When Training Isn’t the Answer: Supporting Critical Information Assurance Audiences with Electronic Performance Support Systems

Jan W. Whiteley, SPHR and Wade R. Sharp, CISSP
NRO Security and Counterintelligence
Training Branch
Identifying Information Assurance Audiences and Their Needs

- Who performs Information Assurance tasks?
- Can individuals who perform like tasks be grouped? If so, how?
- What, if any, relationships would such groups have to each other?
- What does each Information Assurance audience need to know and be able to do in order to perform their jobs?
Our Information Assurance Training Populations

- General Users
- Specialized IA Professionals
- Privileged Users
- Significant IA Responsibilities
- Privileged Users AND Significant IA Responsibilities

- The intersection of the red and blue circles defined a handful of positions with elevated privileges and “make or break” IA responsibilities
Selecting and Identifying the Needs of “Critical” IA Audiences

- An IA position may be considered critical if it:
  - Encompasses key aspects of the IA discipline
  - Directly supports the organization’s mission priorities
  - Is considered critical by senior executives and other major stakeholders

- Stakeholders agreed unanimously that ISSOs were the most critical IA audience in need of training to satisfactorily perform their tasks

- Data collection efforts identified five high-priority areas requiring performance support intervention
  - Additional research and SME input identified many more performance issues that needed to be addressed
Why We Opted for an Electronic Performance Support System Rather Than Formal Training

- The urgency of the need argued against the creation of formal training.
- The need to reach a widely dispersed audience in a relatively short time frame argued against instructor led courses.
- Many of the tasks that ISSOs must perform can be completed satisfactorily with references and job aids – formal training is not needed to ensure desired job performance.

This was the right intervention for the right audience at the right time.
Our EPSS Solution: The ISSO Resource Kit

- A web-based collection of documents, tools, and links:
  - Designed to help ISSOs perform their tasks more efficiently and effectively
  - Populated from items and ideas received from ISSOs throughout the NRO
  - Whose content was thoroughly reviewed by a panel of cross-program SMEs, Security Policy Staff, and Instructional Designers
  - That features a clean, simple, and user-friendly design to promote easy navigation, viewing, and downloading

A very large amount of high-quality information about the ISSO job is now available in a centralized location and in standardized formats
ISSO Resource Kit Home Page

(U) Welcome to the Information Systems Security Officer (ISSO) Resource Kit – a collection of documents, tools, and links that has been created with you in mind! This Kit is targeted primarily to ISSOs at Government Sites. ISSOs at Industry Partner sites can also benefit from Kit material, but should verify its applicability with their Program Security Officers or other security professionals (e.g., ISSM, SCO).

(U) To perform your critical tasks, you must often access data from many different sources. The purpose of the ISSO Resource Kit is to put the majority of that information in one place and categorize it so that it will be easy to find.

The Welcome page contains:
- A brief description of the Kit, its purpose, and its intended audience
- Recommendations for use
- Information about tailoring Kit documents to meet organization-specific needs
- A request for site feedback
The Main Menu Bar

- Reflects an architecture that was repeatedly refined to better accommodate user needs and evolving subject matter
- Shows categories with topical and functional elements
- Was designed to be clean and very easy to use
For the New ISSO Sub Menu

- Useful for quick orientation
- Houses frequently given briefings
- Assists ISSOs with their own and others’ In and Out Processing
- Focuses on ISSO job responsibilities
- Contains valuable background data on other Security functions
Accessing Documents Within A Category

(U) ISSO Duties as Defined in DCID 6/3

(U) A direct excerpt of the "ISSO responsibilities" portion of DCID 6/3, arranged on one sheet for easy reference. Note to ISSOs: DCID 6/3 is a vital source of information for ISSOs. If you are not familiar with its contents, you would be wise to acquaint yourself with it as soon as possible.
Sample Content

