical security:
  - Closed area

    - Restricted area
- Operating system must be NISPOM compliant
    - Peer-to-peer
    - Client-server/Active Directory

1.4.3 Wide Area Networks (WAN)

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. 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.

1.4.4 Types of Networks

1.4.4.1 Unified Networks:

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. The network will 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. See Appendix E for more information concerning SSP submissions for Unified Networks.

1.4.4.2 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 PL1 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. 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.

1.4.4.2.1 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 plans. Essentially, DSS is building in to the process flexibility needed to support the often inevitable expansion of many WANs.

4. it is in accordance with NISPOM 8-700c "An interconnected network also requires accreditation as a unit."

See Appendix G for detailed information on Network Security Plans.

1.4.4.2.2 Memorandum of Understand (MOU)

An MOU between DSS and the Government Contracting Authority (GCA) is required for all government to contractor connections to include connections over STU III, STE, and Secure Data Devices. (A sample MOU is at Appendix G.) MOUs following this format do not require approval by the DSS 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 will be sent to ODAA HQ for signature. Any MOU/MOAs with signatories of General grade/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.

1.4.5 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

These are further explained in Appendix C.

Note: Tactical, Embedded, Data-Acquisition and special purpose systems have other requirements as identified in (Article #40, ISL 2007-01) and are discussed separately in Section 2.3.4 and Appendix L of this Guide.

2.0 Certification and Accreditation (C&A)

2.1 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 lifecycle: from system inception to termination. This section outlines the C&A Life Cycle from the submission of a System Security Plans (SSP) or Master System Security Plans (MSSP) to the issuance of an accreditation letter or Approval To Operate (ATO) and finally the termination of the IS for classified use.

As a general guideline, an information system 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 a system security plan for an IS that will process classified information to ODAA using the instructions within this guide and per the NISPOM/ISLs.
- An ODAA reviewer reviews the plan and makes the following recommendations:
  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 on-site 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 on-site validation.
- At this point the ISSP/C&A Reviewer will make the following recommendations:
  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 on-site validation once corrective action has been made
- In some cases, the ODAA Reviewer can conduct on on-site validation immediately after reviewing the plan and may recommend an ATO without recommending an IATO.
- The ODAA RDAA signs an ATO (3 years) for final accreditation
- If there are security-relevant changes/modifications to the 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

2.2 C&A Process

The C&A Process (NISPOM 8-200) is an integral part of the contractor's 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 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 on-site 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 System Security Plan (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 OSD policy, and that the DAA accepts the operation of the contractor's IS under the stated parameters of the accredited system security plan. 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 the DSS.

The C&A Process is further explained in Appendix D.

2.3 Types of Security Plans

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)

2.3.1 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 (see Appendix D). The submission format is outlined in Appendix E.

2.3.2 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. See Appendix F for more information concerning MSSPs. The following is included in the appendix:

- Defining "Similar"
- Self-certification
- Traveling/Corporate ISSM
- Managing added IS
- ISL 2007-01 Extract

2.3.3 Network Security Plan (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 the requiring the existing nodes to be reaccredited. See Appendix G for more information.

2.3.4 Other

The following are areas that do not fit the three system security plans as outlined above. However, there are documentation requirements that must be met.

2.3.4.1 Protected Distribution System (PDS)

PDS require approval prior to installation of conduit and subsequent cabling/wiring. Appendix H explains the process and procedures to install PDS per NSTISSI 7003. A sample plan is provided to expedite the approval process.

2.3.4.2 Mobile Systems

Systems accredited for processing classified data were not intended to be relocated to alternate sites for classified processing and are not addressed in the current version of the NISPOM. Due to the on-going need to relocate systems, special procedures are required to document applicability, movement, operations, and security of classified systems that are relocated to alternate sites. See Appendix I for further guidelines on Mobile Systems.

2.3.4.3 International

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 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. See Appendix J.

2.3.4.4 Special Access Programs (SAP): TBD next revision

2.3.4.5 Special Purpose, Tactical, Embedded Systems

The requirements of Chapter 8 are written in regards to the general-purpose or office automation system and personal computers. It would be almost impossible to include security requirements for components such as weapons or tactical systems, test stands, simulators, or embedded components (NISPOM Paragraph 8-504) that often are integral elements of a larger IS. To apply the general requirements of Chapter 8 in these instances may result in unnecessary costs and adversely impact operations. 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. See Appendix L for more information.

2.3.4.6 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) – See Appendix M
- 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
- TALON - TBD in future revisions

2.4 Additional Plan Considerations

The following sections pertain to additional procedures that could be seen in a security plan.

2.4.1 Trusted Download Procedures

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 Protection Level (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 are contained in Appendix N.

2.4.2 Clearing/Sanitization

A “DSS Clearing and Sanitization Matrix,” is posted on the DSS website. The contractor is required to document in the 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 determine whether the ODAA, NSA, or an authorized DoD laboratory has performed or can perform an evaluation. Otherwise, the contractor must arrange with the GCA for return of the memory or media.

As of May 2007, there is no overwriting product or process that has been evaluated and validated by the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) that can be used to sanitize classified information systems or electronic media. National policy requires that all IA products used with or within Federal IS be evaluated and validated by the CCEVS.

The “DSS Clearing and Sanitization Matrix” is based on NSA/CSS Policy Manual 9-12, “Storage Device Declassification Manual” dated 1 March 2006. Effective immediately, DSS will no longer approve overwriting procedures for the sanitization or downgrading (release to a lower level classified information controls) of *fixed/rigid media* used for classified processing. Prior approvals will remain in effect until circumstances require re-approval of the affected systems. See Appendix O for additional information on clearing/sanitization.

2.4.3 Voice Over IP/Video Teleconferencing (VOIP / VTC): TBD

Note: The next revision of the Process Guide will include the following:
Call center location; 3 scenarios:

1. new NW

2. Piggyback existing network

3. leverage unclassified network – tunneling – Hardware (HW) Administrative change

2.5 ODAA SSP Process Metrics

The ODAA has estimated that from the time an SSP is provided to an analyst to the issuance of the IATO is approximately 40 to 56 hours (i.e., five to seven working days). This is under ideal conditions with the SSP in an easily readable format, with no need for corrections or additional information from the ISSM. If the format is such that the analyst has to search for data, or if there is missing data requiring correspondence back to the ISSM, the timeframe can be considerably greater.

ODAA collects metrics on all aspects of the C&A process. From the initial submission of the SSP to the issuance of the ATO, all points along the way are recorded to develop metrics that can aid in improving the efficiency of the C&A process over the lifecycle of the systems.

- METRICS
  - Data Collection Instrument (DCI) Form for IATOs
  - DCI Form for ATOs
  - ODAA Database
  - Industrial Security Facilities Database (ISFD)
- Reports: TBD

These forms and instructions are to be used by DSS and are available in the ODAA Standard Operating Procedures for Field Reviewers.

3.0 Annual Review

Annual Reviews are an important part of the C&A lifecycle of the IS. As such, ISSP/C&A Reviewers performing these reviews are to provide initial results for each system that they inspect to document and evaluate the security posture of the system as required by the approved SSP or MSSP. Information Systems will not be rated separately from the facility but the DAA will use this information to develop trends analysis, based on the updated SSP repository, and evaluate the risk to the system based on systems protection measures and not overall facility security inspection ratings. Additionally, to the greatest extent possible, the ISSP/C&A Reviewer will inspect new systems that have been self certified since the last annual security inspection with results of the system security configuration status included in the review. This will validate the number of systems existing with valid authorization to process classified information with the ODAA database. Results will also be documented in the Security Review report and ISFD as appropriate. Failure to properly maintain the systems in accordance with the MSSP or SSP may result in inadvertent revocation of the IS's ATO.

It is extremely important to coordinate with the Field Office Chief (FOC)/IS Rep so that ODAA personnel properly participate in the annual reviews, especially those facilities that fall under the Special Interest List (SIL).

To the maximum extent possible ISSPs will augment team inspections in other regions so that they have an appreciation for the diverse types of technology that encompasses the spectrum of IS.

At least 10 working days prior to every inspection, the contractor will provide the ISSP/C&A Reviewer with the SSP/MSSP Tracking Form so that the ISSP/C&A Reviewer can determine the amount of time required to adequately complete the review. The priority of IS to be inspected are:

1. PL2 IS and higher;

2. all external connections (WANs);
    a. SIPRNET
    b. Other WANs

3. TS systems;

4. self-certified systems;

5. LANs;

6. Standalone workstations.

See Appendix S for additional information on Annual Reviews.

4.0 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 Plan of Action for mitigating the risk. More definitive information is available in Appendix T.

5.0 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. The procedures identified in Appendix U are aligned with DoD and DoD component procedures.

6.0 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 IS Rep will have the contractor conduct an administrative inquiry. If the user agency concurs, but has not given the contractor written acknowledgement 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.

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

Wikipedia (2008, February 16). Local Area Network. Retrieved February 20, 2008, from http://en.wikipedia.org/wiki/Local_area_network

Wikipedia (2008, February 7). Wide Area Network. Retrieved February 20, 2008, from http://en.wikipedia.org/wiki/Wide_area_network#_note-Groth#_note-Groth

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://www.cfisac.org/

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 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	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.
Department of Defense	The Office of the Secretary of Defense (OSD) (including all boards, councils, staffs, and commands), DoD agencies, and the Departments of Army, Navy, and Air Force (including all of their activities).

Designated Approving Authority (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	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).
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 (IATC)	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 information.
Multiple Facility Organization	A legal entity (single proprietorship, partnership, association, trust, or corporation) that is composed of two or more facilities.
Network	An AIS 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 AISs, 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 SSP or MSSP.
Reevaluation	An action taken by DSS 3 years from the date of the ATO for a MSSP or SSP.
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 Requirement	Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.
User	Person or process authorized to access an IT system.
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.

Appendix A Roles and Responsibilities

Office of the Designated Approving Authority (ODAA)

The ODAA is delegated the responsibility for the DSS mission for cleared contractor IS certification and accreditation oversight. ODAA certification and accreditation oversight is comprised of reviewing the System Security Plan (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. The ODAA verifies if the certification and accreditation (C&A) of Industry classified systems is consistent with national computer security information assurance policy and performed in an efficient and effective manner. The ODAA also verifies that systems maintain their accreditation security posture throughout their life cycle by conducting on-site validations and annual inspection reviews.

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 within their level of competence. Additionally, the ISSP will review the SSPs to determine if the physical, operational, and technical controls identified in the plans are adequate to protect the classified information resident on the IS. The ISSP will conduct on-site validations and inspections to verify that the protection measures as certified by the Information Systems Security Manager (ISSM) have been implemented on the IS.

Industrial Security Representative (IS Rep) Responsibilities

This Process Guide only applies to those IS Reps that have completed the curriculum to become C&A Reviewers.

Qualified C&A Reviewers

An IS Rep is authorized to review SSPs and evaluate/validate IS systems after obtaining DSS training, mentoring, and support. Qualified IS Reps are an extension of ODAA and are subject to the roles and responsibilities established by ODAA policies and procedures.

The C&A Reviewer process is outlined in the training section (Appendix B).

It is important to note that the C&A Reviewer will be used to augment the ODAA C&A Process. The role of inspector, reviewer and on-site validator are primarily that of the ISSP. Circumstances may arise where there is an imbalance or reviewers, inspectors, etc. The Regional DAA is responsible for the efficiency and timeliness of the C&A process. Therefore, this additional valued resource might be called upon to fill in where shortages/imbalances may occur.

The C&A Reviewer will be required to maintain a queue of facilities to review so that they may maintain proficiency in this area.

Contractor Personnel

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 ISSO that can configure and manage the systems to verify system security controls are in place and operating. During on-site 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" (see sample below), 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 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.

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 as 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 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.

Traveling/Corporate ISSM (Pilot Program)

See Appendix F for more information related to the traveling/Corporate ISSM.

Information System Security Officer(s) (ISSO)

The ISSO(s) (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. During an IS validation or Security Review, the ISSP or qualified IS Rep will determine what duties and responsibilities have been delegated to the ISSO and verify that the ISSO understands them and is carrying them out. The ISSO must be able to configure and manage the security configuration of the systems under their purview.

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 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.
- Focal point for the network and the connecting node ISSMs, to include collecting Network Security Profiles.
- Generate and maintain approvals for the NSSP and, if applicable, the MOU.
- Verify all systems on the network have an accredited plan.
- Assure 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 NSSP, if necessary, and report any anomalies or violations to DSS and any other accrediting authorities with nodes on the network.

Users of Information Systems (IS)

NISPOM Chapter 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.

During the security review, the ISSP or IS Rep will verify privileged users have access and need-to-know for all information on the system, and that they understand their duties and responsibilities. They will also verify working knowledge of the users of various security functions, policies, technical security safeguards and operational security measures. In general, privileged users should be held to a minimum and attention should be given to excessive numbers of privileged users identified on the IS.

The ISSP or IS Rep will also verify that general users have access and need-to-know for all information they will access and that the users were briefed prior to having access to an accredited IS.

Figure A-1: Table – Roles and Responsibilities

Participant(s)	Responsibilities
Defense Security Service	
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).
Regional DAA (RDAA)	• Subject matter expert on information systems. • Coordinates with field on C&A issues. • DAA responsibilities and authority within their Region. • Supervises the ISSPs. • Oversees and manages status of C&A activities within region and is cleared contractor's primary point of contact for C&A issues arising in region.
ODAA Action Officer	• Subject matter expert in information systems. • Reviews security plans. • Performs regional quality assurance reviews • Serves in the absence of the RDAA • Backup for resource allocation • Develops and manages (MOU/MOA) within the region • Advises and assists the regional ISSPs and ISReps to verify uniformity and consistency • Revising ISOM, Process Guide, ISLs & ODAA SOPs • Gathers/analyzes metrics
ODAA Team Leader	• Performs inspections/reviews at complex facilities • Coordinates ISSP coverage within the team's area of responsibility (AOR) • Reviews SSPs for complex facilities • Provides guidance and technical assistance to the ISSP Team, ISReps and contractors • Advises and assists the ISSP Team and ISReps • Identifies/coordinates training needs for the ISSP Team and ISReps • Verifys regional staff accurately input data into ODAA systems
Quality Assurance/Quick Response(QAQR)	• Assists in establishing, monitoring/enhancing, and oversight performance of the ODAA QA program. • Conducts quality assurance reviews

	• Observes inspections/reviews by IS Reps and ODAA staff at contractor facilities • Provides rapid assistance and oversight support in responding to events ie data spills, inspections, etc • Participates in developing, implementing, or conducting IS security training sessions for DSS and contractor personnel.
Information Systems Security Professional (ISSP)	• Subject matter expert in information systems. • Reviews security plans. • 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 Certification and Accreditation (C&A) process.
Field Office Chief (FOC)	• Directs the IS Reps in certification support and annual inspections. • Coordinates with the RDAA. • Coordinates regional CI Specialist • Signs official correspondence not in the C&A Process
Industrial Security Representative (IS Rep)	• Primary DSS POC to Industry. • Performs validation and annual reviews on certain IS (if qualified). • Notifies the FOC and DAA on IS compliance. • Reviews security plans or SSPs as needed (if qualified). • Coordinates with GCAs. • Provides advice and assistance on the C&A process (if qualified) and other IS matters.
CI 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 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.

Information Systems Security Manager (ISSM)	• Employee appointed by management with oversight responsibility for the development, implementation, and evaluation of the IS Security Program. • Develops MSSPs or SSPs which comply with the NISPOM. • Verifies IS are configured in accordance with security requirements and the MSSPs or 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. • May qualify as Corporate/Traveling ISSM
Information Systems Security Officer (ISSO)	• Supports the ISSMs in their efforts to implement security requirements as mandated by the NISPOM. • May directly participate in the certification and accreditation (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 NSSP 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 NSP and the 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.
System/Network Administrator	• Privileged user with operational responsibility for the accredited IS(s). • Usually assigned to large, multi-user 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 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)	• Support the ISSMs in their efforts to implement security requirements as mandated by the NISPOM.

Appendix B Training

Information System Security Professional (ISSP)

Training ISSPs: The Mentor program for training ISSPs is currently under revision and will be included in the next version of the ODAA Process Guide.

Training IS Reps:

General: Although the DSS Academy has the formal responsibility of training the IS Rep, one of the responsibilities of the ISSPs is to augment that training. Methods for accomplishing this depend on the IS Rep's experience with information systems and the Industrial Security Program (ISP).

Trainee IS Reps: As soon as the FOC and IS Rep mentor believe the IS Rep trainee is ready for instruction in IS, the ISSP will begin the his/her portion of the mentor training.

The new IS Rep Mentoring Guide requires that the ISSPs provide a review of Chapter 8, NISPOM and introduce to new IS Reps the DSS perspective in certifying, accrediting and inspecting contractors' ISs. Basic requirements the ISSP will cover, as a minimum, are certification and accreditation, common requirements, and audit requirements.

The Mentoring Guide also requires the ISSPs to take the new IS Reps on ride alongs, as the ISSPs visit contractors. This could include Security Reviews and advice and assistance (A&A) visits. Also, the Industrial Security Specialist Course (ISSC) has a block of instruction on conducting administrative inquiries. It will be helpful if the new IS Rep has some brief exposure to that subject as well.

Industrial Security Representative (IS Rep)

Authorized ODAA C&A Reviewers

An IS Rep is authorized to review SSPs and evaluate/validate IS systems after obtaining DSS training, mentoring, and support. The IS Rep who becomes qualified as an ODAA C&A Reviewer will only augment ODAA and will be used as a management tool in the event resources become strained for C&A Reviews, on-sites validations and inspections. Qualified IS Reps are an extension of ODAA and are subject to the roles and responsibilities established by ODAA policies and procedures.

Below is an outline of the C&A Reviewer process:

1. IS Reps will receive training on Windows-based multiuser standalones/peer-to-peer LANS at the ISSC or completing the ODAA System Training Class.

2. Upon completion of the course(s), IS Reps will receive additional on-the-job (OJT) with an ISSP mentor.
   i. Training will be tracked using the attached Training Record (TAB A).
   ii. The IS Rep will need to gain competency in reviewing an SSP, conducting an on-site validation and conducting an annual IS Review.
   iii. Additionally, the IS Rep will be trained on how to submit the required documentation for IATO/ATOs and updating the ODAA systems, ISFD and data collection forms. All forms will be provided to the IS Rep by ODAA.

3. The RDAA will make a determination on whether the IS Rep is competent to perform system certification and accreditation and will formally acknowledge through an evaluation using the attached forms TABs B&C. Once the IS Rep has successfully completed the process, a certificate will be awarded (TAB D) by the RDAA.

4. IS Reps will be evaluated annually thereafter as part of the ODAA Quality Assurance Program.

Cleared Contractors

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

1. DSSA
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 are available on the DSS web site:

- SSP Templates – ODAA has available on the DSS website SSP templates to 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 SSP templates provide the ODAA a familiar format tailored to a set configuration under a set environment, which results in an efficient SSP evaluation . Cleared contractors are highly encouraged to use these templates. Significant delays will result and should be expected if these templates are not used.

