

# DOD Information Assurance Training & Awareness Products

To order our products, please go to the following website:  
<http://iase.disa.mil/eta>

## 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. A PKI Cert is required for some of the training products.

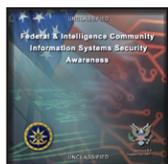
### IA Awareness Training



#### **CyberAwareness Challenge (Information Assurance / Systems Security Awareness for DoD Personnel and Members of the Federal Community)**

**Date 10/12 – Ver 1.0**

The CyberAwareness Challenge is a serious game that simulates the decisions that Federal government information system's users make every day as they perform their work. Rather than using a narrative format, the Challenge presents information assurance (IA) and information systems security (ISS) awareness instructional topics through first-person simulations and mini-games that allow the user to practice and review IA/ISS concepts in an interactive manner. The introduction explains that, in this role, information systems users are responsible for protecting sensitive and classified information and the information system on which this information resides. The introduction also orients users to the types of decisions they are expected to make throughout the Challenge including, understanding the scoring mechanisms. As a user makes these situational decisions, the user is introduced to threats associated with identity theft, spyware, malicious code, and phishing, as well as what to do when encountering classified or sensitive documents on the Internet and the importance of maintaining information security situational awareness when out of a secure area. Users learn security concepts they need to practice in their daily routine at work, while teleworking, and on their home systems. (1 hr)



#### **Federal and Intelligence Community Information Systems Security Awareness**

**Date 09/11 – Ver 5.0**

This training presents a separate Intelligence Community user course, covering classification and handling of Sensitive Compartmented Information (SCI).

#### **For Members of the Federal (Non-Intelligence) Community:**

The Federal Information Systems Security Awareness version 5.0 training has been replaced by the CyberAwareness Challenge version 1.0 product. Please reference the CyberAwareness Challenge product description above for more information.

#### **For Members of the Intelligence Community:**

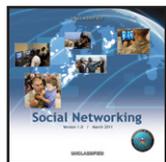
This web-based product presents the fundamentals of information systems security for the Intelligence Community (IC) user, to include the proper classification, marking, and handling of Sensitive Compartmented Information (SCI) within a SCI Facility (SCIF) environment. Precautions in secure SCI custody, transmission, and information sharing are reviewed. This interactive course highlights the dangers associated with the insider threat, social engineering, and peer-to-peer applications in a clear and understandable format. The concept of Malicious Code is introduced, including its impacts and the methods it uses to infect information systems. The course identifies important guidelines that define the sensitivity levels of information, including personally identifiable information (PII), and the IC user's role in protecting this information. Also explained are the threats associated with identity theft, spyware, and phishing, as well as what to do when encountering classified or sensitive documents on the Internet. New material includes guidance on the importance of maintaining information security situational awareness when out of a secure area. Security tips are provided for the user to practice in the daily work routine and at home. (1.5 hrs)



### Smartphones and Tablets

**Date 03/13 – Ver 2.0**

This training is packaged as a single product containing modules on general user awareness, platform specific guidance, and device administrator training. The “Awareness” course provides learners with information about the security risks and vulnerabilities associated with using smartphone and tablet devices. The “User” course will provide users of government-provided and government-authorized smartphones and tablets with a greater awareness of the security risks and vulnerabilities associated with three platforms of government-authorized mobile devices: Google Android, Apple iOS, and RIM BlackBerry and PlayBook. The “Administrator” course will provide specific guidelines that administrators of government-provided devices must follow to protect the mobile devices that they administer, the data on these devices, and the networks and data that these devices can access. (1 hr)



### Social Networking

**Date 03/11 – Ver 1.0**

This interactive presentation provides an introduction to social networking for Department of Defense (DoD) information system users. The presentation acknowledges the positive aspects of social networking, but also familiarizes users with some of the risks associated with social networking services, especially as military, civilian, or contractor members of the DoD. Particular emphasis is placed on the guidance for and limitations on personal use of social networking on DoD information systems. Practical experience is used to assist users with making informed choices on issues encountered when creating an online profile on a fictional social networking service. This training concludes with a brief summary of the dos and don'ts of social networking for DoD members, particularly on government computers. The information in this product can also benefit user's friends and family members. (30 min)



### Using Public Key Infrastructure (PKI)

**Date 12/09 – Ver 1.0**

This training presents separate PKI Overview and Using PKI Certificates courses, each with its own course completion certificate.