ISSO Duties as Defined In DCID 6/3

- Ensuring systems are operated, maintained, and disposed of in accordance with internal security policies and practices outlined in the security plan.
- Ensuring that all users have the requisite security clearances, authorization, and need-to-know, and are aware of their security responsibilities before granting access to the IS. In addition must have signed user agreements.
- Reporting all security-related incidents to the ISSM, DAA Rep and/or the Program Security Director, as appropriate.
- Initiating, with the approval of the ISSM and/or the DAA Rep, protective or corrective measures when a security incident or vulnerability is discovered.
- Monitoring system recovery processes and ensuring the proper restoration of IS security features.
- Developing and maintaining an SSP as described in Appendix C.
- Conducting periodic reviews to ensure compliance with the SSP.
- Ensuring configuration management (CM) for security-relevant IS software, hardware, and firmware is maintained and documented. If a CM board exists, the ISSO may be a member of the CM board if so designated by the ISSM.
- Ensuring that system recovery processes are monitored to ensure that security features and procedures are properly restored.
- Ensuring all IS security-related documentation is current and accessible to properly authorized individuals.
- Formally notifying the ISSM and the DAA when a system no longer processes intelligence or SAP information.
- Formally notifying the ISSM and the DAA when changes occur that might affect accreditation.
- Ensuring that security requirements are addressed during all phases of system life cycle.
- Following procedures developed by the ISSM and defined in CM change control procedures, authorizing software, hardware, and firmware use before implementation on the system.

Note: Because NRO ISSOs work so closely with their PSOs and SCOs, be certain to refer to NRO specific guidance regarding all topics cited. Additionally, be certain to discuss specific ISSO duties with your Team Leaders or contractor supervisors.

- Standard template
  - Yellow indicates reference document

- Example of repurposing
  - Summary/synopsis of responsibilities from DCID 6/3 recast as a quick reference document

- Typical length
  - Most hosted documents are 1-2 pages
  - Deliberate choice to make documents easier to digest and act upon

- Caveated
  - Like almost all documents on the Kit, this one may be modified to reflect organization-specific procedures, PSO/ISSM guidance, etc.
The Policies Section is divided into three subsections for ease of use:

- First category is “must know” directives, instructions, and notes.
- Second category holds foundational documents that give ISSOs the “why” behind some organizational documentation.
- Third category contains supplemental references that provide important background data.

Each subsection is organized by categories of information, rather than policy numbers or names that some ISSOs may not be familiar with.
Key ISSO Related Forms – Topical Organization

(U) This section, "Key ISSO-Related Forms", contains a number of forms that are absolutely central to the life of an ISSO. You'll note that many of these forms contain detailed instructions. For that reason, some ISSOs prefer to print off a copy of the form, and then carefully read the instructions associated with each block of the form.

(U) Want to jump immediately to a specific category of form instead of scrolling through? Then select one of the hyperlinks below:

- Courier Certification
- Equipment Release
- Internet Accounts
- Media Access Devices
- NRO Management Information System (NMIS)
- Portable Electronic Devices
- Privileged Users
- Property Transactions
- Uploads & Downloads
Processes and Checklists

- One of the most eagerly anticipated and heavily populated areas of the Kit

- Contains a mixture of Security strategy, step-by-step instructions, checklists, and action plans
General Best Practices – Topical Categories

- Assessments
- Backups
- Cell Phones
- Co-location
- Couriers
- Destruction
- Digital Cameras
- Enterprise Operations Division (Formerly EMOC)
- Equipment Release
- Incident Response and Reporting
- Internet Access
- ISSO Responsibilities
- Laptops
- Media Access Devices
- Media Release
- Multi-use Switches
- Need to Know
- NRO Management Information System (NMIS)
- Password Management
- Peripheral Devices
- Personal Digital Assistants (PDAs)
- Portable Electronic Devices
- Privileged Users
- Processing (In & Out)
- Property Management/Turn In
- Recording Devices
- Safes
- Sanitization
- Security Concept Assumptions Document
- Software Evaluation & Request
- Test Equipment
- Unauthorized Disclosure
- Uploads & Downloads
- Virus & Malicious Code
- Visitor Access
- Vulnerabilities
Sample Best Practice Guidance

Best Practice Guidance on Cellular Telephones

All cell phones have inherent technical vulnerabilities, which can be exploited to compromise conversations and data processing operations conducted in their vicinity. For example, they have been known to fail to terminate a call even though the user ended the call. In that case, the conversations in the phone’s vicinity could continue to be broadcast without the user’s knowledge. Although this situation is usually accidental, it could theoretically be deliberately induced from a distance – thus posing a significant security risk if those surrounding conversations concerned classified data.