- Technical Configuration Standards – 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 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.

- NISP C&A Tools – these tools are 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. These tools also, are designed in conjunction with the SSP template and technical configuration standards. Specifically, these analysis tools evaluate the operating systems to identify vulnerabilities and non-compliant settings. The use of these tools is highly encouraged and will facilitate the DSS IATO and ATO reviews. Significant delays should be expected and planned if the tools are not used and will result in not obtaining DSS approval to process classified.

- Checklists – these are checklists for a myriad of operating systems that provide step-by-step instructions to configure and evaluate the IS for compliance including potential corrective action guidance.

TAB A

Figure B-1: Enclosure 47: C&A Reviewer Training Record

Industrial Security Rep: **Region/Field Office:** **ISSP(s):** **RDAA:**

PERFORMANCE & TRAINING ELEMENTS	OBSERVATIONS	CERTIFICATION	SYSTEM REVIEW	NOTES
Technical features:				
I&A				
Auditing				
Session controls				
System Recovery				
System Assurance				
Security Testing				
Data transmission:				
Protected Distribution Systems				
NSA Type 1 Encryption				
Area Controls				
Access Controls(physical)				
Complex Hardware(not a standalone)				
Continuity of Operations(contract directed)				
LAN Concepts (topology, Peer-to-Peer, etc)				
TEMPEST Requirements(contract directed)				
Workstation Sanitization				
Verify trusted downloading procedures				
Generic overview of vulnerabilities associated with embedded data				
	DATE COMPLETED			
ISS Course attendance				
ISS System Certification				
IS Security Review				
System Security Plan Review				
C&A Reviewer Mentoring Complete				

I CERTIFY THAT THE ABOVE IDENTIFIED IS REP □ IS □ IS NOT QUALIFIED TO REVIEW SSPS AND CONDUCT IS REVIEWS

DAA Signature: ______________________________________

TAB B

INFORMATION SYSTEM CERTIFICATION EVALUATION FORM

(C&A Reviewer)

INFORMATION SYSTEM CERTIFICATION EVALUATION FORM
(C&A Reviewer)

Person Evaluated:	
Credential #:	
Field Office:	
Date Observed:	
Facility Name:	
Cage Code:	

CERTIFICATION REQUIREMENTS

Q1 – 4 points, indicates that the element was fully covered IAW with the ISOM/NISPOM.
Q2 – 3 point, indicates that the element was addressed but not fully covered IAW with the ISOM/NISPOM.
Q3 – 0 point, indicates that the element was not addressed or provided incorrect guidance.
NA – this element will be eliminated from the possible overall point value, indicates that the element was addressed but does not apply to this facility.

Place an "X" under the assigned rating for each element.

	RATING:	**Q1**	**Q2**	**Q3**	**NA**
Section 1: Certification and Accreditation					
CA-1	Did the ISR ensure ISSM has certified in writing to CSA that each SSP has been implemented, tested and functioning as in SSP? (NISPOM 8-201)	○	○	○	○
CA-2	If the SSP is a Master SSP, did the ISR review the contractor's self-certification process and determine ISSM understands requirements? (NISPOM 8-202g & ISL 2007-01 Q.14)	○	○	○	○
Section 2: Responsibilities and Duties					
RD-1	Did the ISR verify that the ISSM is an employee of the company and has a PCL, NTK and formal access approvals for all information processed on the system under certification? (NISPOM 8-101b & ISL 2007-01 Q.3)	○	○	○	○
RD-2	Did the ISR determine that the ISSM is trained to a level commensurate with the overall complexity of all multiple facilities he or she will manage or has appointed a technically knowledgeable ISSO? (NISPOM 8-101b & ISL 2007-01 Q.5)	○	○	○	○
RD-3	Did the ISR determine the ISSM understands all duties and responsibilities? (NISPOM 8-103)	○	○	○	○
RD-4	Did the ISR determine what responsibilities have been delegated to the ISSO? (NISPOM 8-104)	○	○	○	○
RD-5	Did the ISR determine the ISSM understands that privileged users must have a PCL, NTK and formal access approvals for all information on the system and that they must have working knowledge of security functions, policies, technical security safeguards and operational security measures? (NISPOM 8-105a, 8-307)	○	○	○	○
RD-6	Did the ISR determine the ISSM understands users must be briefed prior to having access? (NISPOM 8-103I)	○	○	○	○
Section 3: Common Requirements					
Clearing and Sanitization					
CR-1	Did the ISR review with the contractor different clearing and sanitization requirements for various memory, media and equipment types as described in the SSP? (ISL 2007-01 Q. 54)	○	○	○	○
CR-2	Did the ISR determine the ISSM understands the degausser must be tested in accordance with the NSA schedule. (ISL 2007-01 Q. 54)	○	○	○	○
Software					
CR-5	Did the ISR determine the ISSM understands that all contractor personnel that design, develop, test, install or modify system or security software must be cleared to the level the IS is accredited? (ISL 2007-01 Q.18)	○	○	○	○

CR-6	Did the ISR determine the ISSM understands that the contractor must follow software testing, approving, installing and maintaining procedures for all software resident on the classified IS? (NISPOM 8-302a)	○	○	○	○
CR-7	Did the ISR determine if unclassified software was written by uncleared people or obtained from an unknown source? (NISPOM 8-302a)	○	○	○	○
CR-8	Did the ISR ensure that all features required by the Protection Level are enabled on both workstations and servers for all operating systems? (NISPOM 8-302)	○	○	○	○
	Hardware				
CR-9	Did the ISR determine that ISSM understands that hardware must be examined for elements such as keystroke recorders or USB flash memory drives and that they are not connected to the classified system prior to processing? (NISPOM 8-302b)	○	○	○	○
CR-10	Did the ISR ensure that all hardware that will retain classified is identified on the hardware list?	○	○	○	○
	Identification and Authentication				
CR-11	Did the ISR determine that prior to accessing the system, the ISSM understands he or she must positively establish the user's clearance, NTK and formal access approvals for which the IS is accredited? (NISPOM 8-303)	○	○	○	○
CR-12	Did the ISR verify that electronic means for uniquely identifying and authenticating the users at logon time is employed and that each user is uniquely identified? (NISPOM 8-607 & 8-303c)	○	○	○	○
CR-13	If standalone workstation or small LAN and no authenticators are being utilized, did the ISR verify that all three conditions of 8-303c apply to the system? (NISPOM 8-303c)	○	○	○	○
CR-14	Did the ISR verify access to authentication data was restricted to authorized personnel through the use of encryption or file access controls, or both? (NISPOM 8-303d)	○	○	○	○
CR-15	Did the ISR determine that the ISSM understands that prior to reuse of a user ID, all previous access authorizations (including file accesses for that user ID) must be removed from the system? (NISPOM 8-303e)	○	○	○	○
CR-16	Did the ISR determine that the ISSM understands that when an employee terminates, loses access to the system for cause, or no longer has a reason to access the IS, that individual's user ID and authentication must be disabled or removed from the system? (NISPOM 8-303f)	○	○	○	○
CR-17	Did the ISR determine that the ISSM understands that active user IDs, to include access lists, must be revalidated at least annually? (NISPOM 8-303g)	○	○	○	○
CR-18	Did the ISR determine that the ISSM understands that authenticators, such as passwords, smart cards or keys, must not be shared with anyone? (NISPOM 8-303h)	○	○	○	○
CR-19	Did the ISR determine the technical controls for controlling passwords on the system? (NISPOM 8-303I, ISL 2007-01 Q.25)	○	○	○	○
CR-20	Did the ISR determine that the ISSM understands that passwords must be protected at a level commensurate with the classification level and classification category of the information to which they allow access? (NISPOM 8-303i)	○	○	○	○
CR-21	Did the ISR verify that the password is not echoed as the user enters it? (NISPOM 8-303i)	○	○	○	○
	Maintenance				
CR-22	Did the ISR determine if remote diagnostics will be utilized on the system?	○	○	○	○
	Marking Hardware, Output and Media	●	●	●	●
CR-24	Did the ISR establish with the ISSM the perimeter area for collocated IS? (NISPOM 8-306c, ISL 2007-01 Q.29)	○	○	○	○
	Review of Output and Media				
CR-25	Did the ISR review the trusted downloading procedures to ensure they conform with the standard procedures from the DSS ODAA Website? (NISPOM 8-310, ISL 2007-01 Q. 21)	○	○	○	○
	Configuration Management				

CR-26	Did the ISR ensure the contractor has a configuration management plan in place? (NISPOM 8-311, 8-610a(1)(d), ISL 2007-01 Q. 32)	○	○	○	○
Section 4: Protection Measures					
PM-1	Did the ISR review the PCLs, NTK and formal access approvals to ensure the Protection Level of the system under review is correct as stated in the SSP? (NISPOM 8-307, 8-402)	○	○	○	○
Section 5: Special Categories					
SC-1	Did the ISR verify how group authenticators were used? (NISPOM 8-505)	○	○	○	○
Section 6: Protection Requirements					
Audit					
PR-1	Did the ISR determine if the audit trail reviewer understands his or her responsibilities with regard to audit trail review and retention requirements? (NISPOM 8-602a)	○	○	○	○
PR-2	Did the ISR verify that all automated audit trails required for the PL are enabled for all operating system platforms on the system? (NISPOM 8-602a(1)(a))	○	○	○	○
PR-3	Did the ISR ensure that the audit trails are configured to capture all audit records during a 12 month period? (NISPOM 8-602a(4); ISL 2007-01 Q. 43)	○	○	○	○
Data Transmission					
PR-4	If data is transmitted through areas within the company where unauthorized individuals may have access, did the ISR verify that requirements for Protected Distribution Systems are fulfilled in accordance with NSTISSI 7003? (NISPOM 8-605; NSTISSI 7003)	○	○	○	○
PR-5	If the contractor is communicating over Type I encryption devices (STU or STE), did the ISR verify whether the requirements of ISL 02L-1 (Receipt and Dispatch) were fulfilled? (NISPOM 8-605a)	○	○	○	○
Session Controls					
PR-6	Did the ISR verify that the initial screen displayed before user access contains a warning notice requiring the user to take positive action? (NISPOM 8-609)	○	○	○	○
PR-7	Did the ISR review how successive logon attempts are controlled? (NISPOM 8-609)	○	○	○	○
Section 7: Interconnected Systems					
IS-1	Did the ISR ensure that the contractor has a COMSEC account or hand receipt?	○	○	○	○
Writing Requirements					
W-1	Did the ISR complete Enclosure 27, IS Security Plan Review Form?	○	○	○	○
W-2	Did the ISR generate the appropriate Comments form to support SSP ommissions?	○	○	○	○
W-3	If applicable, did the ISR complete Enclosure 28, IS Certification Report?	○	○	○	○
W-4	Did the ISR generate an Interim Approval to Operate letter for the RDAA	○	○	○	○
W-5	Did the ISR generate an Approval to Operate letter for the RDAA	○	○	○	○
W-6	Did the ISR input the appropriate information in the ODAA system?	○	○	○	○
W-7	Did the ISR input the appropriate information in ISFD?	○	○	○	○
W-8	Did the ISR fill out the appropriate data collection instruments?	○	○	○	○
	Scoring				
Total points = the total number of elements (excluding N/As) multiplied by 4.		0	0	0	0
Total Points Possible					**0**
Total points achieved in each category. (No. of Q1s x 4 plus No. of Q2s x 3)		0	0	0	NA
Percentage Score					#####

COMMENTS

(The following comments are specific to this evaluation.)

Evaluation Summary:

General Comments on Elements Receiving a Q-2 or Q-3:

Recommendations:

EVALUATOR’S OVERALL FINDING

Evaluation Scale:

Q1 - Pass: Received 90% or more of the maximum points possible.

Q2 - Pass: Received between 75% and 89% of the maximum points possible.

Q3 - Fail: Received 74% or less of the maximum points possible.

EQ-Exceptional Quality (X, if yes): □

Rationale for the EQ Rating:

Signature of Evaluator:	
Name of Evaluator:	
Date of Completion:	

INFORMATION SYSTEM SECURITY REVIEW EVALUATION FORM
(C&A Reviewer)

Person Evaluated:	
Credential #:	
Field Office:	
Date Observed:	
Facility Name:	
Cage Code:	

SECURITY REVIEW REQUIREMENTS

Q1 – 4 points, indicates that the element was fully covered IAW with the Process Guide/ISL/NISPOM.
Q2 – 3 point, indicates that the element was addressed but not fully covered IAW with the Process Guide/ISL/NISPOM.
Q3 – 0 point, indicates that the element was not addressed or provided incorrect guidance.
NA – this element will be eliminated from the possible overall point value, indicates that the element was addressed but does not apply to this facility.

Place an "X" under the assigned rating for each element.

	RATING:	**Q1**	**Q2**	**Q3**	**NA**
	Section 1: Certification and Accreditation				
CA-1	Did the ISR review a copy of the accreditation letter along with all documentation associated with the accreditation in preparation for the IS review? (Process Guide, Appendix D)				
CA-2	Did the ISR use the accredited SSP as the basis for conducting the IS security review? (Process Guide Appendix D)				
CA-3	Did the ISR evaluate the need for reaccreditation of the contractor's IS due to major changes in the IS hardware, software, physical or procedural controls or other security relevant changes from that which was originally approved? (NISPOM 8-202; ISL 2007-01 Q.11; Process Guide Appendix D)				
CA-4	Did the ISR withdraw accreditation if procedures and controls were ineffective or unacceptable changes were made or if an invalidation occurred? (NISPOM 8-202e; Process Guide Appendix D)				
	Section 2: Responsibilities and Duties				
RD-1	Did the ISR verify that the ISSM, ISSO and privileged users have a PCL, NTK and formal access approvals for all information processed on the system under review? (NISPOM 8-101 & 8-307;)				
RD-2	Did the ISR ensure that the ISSM is an employee of the company and trained to a level commensurate with the overall complexity of all multiple facilities he or she manages or has appointed a technically knowledgeable ISSO? (NISPOM 8-101b & ISL 2007-01 Q. 5;)				
RD-3	Did the ISR determine the ISSM and ISSO are carrying out all duties and responsibilities? (NISPOM 8-103 & 8-104)				
RD-4	Did the ISR interview several general users to verify they have a PCL, NTK and formal access approvals for all information they will access and that they were briefed prior to having access? (NISPOM 8-103I & 8-105)				
RD-5	Did the ISR determine all privileged users have a working knowledge of security functions, policies, technical security safeguards and operational security measures? (NISPOM 8-105a, 8-307)				

FOR OFFICIAL USE ONLY

Section 3: Common Requirements

Clearing and Sanitization

CR-1	Did the ISR review with the contractor different clearing and sanitization methods for continued effectiveness? (DSS IA Website, Clearing and Sanitization Matrix)				
CR-2	Did the ISR verify that an audit entry was made when media was cleared or sanitized and that a record of destruction was made if Top Secret or Secret FGI memory or media was destroyed? (Process Guide Appendix O)				

Software

CR-3	Did the ISR verify that the contractor is following software testing, approving, installing and maintaining procedures and that personnel that perform those functions are cleared to the level the IS is accredited? (NISPOM 8-302a; ISL 2007-01 Q.17, 18 & 19)				
CR-4	Did the ISR determine if unclassified software was written by uncleared people or obtained from an unknown source? (NISPOM 8-302a & 305)				
CR-5	Did the ISR ensure that all features required by the Protection Level are configured as certified on both workstations and servers for all operating systems? (NISPOM 8-302)				

Hardware

CR-6	Did the ISR ensure that the hardware is being examined for elements detrimental to the secure operation of the IS prior to processing? (NISPOM 8-302b)				
CR-7	If in the classified mode, did the ISR examine the accredited system to ensure no connections exist to unclassified systems. (NISPOM 8-100)				

Identification and Authentication

CR-8	Did the ISR verify that electronic means for uniquely identifying and authenticating the users at logon time continue to function as certified and that access to authentication data was restricted to authorized personnel through the use of encryption or file access controls, or both? (NISPOM 8-607 & 8-303)				
CR-9	Did the ISR verify that the contractor is adhering to the requirements for user ID reuse, removal and revalidation? (NISPOM 8-303e-g)				
CR-10	Did the ISR determine that the contractor is adhering to the requirements for protection of individual authenticators? (NISPOM 8-303h-i)				

Maintenance

CR-11	Did the ISR review the contractor’s method of controlling NTK for cleared maintenance personnel performing maintenance on the IS? (NISPOM 8-304a)				
CR-12	Did the ISR determine that an authorized, technically knowledgeable individual escorted uncleared/lower cleared maintenance personnel and that escorts understood responsibilities? (NISPOM 8-304b)				
CR-13	If uncleared maintenance personnel are utilized and the system media is removable, did the ISR ensure there is a separate, protected unclassified copy of the operating system? (NISPOM 8-304b(4))				
CR-14	Did the ISR verify that the contractor is sanitizing equipment (including test equipment) before it leaves the contractor's facility and reexamining it upon return before placing it back in service?				
CR-15	Did the ISR ensure that the ISSM or ISSO is evaluating and approving all maintenance diagnostic equipment for memory or storage capabilities prior to introducing the equipment to the IS?				
CR-16	Did the ISR review for maintenance actions or system failures that may have restored standard passwords to original settings or may have disabled other technical features enabled and verified during certification of the IS?				

