Self Inspections

Self Inspection Handbook for NISP Contractors

November 2008
Self Inspection Checklist

• Topics Covered
  A. Facility Clearance
  B. Access Authorizations
  C. Security Education
  D. Consultants
  E. Standard Practice Procedures (SPP)
  F. Subcontractors
  G. Visit Control
  H. Classified Meeting
  I. Classification
  J. Employee Identification
  K. Foreign Ownership, Control, or Influence
  L. Public Release
  M. Classified Storage
  N. Controlled Access Areas
  O. Markings
  P. Transmission
  Q. Classified Material Controls
  R. Reproduction
  S. Disposition
  T. Information Systems
  U. COMSEC / Crypto
  V. International Operations
  W. OPSEC
  X. Special Access Programs
Overview - What is a Self-Inspection

- Understand what the self-inspection means.
- NISP Self-Inspection Handbook
- Identify NISP checklist – Example: Section “T” Information Systems
- Identify NISPOM references – example: Chapter 8 (Information Systems)
- Reference the NISPOM paragraphs i.e.: (8-602 are all protection requirements for the audit requirements recorded)?
- Be able to explain how your facility reinforces the NISPOM.

- **READ** and **THINK** about the question.
  - *What is the question asking?*
IS Self Inspection Requirements

• 1-206 Security Reviews
  – Contractor Reviews. Contractors shall review their security system on a continuing basis and shall also conduct a formal self-inspection at intervals consistent with risk management principles.

• 8-103. IS Security Manager (ISSM). The ISSM:
  – Ensures that periodic self-inspections of the facility's IS Program are conducted as part of the overall facility self-inspection program and that corrective action is taken for all identified findings and vulnerabilities. Self-inspections are to ensure that the IS is operating as accredited and that accreditation conditions have not changed.

• Are Self Inspections enough?
  – “No”

• Enhancements / DSS matrix?
  – Multiples Reviews – more than one per year.
Section “T” of the NISP

- **Summary of sub – Categories**
  - Administrative
  - Responsibilities
  - System Security Plan (SSP)
  - User Requirement
  - IS Hardware
  - Physical Security
  - Software
  - Media
  - Security Audits
  - Security Awareness
  - IS Operations
  - Maintenance and Repair
  - Media Cleaning, Sanitization and Destruction
  - STU III (Out date should be applied to STE)
  - Networks – Network Security Plan (NSP)
Sub - Categories

- Administrative – Approvals and Accreditation
- Responsibilities – IS Security Policy
- System Security Plan (SSP) – Security Plans (Master & Profile)
- User Requirement – Clearances
- IS Hardware – Baseline Configuration
- Physical Security – Area Requirements Close / Restricted
- Software – Safeguarding Software / Employees and Contractors
- Media – Marking, Safeguarding
Sub - Categories Continue

- Security Audits – Records of audits or procedures
- Security Awareness – Training
- IS Operations – Show or demonstrate a understand of the system function
- Maintenance and Repair – Process for repair of IS
- Media Cleaning, Sanitization and Destruction – Procedures for reusing or destruction of media.
- STU III - (Outdated should be applied to STE phones)
- Networks – Network Security Plan (NSP)
Question to understand?

- Question to keep in mind when doing a Self–Inspection.

1. Who is the question directed toward?
2. What is the question asking?
3. When do I seek additional help?
4. Where should I look for a clear understand of the question?
5. How should I address the question?
6. Why are the questions important to understand?
• Documentation

  – 2009 Baseline Standard
  – Customer requirements – Contractual items outlined in a DD254 or other documentation
  – Security Classification Guide

• DSS and Industry are working on an updated version of the NISPOM, ISFO and the Baseline.
Items to Review

- **Security Relevant Software** – Any software or media that may have an impact on the functionality of the system.
  - Operating System – Windows, Linux, UNIX, Mac, & etc…
  - Anti-Virus software
  - Auditing Tools
  - Monitoring Tools
  - Scripts

- **Information System Protection Level.**
  - \( PL-1, PL-2, PL-3 \) or \( PL-4 \)

- **Approval / Appointment letters**
  - ODAA, Customers, Facility Security Manager
Items to Review Continue

- **Purpose of IS function.**
  - Software Development
  - Hardware Development
  - Testing
  - Integration
  - Simulation

- **What is the classification of IS**
  - Unclassified, Confidential, Secret, Top Secret

- **Paperwork / Proposal**
  - DD254, DD147,
  - Contract related, DD147, RFP, RFI, IDIQ, RFQ, ENs and FPR
  - ODAA Letters (IATO, ATO, Withdraw, De-certification)
Items to Review Continue

- Review each MSSP and Profile
- Verify your approval letters for certification
- Check the BIOS setting
  - BIOS password
  - Boot order (Hard drive)
  - Floppy, CD, Network - disable each drive or media from booting.
  - Bluetooth connection on laptops – Disable

Baseline – Verify the Security setting.
  - Auditing
  - File Permissions
  - Password
  - Services
  - User account (General or privileged)
Items to Review Continue

- **Hardware Baseline**
  - Hardware is outlined in the Baseline or Maintenance Log
  - System Make and model
  - Serial Numbers

- **Software Baseline**
  - Security Relevant Software is outlined in the Baseline or Maintenance Log
  - Software Vendor
  - Name of Software
  - Version Number
Items to Review Continue

- Anti-virus definitions updated.
- Upgrade / Downgrade procedures.
- Maintenance Log
- ISSO Checklist
- Visitor Logs
- Audit Trails
- Other Systems Logs
- User Briefing - User must sign one for each Program and must be signed annually.
- Validate users need to access the IS.
Additional Items to Review

• Restricted / Closed Area
  – Should verify with the Physical Security; that the following is in place and correct. Validate that your SPP is updated with the facility’s approval paperwork.

• DD147
• Construction of Area.
• Alarms
• IDS
• Guards
• Access List Updated
• UL Cert Updated
• Open and Close Procedures
• Emergency Procedures - Closed Area
Wrap up

- Always double check your self-inspection review.
- Have others review your work.
- Have team meeting to ensure that nothing is overlooked.
- Keep your Managers in the loop of any findings or corrective actions.
- Correct any issues that DSS noted from the prevised DSS inspection.
- Have general and privilege user briefing on any changes to policies and procedures associated with the IS.
- Every finding should have an action plan to be fixed or mitigated by the company.
- Answer all questions honestly and truthfully to get the best results in your self-inspection and the DSS inspections.

“Remember, you are performing a security review of your company and of yourself. The self inspections will aid you in understand what needs to be corrected and what does not. The information that you obtain will provide valuable information that you otherwise may not have known. Team up with other in your field and do not leave anything overlooked”.
Questions?

When in doubt always ask for help!!!