The list of known passive vulnerabilities regarding cellular telephones is extensive. For that reason, cell phones may only be introduced into NRO facilities if:

- The phone is completely turned off
- The battery has been removed.
- All special features, such as voice activation or auto-answer, have been disabled.
- Any site-specific requirements, such as locations to leave the phones, have been fulfilled

Personal single function cell phones do not need to be registered with the ISSO to be introduced into an NRO facility, but must adhere at all times to the handling guidelines shown above.

Charging of personal cell phones in the facility is strictly prohibited; additionally no charging equipment should be introduced into the facility.

Please note that phones with camera capabilities are also strictly prohibited, even if the battery is removed.

All Government Furnished cell phones must be registered with the ISSO in order to be introduced to an NRO facility. Charging of government owned cell-phones is also prohibited, unless they are charged with the battery removed or charging is done in drawers, overhead storage areas, or other closed areas after normal duty hours.

For additional information, refer to:

- DOS & CI Note 06-09, Government Purchased Cellular Phone Policy
- NROD 50-10a, Portable Electronic Devices
- NROI 50-6a, Portable Electronic Devices
Contains a wealth of information and tools

- Puts commonplace, but not always easily accessible items (such as the correct cover sheet or label) at the ISSO’s fingertips
- Features materials tailored especially for ISSOs and their general users
- Contains templates to prevent the “reinvention of the wheel”
- Features a “mini-tutorial” on the proper completion of the System Security Plan
Resources and References – Acronyms and Glossaries

(U) Acronyms and Glossaries
(U) Administrative Records and Logs
(U) Cover Sheets
(U) Fact Sheets
(U) Guidance for Reviewing/Completing Key Documentation
(U) Key ISSO-related Websites
(U) Labels
(U) Signage and Security Awareness Products
(U) Templates

(U) Glossary
(U) Solid glossary of key Information System terms and concepts, derived mostly from DCID 6/3 and the National Information Systems Security Glossary, that may be of use to ISSOs in the performance of their duties.

(U) The ABCs of Incidents
(U) Brief definitions of many terms associated with a system incident. Also includes a list of “red flag” computer performance issues that should prompt an immediate investigation.
The ABCs of Incidents: A Handy Reference Guide

**Attack**
An intentional act of attempting to bypass security controls on a computer or network.

**Breach**
Any successful defeat of security controls.

**Computer Network Attack (CNA)**
Operations to disrupt, deny, degrade, or destroy information resident on computers and computer networks, or the computers and networks themselves.

**Computer Network Exploitation (CNE)**
Operations to exploit accesses or information resident on computers and computer networks.

**Data Compromise (Data spill)**
- Disclosure of classified information from an information system to unauthorized persons.
- Compromise or potential compromise of classified information or intelligence sources or methods, which could likely result in the loss of human life. (Such a compromise is also reportable to Congress.)
- Compromise or potential compromise of classified information or intelligence sources or methods, which could reasonably be expected to cause exceptionally grave damage to the national security. (Such a compromise is also reportable to Congress.)

**Denial of Service Attack (DOS)**
An intentional attempt to disable (using direct or indirect methods) an IT system, application, network, or service.

**Intrusion**
An unauthorized access or penetration of a system.

**Malicious Code**
Software or firmware included or introduced into an Information System (IS) for an unauthorized purpose. The most damaging types of malicious code are those for which no published countermeasure exists, any new virus whose propagation could likely outrun IC containment capabilities, or any new virus which affects network services.

**Trojan Horse**
An apparently useful and innocent program that contains additional hidden code, which allows unauthorized CNE, falsification, or destruction of data.

**Unauthorized Access**
- Any access gained to privileges, permissions, administrator or root level system controls, monitoring, or other administration functions, by an unauthorized user; to include processes acting on the behalf of a user.
- Any incident involving unauthorized access to a controlled interface, SABI Interface, or TOP SECRET/Special Compartmented Information and Below Interoperability (TSABI)
- Referenced Implementation (TRI), on a domain with a controlled interface or TRI, or any SCI to non-SCI interface.
- Any incident involving attempted access to a controlled interface, SABI interface, TSABI Referenced Implementation (TRI) or on a domain with a controlled interface or TRI – to include scans and probes.

**Unusual or Suspicious activities**
These activities are not, in themselves, evidence of a computer incident or attack. However, they are “red flags” and should be carefully investigated.

