Hiring and Training an ISSO

Pete Hutton
ISSM for D.O.D, S.A.P, and Enterprise Campaigns
Raytheon IIS, Garland Texas
ISSO Defined by the NISPOM

The ISSM will determine the responsibilities to be assigned to the ISSO that may include the following:

– Ensure the implementation of security measures, in accordance with facility procedures
– Identify and document any unique threats
– If a unique local threat exists, perform a risk assessment to determine if additional countermeasures beyond those identified in the NISPOM are required
– Implement a certification test as required by the ISSM
– Prepare, maintain, and implement an SSP that accurately reflects the installation and security provisions
– Notify the ISSM when an IS no longer processes classified information, or when changes occur that might affect accreditation
Where Do Your ISSOs Come From Today

- ISSOs that support classified government systems in the world today are primarily System Administrators or System Engineers that move into the Information Assurance Profession
- ISSOs can also be found as college new hires from the many available Information Assurance programs at universities today
- Military veterans with operational and or system administration computer experience are good candidates for these positions as well
ISSO’s Responsibilities

- Mitigates threat and vulnerabilities to maintain the integrity of the system holding classified government data
- Have a working knowledge of the systems they oversee and be able to apply technical knowledge so that they can speak to the Information Assurance issues facing their programs to the engineers that present the challenges to them
- Be forward thinking and anticipate the changing requirements of the systems within the programs they maintain
- Deal with program personnel in a straightforward non-biased fashion by addressing their concerns and needs in timely and professional manner
- Have a working knowledge of the security requirements and approval cycles of the GVT. Agency being represented (DCID, JFAN, NISPOM, DIACAP, FISMA, etc)
An ISSO A Day In The Life

- Audit Log Review
  - Follow the SSP requirements for reviewing the system audit logs
  - Report any discrepancies to the ISSM
  - Create and maintain procedure for the collection of the system audit logs

- Virus Definition updates
  - Follow the SSP requirements for installing the Virus DAT files
  - Create and maintain procedure for installing the Virus DAT files

- Eyes and ears for Information Assurance for his or her program area
  - ISSOs should be physically located in the Program they support
  - The ISSOs should be in tune with the overall program so they can readily assist new IA requirements (example - a new OS needed)

- Maintain control over the removal and addition of hardware in the controlled space
  - Checking the maintenance log weekly
  - Use some control method for all hardware (bar code stickers)
  - Maintain the classification markings of the hardware in the program area

- Be inspection ready everyday
  - This should be the ISSOs mindset
An ISSO A Day In The Life

- End of Day Checks
  - Checking hardcopy in printers
  - Checking all Information System media devices:
    - Disks, DVDs, CD-Rs
  - Ensuring systems are “logged off” or the password protected screen lock is engaged (when overnight processing has been given prior approval)
  - Ensuring Closed Area is secured properly
  - May have a separate sign-off sheet for end of day checks
  - The use of security monitors to act in place of ISSO with program management approval to complete some of the end of day checks
Security Policy Overview

- ISSO should be able to identify National Security Policies; DoD Policies, Directives, and Instructions for their Customer

- NISPM
- DCID 6.3
- JAFAN 6.3
- Program Security Office (Customer Specific)
System Security Plan

- A System Security Plan is a formal Agreement used to
  - Specify IS Security Requirements
  - Document and Maintain operational systems security

- Defines IS security controls and procedures

- Documents DAA approved standards

- SSP must be
  - Reflective - of system, environment, operations
  - Maintainable - updated/revised to reflect changes
  - Verifiable are you doing what your plan says
Hardware Marking

- Labels should be color coded to indicate classification level. Refer to the NISPOM or ask your customer security rep what they want. If you program area is subcontract follow what the Prime does at their facility.

- Marking Labels should be placed on all removable hard drives. In the case of internal hard drives, place label on CPU case and ensure hard drive is labeled properly immediately upon removal.

