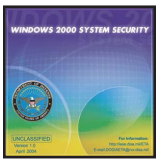
DOD Information Assurance Training & Awareness Products

Web Based Training (WBT)

NOTE: These products are web-deliverable, using html and Flash technology. They can be loaded on web servers for delivery via the Internet or intranet. As with our traditional products, they also run on a LAN or from a CD-ROM drive.



Windows 2000 Security
Date 04/04 – Ver 1.0

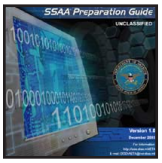
Windows 2000 Security details the steps required to safeguard Windows 2000 systems in a stand-alone or networked environment. This course is designed to provide personnel already familiar with the basics of network security in a Windows NT environment with information and skills necessary to implement security measures in a Windows 2000 environment. After completing the course, users will be able to perform the following tasks: Identify information system security standards (Common Criteria requirements); describe the built-in features of Windows 2000 that can be configured to meet Common Criteria requirements; configure user and group accounts for security; use Windows 2000 Security Policy tools for security configuration and management; use additional Windows 2000 security configuration tools to accomplish miscellaneous system administration tasks; use the Windows 2000 Security Templates and Security Configuration and Analysis tools to create or apply security templates; and configure their systems according to the Gold Standard. The target audience is assumed to have a minimum of one-year hands-on experience in network administration and systems security procedures, as well as, be able to install Windows 2000, set up a network, set up user accounts, and perform standard daily network administration tasks.

Firewall and Router Fundamentals
Date 04/04 – Ver 1.0

This course provides an overview of firewalls and routers and explains how they are used to protect information systems. The course opens with an introduction to networking, that presents basic information about network architectures and security issues. This module also describes the Defense in Depth (DID), model. The firewall module presents basic information about firewalls including the different types that can be implemented, the capabilities of firewalls, various firewall architectures that can be employed, and important considerations for implementing a firewall. The router module introduces routers and includes topics such as routing functionality, protocols, and security. The course can be taken in Track Mode, which allows the user to print a certificate of completion, or in Browse Mode, and can be used for reference.

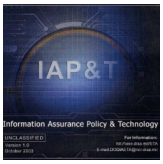
Critical Infrastructure Protection
Date 12/03 – Ver 1.0

The Critical Infrastructure Protection (CIP) WBT provides baseline CIP awareness to enhance the knowledge of DoD personnel in the front lines of defense, DoD and other government CIP planners, infrastructure owners, managers, technicians and users. This product provides an overview of what systems comprise the critical infrastructure, what CIP is, the national organizational structure of CIP, how DoD fits into the national CIP organization, and DoD CIP organizational structure and responsibilities. The course goes into detail on the DoD infrastructure sectors and special function components and concludes with the 6 phases of the CIP lifecycle.



SSAA Preparation Guide
Date 12/03 – Ver 1.0

The "SSAA Preparation Guide" contains guidance on completion of the System Security Authorization Agreement (SSAA) while accomplishing the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). After presenting an overview of the DITSCAP, this web-based product provides detailed guidance on the contents necessary to complete a SSAA, using the outline presented in the DITSCAP Application Manual, DoD 8510.1-M. The target audience for the product is information system certification team members, IAMs, IAOs, system administrators, and other personnel responsible for writing, processing, or reviewing SSAAs. This product is also useful for preparation of a SSAA using the National Information Assurance Certification and Accreditation Process (NIACAP), NSTISSI No. 1000.



Information Assurance Policy & Technology (IAP&T)
Date 10/03 - Ver 1.0

The Information Assurance Policy and Technology (IAP&T) CD-ROM / on-line training program has been created so that users of the program may successfully perform their duties as Information Assurance Officers/Managers (IAO/M) or System Administrators in accordance with DOD guidance pertaining to the defense of information systems (DODD 8500.1 & DODI 8500.2). Individuals assigned to duties involved with policy and oversight, inspection and audit, or other functions supporting the Information Assurance mission, e.g., prevention, detection and eradication of viruses; execution and evaluation of system audit records; access control; disposition of Information Systems (IS) media; and development and compliance with the risk managed approval of system operation (certification and accreditation) plans will find this course useful and meaningful. Depending on your Command, Service, or Agency, the completion of this online course could help the student meet the DOD and C/S/A standards for Level 1 System Administrator certification. This product updates and replaces the OISS CD.