- Suspicious files identified on a server
- Unexplained access privilege changes
- Unusual system performance or behavior
- Missing data, files, or programs
- Multiple simultaneous logins by the same user
- Unusual after-hour system activity
- Multiple failed login attempts
- System crashes or component outages of a suspicious or unexplained nature
- Abnormal delay in network or application services
- Unusual data or system characteristics
- Discovery of unauthorized software
- Suspicious system configuration changes

**Variant**
A version of a virus or other form of malicious code that is modified slightly in an attempt to bypass anti-virus countermeasures.

**Virus**
A malicious, usually self-propagating program or code fragment that is attached to application code or other computer data. It contains a triggering mechanism (event or time) with a payload that contains instructions to carry out a mission (delete files, corrupt data, and/or send data).

**Vulnerability**
A weakness in a system that may leave it open to potential exploitation, which could result in the risk of an information compromise, alteration or destruction of data, or denial of service.

**War Dialing (Auto dialing) Activity**
Any suspicious activity that appears to be related to the probing of phone switches for vulnerable information system entry points.

**Worm**
A worm is a program (usually self contained) that will replicate itself across a network by using a system’s resources to replicate and propagate. Replication and propagation may adversely affect CPU resources and network throughput.
Administrative Record Keeping

(U) This section offers a set of documents intended to help ISSOs manage a myriad of tasks. For ease of use, these documents have been placed in four categories:

- Hardware Inventories
- Sanitization Records
- Sign-Out Sheets
- Tracking Sheets

(U) The use of these documents is optional; they are offered as a convenient means for ISSOs to record data that must be maintained as part of their duties. For example, because ISSOs must carefully control their inventory of laptops available for sign-out, three forms are provided – a classified computer sign-out sheet, an unclassified computer sign-out sheet, and a log that contains information about all laptops that are available for sign out.
User Fact Sheets

(U) Fact sheets are a great way to reinforce verbal instruction.

(U) Privileged User Job Aid
(U) A quick reference document that briefly describes Privileged User Roles and Responsibilities, and defines key terms and concepts.

(U) User Fact Sheet PEDs
(U) A one-page document that captures the most critical information for general users to know about Portable Electronic Devices.
Privileged User Job Aid

Privileged User Roles and Responsibilities

- **System Access Control**
  - Establish systems and data storage areas are secured
  - Limit access to authorized users and groups
  - Know how systems are used and operated within your environment (i.e., operational, development, testing, or staging)
  - Ensure that administrative accounts are restricted to those performing administrative functions
  - Ensure that access to password management policies are satisfied before giving anyone access to a system
  - Serves as the Program Security Officer (PSO) to address the user's security clearance and access authorization needs
  - Assigns access privileges to a user who submits to the minimum privileges needed
  - Reviews and validates users' existing access privileges and requested access (as needed)
  - Ensure that each user has a unique identity that conforms to policy
- **Verify access of groups or user accounts to ensure accuracy**
- **Report the following security-related changes or events to your RSC or RSO**
  - New user requests
  - Changes to systems not made by a system administrator
  - User incidents
  - Unauthorized hardware/software changes
  - Unauthorized influence or pressure to grant access to a user
  - Media mishandling
  - Deleting or not using system security features
  - Any system or network access request
  - Changes to your Privileged User status
  - Any denial of denying or event

Privileged Users Must Not:
- Write down your passwords and passwords or access privileges
- Use a device or computer to log onto the system
- Send passwords or access privileges to others
- Use any unauthorized hardware or software in the performance of duties

Key Terms and Concepts

- **Accountability**
  - Accountability: the process of tracing activities to a responsible source, and holding individuals accountable, responsibilities, and liabilities for specific activities, rules, or policies.
- **Due Care Due Diligence**
  - Due Care Due Diligence: the need to know, the need to be informed, and the need to report such information.
- **Need-to-know**
  - Need-to-know: the need for access to information.
- **Non-repudiation**
  - Non-repudiation: a mechanism or system that assures that a message or transaction cannot be denied.
Completing Key Documentation

(U) RESOURCES & REFERENCES
(U) GUIDANCE FOR REVIEWING/COMPLETING KEY DOCUMENTATION

(U) System Security Plans (SSPs)

To View: Left-click ⬇️ | To Save: Right-click ⬆️ , 'Save Target As'

(U) Use the drop down menu below to further refine your search. Alternatively, you may scroll through the material.