Upon completing the PKI Overview course, Department of Defense (DoD) information systems users will be able to identify what PKI is and why it is important to the DoD, as well as which pieces of Congressional legislation, Federal policy, and DoD guidance mandate the use of PKI. This presentation identifies the different components of PKI and how they are implemented in the DoD. Details discussed include systems, software, PKI credentials, certificates, and keys. DoD users will learn how to use PKI to log on to unclassified DoD networks and access DoD information systems, applications, and websites; as well as how to use PKI to send and receive e-mails securely. Users will understand what the Common Access Card (CAC) is, why they use it, and how and when to obtain or return a CAC. DoD users will be informed on what system elements are needed to use their CAC, to include what a CAC personal identification (PIN) number is and what to do if they forget their CAC PIN. (1 hr)

When DoD information system users have completed the Using PKI Certificates course, they will understand how to safely and securely authenticate their identity to access DoD unclassified networks using the PKI certificates contained on their Common Access Card or Alternate Token. DoD users will also learn how to use their PKI certificates to authenticate their identity to DoD systems, applications, and restricted web sites. In addition, DoD users will know how to validate digital signatures, as well as how to send and receive e-mail securely using their PKI certificates to encrypt the e-mail, when necessary. Finally, they will be able to identify how to read an e-mail that was encrypted using expired certificates taken from a previous CAC. (1 hr)



### Portable Electronic Devices / Removable Storage Media

**Date 03/11 – Ver 2.0**

In this presentation, Department of Defense (DoD) information systems users will learn about significant security risks associated with portable electronic devices (PEDs), and removable storage media. Users will also learn which types of PEDs and removable storage media are of greatest concern to the DoD. Removable storage media is clearly defined, and users will gain a better understanding of exactly what portable electronic devices are. New restrictions on the use of PEDs and removable storage media are introduced, and users will learn what must be done to mitigate the security risks to DoD data, to include DoD policy regarding data encryption, stored on these devices. Users will have an opportunity to test their knowledge of DoD policy relating to storage and processing DoD Information using PEDs. (20 min)



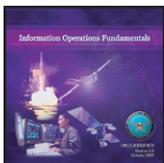
**Phishing**  
**Date 03/12 – Ver 2.0**

This interactive training explains what phishing is and provides examples of the different types of phishing, to include spear phishing, targeting specific groups or individuals, and whaling, targeting senior officials. Phishing techniques such as deceptive e-mails and web sites, as well as browser “tab nabbing,” are discussed. Guidelines are provided to help users to recognize phishing attempts, so that appropriate actions may be taken to avoid these attacks and their consequences. The training explains that phishing is a serious, high-tech scam and that system users are the best line of defense against phishing. Further, the training illustrates why users should always be on the lookout for phishing attempts, even from people from within their own organization. (30 min)



**Identifying and Safeguarding Personally Identifiable Information (PII)**  
**Date 03/13 – Ver 2.0**

This training starts with an overview of Personally Identifiable Information (PII), and protected health information (PHI), a significant subset of PII, and the significance of each, as well as the laws and policy that govern the maintenance and protection of PII and PHI. The course is designed to prepare DoD and other Federal employees to recognize the importance of PII, to identify what PII is, and why it is important to protect PII. The Federal government requires the collection and maintenance of PII so as to govern efficiently. However, because PII is sensitive, the government must take care to protect PII, as the unauthorized release or abuse of PII could result in potentially grave repercussions for the individual whose PII has been compromised, as well as for the federal entity entrusted with safeguarding the PII. This course explains the responsibilities for safeguarding PII and PHI on both the organizational and individual levels, examines the authorized and unauthorized use and disclosure of PII and PHI, and the organizational and individual penalties for not complying with the policies governing PII and PHI maintenance and protection. This training is intended for DoD civilians, military members, and contractors using DoD information systems. This course may also be used by other Federal Agencies. (1 hr)



**Information Operations (IO) Fundamentals**  
**Date 10/07 – Ver 2.0**

IO Fundamentals provides an overview of the military’s need for information, how information operations (IO) helps achieve information superiority, and the vital role IO plays in Joint Force operations. This web and computer based (WBT/CBT) course explains what IO is, why it is important, and how IO differs from other DoD activities that involve information. The course also explains the core IO capabilities, the capabilities that support or are related to IO, what an IO cell is, and identifies who is responsible for implementing IO. In addition, this course identifies the key challenges and considerations that must be understood and assessed when planning IO. This product is based on Joint Publication 3-13. (2 hrs)



**Information Assurance Awareness Shorts**  
**Date 01/09 – Ver 3.0**

This product contains specific information related to the topics listed below.