Web Security
Date 06/03 - Ver 1.3

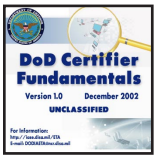
The Web Security web-based training (WBT) product is designed for DOD webmasters and others for use in the development and maintenance of websites for the DOD community. This interactive, multimedia training product covers legal issues, DOD policy and guidance, information protection, server side security and client side security. The audience for this product is System Administrators, Network Administrators, and users of the web, including web masters.

Database Security
Date 06/03 - Ver 1.1

This web-based course provides an overview of elements of database security. It is designed to provide training on Database Security for database administrators in training and general users. Topics covered in this course include: database structures and management systems, Structured Query Language (SQL), administration tools, and database security methods. In addition, the course covers database concepts and terms, discusses privileges and roles used in controlling data access, and introduces profiles and tablespaces, which are used to limit system resources. These individual elements are discussed as they are applied together in the database environment. The last module pulls together the concepts learned throughout the course and applies them to various security methods used to secure the database. The course provides a glossary of terms and resources with further information on Database Security.

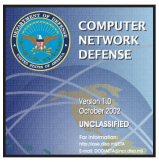
Active Defense: An Executive's Guide to Information Assurance
Date 02/03 - Ver 1.0

This interactive training course is intended for executives in Information Assurance who are the key decision-makers in building a security culture. The training serves as a strategic planning guide that introduces the issues and processes that must be understood in order to develop a strong commitment to protecting information resources. This course presents the goals of an information assurance program, explains why meeting these goals is essential to success, and distinguishes between the roles and responsibilities of all members of the organization. The course also explains how to identify and manage risks to information systems. Valuable checklists are provided at the end of each section.



DOD Certifier Fundamentals
Date 12/02 - Ver 1.0

The "DoD Certifier Fundamentals" web-based course, intended for technically expert students, identifies the place of the DoD system certifier in national cyber defense, presents system certifier job functions, reviews the DITSCAP, and discusses system certifier performance items in competency areas in the context of the four phases of the DITSCAP. This interactive course concludes with a professional enrichment segment placing information assurance in the "Rings of Protection" concept; discussing system life cycle and the DoD acquisition process; and reviewing laws and policy guidance relating to and references for certifiers.
Mapped CNSS (NSTISSI) 4015 National Standards



Computer Network Defense (CND)
Date 10/02 - Ver 1.0

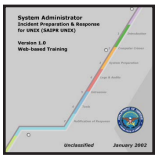
An overview of the protection of computer systems and networks, this interactive CD-ROM details Computer Network Defense (CND) in relationship to the Global Information Grid (GIG), Network Operations (NETOPS), and Information Assurance (IA). Topics include the CND activities performed by DoD and specific CND policies that guide these activities. The user will become familiar with the overall concept of CND.

Designated Approving Authority (DAA)
Date 05/02 - Ver 2.0

This interactive CD-ROM highlights the duties and responsibilities of the DAA (in industry, the Chief Information Officer (CIO) may have these responsibilities). The user will learn about members of the DAA's team, including the Information Systems Security Manager (ISSM), General Counsel, Program Manager, Information Systems Security Officer (ISSO), User Representative, and the Certification Agent. This presentation covers the Department of Defense (DOD) acquisition process, certification & accreditation (using the DOD Information Technology Security Certification and Accreditation Process (DITSCAP) as a representation), legal and regulatory issues, and risk management. Roles of team members are discussed throughout. A glossary of terms and a resources section with relevant web sites and documents are provided for reference. The information in this product can also benefit midlevel and senior managers.