(U) SSP Attachments
(U) SSP Attachments
(U) SSP FAQ
(U) SSP Sections
(U) SSP Template Appendix

(U) SSP Attachments

(U) Detailed description of the kinds of material that should and might be presented in the attachments of an SSP, including organizational charts; facility diagrams; floor plans; listings of major hardware; software listings; and agreements.

(U) SSP FAQ
In Section 7.2.3 describe how authenticators are assigned, distributed, and controlled.

Document the management mechanisms used to ensure the creation of a unique identifier for each user and describe how that identifier is associated with all auditable actions taken by the user.

Describe how initial authenticator content is established and the administrative procedures for initial authenticator distribution.

Document the authenticator construction standards and generation process.

Describe the processes and procedures for change, aging, history, and assurance of non-replication of individual authenticators.

If group identifiers (i.e., shared passwords) are used, provide a rationale for their use. For more information about group identifiers, click here. Otherwise, click the Next button to continue.

Note: Use of a group authenticator, even in conjunction with a unique authenticator, needs to be identified to the certifier as soon as possible.
Key Internal and External Websites

(U) Enterprise Operating Division Website
(U) This site contains a wealth of information designed to prevent or mitigate system attacks. Use the bars at left to navigate through the site; of particular interest is the Information Assurance area.

(U) INFOSYSSEC
(U) http://www.infosyssec.org
(U) An UNCLASSIFIED security portal for Information System Security Professionals (ISSPs), considered by some to be the most comprehensive computer and network security resource on the Internet for ISSPs.

THIS SITE IS ACCESSIBLE FROM THE INTERNET (WORLD WIDE WEB)
Topically Organized Templates

(U) RESOURCES & REFERENCES

(T) TEMPLATES

(U) You can scroll through the page or select from the following categories:

- Action Requests
- Activity Reports
- Authorization Letters
- Business Case Documentation
- Certification Testing
- Concept of Operations
- Continuity of Operations
- Courier Documentation
- Destruction Documentation
- Group Account Documentation
- Incident-Related Documentation
- ISSO In Processing
- Joint Agreements
- Multi-Use Switch Agreements
- Network Script Creation
- Portable Electronic Devices
- Privileged Users
- Security Concept Assumptions Document
- Software Evaluation
- System Security Plans (SSPs)
- Vendor Agreements
Contact and Training Data

For the user’s convenience, separated formal contact lists from Organizational Charts

Divided training into three subsections to increase usability
Task Area Functional Grouping

Added as the result of a suggestion by a Senior ISSO

Organized functionally rather than topically
  - Shows ALL information related to an ISSO function, rather than by type (e.g., policies or forms)

Provides another way of “thinking” about Kit contents
  - Akin to adding other references to an index to accommodate different places that a user might look for data
Task Area Sub Groupings

- **Audits and Assessments**
  - Activity Reports
  - Auditing and Compliance
  - ISSO Assessments

- **Certification & Accreditation**
  - Certification & Accreditation
  - Configuration Management
  - Software Evaluation and Request
  - System Security Plans (SSPs)

- **Configuration Management**
  - Configuration Management

- **File Transfer and Data Handling**
  - Classification
  - Courier Information
  - Dirty Word Searches
  - Media Release
  - Uploads and Downloads

- **Incident Prevention and Response**
  - Computer Incident Response and Reporting
  - Configuration Management
  - Virus and Malicious Code

- **Portable Electronic Devices (PEDs)**
  - Laptops
  - Portable Electronic Devices

- **Physical Security**
  - Physical Security

- **Property Management and Accountability**
  - Configuration Management
  - Destruction
  - Property Management/Turn In
  - Sanitization

- **Risk Management**
  - Risk Management
  - Vulnerabilities

- **User Account Management**
  - Accounts Management
  - Media Access Devices
  - Password Management
  - Privileged Users
  - Processing (In and Out)
  - Internet
(U) Welcome to the Information Systems Security Officer (ISSO) Resource Kit – a collection of documents, tools, and links that has been created with you in mind! This kit is targeted primarily to ISSOs at Government Sites. ISSOs at Industry Partner sites can also benefit from Kit material, but should **verify its applicability with their Program Security Officers or other security professionals** (e.g., ISSM, SCO).