Malicious Code					
CR-17	Did the ISR ensure virus-checking software is installed and if introducing media, that software is updated?				
CR-18	Did the ISR determine if there were incidents involving malicious software? (NISPOM 8-305)				
Marking Hardware, Output and Media					
CR-19	Did the ISR verify that hardware, output and media were appropriately marked and that users were trained on applying accurate classification markings after a review of human readable output? (NISPOM 8-306 & 8-310A, 4-200)				
CR-20	Did the ISR verify that writeable media within a perimeter area that contains collocated classified and unclassified ISs is considered classified and marked accordingly? (NISPOM 8-306c, ISL 2007-01 Q. 29)				
Physical Security					
CR-21	For systems not in a closed area, did the ISR review the contractor's procedures, as outlined in the SSP, to prevent or detect unauthorized modification to the hardware while the system is not in use? (NISPOM 8-100)				
CR-22	If seals are utilized, did the ISR ensure the seals are effective and the contractor is following the seal guidelines? (DSS Website, Seal Guidelines)				
CR-23	Did the ISR determine if visual access to the classified information is obtainable by unauthorized individuals? (NISPOM 8-308c)				
Review of Output and Media					
CR-24	Did the ISR review the trusted downloading procedures to ensure they conform to the standard procedures from the DSS IA Website? (NISPOM 8-310, ISL 2007-01 Q. 21)				
Configuration Management					
CR-25	Did the ISR ensure the contractor has implemented an effective configuration management plan? (NISPOM 8-311, ISL 2007-01 Q. 32, 43)				
Section 4: Protection Measures					
PM-1	Did the ISR verify from interviews with users and audit trail reviews to determine if there is a change to the PL? (NISPOM 8-307 & 8-402)				
Section 5: Special Categories					
SC-1	Did the ISR 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? (NISPOM 8-502; ISL 2007-01 Q. 18)				
Section 6: Protection Requirements					
Audit					
PR-1	Did the ISR review IS manual audit records and logs to ensure compliance with accredited SSP, that required events were properly recorded, the reviewer understands their responsibilities and retention requirements were being met? (NISPOM 8-602a; ISL 2007-01 Q. 41 & 43)				
PR-2	Did the ISR review automated audit trails for compliance? (NISPOM 8-8-402, 602)				
Data Transmission					
PR-3	If data is transmitted through areas within the company where unauthorized individuals may have access, did the ISR verify that requirements for Protected Distribution Systems are fulfilled in accordance with NSTISSI 7003? (NISPOM 8-605; NSTISSI 7003)				
PR-4	If the contractor is communicating over Type I encryption devices (STU or STE), did the ISR verify whether the requirements of Receipt and Dispatch were fulfilled? (NISPOM 8-605a)				
Session Controls					
PR-5	Did the ISR verify that the initial screen displayed before user access contains a warning notice requiring the user to take positive action? If the operating system is not capable of an electronic warning banner, did the ISR verify that other methods of notification were used? (NISPOM 8-609)				
PR-6	Did the ISR review how successive logon attempts are controlled? (NISPOM 8-609)				

Writing Requirements

W-1	Did the ISR update the facility profile to ensure information regarding this system is accurate?				
W-2	Did the ISR complete the Action Security Review form or other action form to accurately reflect the results of the information systems security review?				
W-3	Were the security review findings written and did they provide an accurate NISPOM reference?				

Scoring

Total points = the total number of elements (excluding N/As) multiplied by 4.	0	0	0	0
Total Points Possible				**0**
Total points achieved in each category. (No. of Q1s x 4 plus No. of Q2s x 3)	0	0	0	NA
Percentage score.				####

COMMENTS

(The following comments are specific to this evaluation.)

Evaluation Summary:

General Comments on Elements Receiving a Q-2 or Q-3:

Recommendations:

EVALUATOR'S OVERALL FINDING

Evaluation Scale:

Q1 - Pass: Received 90% or more of the maximum points possible.

Q2 - Pass: Received between 75% and 89% of the maximum points possible.

Q3 - Fail: Received 74% or less of the maximum points possible.

EQ-Exceptional Quality (X, if yes): □

Rationale for the EQ Rating:

Signature of Evaluator:

Name of Evaluator:

Date of Completion:

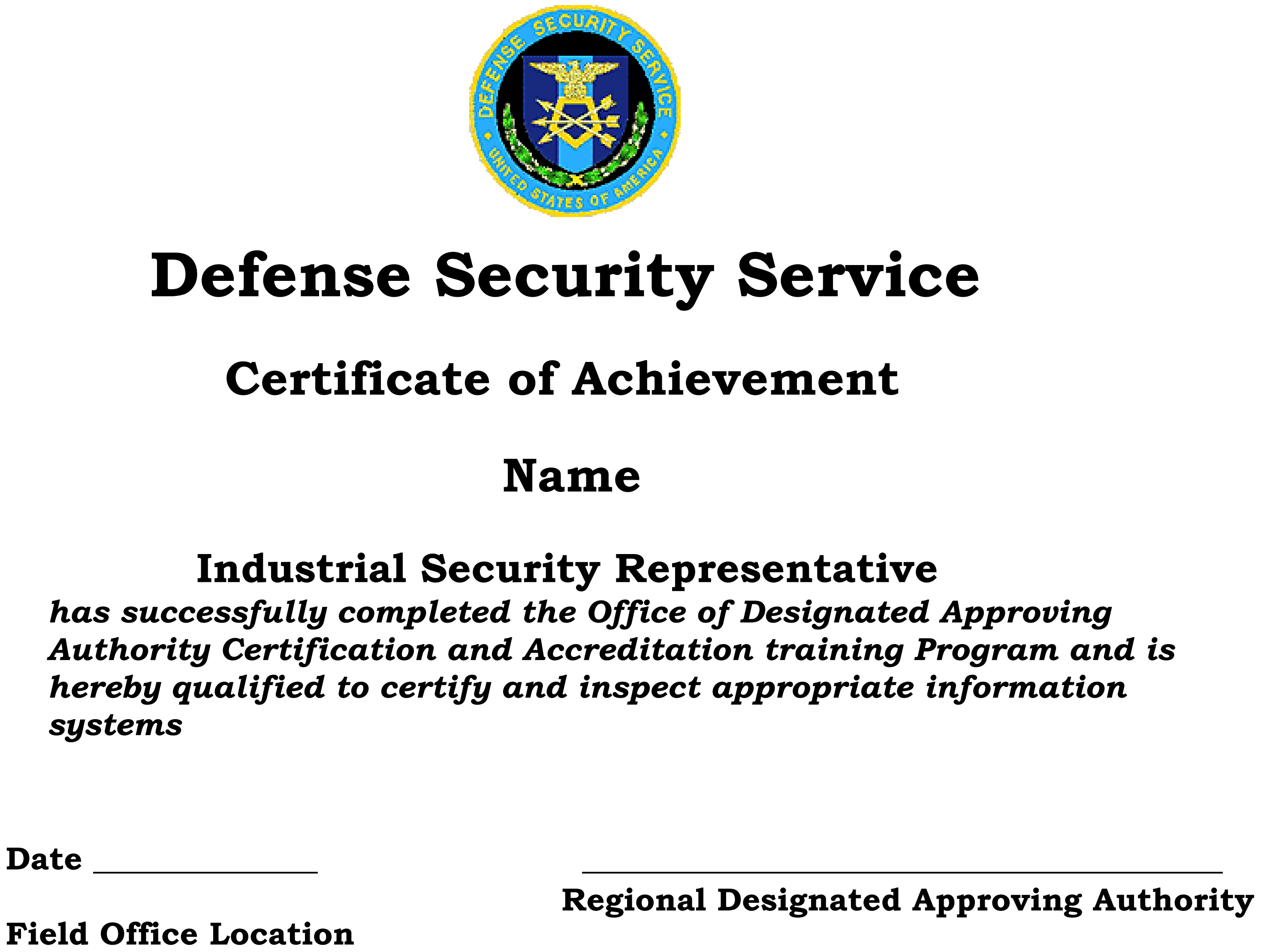
TAB C

INFORMATION SYSTEM SECURITY REVIEW EVALUATION FORM

(C&A Reviewer)

TAB D

Figure B-2 Enclosure 49 – Authorized C&A Reviewer Certificate of Achievement



Defense Security Service

Certificate of Achievement

Name

Industrial Security Representative

has successfully completed the Office of Designated Approving Authority Certification and Accreditation training Program and is hereby qualified to certify and inspect appropriate information systems

Date ______________

____

Regional Designated Approving Authority

Field Office Location

Appendix C 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.

Single-User, Standalone Systems (NISPOM 8-501)

Chapter 8 distinguishes between standalone, single-user and standalone, multi-user 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 multi-user 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 as described below.

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

Periods Processing (NISPOM 8-502)

A. Periods processing is a method of sequential operation that provides the capability to process information at various levels of sensitivity 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 IS Rep will verify with the ISSM that the different processing times are established for the different classification, sensitivity of information, or users.

B. Sanitization After Use: NISPOM Paragraphs 8-301 and 8-502b 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 8-502c 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. 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.

Pure Servers (NISPOM 8-503)

This category of specialized systems, or pure servers, does not fit the protection level criteria, as does the general-purpose or office automation system. The pure server does not have users in the traditional sense, but has clients (e.g., an NSA Type 1 encryption device). The general user never sees or has access to the encryption device, and would be unaware of its existence except for the ISSM’s security briefing. The encryption device accepts encrypted data from outside the network and decrypts it before sending it to the user, or accepts unencrypted data from the user and encrypts it before sending it outside the network. The only users 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 physically be 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.

Test Equipment

Test equipment with non-volatile memory that is going to process or retain classified information requires accreditation. When drafting an SSP for Test Equipment, the generic Section (8-500) will be referenced. Because there are no technical security features associated with test equipment abbreviated procedures may be used in lieu of the standard SSP template used to identify areas such as clearing/sanitization procedures and physical security.

Appendix D Certification and Accreditation (C&A)

Typical C&A Life Cycle of a cleared contractor's IS:

First and foremost the cleared contractor shall have a valid DD254 or contract justifying the use of classified information and subsequent processing of that information on accredited information systems. Based on the classification level, need-to-know and formal access approval, the ISSM will determine a protection level. The ISSM will then formulate a plan to protect the classified information.

The ISSM generates a system security plan using the DSS approved formats available on the DSS web site.

It is important to note that whatever format is being used, the recognized formats are actually templates and must be tailored to the facility's physical and operating environment. A clear and accurate picture of the security measures constructed for the purpose of protecting classified information on the IS must be portrayed. Generalizing or inaccurately/insufficiently tailoring the SSP can only prolong the review process.

Certification:

Contractor:

An ISSM of record submits a system security plan for an IS that will process classified information to ODAA using the instructions within this guide 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 SSP/MSSP. The DSS accreditation decision relies heavily on the accuracy of the ISSM's certification. Additionally, the certification test results and required NISPOM 8-610a DOC 1 signatures must be accompany the SSP/MSSP 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 Appendix E (SSPs) for instructions to submit SSPs/MSSPs to ODAA.

ODAA:
HQ Staff will populate the ODAA database with the information supplied by the contractor's plan submission. As security plans are forwarded to the ODAA they are stored in the appropriate Regional folder. Field Office Chiefs and IS Reps (unless a C&A Reviewer) will be given read-only access to the stored SSPs and MSSPs.

HQ will notify the respective ISSP, IS Rep, RDAA and FOC that the information is available and the plan has been assigned.

Review

ODAA reviewers (ISSPs and Headquarters (HQ) staff) are responsible for the SSPs and MSSPs under their purview for the purposes of review, verification and inspections. The reviewer shall conduct a desktop review of the system's SSP/MSSP to verify compliance with NISPOM Chapter 8 requirements. Security plan reviews will be managed by the Regional Designated Approving Authority (RDAA.)

The ODAA Reviewer (whether an ISSP or Qualified C&A Reviewer) reviews the plan using the attached IS Security Plan and Other Procedures Review Guide commonly referred to as "Enclosure 27". Any NISPOM regulatory issues and/or procedural comments will be captured on the enclosure 27 then transcribed to the ODAA Comments Form. (See SOP for ODAA Correspondence Formats for email and accreditation letter formatting requirements. A Sample Comments Form is also provided below)

The ODAA reviewer makes the following recommendations:

1. Accept the plan requiring no corrective action. In this case the ODAA Reviewer will sign the enclosure 27, generate an IATO letter and forward to the RDAA.

2. Accept the plan requiring some corrective action. In this case the ODAA Reviewer will sign the enclosure 27, generate a Comments Form (outlining the recommendations for corrective action) and an IATO letter and forward to the RDAA.

3. Reject the plan.

When the plan is rejected, the ODAA Reviewer will generate a Comments Form (outlining the recommendations for corrective action) and forward to the RDAA for concurrence. Once the RDAA concurs, the reviewer will forward an e-mail denying the IATO to the ISSM with a copy to the RDAA, ISSP (if different from the reviewer), Field Office Chief, and IS Rep. Comments from the review of the security plan will be attached to the email. The comments shall identify NISPOM required changes and possible system/security plan improvement recommendations. 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 Reviewer (if different from the ISSP), Field Office Chief 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 email 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.

Once the reviewer has completed each review action, the DCI Form for IATOs will be filled out and forwarded to the RDAA for consolidation.
Note: In some cases (schedules permitting), the ODAA Reviewer may be able to conduct on on-site validation immediately after reviewing the plan and may recommend an ATO without recommending an IATO. The DCI Form will still be filled out but the ATO date will be captured vice the IATO date.

Accreditation

Interim Approval to Operate (IATO)

Once the security plan has been reviewed and found to be NISPOM compliant the reviewer shall forward a completed Enclosure 27 and draft IATO to the RDAA. 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 email 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 SSP during the IATO phase without reissuing another IATO. The ODAA should be contacted prior to implementing the changes.

***NOTE**: The SSP and all changes will be frozen one week before the ISSP conducts the on-site validation to ensure the system matches the SSP when inspected. Additionally, IATOs will not be issued to systems with SIPRNET connectivity.*

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/ATO.*** *Failure to do so could result in lapse of accreditation and system operation stoppage. The C&A lifecycle will also restart. Documentation supporting Initial accreditations should be forwarded to ODAA 60 days prior to the facilities anticipated completion timelines.*

The ODAA Reviewer will update their actions in the ODAA database and add the signed IATO, Enclosure 27 and Comments Form (if appropriate) to the associated zip file. If the plan has been rejected, the database will reflect that action as well and update the associated zip file with the Comments Form. The Industrial Security Facilities Database will also reflect these actions in the IS Accreditations section. Amplifying instructions are available in the ODAA Database Guide for Reviewers.

Verification

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

The RDAA, ISSP, Field Office Chief and IS Rep will coordinate to conduct that visit. Prior to the on-site verification, the ISSP/C&A Reviewer (if not the original plan reviewer) should 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 should contact the plan reviewer to resolve the discrepancy prior to the on-site.

During the on-site 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.

If the ISSP/C&A Reviewer who performed the on-site verification was not the reviewer of record he/she will forward the signed IS Certification Report (commonly referred to as "Enclosure 28") to the reviewer. Note: Only the RDAA can waive an on-site validation.

After the on-site validation, the ISSP/C&A Reviewer will make the following recommendations:

1. Issue an Approval To Operate (ATO) for final accreditation. In this case the ISSP/C&A Reviewer will fill out and sign Enclosure 28, and forward to the reviewer who will generate an ATO letter and forward to the RDAA.

2. Issue an ATO once the ISSM has made minor administrative on-the-spot changes. In this case, once the necessary changes/revisions to the plan were received at ODAA, the ISSP/C&A Reviewer will fill out and sign Enclosure 28, forward to the reviewer who will generate an ATO letter and forward to the RDAA.

3. If major discrepancies were discovered during the on-site verification, it may be necessary to schedule a second validation of the IS prior to accreditation being granted. Reschedule another on-site validation once corrective action has been made.

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 Field Office Chief 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 re-submitted and processed as a new system request. The exception to this is "non-existent" 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 re-submit.

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 milestones (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 a Master SSP after the ISSM has been granted authorization to self-certify similar IS (see Appendix F)

DSS Accredits.
After receipt of the Enclosure 28 and draft accreditation letter, the RDAA will email the accreditation letter (i.e., Approval to Operate) to the ISSM with a copy to the ISSP, Reviewer (if different from the ISSP.) FOC, and IS Rep. 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 ODAA Reviewer will update the actions in the ODAA database and add the signed ATO and Enclosure 28 to the associated SSP archive (zip file). If the on-site was rescheduled, the database will reflect that action as well. The Industrial Security Facilities Database will also reflect these actions in the IS Accreditations section. Amplifying instructions are available in the ODAA Database Guide for Reviewers.

The ODAA reviewer/representative will then capture the recommendations above on the DCI Form for ATOs on a monthly basis and submit to the RDAA for consolidation. The RDAA will submit the metrics to ODAA HQ by the 15 of each month for the previous month's activity.

The term "Master" is associated with the self-certification authority granted to an ISSM. However, an ISSM without self-certification can use an SSP for previously accredited IS if that IS is similar and the protective measures identified in that plan are applicable to the new IS. In this case, the ISSM will submit the request using the UID of the previously identified SSP and the new IS, ODAA will review to ensure it is adequately covered by the plan and will issue an IATO if no significant discrepancies exist. Once an on-site validation has been conducted per the instructions above, an ATO will be issued for that IS.

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 two ways:

1. Date an ATO is signed based on an on-site validation

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

The SSP/MSSP Tracking Form will be used to certify, track and validate all IS at the contractor's facility.

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 life cycle will start over again at which time the RDAA may grant an interim approval to operate the system during the review/verification period.

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 email must include the facility name, address, unique SSP or MSSP identifier, NISPOM protection level, and ISSM name, location, and telephone number. See Figure D-1.

If there are significant proposed changes, the plan must be resubmitted like a new request using the appropriate procedures above and the life cycle restarts. Security relevant changes can not 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 re-accreditation 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 interim approval to operate the system during the review/verification period.

Revocation of an IATO or ATO Cole started here

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 SSP or MSSP, an IATO or ATO can be revoked. Prior to revocation, the RDAA will consult with the Deputy Director, ODAA, Deputy Director, Field Operations, the Regional Directors (RD), and the Field Office Chief (FOC). If an IATO or ATO is revoked, the ISSM will be notified via email by the RDAA with a copy to the RD, ISSP and FOC. This email 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 DD, ODAA and DD, 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 Interim Approval to Operate is a temporary approval. If a system has an IATO and the ISSM needs to make changes then the changes can be made to the SSP without reissuing another IATO if ODAA is contacted prior to the changes. However, the SSP and all changes will be frozen one week before the ISSP conducts the on-site validation so that the system matches the SSP when inspected.

Re-accreditation of an IS after a Revocation

Before an SSP or MSSP 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 on-site review will be conducted by the ISSP or IS Rep in coordination with the RDAA and Field Office Chief 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 SSP/MSSP 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 SSP/MSSP

When an Information System 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 Information System must be sanitized, destroyed or disposed of in accordance with the procedures outlined in the system's System Security Plan. Records and logs associated with the Information System must be retained for one inspection cycle.

To disestablish an IS, the ISSM sends a message to the ISSP and IS Rep. The ISSP/C&A Reviewer will validate that the IS has been effectively declassified and forward the recommendation to terminate the accreditation to the RDAA.

The ISSP will use the Disestablishment Letter template (see Figure D-1), names the file "Disestablishment-Ltr-UID.doc" and forwards it to the RDAA. The RDAA signs and emails it to the ISSM, with a copy to the ODAA Regional AO, HQ ODAA Database Administrator (DBA), ISSP, FOC and IS Rep. The database will be updated accordingly. The ODAA HQ DBA will archive the IS.