**Insider Threat Short** provides awareness about the Insider Threat and the employee behaviors that may signify the potential to be an insider threat. (15 min)

**Telework Short** introduces the basic concept of telework and covers the fundamental procedures and basic operating guidelines for doing telework from both a government Telework Center and from the home. (15 min)

**Wireless Security Short** introduces basic concepts in wireless networking security and allows the user to explore the security risks inherent in different network configurations. (15 min)

**Passwords Short** introduces the importance of complex passwords, including the requirements for creating a password as well as hints for remembering these passwords. (20 min)

**Peer-to-Peer Short** provides an in-depth treatment of P2P threats and the OMB and DoD guidance on P2P for Department of Defense personnel. (20 min)

**Social Engineering Short** explains what social engineering is, gives examples of social engineering techniques, describes the possible consequences of social engineering, and provides guidelines to enable the user to recognize and deal with social engineering. (20 min)

## IA Training for Senior Leaders



### **Designated Accrediting Authority (DAA)**

**Date 01/13 – Ver 10.0**

This interactive training provides an understanding of the roles and responsibilities of the DAA. The user will learn about important issues associated with the DAA's responsibilities and the key players that interact with the DAA, including the Principal Accrediting Authority, Chief Information Officer, Certifying Authority, Program Manager, User Representative, Information Assurance Manager (IAM), and Information Assurance Officer (IAO). This presentation also provides legal guidance relating to information system security, to include Congressional legislation, as well as Federal and Department of Defense, or DoD, policy. An overview of DoD certification and accreditation, to include details on the DoD Information Assurance Certification and Accreditation Process (DIACAP) is provided. The DAA's responsibilities concerning system connection and the DoD IA Workforce Improvement Program are reviewed. Content contains update material on IA Workforce Specialty Categories, guidance on social networking issues, handling of leaked Government documents on the web, and information on the forthcoming Federal Risk Management Framework (RMF). The information in this product can also benefit mid-level and senior managers. (3 hrs)

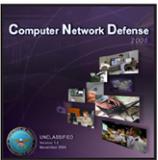


### **IA Briefing for Senior Operational Leaders**

**Date 03/10 – Ver 1.0**

The Information Assurance (IA) Briefing for Senior Operational Leaders presents five short scenarios based on problems observed during operations, with the actual or possible consequences that could result from the actions that caused the problems. You, as the senior leader, are challenged to consider how your planning, action, and response could lessen or eliminate these vulnerabilities. (30 min)

## IA Training for IA Professionals



### **Computer Network Defense (CND)**

**Date 12/06 – Ver 2.0**

This product is designed for high-level managers who need to acquire a Computer Network Defense Service Provider (CND SP) for their organization, information assurance (IA) professionals who want to transition into a CND SP career path, and individuals who desire a general knowledge of computer network defense (CND) and CND SPs. This interactive web-based training defines CND, identifies CND requirements for DoD components, key requirements that CND SPs must meet, and the principal services provided by CND SPs. This training presents a high-level explanation of the certification and accreditation (C&A) process for CND SPs. The CND SP principal services are enumerated, to include system protection services, anti-virus, system scanning tools, Information Operations Conditions (INFOCON) Program support, Information Assurance Vulnerability Management (IAVM) support, vulnerability assessment monitoring, analysis, and detection services, as well as incident response. An explanation of the training and future certification requirements for those who work as CND SPs is also included. (1 hr)



### **DoD Information Assurance Certification Accreditation Process (DIACAP)**

**Date 01/09 – Ver 1.0**

This training presents separate DIACAP Overview and DIACAP Implementation courses.