(U) To perform your critical tasks, you must often access data from many different sources. The purpose of the ISSO Resource Kit is to put the majority of that information in one place and categorize it so that it will be easy to find.
Product Launch – Keys to a Successful Release

- Capitalize on existing buzz to launch the product in an atmosphere of celebration
  - Prominent venue
  - Certificate presentations and photos

- Deploy multi-faceted communications and marketing effort
  - Hard copy "save the date" brochures
  - Briefings to the ISSO Community of Practice
  - Status updates to senior leadership
  - Update emails to ISSOs
  - Detailed brochure to serve as both a marketing pitch and post-demo orientation/job aid

- Encourage Active Senior Leadership Participation
  - Ask the most senior level stakeholders and committed champions to speak
  - Have executives or senior managers give out certificates

- Publicly recognize all levels of SME contribution (from modest to significant)
  - Generates tremendous goodwill in the community; all contributors feel invested
  - Lays the groundwork for future participation in update and maintenance efforts
  - Provides a well-deserved pat on the back

- Provide a detailed demonstration walkthrough that highlights Kit content, structure, and navigation

- Create a viable product tie-in
  - Tangible
  - Job related
  - Appropriately themed
Keeping the Kit Current

- Concurrent with rollout activities, the team created a detailed maintenance plan
- The plan outlined the:
  - Creation and composition of an ISSO Resource Kit SME Review Board
  - Procedures that would be followed to ensure that every Kit item stayed accessible, accurate, and relevant
  - General timetable for completing each set of reviews
  - Steps to be taken to add, delete, or modify materials “out of cycle” to support mission needs
- Content-related site feedback will be shared with the SMEs for their action/concurrence
Keeping Current - User Suggestions

(U) SITE FEEDBACK

(U) We welcome your comments and suggestions! Your feedback will help ensure that all of the information presented in the ISSO Resource Kit is:

- Easy to use
- Technically accurate
- Complete
- Relevant to the performance of ISSO tasks

(U) Please fill in the form below to submit your thoughts and suggestions for improvement. If you wish to submit documents for consideration, please indicate that in your comments, and provide a name and phone number so that we may follow up with you.
Project Success Factors and Drivers

- Management and Stakeholders were fully committed to addressing critical ISSO needs in the most efficient, expeditious, and cost-effective manner.
- Senior ISSOs were willing to capture and share their knowledge and insight to “kick-start” the program/shape the outcome to be beneficial for junior staff.
- Instructional Designers enjoyed a close, mutually beneficial partnership with Security Policy that ensured that all Kit content was consistent with existing policy.
- The ISSO community was actively involved in structuring and populating the Kit with accurate and relevant task information.
- Web Designers and graphic artists worked in close collaboration with Instructional Designers to refine the relationship between data and site architecture.
- Among ISSO, word of mouth “buzz” about the functionality, content, and impact of the kit sustained interest and anticipation during the development phase – the spirit of “By ISSOs, for ISSOs”.
- Generic data that would have been of limited use was repurposed and tailored to meet job-specific needs.
- The Resource Kit Team created high-value content through analysis, brainstorming, data reconstitution, and other in-depth work; not just compilation and categorization of existing material.
Moving Forward – Recommendations for Future Efforts

- Cast your net widely: It is not easy in the beginning to know the whole “cast of characters” who may need to weigh in on specific issues, such as use and interpretation.

- When dealing with a critical audience that has immediate information/training needs, first work with highly impactful but relatively simple information. Then work with other vital data as time permits. Incremental improvement is the key.

- Proactively address concerns about whether material is mandatory or recommended, thus precluding misunderstandings that could derail the effort or cause individuals not to contribute needed information.

- Strive for consensus, but not at the expense of any audience member feeling excluded. Design the Kit in such a way that differing approaches to accomplishing a task can be accommodated.

Maintain your focus on meeting identified needs. Be flexible and creative in your solutions; don’t let an obstacle become a showstopper.
Questions and Contact Data

For More Information, contact:
– Thaddeus Ross
  Chief (acting), OS&CI Training Branch,
  703-808-4505
– Jan Whiteley
  703-808-6510;
  whiteley_jan@bah.com
– Wade Sharp
  703-808-2979;
  sharp_wade@bah.com