Figure D-1 Flow Diagram for initial MSSP or SSP

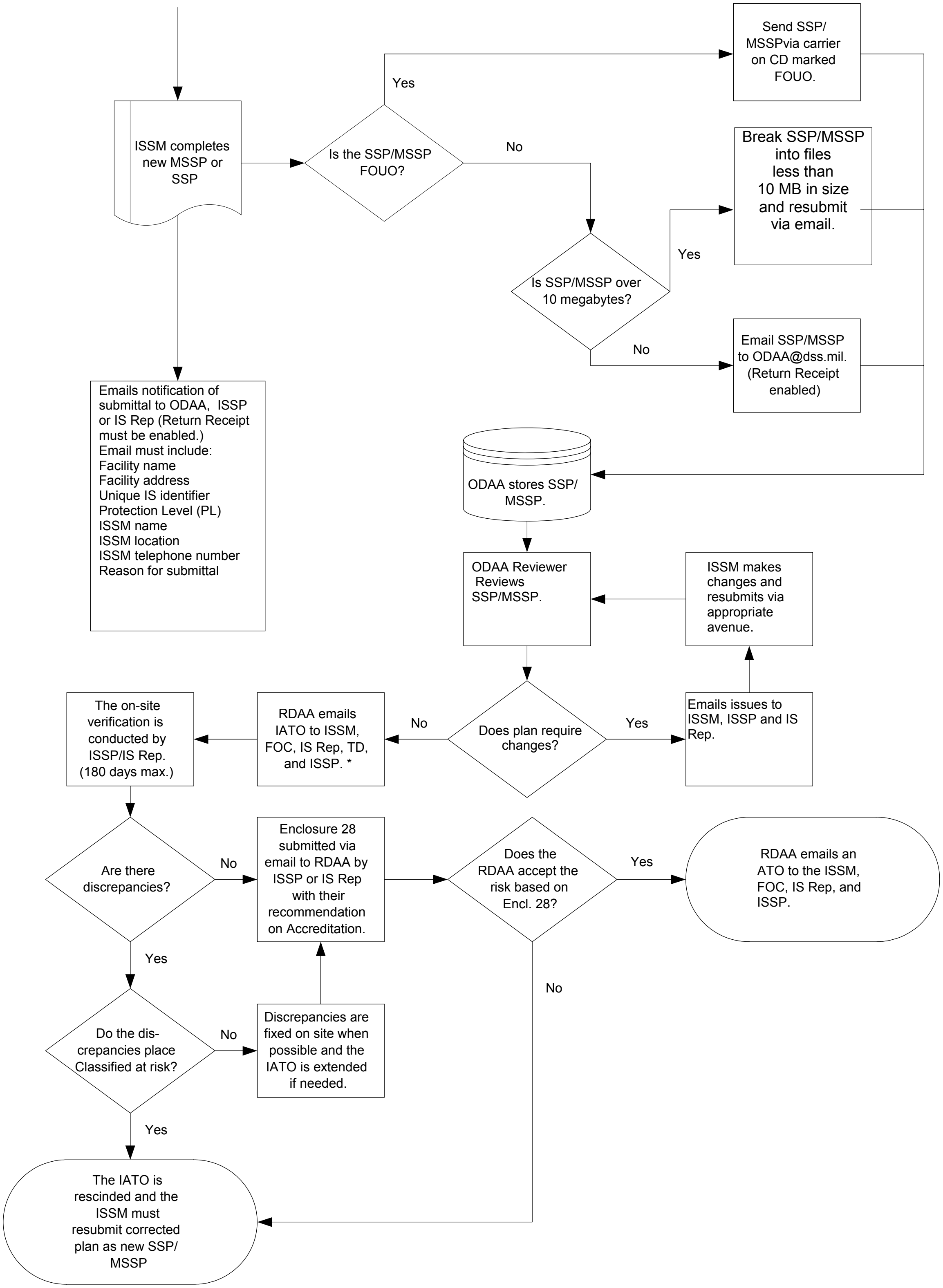
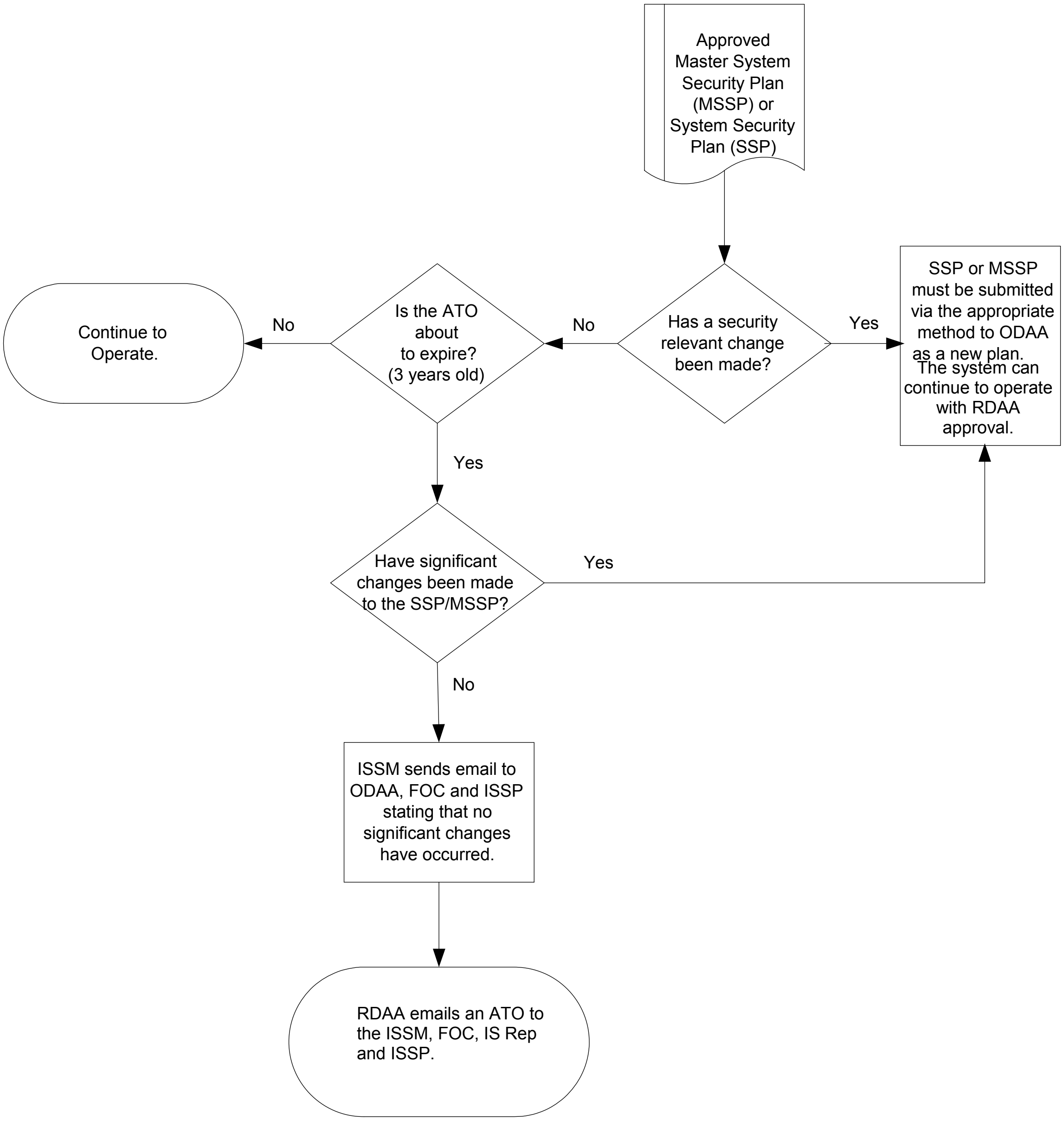

ISSM completes new MSSP or SSP
Is the SSP/MSSP FOUO?
Yes
Send SSP/ MSSPvia carrier on CD marked FOUO.
No
Is SSP/MSSP over 10 megabytes?
Yes
Break SSP/MSSP into files less than 10 MB in size and resubmit via email.
No
Email SSP/MSSP to ODAA@dss.mil. (Return Receipt enabled)
Emails notification of submittal to ODAA, ISSP or IS Rep (Return Receipt must be enabled.)
Email must include:
Facility name
Facility address
Unique IS identifier
Protection Level (PL)
ISSM name
ISSM location
ISSM telephone number
Reason for submittal
ODAA stores SSP/ MSSP.
ODAA Reviewer Reviews SSP/MSSP.
ISSM makes changes and resubmits via appropriate avenue.
Does plan require changes?
Yes
Emails issues to ISSM, ISSP and IS Rep.
No
RDAA emails IATO to ISSM, FOC, IS Rep, TD, and ISSP. *
The on-site verification is conducted by ISSP/IS Rep. (180 days max.)
Are there discrepancies?
No
Enclosure 28 submitted via email to RDAA by ISSP or IS Rep with their recommendation on Accreditation.
Does the RDAA accept the risk based on Encl. 28?
Yes
RDAA emails an ATO to the ISSM, FOC, IS Rep, and ISSP.
No
Yes
Do the dis-crepancies place Classified at risk?
No
Discrepancies are fixed on site when possible and the IATO is extended if needed.
Yes
The IATO is rescinded and the ISSM must resubmit corrected plan as new SSP/ MSSP

Figure D-2 Flow Diagram for a re-accreditation and re-evaluation


Approved Master System Security Plan (MSSP) or System Security Plan (SSP)
Has a security relevant change been made?
Yes
SSP or MSSP must be submitted via the appropriate method to ODAA as a new plan.
The system can continue to operate with RDAA approval.
No
Is the ATO about to expire? (3 years old)
No
Continue to Operate.
Yes
Have significant changes been made to the SSP/MSSP?
Yes
No
ISSM sends email to ODAA, FOC and ISSP stating that no significant changes have occurred.
RDAA emails an ATO to the ISSM, FOC, IS Rep and ISSP.

Enclosure 27 – IS Security Plan and Other Procedures Review Guide

Unique Identifier:	**Submission Date:**	**Reviewed By:**	**Date:**

Administrative

ISSM

Name:

Email:

Address:

Telephone:

Notes: interpretive

Portions of NISPOM Chapter 8, as well as 8-610a (Doc 1) requires the following items to be included in the SSP.

8-XXX = NISPOM Reference.

ODAA PG = ODAA Procedure Guide.

ISL =Industrial Security Letter.

	YES	NO	N/A
The security plan is a: SSP□ MSSP □			
Does the System Security Plan (SSP) reflect the correct name, address of the contractor and use a correct unique identifier?	□	□	
8-401b. Confidentiality level of concern is: high (Top Secret)□ medium (Secret) □ or basic (Confidential)□?			
8-401c. Integrity level of concern is: high□ medium□ basic□ not contractually imposed□?			
8-401d. Availability level of concern is: high□ medium□ basic□ not contractually imposed□?			
8-402. IS Protection level required: PL 1□ PL 2□ PL 3□ PL 4□?			
Does the SSP fall under any of the following categories: Mobile system□ International□ SAP□ FOCI□ Special Category as defined by NISPOM Chapter 8□ PL3 or PL4□ (If necessary, use the comments field to provide additional information for systems		□	

	YES	NO	N/A
that fall in one of these categories)			
Section 1. Responsibilities & Duties			
8-101b. Has an Information System (IS) Security Policy been published and promulgated?	□	□	
8-101b. Has an IS Security Manager (ISSM) been appointed?	□	□	
8-104. Has an IS Security Officer or Officers (ISSO) been identified?	□	□	
8-105. Are users required to acknowledge in writing their responsibility for the protection of the system & information?	□	□	
Section 2. Certification & Accreditation			
8-202. What type of accreditation is being sought: Initial□ Reaccreditation□ Review□ Re-evaluation□			
8-202. If it is a Master SSP, is certification information provided for all systems?	□	□	□
8-201. Has the ISSM certified that the ISs have appropriate protection measures in place & validated same?	□	□	□
Section 3. Common Requirements			
8-301a. Does the SSP adequately provide for clearing of memory and media?	□	□	
8-301b. Does the SSP adequately provide for sanitization of memory and media?	□	□	
8-302a&8-610a. Is security-relevant software tested to verify the security features function as specified?	□	□	
8-302b. Is hardware examined appropriately when placed under the facility's control?	□	□	
303a&610a. How is the user identified upon logon? Unique□ Reused□ Manual□ Electronic□ No identification□			
8-303b. Does the IS require user authentication? What is the method of authentication?	□	□	
8-303d. Is access to authentication data restricted?	□	□	
8-303e. If user IDs are reused, are previous access authorizations removed?	□	□	
8-303f. Are user ID removed or disabled when access is no longer required?	□	□	
8-303g. Are user IDs revalidated at least annually?	□	□	
8-303i. If using passwords, do they meet requirements?	□	□	
8-304. Are procedures spelled out to protect the IS when uncleared personnel perform maintenance?	□	□	
8-304. Does the procedure adequately address maintenance personnel that are	□	□	

	YES	NO	N/A
cleared and those that are uncleared?			
8-304. Is a separate marked & protected copy of the OS maintained for maintenance purposes?	□	□	□
8-305. Does the SSP adequately address detection of malicious code?	□	□	
8-306. Does the marking of hardware, output and media conform to NISPOM Chapter 4?	□	□	
NSTISSI 7003. If PDS is used, are all construction requirements met?	□	□	□
NSTISSI 7003. If PDS is used, are all inspection requirements met?	□	□	□
8-308. How is the IS physically protected? (Check all that apply) Closed Area□ Restricted Area□ Approved Containers□ Seals□ PDS [*]□ Approved Locks□ Access Control Devices□ Alarms□ Guards□ Patrols□ Intrusion Detection System□ Other (Specify)□ [*] Protected Distribution System Is a signed 147 included?		□	
ISL 03L_1 If this is a "Closed Area" are there any false ceilings and raised floors?	□	□	□
ISL 03L_1 If this is a "Closed Area" are alarms present? Were they tested?	□	□	□
8-309. Is media protected accordingly?	□	□	
8-310. Does the SSP provide for the review of Printed Output□ Electronic Media NOT UTILIZING THE DSS STANDARD□ before release?	□	□	
8-310. Are procedures for trusted downloading sufficient?	□	□	□
8-311d. Is the Configuration Management (CM) Plan documented in the SSP?	□	□	
8-311a. Does the plan include all hardware and security-relevant software used during classified processing?	□	□	
8-311d. Does the CM Plan include formal change control procedures for security-relevant hardware and software?	□	□	
8-311d. Does the CM Plan include procedures for documentation management?	□	□	
8-311d. Does the SSP include procedures to implement, test, and verify the CM Plan?	□	□	
Section 5. Special Categories			
8-501. Does the SSP address only single-user, stand-alone systems?	□	□	
8-502. If multi-user standalone system, is "periods processing" used correctly to control users and/or programs?	□	□	□
8-503 &Q52. If the SSP describes a pure server, have all the requirements been met?	□	□	□

	YES	NO	N/A
8-504. Does the procedure describe tactical□ embedded□ data acquisition □ other special purpose system□? (if other, provide more information in the comments section of this document.)		□	
8-505. If using group authenticators, have the requirements been met?	□	□	□
Section 6. Confidentiality Protection Requirements (PL 1 and PL 2 only)			
Audit 1(PL-1)			
ISL. Does the SSP identify and provide manual logs of: (check if available in SSP) Maintenance□ Repair, installation or removal of hardware□, Installation, testing, and modification of OS and security-related software□, Periods processing times□, Sanitization of memory or media□ Application of seals□?		□	
8-602. Does the system create and maintain an internal audit log?	□	□	
8-602. Is all relevant data captured with respect to: (check if data is captured) logons & logoffs□, unsuccessful attempts to access objects (as defined in ISL) □ changes to authenticators□, disabling User ID□, terminal or access port □ account lockout□		□	
8-602. Does the IS provide adequate protection of audit trail logs?	□	□	□
8-602. Does the SSP identify weekly audit analysis?	□	□	□
ISL. Does the SSP provide for the retention of audit records covering the most current 12 months?	□	□	□
Audit 2 (PL 2)	□	□	□
ISL Are both successful and unsuccessful attempts to access user files and classified data audited?	□	□	□
8-602b. Does the audit mechanism provide granularity to the individual user level?	□	□	□
Trans 1 (PL 1+)	□	□	□
8-605. Information is distributed only within a closed area□**,** transmitted via PDS□, or transmitted via NSA-approved encryption mechanism□.	□	□	□
Access 1 (PL 1)	□	□	□
8-606a. Does the SSP provide that unauthorized persons are denied physical access to the system or systems?	□	□	□
Access 2 (PL 2)	□	□	□
8-606b. Does the system or systems provide Discretionary Access Controls?	□	□	□

	YES	NO	N/A
I&A 1 (PL 1)	□	□	□
8-607a. Are uses uniquely identified and authenticated to the system by external (procedural)□ or internal (technical) means□?	□	□	□
Identification & Authentication 2,3,4 (PL 2)	□	□	□
8-607b. Does the SSP specify initial authenticator content and procedures for distribution?	□	□	□
8-607b. If group authenticators are used, does the SSP provide their use in association with individual authenticators?	□	□	□
8-607b. Are the length, composition, and method of generation for authenticators specified in the SSP?	□	□	□
8-607b. Are the authenticator change processes specified in the SSP?	□	□	□
8-607b. Does the SSP specify the password aging interval?	□	□	□
8-607b. Does the system maintain a history of authenticators to ensure non-replication?	□	□	□
8-607b. Does the system provide adequate protection for authenticators?	□	□	□
Resource Control (PL 2 +)	□	□	□
8-608. Does the system ensure that resources contain no residual data before allocation?	□	□	□
Session Controls 1 (PL 1)	□	□	□
8-609a. Does the system or systems display the DOD Warning Banner?	□	□	□
8-609a. Does the system control successive logon attempts by locking the account (check all that apply): after successive failures□, limiting access attempts in a specific time period□, by use of time delay□, or other means□?	□	□	□
8-609a. Does the system grant entry only in accordance with the conditions associated with the user's profile?	□	□	□
Session Controls 2 (PL 2)	□	□	□
8-609b. Does the system or systems limit a user to a single logon session?	□	□	□
8-609b. Does the system close a logon session after a specified period of user inactivity?	□	□	□
8-609b. Does the system notify users of the date and time of the users last logon & the number of unsuccessful access attempts using his/her User ID since last logon?	□	□	□
Security Documentation 1 (PL 1+)	□	□	□
8-610. Does the SSP identify all appropriate security personnel?	□	□	□
8-610. Does the SSP include a narrative description of the system mission or	□	□	□

	YES	NO	N/A
purpose and architecture?			
8-610. Does the SSP detail sensitivity and classification of the information to be processed and clearance, access authorization, and NTK of the user community?	□	□	□
8-610. Does the SSP specify levels of concern for confidentiality, integrity, and availability?	□	□	□
8-610. Does the SSP identify all required protection measures and how they will be met?	□	□	□
8-610. Does the SSP detail any approved variances from the required protection measures?	□	□	□
8-610. Does the SSP describe any threats or vulnerabilities unique to the system?	□	□	□
8-610. If identified, has the ISSM identified and implemented countermeasures?	□	□	□
8-610. If not identified, does the SSP contain a statement to the effect?	□	□	□
8-610. Is a description or the system architecture, to include a block diagram of the components included?	□	□	□
8-610. If the system or network connects to other accredited systems, is an MOU included?	□	□	□
8-610. If describing networked systems, does the SSP include a description of the Security Support Structure?	□	□	□
8-610. Does the certification documentation include test plans, procedures, and initial test results?	□	□	□
8-610. Does the certification/accreditation documentation provide for on-going testing?	□	□	□
8-610. Has the ISSM certified that the system complies with PL requirements & levels of concern?	□	□	□
System Recovery 1 (PL 1+)	□	□	□
8-612a. Does the SSP ensure system recovery will occur in a controlled manner?	□	□	□
System Assurance 1 (PL 1/PL 2)	□	□	□
8-613a. Is access to hardware/software/firmware that performs system or security functions controlled?	□	□	□
Security Testing 1 (PL 1)	□	□	□
ISL. Does the SSP include a statement that security features, including access controls and configuration management, are implemented and operational?	□	□	□
Security Testing 2 (PL 2)	□	□	□
ISL. Has the ISSM provided a written statement that each of the requirements of Table 5 are implemented and operational and that access controls and configuration management are implemented?	□	□	□

	YES	NO	N/A
Section 7. Interconnected Systems			
8-700. The SSP describes a unified network□ or an interconnected network□.	□	□	□
ISL. Does the plan involve systems or networks with different classification levels or compartments?	□	□	□
ISL. Has the Communication Interface been evaluated and found to meet EAL6 of the Common Criteria?	□	□	□
If the plan contains an International connection, has it met all the necessary requirements?	□	□	□

Section 2: Comments	
Reference	**Comments**
1	
2	
3	
4	
5	
6	
7	
8	

___□___ I certify that I have reviewed the System Security Plan (SSP) and it adequately addresses the requirements of NISPOM Chapter 8. I recommend that interim accreditation be granted. This is based on the ISSM's certification that all systems have the appropriate protection measures in place and has validated that they provide the protection measures intended. I will perform an onsite technical review of the system within 180 days of the issuance of the Interim Approval to Operate (IATO).

