System Security Plan (SSP) Preparation

- Gather all required information—

  What program plans to utilize the system?
  What is the level of the information?
  Where does the program want it to be utilized?
  What hardware & software is involved?
  What types of memory does is involved?
  What physical security must be in place?
  How many people will utilize at the same time?
  What Protection Level (PL1, PL2, etc.)?
Protection Levels

• NISPOM Para 8-402:

• PL 1: All users have PCL, NTK, Formal Access Approvals for all information on system.

• PL 2: All users have PCL and Formal Access Approvals for all information on systems, but at least one user lacks NTK.

• Periods processing (8-502) avoids PL 2.
System Security Plan (SSP) Preparation

• Determine whether to write SSP or MSSP

• SSP – Individual, unique system

• Master SSP (MSSP):
  • Most commonly used
  • Allows self-certification for similar systems
Master SSP

• MSSP in two sections:
  • MSSP:
    Boilerplate
    Operating System
    Technical Configuration Information
    Other general information
  • Profile:
    HW & SW Baselines
    Diagram
    Manual logs
    Trusted Downloading
    ISSM System Certification Test Checklist
System Security Plan (SSP) Preparation

- Choose appropriate DSS template:
  - Single-User Non-networked (SUSA)
  - Multi-User Non-networked (MSSP MUSA)
  - Peer to Peer LAN (MSSP P to P)
  - Domain Controlled LAN (Network)
Let’s review documents

• Multi-user Standalone MSSP
• Multi-user Standalone IS Profile
• Multi-user Standalone IS Security Package Submission and Certification Statement
Steps to Prepare for Submission

• Prepare appropriate SSP or MSSP template

• Certify the system as being properly configured

• Prepare other certification documentation

• Convert Word documents into .pdf

• Prepare email to ODAA
Certifying the System

- Be very thorough
- Double-check your work
- Ensure you perform a complete system review
- Be truthful
- You are signing:

By signing below I certify that the information provided in the attached security package is true and correct. I also understand that my submission of this letter and the attached security package constitutes a statement on a matter within the jurisdiction of the Executive Branch of the United States. I understand that the United States Criminal Code (Title 18, section 1001) provides that making willful false official statements or concealing a material fact in this information system security package is a felony which may be punished by fine or imprisonment or both.
Gentlemen:

Attached please find Southern-OWEC9-20081217-00015-MSSP-REV 1.0 & Southern-OWEC9-20081217-00015(MSSP-REV 1.0. This is the first of two SSP’s for identical ruggedized laptops.

There is an urgent need for approval of this system. It will be utilized by active duty personnel in theater to reload software on the fly for a black box incorporated into the F-16 aircraft called the Commercial Central Interface Unit (CCIU) which is classified Confidential. Presently the unit must be returned to our facility for reloading. Use of this unit will save the aircraft a lot of down time.

ERW plans to meet with Hill AFB, UT personnel at Fort Worth’s Joint Reserve Base the end of January to demo use of this box with hopes of selling it off to the customer on the spot.

We would appreciate your prompt attention and will try not to make this a regular practice.

Carolyn R. Shugart
Information Systems Security Manager
Eldi Systems of America Fort Worth Operations
4700 Marine Creek Parkway
Fort Worth, TX 76136-9969
Carolyn.Shugart@eldisystems-us.com
(Desk) 817-231-4478
(Cell) 817-217-5112
Accreditation Documentation

• Interim Approval to Operate (IATO)
  • Once received you may begin processing
  • Does not involve DSS onsite review
  • Valid for 180 Days
  • YOUR RESPONSIBILITY to track expiration
  • Remind DSS 60 days from expiration
  • DO NOT PROCESS if expired
  • No self-certification allowed under IATO
Accreditation Documentation

• Approval to Operate (ATO)
  • This is your final approval
  • DSS performs onsite prior to granting
  • Valid for three years
  • YOUR RESPONSIBILITY to track expiration
  • For MSSP, automatically grants self-certification except under certain circumstances.
Guidelines for MSSP’s and Self Certification

• 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 granted automatically in ATO unless ISSP/C&A Reviewer specifically requests it not be granted with specific justification that the ISSM not technically competent, no adequate experience or violated trust in the past.
Self-Certification

• Self-certification is only authorized for systems fully compliant and meet all NISPOM requirements. No waiverable items can be self-certified.

• An ISSM authorized to self-certify Peer to Peer can self-certify MUSA workstations under separate MSSP.

• An ISSM authorized to self-certify IS under an MSSP for multi-user systems workstations cannot self-certify single-user workstations.
Systems under one MSSP must be

- Same Protection Level: PL 1 or PL 2
- Same type of system: SUSA, MUSA, P to P, Domain Controlled Network
- Same Confidentiality – TS/Secret/Confidential
- Similar Physical Security – Closed Area/Restricted Area
- Similar Operations -- Trusted Downloads, Periods Processing, Mobile Systems
Self-Certification

• See Appendix F, ODAA Manual, for information on self-certification.