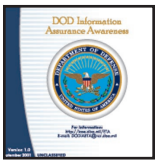
Federal Information Systems Security Awareness
Date 02/02 - Ver 2.0

Designed specifically for users of federal computer systems, this web based training product explains the importance of Information Systems Security. Topics include: threats and vulnerabilities, malicious code, user responsibilities, and new developments affecting Information Systems Security. Non-DOD government personnel should use this product as an alternative to DOD Information Assurance Awareness.
2002 Silver AXIEM Award



System Administrator Incident Preparation & Response for UNIX
Date 01/02 - Ver 1.0

This web based training product teaches users to prepare for and respond to information systems security incidents from a generic law enforcement perspective. Topics covered include: computer crimes, system preparation, logs and auditing, defensive tools, intrusions, and response notification and record maintenance. SAIPR UNIX is designed for individuals with three to five years of experience as System Administrators (SAs) or Information Systems Security Officers (ISSOs), and is follow up training to "UNIX Security for System Administrators."

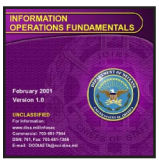


DOD Information Assurance Awareness
Date 09/01 - Ver 1.0

An updated version of DOD INFOSEC Awareness, this web based training product explains the components of Information Assurance, as well as the laws and policies designed to ensure it. In addition, DOD IA Awareness includes expanded sections to reflect the ever-changing world of information technology. Descriptions of Internal and External Threats to Information Systems, new information about technology specific vulnerabilities, and an additional focus on the Internet, including detailed discussions of email, Macro Viruses, Hoaxes, and Distributed Denial of Service (DDOS) attacks bring this product into the 21st century.

Information Assurance in Defense in Depth
Date 08/01 - Ver 1.0

Based on the Joint Vision 2020 concept of Information Superiority, and intended for military and civilian personnel responsible for the defense of DOD computers and computer networks, this web based training product explains the concept of "Defense in Depth." Using the multi-dimensional defenses of a mediaeval castle as a model, this presentation demonstrates the importance of a layered defense, which integrates the capabilities of People, Operations, and Technology. The user will learn how to defuse, detect, and react to a wide range of threats to networks, enclave boundaries, local computing environments, infrastructure support, and emerging technology.

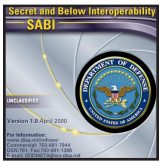


Information Operations (IO) Fundamentals
Date 02/01 - Ver 1.0

IO Fundamentals provides an overview of IO in the joint context throughout the range of military operations. It addresses IO principles relating to both offensive and defensive IO and describes responsibilities for planning, coordinating, integrating, and deconflicting joint IO. This product is based on Joint Publication 3-13, "Joint Doctrine for Information Operations." IO Fundamentals is an update and expansion of INFOWAR Basics.

Windows NT Security
Date 02/01 - Ver 1.0

Windows NT Security details the steps necessary to safeguard system resources in a stand-alone or networked Windows NT operating environment. It provides virtual hands-on exercises to reinforce instruction of key security features. The target audience for the product is system administrators, ISSOs, and other personnel responsible for information systems administration. The user should have a basic hands-on understanding of computer systems and applications. The Resources section contains a library of Windows NT security documents to support and augment the content and exercises in the modules. There are also links to web sites related to Windows NT security.



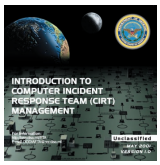
Secret and Below Interoperability (SABI)
Date 06/00 - Ver 1.0

This product explains SABI, a network-centric process that incorporates risk management into all decisions for secret and below connectivity. It discusses the core functions and goals that have been established for the SABI process. The roles and responsibilities of the SABI community are addressed in detail.

UNIX Security for System Administrators
Date 06/00 - Ver 1.1

This product provides a basic understanding of UNIX Security. It is designed to help the beginning to inter-mediate-level administrator understand what makes up a secure UNIX system, what tools exist to protect the system, and provide assistance in the day to day tasks of monitoring and securing the network. At the completion of this course, the user will understand different UNIX environments and their origin, various UNIX threats and appropriate countermeasures, and basic encryption and security concepts. In addition, the user will learn fundamental system administration concepts, including basic commands, specific tools, network maps, sniffers, and network vulnerabilities. The resources section features links to relevant computer security web sites and a glossary of terms. Virtual hands-on exercises are provided throughout. While the exercises are based on Solaris, comparable commands in Linux Red Hat and HP-UX are demonstrated.

