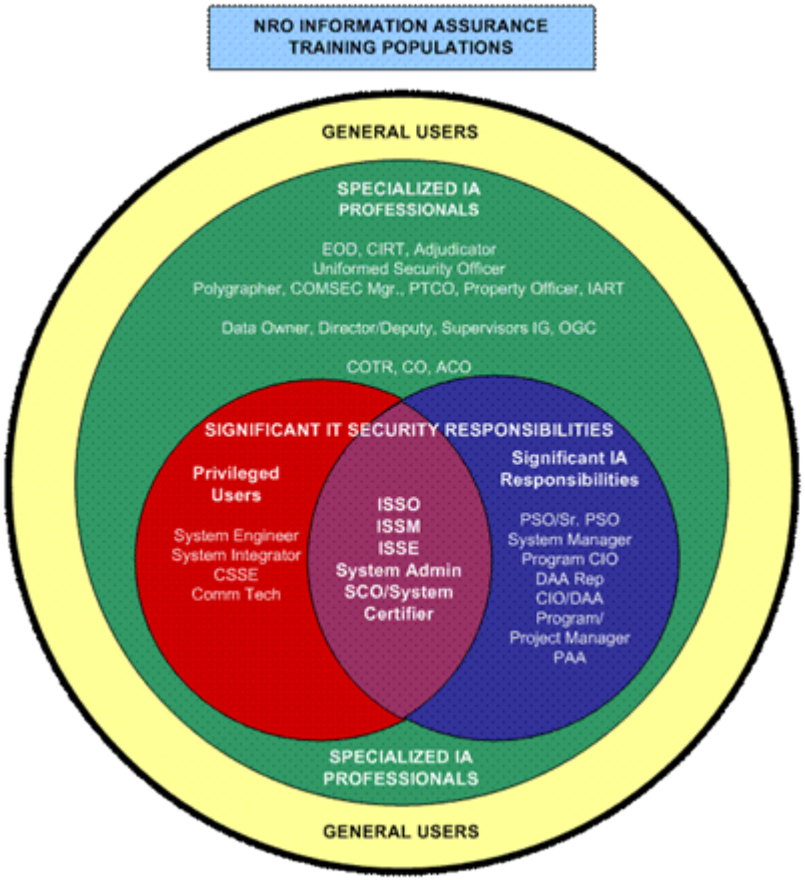
When Training **Isn't** the Answer: Supporting Critical Information Assurance Audiences with Electronic Performance Support Systems