- Labeling with your Systems
  - Color coded network cables
  - Especially when sharing physical space with Unclassified Systems
  - Labeling network jacks
    - Classified
    - Unclassified
Classification Markings

- Classification markings warn and instruct the holders to the degree of protection required to protect the media, and the systems they are installed on.
- Markings are required for all classified information.
- All media once opened should be marked if held in a closed area.
- All material stored in a security container should be marked including factory media.
Media Write Protection

- Physical Write-Protection requires physical action to change and should be verified each session
  - Floppy
  - 8mm tapes
  - 4mm tapes
  - DLT tapes
  - USB Jump Drives (May not be allowed for use in area per customer)

- Logical Write-Protection software action to change
  - CD-R, DVD-R
  - Zip
  - JAZ (Reference http://www.dss.mil/infoas/FAQ120704.doc)

- Other Considerations
  - CD-RW
Media Write Protection

- Media Must be write-protected and tested once each use (session) by attempting to write to the media

- Physical Write-Protect Issues
  - USB Jump Drives
    - Multiple partition jump drives contain a boot partition that does not allow for write-protect, therefore, these cannot be used in classified and unclassified environments (Switchblade hack)

- Logical Write-Protect Issues
  - CD-R
    - Write-Protect specific to CD Burning Application
    - Finalizing session
  - JAZ
    - Use “write-protect” option
  - Zip
    - Use protect option
Trusted Download

- Trusted download (at link below) refers to a procedure, or series of procedures, that permits information to be released below the accredited level of the Information System
  - Authorized File Types/Formats
  - Factory-Fresh media required
  - Procedures must be within an approved Protection Profile/Security Plan

- Government Approved Procedures
  - Required when DSS authorized file types/formats are not sufficient for data transfer
  - Must be done in conjunction with the DSS Information System Security Professional
  - Request to Government via “Risk Acknowledgement Letter”
  - Procedures must be within an approved Protection Profile

Trusted Download Problems

- Common Mistakes with Trusted Downloads
  - Failure to consult the Security Classification Guide when generating classified and seemingly unclassified information
  - Failure to thoroughly review documents
  - Failure to conduct the approved trusted downloading procedures as outlined in the System Security Profile
  - Engineers in a Hurry (The world will end if I don’t get this out!!)
Data Sharing

- Co-Location or Multiple Program Facilities (MPFs)
  - Physical

- Memorandum of Understandings (MOUs)/Memorandum of Agreements (MOAs)
  - Data, Physical or Data and Physical

- Security Considerations
  - Highest level of classification across the programs will take precedence when there is a classification discrepancy
  - Protect all data NISPOM, ITAR, affected Contracts and all other applicable requirements
Data Sharing

- Data Sharing Agreements
  - A formal written agreement between various U.S. Government Project Offices
  - Applies to the sharing of “data” (i.e., program information)
  - Specifies the reason for the sharing agreement
  - Explains Security requirements for such things as the NISPOM, discrepancies in classification levels and Need-to-Know
Memorandum of Understanding

- Memorandum of Understanding/Agreement
  - Typically involve multiple government or contractors
  - Physical, data or networks
  - Need to be coordinated with the FSO
    - May impact physical or operational security measures

- IS Perspective
  - Apply when you have Contractor to Government connectivity
  - Requires more lead time to get authorization for IS
  - All Parties must approve in writing
Data Transfer Issues

- Data transfers are risk managed not risk avoidance
- Data transfers should be Mission Critical
- Recognize where embedded data resides
- Use factory Fresh media always

Associated Risks
- Hidden code/data
- Slack Space (internal fragmentation called *file slack* or *slack space*)
- Media
- Compilation of information

Websites and tool
- Microsoft’s technet
- Metadata Assistant
- NT Toolbox
Protection Rating & Profile

- Protection Levels are used to determine the overall protection profile given to an Information System based on
  - Required clearance
  - Formal access approval
  - Need to know

- Protection profile security features are specified for Confidentiality, Integrity, and Availability to an IS which all have features rated at level of concern basic, medium, and high
  - Confidentiality
    - Features - Access Control, Auditing, Labeling
  - Integrity
    - Features - Backups, Change Control, Configuration Management
  - Availability
    - Features - Recovery, Prevent Denial of Service, Maintenance Schedules
Configuration Management

- Configuration management is the primary means to control an IS in a secure area

- Configuration Management Concepts
  - Ensures Protection measures are implemented and maintained
  - Creates a level of discipline and control to maintenance
  - Provides users and customers with a measure of assurance

- CM is vital in all three aspects of the IS Life cycle
  - Acquisition
  - Maintenance
  - Release
Risk Management

- The risk to an IS include
  - What is the asset and its value
  - What are the threats or vulnerabilities to the asset
- What damage will be done if protection of an asset is lowered
- What countermeasures are necessary for protection of the asset
- What is the cost consideration versus the risk involved
- Mission criticality
- Risk Tolerance of the data owner
Identification & Authentication