In the DIACAP Overview course, you will learn that Department of Defense (DoD) information systems, in order to operate, must be certified and accredited, using a standard set of activities defined within the DoD Information Assurance Certification and Accreditation Process, or DIACAP. You will also learn about the DIACAP's purpose, objectives, and implementation, as well as the crucial role that enterprise risk management plays in the certification and accreditation process. DIACAP roles and responsibilities will be explained, to include the DoD enterprise governance structure, DoD Component responsibilities, and DIACAP implementation responsibilities. Further, you will be introduced to the key components of the five DIACAP activities used for DIACAP implementation. Finally, you will learn about transition to the DIACAP from the previous DoD Information Technology Security Certification and Accreditation Process, or DITSCAP. (1 hr)

The DIACAP Implementation course is designed for IA professionals responsible for implementing or involved in supporting activities in different capacities in the certification and accreditation, or C&A, of Department of Defense (DoD) information systems. You will learn about the complete DoD Information Assurance Certification and Accreditation Process, or DIACAP, and how the contents of the DIACAP package are generated. This instruction covers, in detail, the five activities of the DIACAP and the tasks that occur within each DIACAP activity. How to access the tools and resources used to execute DIACAP tasks is illustrated. Finally, the course walks through the roles of the key players involved in implementing the DIACAP activities and tasks that lead to the certification determination and accreditation decision that are needed in order to operate a DoD information system. (1 hr)



### Enhancing Information Assurance through Physical Security

**Date 10/07 – Ver 1.0**

This interactive course is designed for employees needing a general awareness of how the Department's Information Assurance (IA) program is enhanced through physical security. The course consists of four sections. The first section discusses the discipline of physical security, defines terms, and looks at site selection, physical perimeter, and facility controls. The second section describes some of the threats and vulnerabilities involved in protecting the Department's IA, as well as ways to protect the resources. The third section defines the various types of equipment, and addresses what some of the risks are in using them. The last section introduces policy and best practices for protecting the Department's equipment and information. (2 hrs)



### Information Assurance/Computer Network Defense Information Sharing

**Date 03/10 – Ver 1.0**

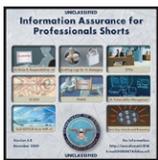
The Information Assurance (IA)/Computer Network Defense (CND) Information Sharing course is designed to instruct students on the processes and policies involved when attempting to share computer network defense information with coalition partner nations. This course explores the methods and techniques required for implementing an information sharing program. The course defines information sharing and the concept of valuable information. Course material then identifies the types of barriers to effective information sharing, as well as describing approaches to overcoming these barriers. (30 min)



### Information Assurance for DoD Auditors and IGs

**Date 03/10 – Ver 2.0**

This interactive web-based training introduces the role of the auditor and inspector in information assurance (IA) in the Department of Defense (DoD), to include practical challenges concerning the protection of DoD information systems. This training emphasizes the importance of IA to the DoD's mission, key DoD IA operational roles, and Federal Government, as well as DoD, legal and policy guidance for IA. Use of IA and IA-enabled technology in compliance with the International Common Criteria is detailed. Application of mission assurance category (MAC) and confidentiality level for a DoD information system and enclave is explained. The presentation includes an overview of certification and accreditation of information systems in the DoD, with an amplifying discussion of DoD risk management validation. The basic principles of DoD connection approval processes are addressed. The training concludes with a practical exercise using an audit or inspection of a DoD organization at a forward-deployed location to review the knowledge and IA audit techniques presented. (8 hrs)



### Information Assurance for Professionals Shorts

**Date 12/09 – Ver 5.0**

This product contains specific information related to the topics listed below.

**IA Roles and Responsibilities Short** introduces the Information Assurance hierarchy, including the roles and responsibilities of key leadership positions as well as the responsibilities of all Authorized Users. (25 min)

**Auditing Logs for IA Managers Short** introduces the auditing responsibilities of IA Managers. It describes the audit log and event information displayed by the system's auditing software. (20 min)

**Security Technical Implementation Guides (STIGs) Short** introduces the purpose and uses of STIGs. (20 min)

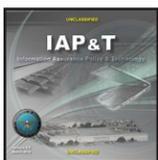
**SCADA Short** describes how Supervisory Control and Data Acquisition systems function and significant cyber-security issues associated with DoD SCADA systems. (15 min)

**FISMA Short** explains what the FISMA is, why it is important, how it is implemented within the Federal government and the DoD, and identifies where to obtain guidance for FISMA responsibilities. (20 min)

**IA Vulnerability Management Short** describes the vulnerability management process in DoD and the tools that support the process. (20 min)