CD-ROMs

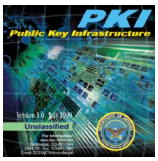


Introduction to Computer Incident Response Team (CIRT) Management
Date 05/01 - Ver 1.0

This is an interactive CD-ROM intended for CIRT managers and others responsible for computer security. The user will learn how to set up and manage a CIRT, and how to handle and report computer security incidents. Procedures for hiring CIRT personnel, tools for preventing and dealing with incidents, and CIRT reporting requirements, including an explanation of IAVAs (Information Assurance Vulnerability Alerts) and INFOCONs (Information Operations Conditions), are among the topics covered. The CD-ROM also includes review exercises that highlight customer service, different types of network attacks, and incident priority.

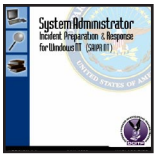
CyberProtect
Date 07/99 - Ver 1.0

CyberProtect is an interactive computer network defensive exercise with a video game look and feel. It is intended to familiarize players with information systems security terminology, concepts, and policy. Players learn about defensive security tools, which must be judiciously deployed on a simulated network. They then face a spectrum of security threats and must make practical decisions for allocating resources (in quarterly increments) using the elements of risk analysis and risk management. Play is divided into four sessions (simulating a fiscal year). After each session, players receive feedback on how well they are doing. At the end of the last session, players are given a report detailing their cumulative operational readiness rating. The report also details every attack by type, origin, and effectiveness of defensive tools.
1999 NewMedia Gold INVISION Award (Best Overall Design)
1999 NewMedia Gold INVISION Award (Technical Training)
1999 International Cinema in Industry (CINDY) Competition Silver Award



Public Key Infrastructure (PKI)
Date 07/99 - Ver 1.1

This multimedia CD-ROM introduces PKI—what it is and the security services it provides. PKI user roles are discussed, including the functions of the Registration Authority (RA), Local Registration Authority (LRA) and the End User. User Registration is covered, as well as the generation and use of certificates and keys. The Resources section has points of contact for help with PKI, including useful web sites and PKI-related documents and templates. There is also a glossary of terms for reference.



System Administrator Incident Preparation & Response (SAIPR) for Windows NT
Date 07/99 - Ver 1.1

SAIPR is an interactive multimedia training CD-ROM. It provides a virtual hands-on experience, taking the student through the steps necessary to configure networks to collect and protect event information that may be useful in an investigation of suspected unauthorized activity. The user will learn about techniques used to commit computer crimes; what information to collect prior to an incident; how to prepare systems for a possible incident; how to implement policies; how to log and recognize unauthorized activity; and how to respond to suspected unauthorized activity. Other topics covered include policies and procedures to simplify a computer emergency investigation, audit strategy, audit implementation, recognizing unauthorized activity, and notification and response strategies for security incidents. A glossary of terms and links to Service/Agency Computer Emergency Response Teams are provided for reference. This CD-ROM is a product of the DOD Computer Investigations Training Program (DCITP).

Introduction to the DOD Information Technology Security Certification & Accreditation Process (DITSCAP)
Date 03/99 - Ver 1.2

This interactive CD-ROM provides the user with an overview of the DITSCAP, including its definition, the evolution of information systems security, and roles and responsibilities. Modules 2 through 5 cover Definition, Verification, Validation, and Post-Accreditation. All modules include an overview of topics covered, a description of process activities, and individual, team, and group roles and responsibilities.

Videos

Information Assurance Compilation Series 1:

Bringing Down the House (US Govt)
This video describes various hacker intrusions and how they relate to Information Warfare. The main portion of the video covers how hackers use the information superhighway to access systems. (10 minutes)

Computer Security 101 (DOJ)
John Walsh of America's Most Wanted hosts this video about safeguarding computer information. Three aspects of computer security are discussed: sensitive information (what kind of information needs to be protected), risk management (reasons why computer security is important), and accountability (assuming responsibility for protecting one's computer). (11 minutes)

Computer Security, The Executive Role (DOJ)
This video stresses the need to protect information systems at all levels of government. The user should be aware that the Office of Management and Budget (OMB) has classified all federal information as "sensitive." To this end, steps to secure workspaces and protect data are delineated. Topics covered include the Computer Security Act of 1987, types of threats to information systems, and risk management. (9 minutes)