- Identification - process that an IS uses to recognize an entity
- Authentication - Security measure created to establish validity to view, send, or receive specific information
- Types of Authentication *(need to be described in SSP)*
  - Passwords
  - Smart Cards
  - Biometrics
- Password Protection
- Group log-on Passwords
Maintenance Procedures

- IS Life Cycle Protection
  - Acquisition
  - Maintenance
  - Release

- Maintenance Vulnerabilities
  - Uncleared maintenance personnel (never to be left alone)
  - Cleared employees ISSO still must enforce need to know

- During Maintenance remember C.I.A
  - Confidentiality - don’t disclose information or associations
  - Integrity - virus and malicious code
  - Availability – System outages & Denial of Service
Maintenance Escort Policies

- Prior to Maintenance Requiring Escorts
  - Provide separate Escort briefing to program personnel
  - Remove all classified
  - Remove non-essential, removable storage media
  - Disconnect device from network
  - Check all equipment of maintenance personnel for non-volatile memory or the ability to transmit
  - If system has failed and cannot be properly cleared before maintenance get prior approval from customer
  - Announce uncleared
  - Have the visitor sign log
System Auditing

- Importance of Auditing IS
  - Troubleshooting
    - Network problems
  - Resource Tracking
    - Capacity of system resources
  - Security
    - Controls
    - Policies
    - Procedures
  - Contractual required

- What Auditing will not do
  - Detect accounts without passwords
  - Detect accounts with insecure passwords
  - Identify dormant accounts
  - Files accessible to everyone
  - Prevent Illegal activity
Reasons for System Auditing

- **Account login events**
  - Discover Brute Force Attacks on your network.
  - Stolen Passwords someone just logged in who is on vacation

- **Audit Account Management**
  - Misuse of Privilege a new user has been added to your systems admin group

- **Audit Object Access**
  - An attacker is trying to gain access to sensitive compartmented files
  - Inappropriate changes to .exe and .dll files could signal a virus or an attacker modifying system files
TEMPEST

- An ISSO should have a basic understanding of TEMPEST (EMSEC): Referring to investigations and studies of compromising emanations.

- The ISSO should understand the importance of Red Black separation to maintain the TEMPEST Standards are reduce the risk of Compromising Emanations.

- The uses and inspection of PDS (Protected Distribution Systems) Cabling (CAT5, fiber, etc.) used to transmit unencrypted classified information through an area that is not controlled.
Special Category IS

■ IS with group authenticators
  – Group Authenticators more than one individual using the same identifier and authenticator
  – Avoid a group authenticator as the sole access control mechanism
  – Application should be identified in the SSP

■ IS Using Periods Processing
  – Different Protection Levels using the same IS during different periods
  – Sanitization Procedures must be approved

■ Interconnected System
  – Connected systems that are independently accredited
  – Must have mechanism to adjudicate varied security policy
  – Possible Confidentiality and Integrity concerns
Controlled Interface

- Mechanism that handles the adjudication of different interconnected system security policies
- Examples include firewalls and a High Assurance Guard
- Controlled interface common requirement
  - Audits all direct user access to the interface
  - Be included in the CM process
  - Protected against failure or compromise
  - Physically protected
  - Routing information is completely controlled by the interface
  - Thoroughly tested to ensure it satisfies all security requirements
Incident Response

- Conducting the Interview
  - Get a statement signed and dated
  - Explain why the interview is being conducted

- System Contamination Response and Reporting
  - Cease and Isolate
  - Immediately report contamination to FSO
  - Identify source and receivers
  - Coordinate contamination efforts
  - Provide written report

- Follow-Up
  - Submit formal incident report
  - Provide security training
Insider Threat Awareness

- **Insider Threat** - Majority of the damage to National Security has been the result of a person who had authorized access
  - Espionage
  - Equipment Misuse
  - Disgruntled Staff

- **Insider Threat Patterns** - Majority of perpetrators of insider threat have above user level access
Threat Countermeasures

- Informed Knowledgeable Users
  - Initial IS indoctrination Brief
  - Security Awareness Training
  - Signed Non-Disclosure Agreements

- Properly Configured Systems
  - Audit Trail
  - Disable inactive accounts
  - Proper Access control (only give them what they need)

- System vulnerability countermeasures
  - Backup planning
  - Recovery Planning
  - Encryption
Questions