DSS Reviewer Signature and Date: ________________________

Sample Comments Form

COMPANY NAME

System Name
(Example: Master System Security Plan #SOF-FWB-001 for PL1 Multi-User Systems and Small Internal LANS within Restricted Areas with Removable Media.)
(ODAA Unique Identifier: CAGE-YYYYMMDD-#####)

ISSM: ISSM Name
(Example: John Doe)

Review Results:

We carefully reviewed the Master System Security Plan and found the following items were either not discussed or need clarification in the plan:

Regulatory Compliance Issues:

- The submitted SSP does not adequately describe the procedures and technical IS features to be implemented to make certain that IS recovery is done in a controlled manner. (Applicable comment)
  REF: NISPOM 8-612.a. (NISPOM Reference or valid ISL reference.)

- The ISSM has not made a statement that they have certified that the ISs have appropriate protection measures in place and that they have been validated. Signatures are lacking on the IS Profile Revision Log which would meet this requirement.
  REF: NISPOM 8-201.

ODAA Recommendations:

- For ease of reference and consistency, please label the SSP and attached Protection Profile with the plan's unique identifier. (022T1-20060320-00001)

- It is recommended that you change the FAISSR provided suggestions/verbiage to actually reflect your procedures and system.

- The MSSP identifies that media will be sent to NSA for destruction. Please be aware that NSA has changed it policy on destruction of classified materials for Contract Companies. Please verify with your IS Rep whether or not your materials can be sent to NSA for destruction.
  REF: NISPOM 8-301b.

Please update the Master System Security Plan and resubmit the plan to ODAA. We appreciate your efforts to properly document this system and will expedite processing of your new submittal. Indication to the reviewer of the changes made will help to expedite the re-review of the Plan.

Enclosure 28 – IS Certification Report

IS CERTIFICATION REPORT

AREA/FO: DATE:

IS REP: Qualified C&A Reviewer: Yes PHONE:

ISSP: PHONE:

CONTRACTOR: CAGE CODE:

ADDRESS:

ISSM: PHONE:

IS IDENTIFICATION:

SPECIAL BRIEFINGS:

SYSTEM CONFIGURATION

Protection Level 1

SL 2 □ (Standalone-media destroyed-trusted downloading not authorized)
SL 3 □ (Standalone-media sanitized-STU-III/STE authorized)
SL 4 □ (Standalone or LAN-trusted downloading authorized)
SL 5 □ (WAN-Contractor only)
SL 6 □ (WAN-Contractor and Government)

Protection Level 2

SL 7 □ (Multi-user or LAN)
SL 8 □ (WAN-Contractor and Government)

Protection Level 3

SL 9 □

Protection Level 4

SL 10 □

IS REP CERTIFICATION STATEMENT

Based on this report and my judgment I hereby certify, with the exceptions or clarifications noted below, that the contractor's SSP meets the criteria of the National Industrial Security Program Operating Manual, DoD 5200.22-M dated February 28,2006, Chapter 8. In addition, weighing the remaining residual risks against operational requirements, I recommend that you grant full accreditation.

IS Rep Signature and Date: ____

ISSP ACCREDITATION STATEMENT:

_□_ I certify that I have performed onsite verification of all technical security features of the system, and certify that this system has all appropriate measures in place. I recommend that final accreditation be granted.

Onsite Verification Date:

ISSP Signature and Date:____________________

_□_ I certify that I have reviewed the SSP and recommend that from a technical perspective accreditation be granted. This is a standalone system (single-user/multi-user) and ISSP onsite verification is not required. RDAA signature required.

RDAA Signature and Date:____________________

EXCEPTIONS OR CLARIFICATIONS:

CERTIFICATION REPORT	**YES**	**NO**	**N/A**
INTERIM ACCREDITATION GRANTED (PROVIDE EXPIRATION DATE)	□	□	□
CLOSED AREA	□	□	□
PROTECTED DISTRIBUTION SYSTEM (PDS)	□	□	□
COMSEC			
STU-III/STE	□	□	□
OTHER	□	□	□
TRUSTED DOWNLOADING	□	□	□
MEDIA			
SANITIZED	□	□	□
DESTROYED	□	□	□
MEMORY			
SANITIZED	□	□	□
DESTROYED	□	□	□
MOU(s) GOVERNMENT	□	□	□
EQUIPMENT DISCONNECT PROCEDURES	□	□	□

Sample Disestablishment Letter

DEFENSE SECURITY SERVICE
Office of the Designated Approving Authority
1340 Braddock Place
Alexandria, VA 22314

` January 2, 2008

ISSM Name
Company Name
Address Line 1
City, State XXXXX

Dear ISSM Name,

I am acting upon your request dated D Month YYYY to Industrial Security Representative (ISR) IS Rep Name to disestablish the Information System identified as [UID or system name if no UID exists]. Accordingly, the accreditation granted to Information System [UID or system name if no UID exists] to process classified information is hereby withdrawn.

It is your responsibility as the Information System Security Manager (ISSM) to adhere to the procedures from the (M)SSP are followed for final disposition of the classified information associated with this IS. You are also reminded to retain essential records associated with the Information System for one inspection cycle. If you have any questions, please feel free to contact ISR IS Rep Name at (XXX) XXX-XXXX.

Sincerely,

RDAA Name
Region Region Designated Approving Authority
Office of the Designated Approving Authority
Defense Security Service

Appendix E System Security Plans

Plan Submissions:

The following procedure should be used for submitting an initial SSP/MSSP. Table 2.1 outlines the required elements for submitting plans. Once an ISSM develops an SSP or MSSP 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 email with the SSP as an attachment to the ODAA mailbox at ODAA@dss.mil with the subject line as explained in Table 2.1. The subject line unique identifier format is mandatory for the proper routing of the SSP. The Region must be the first variable in the subject line. The body of the email must include the facility name, address, unique identifier of the system, NISPOM protection level, and ISSM name, location, telephone number and reason for submittal, i.e. initial, reaccreditation, review, re-evaluation, informational. If the system is being reaccredited, please include a list of changes made to the plan to assist in reaccreditation processing.

The **second method** for 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 SSPs.

Regardless of the method used, the ISSMs must copy on the e-mail to ODAA, the local ISSP and IS Rep stating that the plan has been submitted. If the ISSMs are unsure of the personnel to be notified, they should contact the local IS Rep, FOC or ISSP. Their information will be provided on the DSS web site. The e-mail will include the facility name, address, ODAA unique identifier of the system, NISPOM protection level, and ISSM name, location, telephone number and reason for submittal, (i.e. initial, reaccreditation, review, re-evaluation, informational). The ODAA Unique Identifiers (UID) applies to the SSP and the IS Description (or 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 SSP. This can occur in one of two ways:

1. ODAA conducts an on-site verification to validate the IS can be protected by the existing 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. See Appendix F for more information on self-certification.

UIDs will not change when plans are rejected and subsequently resubmitted to the ODAA. Changes in the UID may result in delays.

Table E-1 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.
Variables	
MSSP	Use MSSP when the plan is a Master 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
SAP	Use when the IS seeking accreditation is associated with Special Programs
INT	Use INT for SSPs with International connections
NSP	Use NSP for Network 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) Standard SSP #13 from the Northern region from Cage Code 10101, dated Nov. 18, 2005 protecting IS#10

Northern 10101-20051118-00013-00010

SAMPLE EMAIL 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 a Master System Security Plan

----
From: (Recipient address)

To: DSS, ODAA, (ISSP address)

CC: (ISRep address)

Subject: ODAA Submission - Region – UID (Please input Region designation i.e. Capital, Northern, Southern, Western; and the Unique Identifier)

Attachment: (Attached Plan and Associated files)

ODAA Submission Information

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

Date of System Security Plan:

Receipt Date (Email Date):

Type of Plan: (SSP, MSSP, NSP, SIPR)

Protection Level: (PL 1, PL 2, PL 3,)

Classification: (High (Top Secret), Medium (Secret), Basic (Confidential))

System Type: (LAN, WAN, Standalone Multi-User, 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:

Email:

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))

Additional Information/ Comments:

Example ODAA Submission Email

From: John.Doe@ABC.com

To: DSS, ODAA, Frank.Smith@dss.mil

CC: Tom.Jones@dss.mil

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

ODAA Submission Information

Tracking ID: 12345-20080310

Date of System Security Plan: March 10, 2008

Receipt Date (Email Date): 03/11/2008

Type of Plan: MSSP

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. AIS 345

2. AIS 234

IS Rep Name: Tom Jones

ISSP Name: Frank Smith

ISSM Name: John Doe

Phone: (212)555-4567

Address: 101 Anywhere St
Alexandria, VA, 22314

Email: 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 Email 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 email as well, potentially there could be significant delays in processing the plan for review. If the necessary information cannot be readily obtained, the email will be rejected returned for administrative correction.

Additional Considerations:

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 8-303c):

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 local area networks) 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.

Commingling of data from Multiple Programs or GCAs on a Single IS

For a single IS to be accredited to process classified information from multiple programs and/or government contracting activities (GCAs) at PL-1, the following prerequisites must be met:

a. The programs must be of similar or like nature. (e.g., programs share similar technology/information and/or require integration/interoperability of contract deliverables).
b. The contractor must be able to determine that all users have a need-to-know for all classified information to be processed on the system.
c. The highest level of classified information to be processed is SECRET.
d. Access is limited to those appropriately cleared employees of the company possessing the required clearance and need-to-know for all information on the system.
e. Written notification must be made to each cognizant GCA at least 30 days prior to their classified information being placed on the system. Notification must be made to an appropriately responsible official of the GCA – e.g., Program Manager or Deputy Program Manager. Should a GCA raise an objection, the facility is prohibited from including that program's classified information on the system.

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 underlying requirement to create and retain receipt and dispatch logs has not changed. For those transmissions where the two entities have a contractual relationship, the contractor may place a letter in document control to state electronic data transmissions occur. The information is to be maintained for two years. For non-contractual transmissions, the contractor must maintain the required data (audit trails) for two years.

Receipt and dispatch records (NISPOM paragraph 5-202) are required when transmitting classified information electronically. Discussed in ISL 03L-1 (rescinded - will be included in the next ISL.) was the option of utilizing either manual or automated record systems provided each included the required five reflected items. Numerous questions and concerns have been received from industry regarding this article resulting in a second look at the implementation of this requirement.

The intent of requiring receipt and dispatch records for classified information transmitted electronically remains valid. Contractors are required by paragraph 5-200 to establish an information management system and control all classified information in their possession. The problem facing industry with this requirement is the volume of receipt and dispatch records that can be generated by an accredited Information System (IS). The following guidance is intended to assist in that regard.

a. Protection Level 1 (formerly Dedicated Security Mode), connections between entities with direct contractual relationship. Record in document control each facility that information is transmitted to or received from by CAGE code, contract number, expiration date and classification level. This information is recorded once and updated upon change of contract status. 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.

b. Protection Level 1, connections between entities without direct contractual relationship. For each classified session, the audit requirements identified for Audit 1 (NISPOM Chapter 8, paragraph 8-602a) will record the required information. In the event the IS cannot provide an automated audit capability, the contractor is required to capture the information in a manual receipt and dispatch log. Records shall be retained for 2 years.

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 to so that no users have access to the accredited information systems. The request should be routed through the ISSP, RDAA and to the Deputy Director, ODAA for approval.

Deviations from automated auditing

NISPOM 8-602a(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 maybe 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/Protection 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 an extended period of time, the ISSM should de-certify the system and then re-establish it when needed. This should be evaluated when the system has not been used for three or more months.

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, or 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 unique ID
- Operating System
- Operating environment
- NISPOM requirement(s) that cannot be met and how the requirement is mitigated

For systems that are designated tactical/special purpose, the GCA should identify exceptions at the component level instead of for the entire system.

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

NOTE: Protection Profiles for legacy systems may be grouped into one System Security Plan, (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 MSSP's.

Include sample letter

Unified Networks 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. The network will 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 System Security Plan 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 on-site verification of the host system and provide the Enclosure 28 to ODAA.

5. The ISSP/C&A Reviewer for each connecting node is not required to complete another Enclosure 27, but 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. ISSP/C&A Reviewer will complete the Enclosure 28, then send it via email to the ISSP/C&A Reviewer of the host node.

6. Following onsite verifications and completion of the Enclosure 28 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.

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

Appendix F Master System Security Plans (MSSP)

Master Plan Concept

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. The IS covered by an MSSP may range from stand alone workstations up to and including multi-user IS and local networks that meet the criteria for a Master SSP approach. This type of approval applies only to IS operating at Protection Levels 1 or 2.

Included at the end of this appendix is the ISL 2007-01 Article #4 Extract relating to MSSP/self-certification for ease of reference.

Master Plan Structure

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 Master, those changes will affect every IS that fall under and are protected by that Master SSP.

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 maximum. 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 Master SSP. This self-certification, in effect, 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 new IS profile to be considered for accreditation by emailing the ODAA mailbox at ODAA@dss.mil and copy the ODAA. The email will reflect the information provided in Appendix D.

Once the submitted plan is received by the ODAA database administrator, it will be assigned to the responsible ODAA Reviewer/Rep for review and onsite validation. The C&A Process identified in Appendix D still applies. The RDAA will issue an IATO for the new IS profile once a favorable review is completed. 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 email. While the MSSP will not need to be re-approved, the ISSP/C&A Reviewer must certify the new IS profile within 180 days. 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 Master SSP.

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 appendix (see the SSP/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. (Please see the suggested format for the letter notifying of a new self-certified systems). Every self-certified IS profile must be forwarded to the ODAA mailbox to ensure contractor systems and ODAA database match. The listing provided at the end of this appendix will also be used to reconcile all existing IS at the facility.

MSSPs must be re-accredited every 3 years or when security relevant changes are made to the MSSPs. The 3-year time frame will begin from the initial approval of the MSSP as it applies to the first IS. Any IS that have been self-certified will have its own expiration based on the date it was added to the Master. The SSP/MSSP Tracking Form at the end of this appendix will be used to manage the additions of self-certified IS.

If there are no security relevant changes, the 3-year re-accreditation 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 3-year re-accreditation.

If either the levels of concern or protection level change for any IS covered by in the MSSP, the MSSP must be revised and re-accredited 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

The following are general guidelines on writing Master System Security Plans (MSSP) and self-certifying systems under an approved MSSP by an ISSM.

Master Plans

An MSSP must be specific to the operating environment. For example, a separate plan must be prepared for restricted areas, closed areas.

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. ODAA recommends that IS with caveated information be sent to ODAA. The IS can be given a separate ATO based on an on-site validation by an ISSP/C&A Reviewer.

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

An IS Profile under an MSSP is written for a system type (Single-User Non-networked, Multi-User Non-networked and 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 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. An ISSM authorized to self-certify IS under an MSSP for Peer to Peer Networks can self-certify both Peer to Peer Networks and multi-user non-networked workstations under a separate MSSP. An ISSM's authorization to self-certify IS under an MSSP for multi-user systems cannot be used to self-certify single-user workstations.

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 is granted automatically in the MSSP Approval to Operate (ATO) unless the ISSP/C&A Reviewer specifically requests 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.

An ISSM can use operating systems from any CSA approved IS to self-certify systems in other operating environments already approved under an MSSP.

Self-certification is based on similar systems. A similar system is defined as a system that that operates in the same operating environment, classification level, system type (Single-User Non-networked, Multi-User Non-networked and Peer to Peer LAN, or Domain Controlled LAN), similar operating system(s), and similar operations (Trusted Downloads, Periods Processing, Mobile System, etc) as indicated in the IS profile accredited by DSS which will be the basis for all self-certified systems under the approved master plan.

Example 1

1. IS ‘1’ (under MSSP#1) covers a PL1, Secret, XP Peer to Peer LAN in a Closed Area with no periods processing using the DSS trusted download procedures.
2. IS ‘2’ (under MSSP#2) covers a PL1, Secret, Peer to Peer Solaris LAN in a Restricted Area with periods processing using DSS trusted download procedures.
3. The new system, IS ‘3,’ will be a PL 1, Secret, XP Peer to Peer LAN in a Restricted Area without periods processing and no trusted downloading.

The ISSM **can** self-certify the new PL 1, Secret, XP Peer to Peer LAN in a Restricted Area without periods processing and no trusted download procedures based on using any combinations of the operating systems from both IS Profiles ‘1’ and ‘2’. (Specifically the o/s from IS #1)

In this example, the ISSM has effectively self-certified a new IS under MSSP#2.

Example 2

1. IS '1' (under MSSP#1) covers a PL1, Secret, XP, and Windows 2000 Peer to Peer LAN in a Closed Area with periods processing and using the DSS trusted download procedures.
2. IS '2' (under MSSP#2) covers a PL 1, Confidential, Linux 9 and Solaris 9 Peer to Peer LAN in a Restricted Area with periods processing and no trusted download procedures.
3. The new system, IS '3' will be a PL 1, Secret, Peer to Peer LAN with Solaris 9 and XP in a Restricted Area with periods processing using the alternate trusted download procedures.

The ISSM **cannot** self-certify the new system. Neither MSSP would be appropriate. Although MSSP#2 would seem logical due to similar physical security environments (Restricted Area), the levels of concern are not the same.

In this example, the ISSM would have to submit a separate MSSP for IS '3' if they are requesting self-certification.