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

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

Main Menu Bar – Primary Navigation

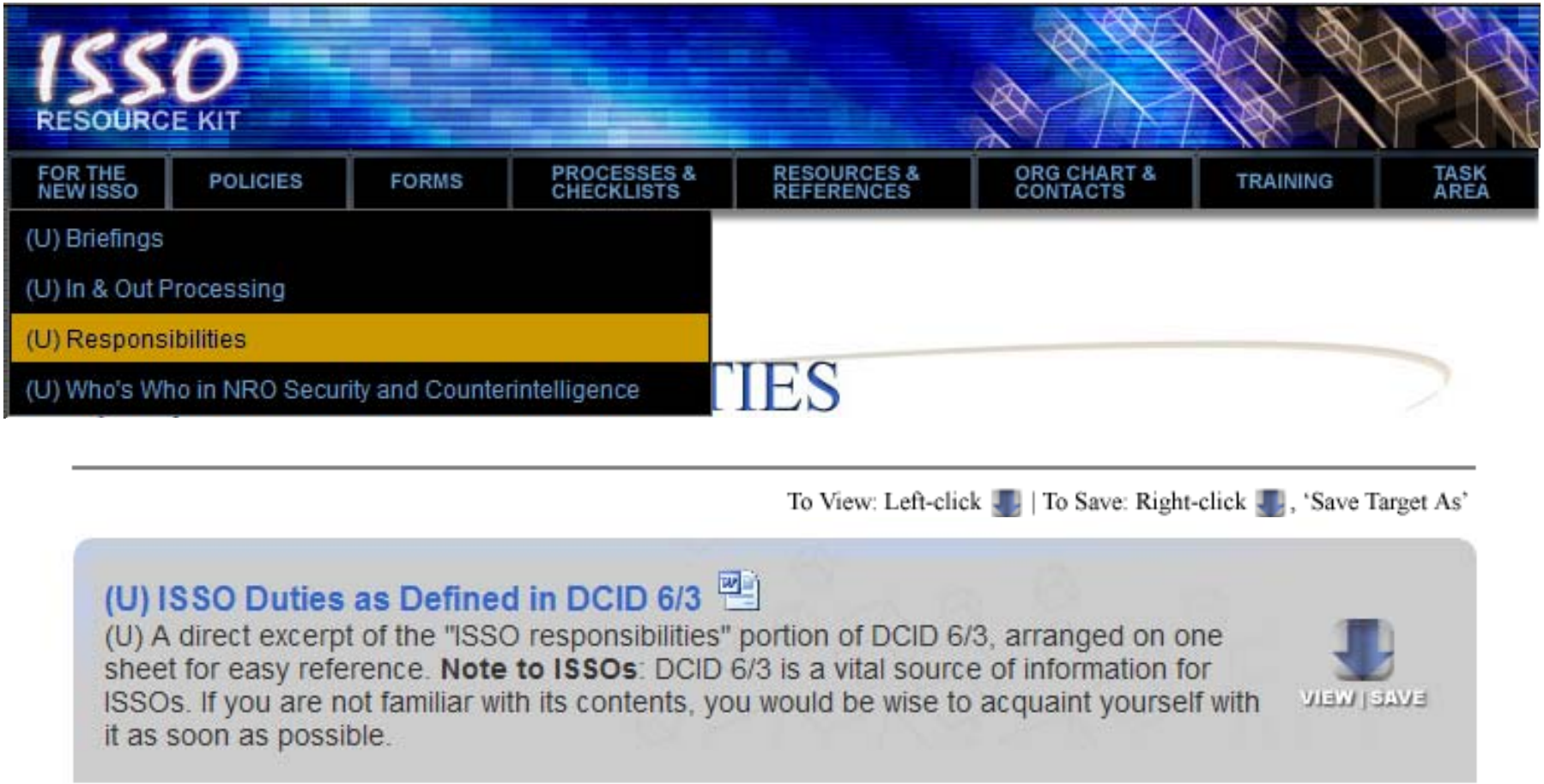
The Main Menu Bar

- 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



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.

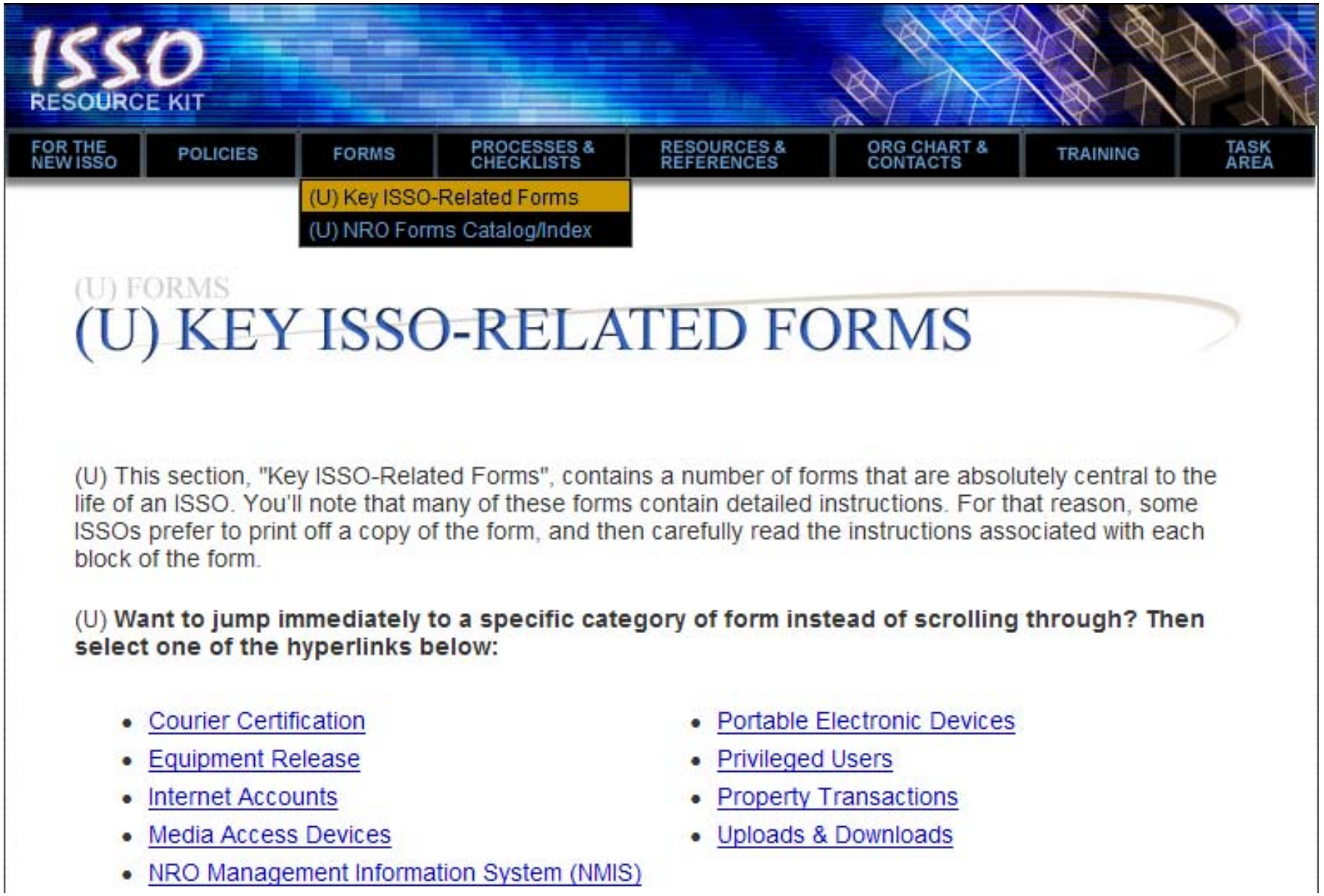
- Standard template
  - Yellow indicates reference document
- Example of repurposing
  - Summary/synopsis of responsibilities from DCID 6/3 recast as a quick reference document
- Typical length
  - Most hosted documents are 1-2 pages
  - Deliberate choice to make documents easier to digest and act upon
- Caveated
  - Like almost all documents on the Kit, this one may be modified to reflect organization-specific procedures, PSO/ISSM guidance, etc.