**The DoD 8570.01-M IA WIP Short** presents an overview of the IA Workforce Improvement Program, defines the DoD IA workforce, and outlines the IA workforce training and certification requirements. (1 hr)

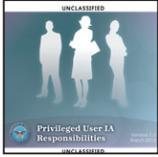
**The Zero Day Attack Short** provides an introduction to the steps an IA professional needs to follow if they suspect that their system has been compromised by an attack which otherwise is unknown to the IA technical community (aka Zero Day Attack). (20 min)



### Information Assurance Policy & Technology (IAP&T)

**Date 03/10 – Ver 5.0**

The Information Assurance Policy and Technology (IAP&T) training has been created for Information Assurance Officers (IAOs), Information Assurance Managers (IAMs), and System Administrators (SAs) to aid them in successfully performing their duties in accordance with DoD guidance, pertaining to the defense of DoD information and DoD information systems. Individuals whose duties include IA policy and oversight, inspection and audit, or other functions supporting the Information Assurance mission 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 standards for Level 1 System Administrator certification. This product updates and replaces the IAP&T dated 01/09, version 4.0. (4.5 hrs)



### **Privileged User IA Responsibilities**

**Date 03/13 – Ver 1.0**

Developed to be used in conjunction with annual DoD information assurance (IA) awareness training, this course presents the additional IA responsibilities for DoD information system users with access privileges elevated above those of an authorized user. The course identifies key terminology describing elevated user privileges, specific ethical and legal IA responsibilities of a privileged user, and DoD Public Key Infrastructure (PKI) responsibilities of a privileged user. Privileged user general IA responsibilities and restrictions covered include: reporting requirements, restricted and prohibited actions, protecting sensitive information, and the consequences of failure to comply. The PKI responsibilities of privileged users portion of the course reviews general rules for PKI credential use by privileged users, as well as general configuration guidelines for public key enabling of DoD information systems. The course stresses use of appropriate PKI tokens by privileged users for PKI identification and authentication, in addition to ensuring that the system correctly maps PKI certificates to an account with a set of associated privileges. The training delineates the seven sensitivity levels the DoD has defined for sensitive Unclassified and Secret information. These sensitivity levels, in combination with the environments from which users may access the information, are used to determine acceptable types of authentication credentials based on the credentials' strengths. (30 min)

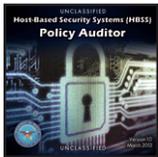


### **Security Requirements Guides (SRGs) & Security Technical Implementation Guides (STIGs)**

**Date 01/13 – Ver 1.0**

This presentation defines Security Requirements Guides (SRGs) and Security Technical Implementation Guides (STIGs) in the context of how these documents provide mandatory guidance for cyber security configuration practitioners and software developers. This course describes how SRGs provide general security compliance guidelines, which serve as source guidance documents for STIGs, which document applicable DoD policies and security requirements for specific technical products, as well as best practices and configuration guidelines. The training discusses the four Core SRGs that are the highest level SRGs, providing general security guidelines for operating systems, network infrastructure, applications, and non-technical policy controls. Core SRGs contain all security requirements for their specific technology and policy areas. Technology SRGs are subordinate to the Core SRGs. Technology SRGs do not refer to a specific product or product version, but contain all requirements that have been flagged as applicable from the parent level Core SRGs. The technology SRGs, in turn, provide the basis for product-specific STIGs. This training concludes by describing how SRGs and STIGs are developed and what role the STIG Community has in their development, as well as how users may join the STIG Community and participate in SRG and STIG development. (20 min)

## **IA Technical Training**



### **Host-Based Security Systems (HBSS) Policy Auditor**

**Date 03/13 – Ver 1.0**

This interactive course is designed for the Host Based Security System (HBSS) auditor and others with roles related to conducting HBSS system audits. The goal of the course is to equip users with a working knowledge of the functionality of HBSS Policy Auditor and its operational capabilities within DoD information networks. Topics covered in this course are responsibilities by HBSS role, procedures to successfully implement HBSS Policy Auditor, strategies to effectively implement HBSS Policy Auditor in the DoD environment, and processes to successfully execute the functions of HBSS Policy Auditor. (1 hr)