Example 3

1. IS '1' (under MSSP#1) covers a PL 1, Secret, Domain Controlled Network, with NetApps pure server, Windows 2003 Server, Windows XP, and Solaris 8 operating in a Closed Area with DSS approved Trusted Downloads.
2. IS '2' (under MSSP#2) covers a PL 1, Confidential, Domain Controlled Network with Enterprise 5, RHEL 4, Solaris 9, and Solaris 10 in a Closed Area without Trusted Downloads.
3. The new system, IS '3' will be a PL 1 Confidential, Domain Controlled Network, with NetApps pure server, Solaris 10, Solaris 9, and Solaris 8 in a Closed Area without Trusted Downloads.

The ISSM **can** self-certify the new Domain Controlled in a Closed Area using the operating systems from both IS profiles and add IS '3'under MSSP#2 (same levels of concern, same physical environments, etc).

In this example the ISSM is authorized to create a new compliant system using any combination of the operating systems from both CSA approved IS without Trusted Downloads based on IS Profiles '1' and '2' provided the levels of concern are the same.

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:

- Copy of the MSSP Accreditation Letter
- Copy of the approved Master Plan
- 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 accreditation 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 Rep when a new system is self certificated. Frequency and format of self certification notification should be decided upon between the ISSM and ISSP/C&A Reviewer.

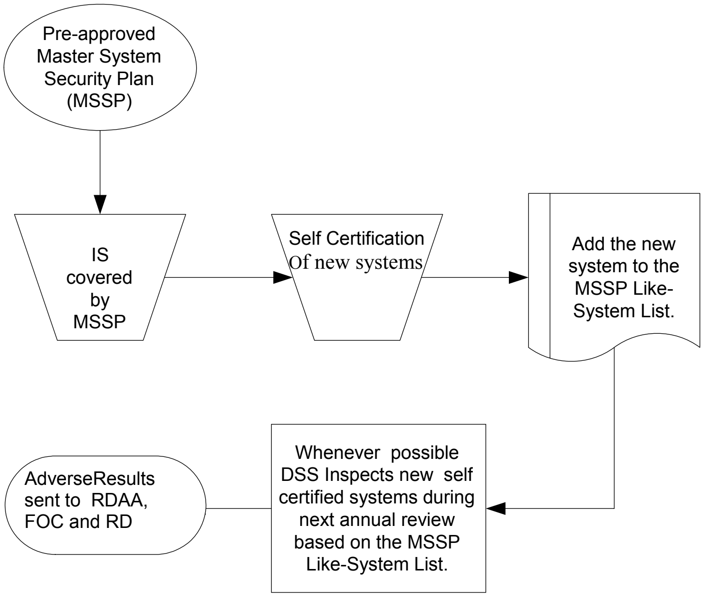
Notification Requirements of Self-Certified Systems

The ISSM will submit a list of all self-certified systems to the ISSP and IS Rep using the attached Tracking Form. The frequency of submitting the self-certified IS documentation will in accordance with an agreement between the ISSP/C&A Reviewer and the ISSM. This will vary due to the size of facilities, and the amount of systems which are self-certified. For each system self-certified, the ISSM will provide a letter identifying the self-certified system(s), a self-certification document identifying the Master Plan and protection profile used to self-certify the new system, a complete IS profile, all supporting documents, and the certification test guide.

MSSP Like-System Addition List

The ISSM does not have to wait for DSS certification to install a system and begin processing under a Master System Security Plan (MSSP) that has already received an ATO. However, the ISSM must maintain the IS Certification Report with the MSSP and a listing of all systems added or deleted under an MSSP. The list should include enough information to allow for the system to be easily identified. The list should be maintained for at least one year from the date of the last annual security review or issuance of the initial ATO for the MSSP. This listing should be presented to the IS Rep, ISSP or FOC at the next annual security review.

Figure F-1 Flow Diagram for Self-Certification under an MSSP



Pre-approved Master System Security Plan (MSSP)
IS covered by MSSP
Self Certification Of new systems
Add the new system to the MSSP Like-System List.
Whenever possible DSS Inspects new self certified systems during next annual review based on the MSSP Like-System List.
AdverseResults sent to RDAA, FOC and RD

Limitations on Self-Certification of Similar Systems

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

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 Master Plan 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 ODAA. The request letter must identify the following information:

- Copy of the self-certification letter identifying the system ID and associated Master Plan
- Detailed procedures explaining physical and technical audit procedures
- Frequency Technical Audits will be performed.

Once approved, the procedures and DSS audit variance approval letter must be retained as an attachment in the protection profile for the specific system approved for the variance.

NOTE: The approval letters will be system specific and will expire when the associated Master Plan 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 protection 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 Master Plan 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 Risk Acceptance Letter. 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 Master Plan Accreditation Letter.
- Copy of the self-certification letter identifying the system ID and associated Master Plan
- Detailed procedures and file types applicable under the alternate procedures.
- A signed copy of the customers Risk Acceptance Letter 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 customer Risk Acceptance Letter.

Once approved, the procedures, the customers Risk Acceptance Letter and ODAA approval letter must be retained as an attachment in the protection profile for the specific system approved for use.

NOTE: The approval letter will be system specific and will expire when the associated Master Plan 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 Master Plan. (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 Master Plan protection 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 CSA approved protection profiles. Additionally, the CSA recommends that you develop 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. 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 unique ID for the test equipment document.
- Listing of test equipment, matching the unique ID 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.

Re-accreditation and Re-evaluation of an MSSP

Re-accreditation 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 email must include the facility name, address, unique SSP or MSSP identifier, NISPOM protection level, and ISSM name, location, and telephone number. See Figure D-2.

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 can not 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 re-accreditation with changes are submitted with enough time 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, 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. This is important because for those ISSMs that would like to consider themselves candidates for the Corporate/Traveling ISSM, withdrawal of self-certification could have significant operational consequences.

Traveling/Corporate ISSM (Pilot Program)

Under certain circumstances, an ISSM may be designated as a Traveling or Corporate ISSM. This Traveling/Corporate ISSM would be responsible for oversight of multi-location facilities that are geographically dispersed. This designated ISSM must be able to effectively manage and quickly respond to situations so that classified data is not compromised. Specifically, the ISSM must be able to effectively manage more than one situation in order to prevent further classified data being inadvertently dispersed or compromised, (i.e. such as multiple spills at different locations). Self-certification can be approved for this position, however, if DSS deems that the oversight was ineffective which likely increases the risk of compromise, self-certification can be withdrawn from the entire structure under the purview of the designated ISSM. Therefore care must be given by contractor management when considering the scope of oversight by the Traveling/Corporate ISSM.

ISL Extract

ISL 2007-1 #4. (8-101b, 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. (8-202g) Can one Master SSP (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. (8-202g) Can one MSSP be written that covers all IS within the contractor's facility that operate at PL 1 and PL 2?

Answer: No. Paragraph 8-202g 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).

Self-Certification

Certification and accreditation of similar systems, commonly referred to as self-certification, is discussed in NISPOM paragraph 8-202g. When specifically authorized in writing by DSS, an ISSM may extend an existing DSS accreditation to (i.e., self-certify) similar systems. ISSMs may self-certify similar systems only within specified parameters.

The general rules and parameters for self-certification are:

a) Self-certification must be based on a DSS-approved Master System Security Plan (MSSP). WANs and WAN interconnections (adding a node to a Network Security Plan) cannot be self-certified.

b) Any self certified system must be in compliance with applicable NISPOM requirements.

c) If a contractor is uncertain of the self-certification authority granted to them by DSS, the contractor should consult with DSS ODAA about the extent of their authority.

d) All required documentation for self-certified systems must be readily available for DSS review as detailed in the DSS ODAA Process Guide.

e) Self-certification authority is granted by DSS to a specific person at a particular CAGE Code in the Approval to Operate (ATO) letter. Self-certification of systems outside of the CAGE Code specified in the ATO is not permitted.

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

Table F-1 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.

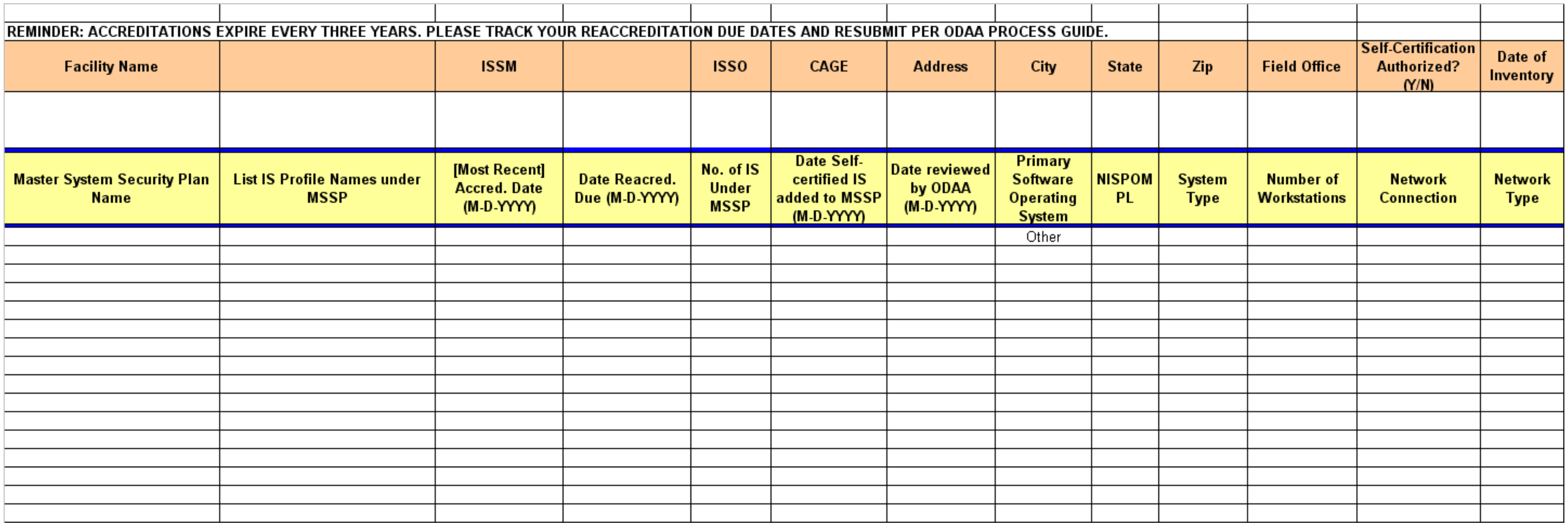
Note: 2 – Level of Concern (NISPOM 8-401) must be the same. This refers to the classification levels of information (Top Secret, Secret, and Confidential)
Note: 3 – Physical. This pertains to the physical security environment (most notably restricted areas and closed areas). Be mindful that there are 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. However, a new OS can be added to an approved Protection Profile provided it's been previously approved by ODAA under another Protection Profile or Master Plan. In addition, 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, Multi-user standalones (MUSA) or LANs. It can also refer 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 - TDP (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.

15. (8-202g(3)) Paragraph 8-202g(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 F-2 MSSP IS Tracking Form

MSSP IS Tracking Form



REMINDER: ACCREDITATIONS EXPIRE EVERY THREE YEARS. PLEASE TRACK YOUR REACCREDITATION DUE DATES AND RESUBMIT PER ODAA PROCESS GUIDE.												
Facility Name		**ISSM**		**ISSO**	**CAGE**	**Address**	**City**	**State**	**Zip**	**Field Office**	**Self-Certification Authorized? (Y/N)**	**Date of Inventory**
Master System Security Plan Name	**List IS Profile Names under MSSP**	**[Most Recent] Accred. Date (M-D-YYYY)**	**Date Reacred. Due (M-D-YYYY)**	**No. of IS Under MSSP**	**Date Self-certified IS added to MSSP (M-D-YYYY)**	**Date reviewed by ODAA (M-D-YYYY)**	**Primary Software Operating System**	**NISPOM PL**	**System Type**	**Number of Workstations**	**Network Connection**	**Network Type**
							Other					

Appendix G Network Security Plans

Wide Area Networks (WANs) and Interconnected Systems

The following section provides general guidance for certification and accreditation of WANs and other interconnected systems. This section of the ODAA process guide will explain the requirements for a network security plan (NSP) and the approval process for connecting systems to existing WANs. For the purposes of this guide, all separately accredited interconnected systems are treated in the same manner and must meet the same requirements.

Network Security Plans (NSPs)

The requirement for an NSP is derived from the NISPOM requirement that states "An interconnected network also requires accreditation as a unit" (NISPOM 8-700.c). 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 information system security manager (ISSM) at the same facility, campus, or Commercial and Government Entity **(**CAGE) code and/or same DAA.

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 the requiring the existing nodes to be reaccredited.

NSPs are submitted to DSS for review and accreditation in the same manner as a System Security Plan (SSP) or Master System Security Plan (MSSP).

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 information system (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 and MOUs will be discussed in detail later.

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 and
15) Access control lists (if applicable) IDS requirements (if any)
16) For auditing purposes, record activities occurring across the interconnection
17) Identify any identification and authentication (I&A) methods used to authenticate users across the interconnection
18) Specific virus scanning or anti-virus requirements (if any).
19) 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 are 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 Profile ID 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 email 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 (discussed later). 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 network security plan (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. Emails the completed package to DSS ODAA and copies DSS personnel as required by the process guide.
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) The ISSP will forward draft ATO (possibly IATO) to the RDAA.
6) RDAA will sign and distribute the NSP's ATO. The NSP ATO will be sent back to the Network ISSO and responsible DSS personnel.

7) 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 SSP or MSSP. 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 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 need to know. The IT Security Inc. 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 need to know 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 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.

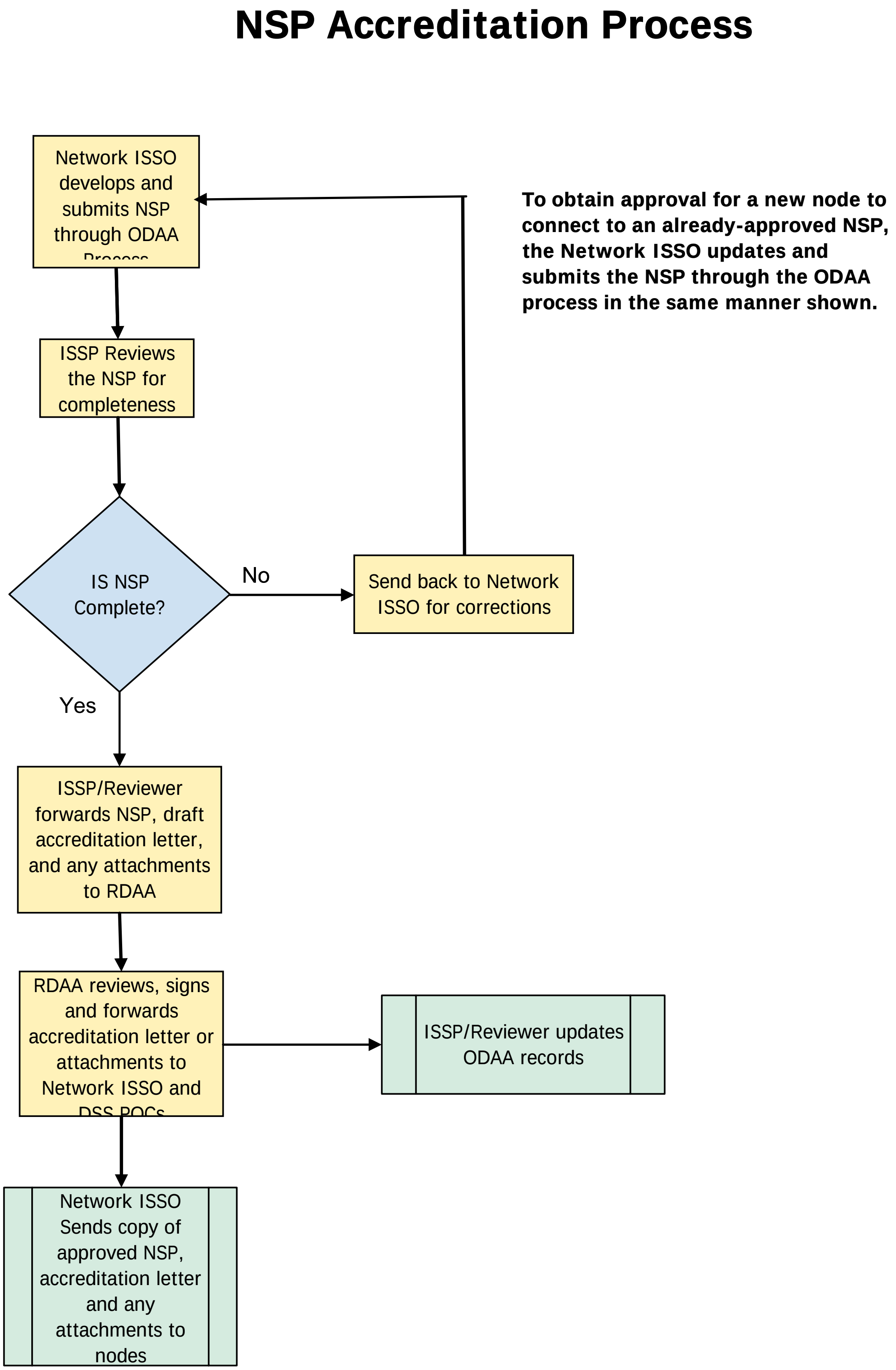
Example 4: A PL1 WAN owned by Company "A" has an ATO and is processing Secret Collateral. It has 2 Company "A" PL1 nodes one with an ATO and one with an IATO. Company "B" has a PL1 node also only processing Secret Collateral and wishes to connect to the WAN. It is determined that this node has the same 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. Provide email addresses are in the package 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 (discussed later). 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. Emails the completed package to DSS ODAA and CCs DSS personnel as required by the process guide.
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.

Figure G-1 below 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 G-1 NSP Accreditation Process Diagram


NSP Accreditation Process
Network ISSO develops and submits NSP through ODAA Process
ISSP Reviews the NSP for completeness
IS NSP Complete?
No
Send back to Network ISSO for corrections
Yes
ISSP/Reviewer forwards NSP, draft accreditation letter, and any attachments to RDAA
RDAA reviews, signs and forwards accreditation letter or attachments to Network ISSO and DSS POCs
ISSP/Reviewer updates ODAA records
Network ISSO Sends copy of approved NSP, accreditation letter and any attachments to nodes
To obtain approval for a new node to connect to an already-approved NSP, the Network ISSO updates and submits the NSP through the ODAA process in the same manner shown.

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 or MOA must require all nodes and the WAN be accredited in accordance with the respective certification and accreditation requirements documents. MOAs and MOUs will be discussed in detail later.

The contractor can write a Master System Security Plan (MSSP) for the node under DSS cognizance provided that it is not explicitly denied in the MOU or 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 Office of the Designated Approving Authority (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 system security plan (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: 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.