Policies Sub Menu

- 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



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

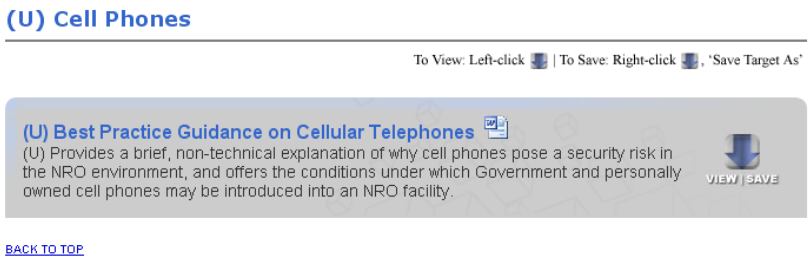
General Best Practices – Topical Categories

(U) PROCESSES & CHECKLISTS

(U) GENERAL BEST PRACTICES

- 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 Practices

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**

Resources and References Sub Menu

- 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

Sample Content – Acronyms and Glossaries

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 intelligences 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

User Fact Sheets

Privileged User Job Aid

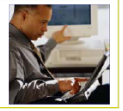
NRO PRIVILEGED USER PROGRAM

Privileged User Roles and Responsibilities

System Access Control

- Ensure 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 storage)
- Ensure that administrative accounts are restricted to those performing administrative functions
- Ensure that access and password management policies are satisfied before giving anyone access to a system
- Ensure the Program Security Officer (PSO) has verified the user's security clearances and access authorizations
- Assign access privileges on a need-to-know least privilege basis
- When activating a user ID or granting access to an IS, ensure that the request comes from the user's manager in writing
- Review and validate users' existing access privileges and requested access (as needed)
- Ensure that each user has a unique identity that conforms to policy
- Verify accesses of groups or shared accounts to ensure accuracy
- Respect the privacy of and protecting passwords, information, communication, and data access rights from unauthorized disclosure

Security Monitoring



- Identify needs and requirements for both internal and external audits.
- Keep documentation and records (i.e. logs, audit reports).
- Review audit trails to identify possible unauthorized access or suspicious activity.
- Notify your ISSM, ISSO or PSO immediately when you discover anything suspicious.