Dr. D. Stroye (US Govt)
This video discusses correct methods for magnetic media destruction, while providing humorous examples of how not to safely destroy data. (8 minutes)

The Information Frontline (US Govt)
This video on Defensive Information Warfare (IW-D) awareness demonstrates how information is easy to exchange but difficult to protect, the types of IW threats that exist, and the vulnerabilities of information systems. Also describes intelligence agencies that perform IW-D functions. (10 minutes)

Networks at Risk (US Govt)
This video, produced by NCS, deals with hackers, network intrusion, and computer security in the workplace. Topics covered include the selling of electronic information, prevention of network intrusions, password protection, and the importance of auditing network security. (10 minutes)

Protect Your AIS & Protect Your AIS, The Sequel (US Govt)
These videos contain INFOSEC-related dramatizations of security concerns in the workplace. These sketches demonstrate the need for password protection, virus prevention, safeguarding data, user ID security, and controlled access to computer equipment. (51 minutes)

Safe Data: It's Your Job (DOL)
This video is relevant to DOD because it focuses on the need to safeguard sensitive but unclassified data, such as medical records and personnel files. It discusses ways to secure data to prevent sensitive information from getting into the wrong hands. The role of the end user in computer and network security is emphasized. Tips for preventing data from being compromised by hackers and unauthorized users, such as good password management, virus protection, and physical security are also provided. (19 minutes)

The Scarlet V (US Govt)
This video discusses the need to use virus-scanning software on a regular basis to prevent file infection. The segment parodies the life of the individual who inadvertently introduces a virus into a networked system. (7 minutes)

Think Before You Respond (NRO)
This video deals with Internet security, stressing the need to be careful about what information you provide over this medium. Internet users should use caution when discussing topics in live chat sessions or when responding to requests for information. (3 minutes)

Information Assurance Compilation Series 2:

Bad Characters (US Govt)
Logon to the Internet and your computer sends out information about you: your browser type and version, your network address, your operating system software. Some websites may be set up to track your activities and even take over your computer. Such sites could actually be fronts for information gathering by extremists groups and foreign operatives hostile to the US Govt. In three vignettes, this video depicts how the use of embedded codes (bugs) and other techniques allow these groups to glean a wealth of information from one quick website visit. Fortunately, such activity can be easily thwarted. This video explains specific steps ou can take to increase Net security and protect against "bad characters". (9 minutes)

Bits & Pieces (US Govt)
This humorous video follows the exploits of Agent 000 on his bungled attempts to access proprietary information; that is until he discovers computer hacking as a means to obtain "bits and pieces" of information. (5 minutes)

Ears Looking at You (US Govt)
Security Officers Joe January and Frank Jones (think "Dragnet") investigate the security vulnerabilities of cellular phones. Cellular phones act as receivers/transmitters and January and Jones know they can be a security threat to classified or proprietary information. (8 minutes)

Identity Theft: Protect Yourself
Information technology continues to alter the way in which personal information can be compromised or stolen. With the number of cases involving identity theft continuing to increase, this video assists individuals in gaining a better awareness and understanding of privacy-related issues within the private and public sectors. Topics include prevention and protection of identity information on the Internet, postal mail, and banking transactions, as well as guidance for victims of identity theft. This video also provides a variety of Internet links to many other authoritative and informative sources of privacy protection information, in addition to information on various Federal guidelines about privacy. (12 minutes)

Just the Fax, Sir (US Govt)
Security Officers Joe January and Frank Jones investigate security risks associated with the use of fax machines. As faxes are part of life in the workplace, care needs to be taken when using them to send and receive information; January and Jones help clear up the confusion. (8 minutes)

Magnificent Discretion (US Govt)
This video stresses the importance of maintaining high standards of information security, especially when working or surfing the web at home. (5 minutes)

Sherman on My Mind (US Govt)
This humorous video examines the issue of personal projects at the workplace. As they each waste time with personal projects, four different employees are reminded of Sherman, a former employee who lost his job because of unauthorized side projects. (11 minutes)