Memoranda of Understand and Memoranda of Agreement (MOU/MOA)

For the purposes of this guide, 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 guide.

DSS has an approved template or sample MOU document available. It can be downloaded from the DSS website, or may be requested through the DSS ISSP or IS Representative. Using this document to create an MOU will reduce time required for review and processing by DSS.

MOU Requirements

When information systems 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.

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 government contracting agency (GCA) or user agency (UA) should sign the MOU first. The MOU is then sent to the responsible DSS DAA 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.

MOU Content

The purpose of an MOU is to adjudicate the differences in requirements of different DAAs and to establish roles and responsibilities. Some User Agencies (UA) or Program Offices may already have standard MOU formats that are routinely utilized for connections. If the UA wishes to use their own format for the MOU, they may do so. DSS requires some additional information be added to the MOU in order to meet NISPOM requirements.

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 until no longer needed 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.

Controlled Interfaces

This section serves to clarify the requirements from the NISPOM Chapter 8, Section 7, Interconnected Systems.

1) 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.

2) 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.

3) 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.

Joint Staff, in coordination with DISA, requires 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 Intrusion Detection System (IDS) that is equivalent to the established US Protection Profile identified by the red PP on the NIAP webpage. For questions relating to approved boundary devices please contact the SIPRNet SCAO at 703-882-1455.

Figure G-2 IS Profile Form

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

Date:	Revision #:	Facility Address:	CAGE Code:

Contact Information

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

Network Identification

High-level description and usage of overall network:

Contract Number(s):

Network Communications Matrix

The following table summarizes the connectivity and access between all sites on the network. A sample is provided, and should be modified to accommodate all node names and all access types. The data to complete this table should be gathered from the individual network profiles for each connecting site.

	Network Host Node A	**Node B**	**Node C**		
Network Host Node A	N/A	A to B – Shared Folder	A to C – FTP & OS Login		
Node B	B to A - Web & FTP	N/A	B to C – Database		
Node C	C to A – Web & FTP	C to B – No Access	N/A		

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 re-accreditation of the Network Security Plan if necessary. Re-accreditation 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.

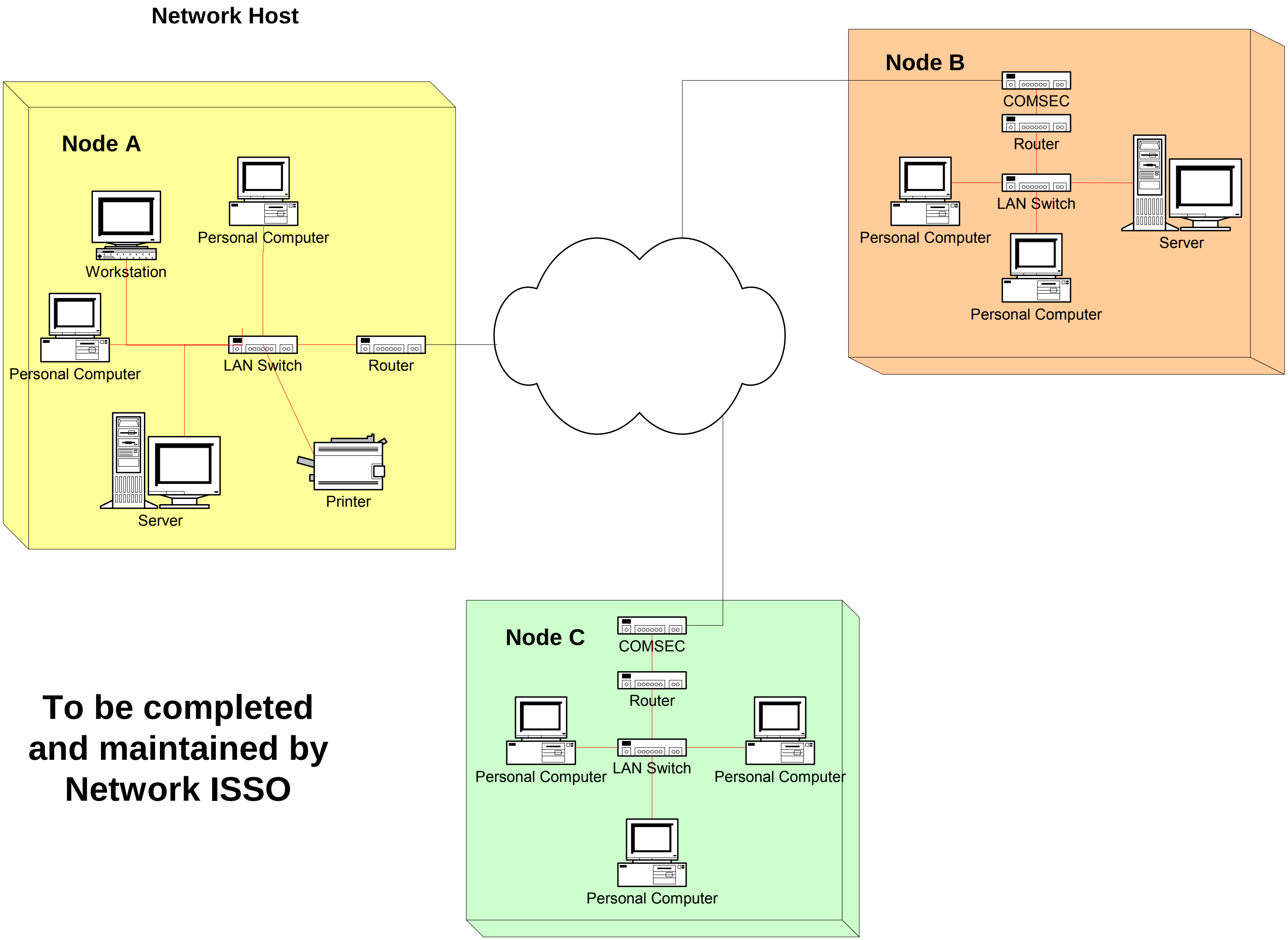
Data Transmission Records

1. All nodes of the classified network have a contractual relationship.
2. In accordance with DSS ISL 02L-1 dated April 22, 2001, each node will maintain a record in document control that identifies each facility to which they transmit or receive classified information via the classified network. The following information must be included in the record: facility CAGE code, contract number, contract expiration date and the highest classification level of information transmitted.
3. The above information is recorded once and updated upon change in contract status.
4. 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:



Network Host

To be completed and maintained by Network ISSO

Figure G-3 NSP Architecture Diagram Example

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

Date:	Facility Address:	CAGE Code :

IS Contact Information

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

Contracts Supported (Contract Numbers):

Describe role in supporting the above contract(s):

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

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

Specify all nodes accessing your node:

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

Description of local systems/network:

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

IS Protection, Sensitivity Level, and User Information

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

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 G-4 NSP IS Profile Form

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

Date:	Facility Address:	CAGE Code :

Contact Information & Description of Network Participation

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

Contracts Supported (Contract Numbers):

Describe role in supporting the above contract(s):

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

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

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

Description of local systems/network:

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

IS Protection, Sensitivity Level, and User Information

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

Date:	Facility Address:	CAGE Code :

Accredited Protection Level: PL1PL2PL3PL4
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:

Memorandum of Understanding (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) DODD 8500.1
(b) NISPOM, Chapter 8
(c) (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**).

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 Information**). 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) or applicable Department of Defense policy . 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. Additionally, the user agency will notify DSS in writing of cancellation of the MOU.

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.

Memorandum of Understanding

(Signature Sheet)

Network Identifier:	**Network Host Facility:**
Network Type: **Network PL:**	**MOU expiration date (if applicable):**

Network Host Signatory (Government or Contractor)

Network Host Site	**DAA for Network Host Site** **IS Accreditation Date:**	**Type**	**Node Identifier**
Facility Name: Facility Address: Network ISSO Name: Phone: Email: Signature:________________Date:_________	Name: Title: Phone: Address: Email: Signature: ________________Date: _________	☐ Government ☐ Contractor CAGE:	**Node PL:**

Government MOU Signatories

Interconnected Site	**DAA for Interconnected Site** **IS Accreditation Date:**	**Type**	**Node Identifier**
Facility Name: Facility Address: Network ISSO Name: Phone: Email: Signature:________________Date:_________	Name: Title: Phone: Address: Email: Signature: ________________Date: _________	☐ Government ☐ Contractor CAGE:	**Node PL:**

Note: Add as many signatures as you have DAAs

Figure G-5 MOU Form

Appendix H Protected Distribution Systems (PDS)

(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 must *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 the alarms for 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 1-206a of the NISPOM, DSS will conduct periodic on-site 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 and 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.

Appendix I Mobile Information Systems

Mobile System Processing

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 on-going 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 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 a Master Plan to process classified information at one location, and relocated to another location for classified or unclassified processing. The mobile system may be a complete system or components of a larger more complex system.

Types of Mobile Systems

There are three categories of mobile systems. Systems that are relocated within the facility under the same cage code, moved 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 email.
- 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 Interim Approval to Operate under unique circumstances and will require ODAA approval.

Notification to DSS

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

Procedures

The security plan and protection 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 security plan 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 protection profile. The protection 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 email 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 utilize the system.
- 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 gaining 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.
- Prior to relocation, the gaining ISSM must provide signed written acknowledgement that the gaining facility accepts and is capable of meeting the security requirements specified in the SSP.
- 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 DSS IS Accreditation Letter along with DSS Form Letter 16, Letter Acknowledging Relocation of IS By Government Activity/Site. See I-13 for Sample Letter.
- 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 while at that activity.
- Notification to the IS Rep must be made before the IS can be relocated.

NOTE: All letters 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, protection 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

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]** 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 valid signed User Briefing Statements will be allowed to operate the computer.

Figure I-1Authorized Alternate Site Locations

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

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. Hand carrying is only authorized in emergency situations.

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) Maintain 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) Establish a process so that media (paper and magnetic) is properly reviewed and labeled.
    e) Ensure that the Weekly Audit (review) is performed and annotated on the review record.
    f) Bring any discrepancies to the attention of the ISSO, alternate and Security
    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 I-2 Authorized Sites for Mobile Processing

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

System/Component Information

Page 1 of 2

[Facility Information]

System Identification

To relocate a system approved for Mobile Processing, this form must be completed and submitted by the Information System Security Manager (ISSM) the local DSS Industrial Security Representative (IS Rep) five workdays 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.	

If the relocation site is government facility, will the system be connected to the gaining facility's network? □ Yes □ No

Figure I-3 System Component Information Form

System/Component Information

[Facility Information]

Page 2 of 2

System Identification

Privileged User Information /Relocation Site ISSO

Users Identified Below have been Briefed/Trained and are Responsible for Conducting Weekly Audits and Antivirus Definition 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

Transportation Plan

For the Movement of Classified Information Systems (IS)

Facility
Address
City. State. Zip Code

Date of Transportation 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 System 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 System 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 Protection Profile. The ISSM shall notify the DSS Representative no later then five days 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

1. Program name
2. Classification
3. Will the shipment contain hazardous material? If so, provide MSDS Sheet or IHC letter from customer
4. Size and weight of equipment
5. 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. Courier briefings are given by the Classified Document Control Center (CDCC). 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 Contractor Site (Sample)

CONTRACTOR LETTERHEAD

(To be used when releasing IS to contractor or test site for over one week.)

(DATE)

FROM: (ISSM)

TO: (Name of contractor site ISSO and address)

SUBJECT: Relocation of DSS Accredited Information System (number) from (Company Name) to (Company Name).

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 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 contractor site) in order to process classified information for (Purpose). During the period when this will be resident at (Name of contractor 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 [where indicated below] 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 email at (email).

Sincerely,

(ISSM's Name)
(Title/Company)

Attachments: DSS Accreditation Letter
Dated (Date)

Copy to: (Cognizant DSS ISR)

CONCURRENCE:

____
(Name/Title of Authorized Official)

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 for over one week.)

(DATE)

FROM: (ISSM)

TO: (Name of government site ISSO and address)

SUBJECT: Relocation of DSS Accredited Information System (number) 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 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 [where indicated below] 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 email at (email).

Sincerely,

(ISSM's Name)
(Title/Company)

Attachments: DSS Accreditation Letter
Dated (Date)

Copy to: (Cognizant DSS ISR)

CONCURRENCE:

____
(Name/Title of Authorized Official)

Appendix J 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 may have additional documentation requirements in accordance with the MOU or Bilateral agreement between the countries involved. These documents must be reviewed to determine the documentation and approvals required before transmission of data can take place. The ODAA is concerned with two documents in this process; the System Certification and Accreditation (C&A) package and the Secure Communication Plan (SCP).

Certification and Accreditation Package

All System Security Plans 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 re-accreditation as an International Wide Area Network (WAN) because of the security relevant change (See "ODAA" below). For more information on the Certification and Accreditation Packages see Appendix D.

Secure Communications Plan (SCP):

Background

Requests to establish international secure communications links between US cleared contractors and foreign governments or foreign cleared defense contractors can originate from one of three sources. These sources are:

- The US cleared facility
- The foreign government
- A US 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 Office of the Designated Approving Authority (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 US 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 information system (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 approval to operate is received from the foreign government the ODAA will advise the US 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 a Secure Communications Plan 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 US systems are certified and accredited. If the connection involves establishment of secured networks among US contractors, ODAA will assure the appropriate Memorandum of Agreements (MOAs) are executed.
6. See "ODAA" below.

Requests by US program office

1. When IPB receives a request from a US program office to facilitate a secure connection involving a US cleared facility, IPB will confirm that the Program Security Instruction (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 US systems are certified and accredited. If the connection involves establishment of secured links to the program office and or US contractors, ODAA will assure the appropriate MOAs 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 System Security Plan (whether it is under an IATO or an ATO) for re-accreditation 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 US. The ODAA will then store the approved Secure Communications Plan and the approval documentation on the "I" drive under the International folder (I:\ODAA\Non-SSP files\International). Each Secure Communications Plan should have its own unique Identifier and it's own folder that contains all correspondence relating to the SCP, as well as the ODAA Unique Identifier of each SSP that is a party to the SCP. SSPs with international connections should have the address of the SCPs location in the SSP folder for on the DSS Internal "I" drive.

Appendix K Processing of Special Access Program Information

(Will be included in a future revision)

Appendix L Tactical, Embedded, Data-Acquisition, and Special-Purpose Systems

A. (NISPOM 8-504) The requirements of Chapter 8 are written in regards to the general-purpose or office automation system and personal computers. It would be almost impossible to include security requirements for components such as weapons or tactical systems, test stands, simulators, or embedded components (NISPOM Paragraph 8-504) that often are integral elements of a larger IS. To apply the general requirements of Chapter 8 in these instances may result in unnecessary costs and adversely impact operations. 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. 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 (Article #40, ISL 2007-01).

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.

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.

Appendix M Defense Information Systems Network (DISN) Connections

SIPRNET Plan Review and Accreditation Process

The objective of this section is to establish a consistent process to support the unique certification and accreditation requirements of SIPRNet systems.

Process Flow

The Government Sponsor must submit a request for SIPRNet to Joint Staff (J6) on behalf of the contractor. Once the request is validated, Joint Staff (J6) will forward the approval letter to the DSS Program Manager (DSS PM), the Defense Information Systems Agency (DISA) and Sponsor. The J6 validation is good for the life of the program.

DISA then assigns the request a Control Number (CXXXXXX) which it sends to the DSS PM. The DSS PM will forward a prepackaged notification memorandums and SIPRNet connection approval documents for dissemination to the contractor.

The ISSM for the requesting facility must complete the documentation and send it to the IS Rep who will review and make any needed modifications. If changes must be made by the IS Rep, a copy of the modified documentation will be sent to the ISSM.

The IS Rep and ISSP provide guidance to the ISSM to prepare the system/site for accreditation. Additionally, IS Rep and ISSP will communicate to the ISSM that the following documentation must be submitted as part of their SIPRNet request package:

- SSP + protection profile
- M Network Topology Diagram
- Consent to Monitor memorandum completed with Contractor Signature
- SIPRNet Connection Questionnaire (SCQ) completed with site/system information. Form will eventually be signed by the DAA
- Statement of Residual Risk completed with Contractor signature
- Joint Staff validation letter.

The IS Rep and ISSP will conduct a comprehensive review of the SSP and required connection approval documents. When ready, the IS Rep and ISSP will conduct an onsite validation. When a favorable validation has been conducted, the IS Rep will forward the recommendation to accredit to the RDAA. The RDAA is required to sign both the ATO letter and the SCQ.

The contractor emails/mails the completed Connection Package to DISA (includes SSP, DSS DAA accreditation letter, Statement of Residual Risk with ISSM signature, Letter of Consent with ISSM signature, System Connectivity Diagram and SIPRNet Connection Questionnaire with DSS DAA signature).

DISA sends an email acknowledgement of receipt to the contractor. DISA reviews the Connection Package and if correct issues IATC. If not correct DISA will correspond with the contractor to resolve issues. DISA will email the IATC to the contractor and DSS PM. DISA will then run the vulnerability test (time period undetermined). When the system passes the vulnerability test, DISA will then issue an ATC and email it to the contractor. The contractor will email a copy of the ATC to the IS Rep.

Open Email and Domain Name (DNS) Registration

Government sponsors are required to provide these services to the contractor.

Disclosure Form

Contractors are NOT allowed unfiltered access to the SIPRNet. The government sponsor determines access requirements. The Joint Staff letter must identify access requirements (i.e., websites and ports and protocols.)

- Sponsor sends disclosure form received from DSS PM to sites that contractors need access to
- Site agrees, signs the form and submits it back to the Sponsor
- Sponsor sends form to DISA SMC smc-ctr@disa.mil
- DISA SMC builds/updates contractor filter.

Re-Accreditation

When authorization expires the system is no longer legal and must be disconnected (looped-away). Follow the steps below to extend connectivity. Be advised to update packages with current information (dates, POC, system changes, etc).

- If the contract expires then **sponsor action is required.** The sponsor must submit an extension letter to the contractor. The contractor must submit the extension letter to the IS Rep who will forward a copy to the DSS PM.

- If accreditation expires then the **contractor** must obtain a new accreditation letter from the RDAA and submit it to DISA.

With re-accreditations, the ISSP may submit an accreditation recommendation to the RDAA in the absence of an encryption device and an installed circuit. DISA is allowing current contractor connections to SIPRNet up for re-validation to connect to SIPRNet on a limited ATO. This is to permit them the time needed to acquire and install an approved firewall and IDS. This temporary

ATO does not apply to new SIPRNet connection requests, for which the workstations, firewall and Intrusion Detection System (IDS) must be in place at the time of certification.

Points of Contact

Defense Security Service:
Email disn@dss.mil
Address: Defense Security Service
1340 Braddock Place
Alexandria, VA 22314

DISA SIPRNET Connection Approval Office:
Email: scao@ncr.disa.mil
Address: Defense Information Systems Agency
ATTN: GS213/SCAO
P.O. Box 4502
Arlington, VA 22204-4502

Joint Staff:
Email: joyce.bernard@js.pentagon.mil

Disclosure Authorization Office:
Email: smc-cntr@disa.mil

Appendix N Trusted Download Procedures

Background

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 Protection Level (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.