Configuration Management

- Ensure that your sources for updates and patches are appropriate.
- Help your ISSO or PSO maintain configuration control of the systems and application software in your area.
- Ensure that your configuration for passwords follow NROI 50-7b instructions.
- Make only authorized configuration changes according to NRO practices and procedures. Adhere to appropriate system hardening procedures
- Make sure that systems are maintained according to approved standard security procedures and the NRO C&A process.
- Follow prescribed procedures, instructions, and manuals for system operations.
- Adhere to program office CM program for systems within your purview.

Incident Response and Reporting

- Identify and report any incidents, breaches and violations.
- Know NRO incident response policies and procedures.
- Know the points of contact (POCs) for your office or location and how to reach the Computer Incident Response Team (CIRT).

Report the following security-related changes or events to your ISSO or ISSM:

- New system requirements
- Changes to systems not made by a system administrator
- Virus incidents
- Unauthorized hardware/software changes
- Unreasonable influence or pressure to grant access to a user
- Media mishandling
- Disabling or not using system security features
- An incorrect or inaccurate logon dialog box
- Any unauthorized system and/or network access request
- Changes to your Privileged User status
- ANY unusual anomaly or event

Report the following security-related changes or events to your PSO:

- Any unauthorized disclosure
- Counter-Intelligence (CI) incidents
- An inadvertent exposure of information exceeding a user's documented access
- Changes to your Privileged User status

NRO PRIVILEGED USER PROGRAM

Privileged Users must NOT:

- Share passwords or access privileges
- Use IS resources for private gain
- Duplicate or install software except in strict compliance with applicable licensing agreements and as approved through the appropriate system CM procedures
- Attempt to compromise the integrity or performance of any internal or external system or network
- Attempt to use IS resources to gain unauthorized access to any data, site or network
- Use any unauthorized hardware or software in the performance of duties
- Write down or keep logs of passwords
- Use weak passwords
- Browse or access the contents of any user data, whether online or offline, without explicit permission
- Collect information on individuals' information usage patterns except as required and authorized for system audit purposes
- Employ or create software of system "back doors"
- Use hacker/forensic tools without permission
- Conduct investigations of suspected system abuse or misuse without prior coordination with the ISSO, ISSM, or PSO
- Call users to ask them for their passwords

Key Terms and Concepts

Availability: Assurance that authorized users have timely, reliable access to data and information services.

Integrity: Assurance that data remains unchanged from its source and is not accidentally or maliciously modified, altered or destroyed.

Confidentiality: Assurance that information is not disclosed to unauthorized persons, processes or devices.

Accountability: the process of tracing IS activities to a responsible source, and holding individuals answerable, responsible, and liable for specific activities. User IDs, account names, and passwords unique to single users ensure accountability of individual user actions on the system.

Need-to-Know: The necessity for access to, or knowledge or possession of, specific official information required to carry out official duties. Need-to-know is determined by an authorized holder of information who decides that a prospective recipient requires access to that official information to perform his duties.

Identification –vs.- Authentication: Identification establishes the identity of a person, process or device. Authentication establishes the validity of a transmission, message, or originator. It provides verification of an individual's authorization to receive specific categories of information.

Due Care or Due Diligence: the 'civic responsibility' of every organization to be attentive to security, to protect itself against known threats, and to ensure that its computing environment is secure. It requires monitoring the network, detecting problems, and examining vulnerabilities no matter how minor they seem.

Password management: a set of rules designed to enhance computer security by encouraging users to employ "strong" passwords and use them properly. For specifics on NRO password policy, refer to NROI 50-7b.

Restricted Access/Least Privilege: a basic principle in information security, which states that entities (people, processes, or devices) should be assigned the fewest privileges consistent with their assigned duties or functions.

Non-repudiation: Proof that data was delivered to, and received by, the intended recipient.

Defense-in-Depth: a "best practices" strategy for achieving IA in today's networked environments. It relies on the intelligent application of techniques, technologies, and procedures.

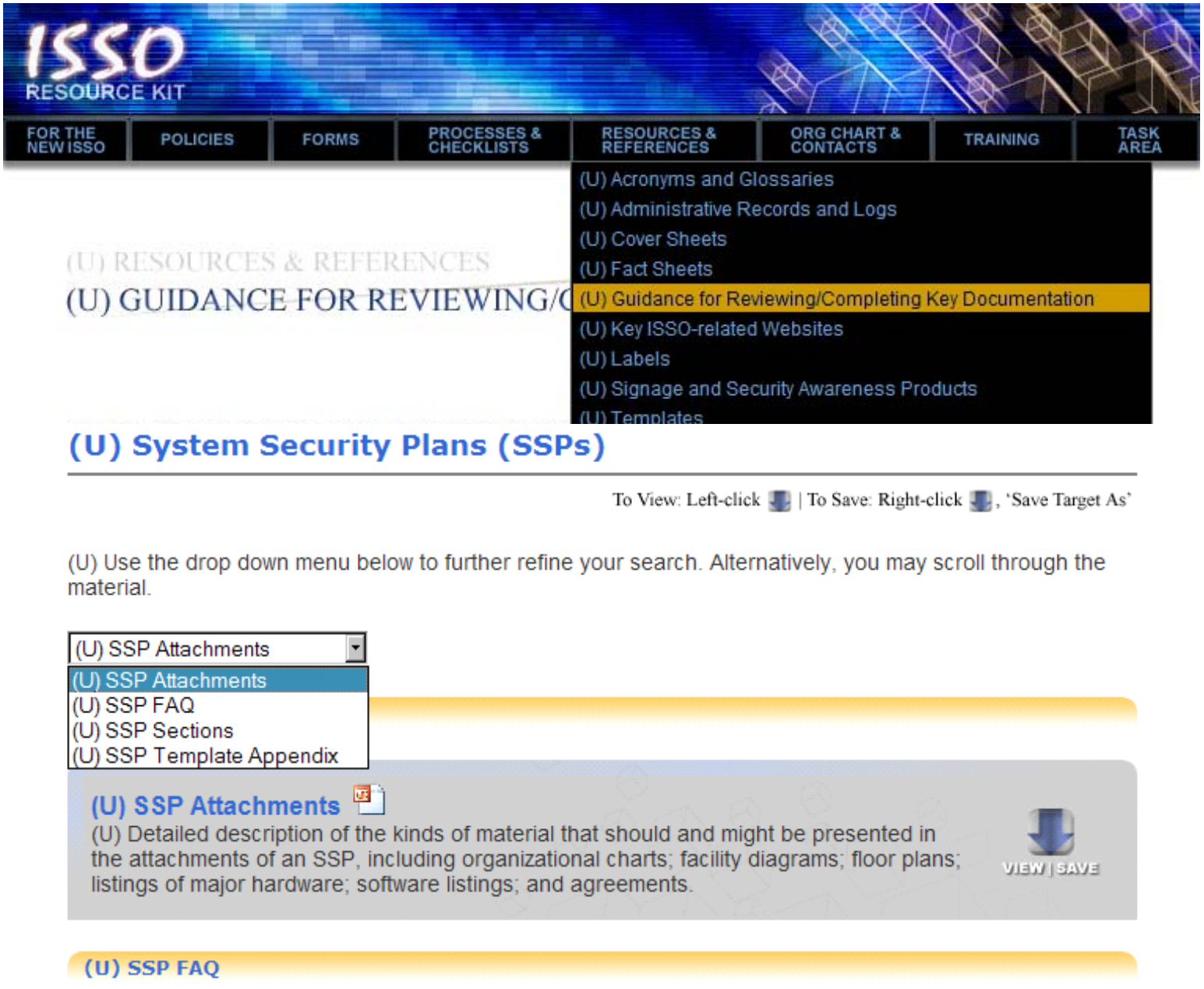
Authentication: Any security measure designed to establish the validity of an individual's eligibility to receive specific categories of information

ACKNOWLEDGEMENT:

"I understand and accept the special responsibilities incurred with my elevated permissions. I agree to comply with all applicable U.S. laws, national policies, and NRO information assurance directives, instructions, and procedures. I understand that deliberate or willful violation of this agreement may result in termination of my privileged access, removal from a position of special confidence and trust, suspension or revocation of my access to SCI, criminal prosecution, and/or termination of my employment."

The statement above appears in Attachment 2 of NROI 61-8-1, the implementation guidance for the NRO Privileged User Program. As a Privileged User, your acceptance of this statement and signature of acknowledgement is required prior to your receiving elevated permissions or associated passwords. If you have not signed this statement, or taken the Privileged User Program Acknowledgment Briefing CBT, please notify your ISSO, ISSM, or PSO.

Completing Key Documentation



7.2.3 Discuss procedures for assignment, distribution, and control of authenticators. **[I&A2]**

Narrative

Sections 7.2.3 through 7.2.9 should be completed by all SSP authors whose systems use passwords to control access.