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 System Security Plan (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

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

1. 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).

2. Acknowledgement 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.

3. 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 SSP.

4. 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.

5. 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).

6. 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.

7. 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.

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 acknowledgement of risk from the government customer, but only after a comprehensive review:

Table N-1 DSS Authorized File 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.

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 acknowledge 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 System Security Plan must include a description of how and why the contractor has deviated from the standard, and a risk acceptance statement by the GCA.

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).

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, 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.

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, 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 N-1 Trusted Download Authorization

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 N-2 Trusted Download Record

Date	Person	File Type	File Description

Risk Acknowledgement Letter

[Contractor Name]
[Address]

SUBJECT: Acknowledgement of Risk to Classified Information

TO: *[GCA/Data Owner]*

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 acknowledged 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.

____
Contractor Signature (Information System Security Manager)

______________________________ ( ) -
Printed Name Phone #

Attachment: Alternate Procedure

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 acknowledge the Alternate Procedures falls well within the governments standards for acceptable risk.

____
Customer/sponsor or data owner Signature

______________________________ ( ) -
Printed Name Phone #

Appendix O Clearing/Sanitization

Clearing and Sanitization will be done according to the DSS Clearing and Sanitization Matrix at the end of this appendix. An explanation of clearing, sanitization and overwriting is below.

Clearing

NISPOM 8-301a 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, and before maintenance personnel who have been authorized to have access to classified information are present (NISPOM Paragraph 8-304b(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.

Sanitizing

NISPOM 8-301b refers to a procedure by which the classified information is completely removed and even a laboratory attack using known techniques or analysis will not recover any information. Sanitizing of memory and media is required if a system is being "released" to users with access level lower than the accreditation level.

Overwriting

This section refers to sanitization procedures not associated with fixed/rigid media to render such media unclassified. This section pertains to methods to use such media at lower classifications.

Contractors cannot be expected to destroy TOP SECRET media at the end of a downgrading action. Therefore, when the media is downgraded for other use, the contractor must develop an alternative procedure, such as a three-time overwrite, for the media. The passes that are developed must be a character, its complement, and then a third pass with random characters. The ISSP will verify this is done with an approved overwrite utility. This process will only be utilized as a clearing action and the media must be safeguarded at the TOP SECRET level. When the media is no longer needed, it must be destroyed.

An authorized DoD laboratory must evaluate overwrite utilities for proper functionality. More information about DoD authorized testing laboratories can be found at the NIAP Common Criteria Evaluation and Validation page at http://www.niap-ccevs.org/cc-scheme/. ISSPs will not evaluate any media overwrite products. NSA has written a protection profile that must be utilized as the standard. Vendors with proposed overwrite products may submit their products to one of these laboratories for evaluation. Only overwrite utilities listed on the NIAP Validated Products List (VPL) may be used. The VPL can be found at http://www.niap-ccevs.org/cc-scheme/vpl/. Refer to the DSS Clearing and Sanitization Matrix.

The contractor requests use of an overwrite utility by submitting an SSP with the overwrite utility identified as its method of clearing/sanitizing media and/or equipment.

Vulnerabilities for overwrite utilities focus on two key areas:

1. understanding “all addressable locations” and

2. identifying “bad blocks” or areas on the disk that are either questionable or that fail during use.

Many media manufacturers reserve special areas on the disk for maintenance and diagnostics. System software is generally unable to access these areas. The utility is required to verify that every location contains the last character written by the overwrite program or the contractor will verify manually using disk editing software such as Norton’s Disk Editor.

Media is delivered from the manufacturer with some surface areas that are identified by the system software as being questionable or bad (i.e., bad blocks). The system software marks these areas as unusable and will not write any information to them. However, throughout the IS classified life cycle, areas that contain classified information might go bad, be marked as unusable, and remain in the marked area. This vulnerability has been exploited in the past. Therefore, DoD will not authorize overwriting for the sanitizing of media without first knowing the number and contents of these bad blocks. This is the one area in which contractor-written utility programs often fail.

A good overwrite program will notify the user when bad blocks are discovered, give the user the option of verifying and changing the contents of the bad block(s) (unless completely unusable), and record the location and contents for further investigation and analysis. Other utilities overwrite the media without attempting to change the contents of these bad blocks. Some utilities attempt an overwrite, but continue if the content remains unchanged. If a contractor uses a utility that does not change or identify bad blocks, the media must be “mapped” before the IS is used to process classified information, and again when the media is sanitized. If a comparison of the first and most recent mapping shows additional bad blocks, the evaluator must determine whether the media can be declassified or destroyed based on the level of classification of the media (i.e., S or C), the number of bad blocks identified, and an understanding from the ISSM as to whether the media is to remain within the contractor facility for other classified or unclassified use or released outside the facility.

Non-volatile Memory Verification

While the ISSP does not evaluate media overwrite products, the ISSP must validate non-volatile memory (Battery Backed RAM, Flash, EEPROM,) clearance or sanitization procedures that the contractor develops or proposes to use to sanitize a system. Any user accessible or addressable memory such as Flash BIOS, must be either locked and password protected or sanitized. Memory functioning as scratch-pad memory must be sanitized. The ISSP will utilize the following procedures to validate a clearance or sanitization procedure for non-volatile memory:

- Define the size and type of memory to be sanitized.
- Use the Clearing and Sanitization matrix on the DSS Web site for guidance.
- Document the procedure in the SSP. This can include a copy of a statement or certificate of volatility, the manufacturer’s specifications or a copy of the source code. If you do not

read the programming language in which the source code is written, ask the writer of the code or someone familiar with it to go through it with you line by line. If possible, the company should also keep a copy of all documentation in their copy of the SSP.

- The ISSP must witness the running of the procedure. If possible, have the technician randomly view the contents of portions of the memory to verify that the program wrote what the source code said it wrote.
- Once the validation is performed and is successful, if the process is one that will be helpful to other ISSPs dealing with similar equipment, the validating ISSP will send a copy of the procedures to the ODAA.

Magnetic Tape

Magnetic tape can be cleared using a Type I, II, or III approved tape degausser. Reference Matrix C10.5. 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 NSA's Information Systems Security Products and Services Catalog. In addition NSA regularly posts on its web site (http://www.nsa.gov/ia/government/index.cfm) an updated Evaluated Product Listings (EPL) of equipment that securely erase the most common types of storage devices that retain classified or sensitive data.

Note: The terms "Type I-III" are being replaced by the actual media coercivity rating.

If a degausser was used that was not listed on the NSA EPL, 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 O-1 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 or SECRET FGI 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 TS must be retained for two years.

Contractor Destruction Options

With the ever increasing use of computers, the destruction of classified hard drives that are no longer needed is becoming a real issue. NSA has discontinued accepting classified hard drives unless they were Government Furnished Equipment and the appropriate GCA official signs a request for NSA to handle the destruction. Most GCA client organizations do not want to accept old hard drives for destruction either.

There are 3 options available to industry for the destruction of classified hard drives:

1. Return to customer - Unless specifically prohibited from doing so in their contract, industry 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) the contractor 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. They must then fill out a Contractor's Approval Form (this is provided by NSA) and follow the instructions given to them by the destruction engineers at NSA

3. Destroy it themselves – If the contractor does not meet the criteria of option 1 or 2, they must destroy the materials themselves. The Contract Manager should call the NSA Media Destruction Customer Service Center at (301) 688-6672. Here the contractor can get information on approved media destruction equipment or information on approved destruction sites.

(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 on the classification sensitivity of the information and the type (size, capacity and connectivity) of the media. Wiping can be used, however drives that have been wiped must be tracked by serial number and must be degaussed or destroyed before being released outside of the company.

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 IT resources, and mitigate the risk of unauthorized disclosure of information.

Only overwrite utilities listed on the NIAP Validated Products List (VPL) may be used. The VPL can be found at http://niap.bahialab.com/cc-scheme/vpl/. Any time a wiping operation results in bad sectors that could not be overwritten the drive must be degaussed or destroyed.

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, e.g. EEPROM sanitization: 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, e.g., Laser Printer sanitization**:** **n** must be performed, then **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. Overwrite all addressable locations with a character, its complement, then a random character utilizing an approved overwrite utility.
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:

A. 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 should be reflected in the System Security Plan and reviewed/approved in connection with the information system certification and accreditation process. The following summary information is provided for contractor facilities in updating system security procedures for destruction of classified media:

- Incineration 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. Contractors 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 of the CSA is required.

- Smelting, disintegrating, or pulverizing hard disks or drums at an approved metal destruction facility. Prior approval of 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 CSA approval 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.

B. The National Security Agency (NSA) Classified Material Conversion (CMC) destruction facility may be utilized by qualified and registered contractors. NSA CMC will accept all COMSEC hardware and materials (regardless of ownership), classified Government Furnished Equipment (GFE) (including media), and Special Access Program (SAP) information from contractor facilities, 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.

Appendix P Voice Over IP/Video Teleconferencing (VOIP/VTC)

(Will be included in a future revision)

Appendix Q Masking/Coding/Disassociation

(Will be included in a future revision)

Appendix R   Metrics

(Will be included in a future revision)

Appendix S Annual Reviews

Information System (IS) Inspection / Security Review Checklist

1. Check for system accreditation.

   a. Check date and environment specified in accreditation letters.

   b. Check the SSP and compare to the actual system:

      1. Accurate system description.
      2. Certification checklist signed by ISSM.
      3. Responsible officials designated by profile.
      4. Applicable supporting documentation; NSP, MOU, MOA, waiver letters by user agency.
      5. Check system diagram for completeness and accuracy.
      6. Check the software baseline, hardware baseline and maintenance log(s) for accuracy.
      7. Check the trusted download procedure(s) are accurate (if applicable). Have the user demonstrate he/she is able to perform them correctly.
      8. Check the user briefing form is signed, and includes:
         a. Duties.
         b. Responsibilities.
         c. Clearance level.
         d. Need-to-Know.
         e. COMSEC/RD/FRD/NATO.
      9. Check for proof of annual user training.
      10. Check for the correct ODAA UID.
      11. Check SSP has applicable security policies:
         a. Password requirements.
         b. Audit requirements and resolution(s).
         c. ISSM/ISSO roles and responsibilities.
         d. Promulgation to appropriate personnel.
         e. Log on/log off procedures.
      12. Check system protection level and classification.
      13. Check for effective configuration management.
      14. Check the DSS Form 147 for accuracy.
      15. Check procedures in the SSP for ensuring the system has current version of the antivirus executable, and the latest signature file.
      16. Check listed procedures for patch management.
      17. Check if there is supposed to be a dedicated copy of the operating system, properly marked.

2. Check for unaccredited operation. If the DD254 has expired, coordinate with the IS Rep.

3. If self-certified, was DSS properly notified?

4. Is SSP readily available to all users by physically locating it at the AIS?

5. Check marking and labeling for:
   a. Media.
   b. Hardware.
   c. Seals (if applicable).

6. Check the audit reviews:
   a. Weekly.
   b. One year retention.

7. Have a competent individual demonstrate start up/shut down and proper disconnect procedures.

8. Verify maintenance procedures:
   a. Proper personnel, U.S. citizen.
   b. Cleared vs. un-cleared (escorted by knowledgeable individual).

10. Interview all appropriate personnel.

Appendix T Foreign Ownership, Control & Influence (FOCI)

Foreign Ownership and Control (FOCI) Information Systems Assistance

The NISPOM establishes policy concerning the initial or continued eligibility for access to classified information by U.S. companies with foreign ownership, control or influence; 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 a contractor is owned, controlled or influenced by foreign interests. If FOCI is present, DSS must evaluate the associated risks and the FOCI mitigation or negation 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 FOCI. The FOCI Branch is ultimately responsible for approving the contractor's Plan of Action for mitigating the FOCI 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 ISR. 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 Information System
    - 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 email servers. If a shared email server exists, a procedure should be in place to mitigate the risk of inadvertently sending email 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 the International Section of the ODAA Process Guide for information pertaining to Classified Information Systems with Foreign Interest.

Appendix U Spills

CLASSIFIED SPILLS and MEDIA DISPOSITION

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. The following procedures are aligned with DoD and DoD component procedures.

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.

All cleared facilities will have a plan in-place for dealing with classified spills, whether the facility has accredited systems or not. Spills will be cleaned up according to this plan. A DSS-approved plan is included below. Modification of the DSS-approved plan or use of any other plan requires ISSP approval. The approval must be in writing and kept with the plan. The current DSS Clearing and Sanitization Matrix is in Appendix O or can be downloaded from the DSS web site.

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.

Media Disposition

Hard drives that were used in a classified environment or involved in a classified spill can be wiped according to the current DSS Clearing and Sanitization Matrix from Appendix O. The drives will be logged and tracked by their serial number. The drives will remain under company control until the end of their usefulness and then degaussed or destroyed. Before systems are released from company control hard drives will be checked against the log and disposed of accordingly. The log will be checked during DSS facility reviews. Failure to account for any hard drives that were used in a classified environment or involved in a classified spill will require an Administrative Inquiry. This applies to leased drives and drives requiring repair.

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 along with the required additional administrative controls 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.

DSS-Approved Classified Spill Cleanup Plan

General

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

Classification Level: These procedures are intended for use on contaminations involving information at or below the TOP SECRET collateral level. Procedures for contaminations involving special access information (SCI/SAP/SAR) should include any special requirements dictated by the customer (DAA).

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 emails. 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).

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 email 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.

- 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.

The local Facility Security Officer (FSO) will conduct the investigation, coordinate the cleanup actions with the ISSM or designated on-site representative and will provide a written report to the DSS as soon as practical following the cleanup action.

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.

Contamination Cleanup Procedures

Reporting and 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. STU III secure communications are recommended.

Lead FSO: The local FSO for the facility where the contamination is first reported leads the effort. The FSO will coordinate immediately plan the investigation/cleanup considering detailed information such as sender, recipient(s), subject, time sent, day sent, systems and peripherals potentially affected, etc.

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 U-1 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 U-2 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: That they are to cease all email activities until further notice. b: Under NO circumstances should the contaminated email be deleted. The original email (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 email has traveled, and ascertain if it is necessary to cleanse more than a single Exchange Server. If it is discovered that the contaminated email has left the company email System, and/or crossed an internet boundary, additional cleansing of all recipient email systems may be required. The ISSM should be notified immediately if Message Tracking indicates a contaminated email has left the company network.	
□	B3	Determine if the contaminated e-mail was contained within the 'Domain of Responsibility' (your system). Was the e-mail message released outside of the 'Domain of Responsibility' (your System) (Y/N)? _____________. If 'Yes' proceed to step B5, If 'No' proceed to step B4	
□	B4	If e-mail message has been released outside of the 'Domain of Responsibility' (your system), notify ISSM. Continue with step B5.	
□	B5	Disable all affected User's Exchange mailbox access. 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'.	

Check Box	Step ID	Step Description	Step Owner
□	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 email has traveled so that all compromised Exchange servers can be targeted for cleansing. b: Determine all recipients of the contaminated email so that each contaminated Mail Box can be cleansed. c: Determined if ISSM must be notified in the event the email has contaminated an email 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 email system may be contaminated, ISSM must be informed immediately. If 'No' to B6, perform Step B9.	
□	B7	Add these additional Users to the 'Client Cleansing Process' list.	
□	B8	Dispatch a team to secure these Client Workstations within an approved, Classified storage location. Include these Client machines on the list for Client Cleansing. Name(s) of individuals assigned to secure these machines: ____ ____	
□	B9	Open the individual's mailbox with an Exchange Administrator account. Delete the message from the Inbox and/or Sent Items.	
□	B10	Empty the deleted items folder.	
□	B11	Go to Deleted Item Recovery and delete the message again.	
□	B12	Identify if the User saves and/or backs up e-mail messages to other locations. **Archives:** Location of *.pst and/or *.ost files – local or server. **Back-ups:** Local hard drive, network drive, zip drive, floppy drive.	

Check Box	Step ID	Step Description	Step Owner
□	B13	As necessary, perform the following activities: External Media: Identify, secure, and lock-up all external media (floppy and zip). Local Drive Storage: Ensure that the Desktop Client machine has been identified for 'Client Cleansing'. Network Storage: Ensure that affected server(s) has been included for server cleansing sub-process(s) (GroupWise and/or Exchange). Provide comments that clarify the actions taken at this step. ____ ____ ____ Continue with Step B12.	
□	B14	Confirm that "Database Zeroing" is enabled on the Exchange Server you are cleansing. (This setting is/should be enabled for all Exchange Servers). To verify "Database Zeroing" has been enabled: 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.	

Check Box	Step ID	Step Description	Step Owner
□	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 Database Zeroing are as follows: a: Start Zeroing = MS Event ID# 706,712 b: Finished Zeroing = MS Event ID# 707,713 Save the Application entire application log from the MS Event Viewer and note the times in which Database Zeroing Started and Stopped. This log will be submitted to the FSO as proof that the Exchange Server has been sanitized.	
□	B17	Re-activate each User's Mailbox on the server. 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 U-3 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.	
□	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	

Check Box	Step ID	Step Description	Step Owner
□	C7	Add these additional Users to the ‘Client Cleansing Process’ list.	
□	C8	Dispatch a team to secure these Client Workstations within an approved, Classified storage location. Include these Client machines on the list for Client Cleansing. Name(s) of individuals assigned to secure these machines: ____ ____	
□	C9	Identify if the User saves and/or backs up e-mail messages to other locations. **Archives:** GroupWise archiving schema – local or server. **Back-ups:** Local hard drive, network drive, zip drive, floppy drive.	
□	C10	As necessary, perform the following activities: External Media: Identify, secure, and lock-up all external media (floppy and zip). Local Drive Storage: Ensure that the Desktop Client machine has been identified for ‘Client Cleansing’. Network Storage: Ensure that affected server(s) has been included for server cleansing sub-process(s) (GroupWise and/or Exchange). Provide comments that clarify the actions taken at this step. ____ ____ ____ Continue with Step C11.	

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.	

Check Box	Step ID	Step Description	Step Owner
□	C13	Re-activate each Users Mail Account on the GroupWise server.	
□	C14	Verify that each Users Mail Account is working.	
□	C15	Inform each User that their GroupWise Mail account has been cleansed.	
□	C16	Complete and verify GroupWise server Cleansing Checklist.	

GroupWise Server Cleansing Completion Date: ________________________________.

Signature of Verification:

Print Name: ____.

Signature: ____.

Figure U-4 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 U-5 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. On Windows systems delete the file from the Recycle Bin.	
□	D6	Clean the Users Outlook archive file(s) (*.pst and *.ost). Delete the Recycle 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 FSO approval return the Client Desktop machine to its appropriate working location.	

Desktop Client Cleansing Completion Date: ________________________________.

Signature of Verification:

Print Name: ____.

Signature: ____.