[I&A2]: An Identification and Authentication (I&A) management mechanism that ensures a unique identifier for each user and that associates that identifier with all auditable actions taken by the user. The following must be specified:*

[*Alternate controls, such as biometrics or smart cards, may be used at the discretion of the DAA. These alternate methods may have similar requirements. For example, the electronically stored version or biometric authentication patterns need to be protected, as do password authenticators.]

- Initial authenticator content and administrative procedures for initial authenticator distribution.
- Individual and Group authenticators (Group authenticators may only be used in conjunction with an individual/unique authenticator prior to use of a group authenticator).
- Length, composition, and generation of authenticators.
- Change Processes (periodic and in case of compromise).
- Aging of static authenticators (i.e. not one-time passwords or biometric patterns).
- History of authenticator changes with assurance of non-replication of individual authenticators per direction in approved SSP.
- Protection of authenticators to preserve confidentiality and integrity.

In Section 7.2.3 describe how authenticators are assigned, distributed, and controlled.

Document the management mechanisms used to ensure the creation of a 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

Topically Organized 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

Demonstration Summary

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

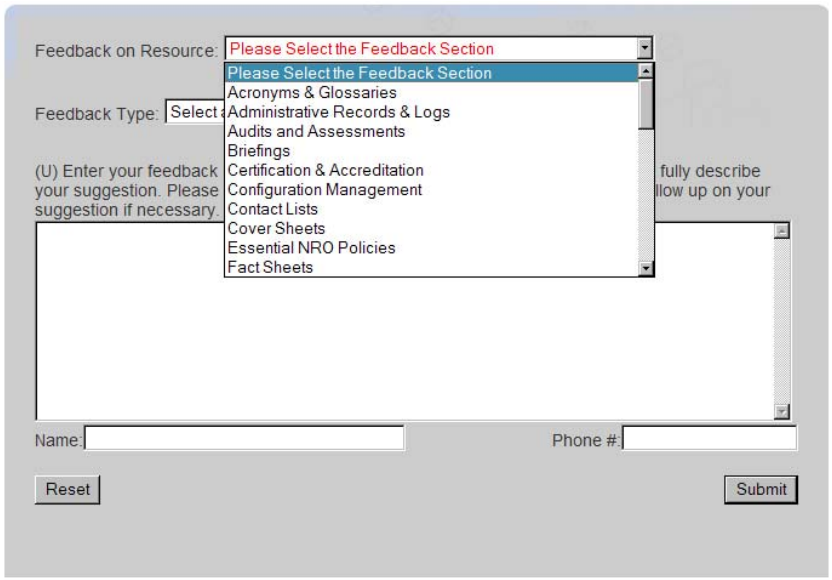
Keeping Current - User Suggestions

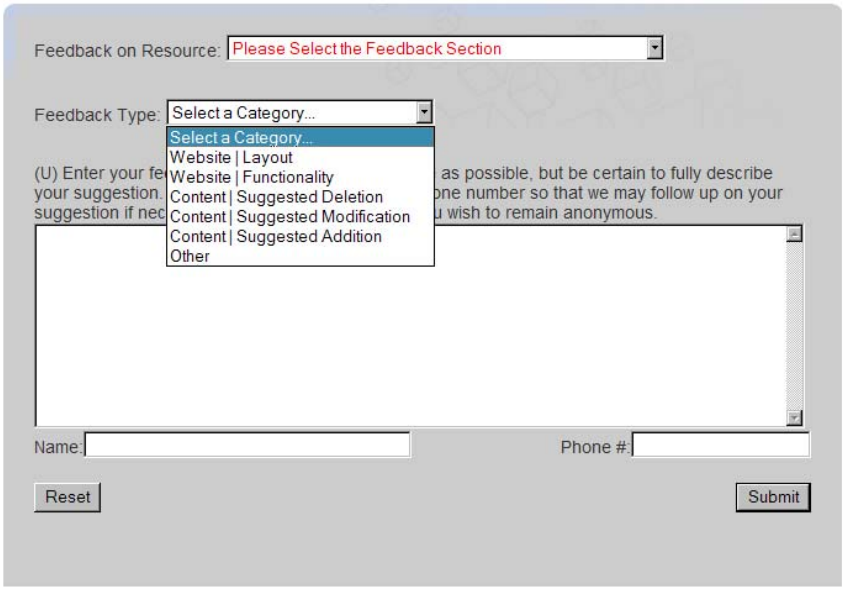
(U) SITE FEEDBACK

(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