### **Introduction to DoD Intrusion Detection System (IDS) Analysis**

**Date 03/11 – Ver 1.0**

This interactive presentation is designed for newly appointed DoD Intrusion Detection System analysts. This course takes each student through a series of lessons which range from basic computer security concepts to real world IDS analyst examples. It focuses on what the IDS analyst should look for when investigating suspicious IDS alert logs while defending DoD networks. The topics covered in this course are: IDSeS and the DoD; Networking Fundamentals; IDS Overview; Implementing IDSeS; and Advanced Concepts in Incident Detection. Students are advised to review such concepts as TCP/IP and the OSI model prior to taking this course. (3.5 hrs)



### **DoD Intrusion Detection System (IDS) Analysis Part 2**

**Date 01/12 – Ver 1.0**

This interactive presentation is designed for DoD Computer Network Defenders that regularly review CND tool logs and network data. This course takes the student through a series of lessons which range from a description of tools to perform intrusion analysis on raw network packet data to techniques for identifying malicious traffic. The focus is on what a CND analyst should be looking for when investigating the alert logs of CND tools while defending DoD networks. The topics covered in this course are: Sniffers; Wireshark and the Analysis Process; Client-Side Attacks; and Bots and Botnets. It is recommended that students complete the *Introduction to IDS Analysis* WBT before taking this course. (3 hrs)



### **IDS Analysis Part 3, CND Analysis: A Structured Approach to CND Analysis**

**Date 01/13 – Ver 1.0**

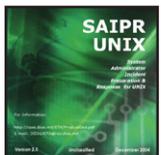
This training is packaged as a single product containing two distinct courses, CND Analysis: A Structured Approach to CND Analysis and DoD Intrusion Detection Systems: Custom Rules. The “CND Analysis” course is for DoD Computer Network Defenders, from the novice analyst to the most advanced, to clarify the role of the CND analyst and provide a methodical approach that they can use in conducting CND analysis. The “Custom Rules” course is designed for Computer Network Defense Infrastructure Support (CND-IS) specialty or other personnel contributing to the administration of IDS rule sets. The goal of the IDS Analysis Part 3 training is to clarify the role of the CND analyst and to propose a framework to use in conducting CND analysis that would be adaptable to their unique work environments. It is recommended that students complete the Introduction to IDS Analysis WBT and DoD Intrusion Detection System (IDS) Analysis Part 2 before taking this course. (2 hrs)



### **IDS Analysis Part 4, CND Analysis: Incident Analysis and Response**

**Date 03/13 – Ver 1.0**

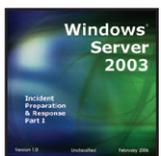
This course is for Computer Network Defense (CND) analysts and members of contractual organizations employed by the DoD to further equip CND analysts with the knowledge and skills needed to be effective in this role. This training is centered around the procedures used to conduct CND analysis within the DoD. The course provides analysts with some of the tactics, techniques, and procedures needed in conducting CND incident analysis and in developing appropriate responses. (1 hr)



### **System Administrator Incident Preparation & Response for UNIX (SAIPR UNIX)**

**Date 02/05 – Ver 2.01**

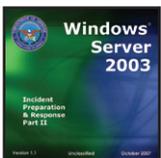
This product was designed to provide Federal System Administrators (SAs) or Information Assurance Officers (IAOs), who have three to five years of experience, with a follow-on course that builds on “UNIX Security for System Administrators, Version 2”. It is intended to provide training in preparing for, recognizing, and responding to information systems security incidents from a generic law enforcement perspective. The course touches on computer crimes and laws, system preparation, logs and auditing, mechanics and indicators of intrusion, and the architectures of some common but complex attacks. Updates include more and newer tools to assist the SA, as well as information from newer versions of policies and resources. Biometrics, steganography and other complex techniques are introduced. Intrusion reporting is also discussed. Although some technical aspects of intrusion and malicious code are presented, this is NOT a “hacker’s” course. The course supports knowledge needed for Information Assurance Technical and Management Level II, and is appropriate as a refresher at Technical Level III. (6.5 hrs)



### **Windows Server 2003 Incident Preparation & Response (IP&R): Part I**

**Date 02/06 – Ver 1.0**

This course is intended for Information Assurance (IA) Level II Technicians and Managers and for review by Level III Technicians and Managers. Level I IA Technicians and Managers can use the course to prepare for the network responsibilities of Level II positions. Part I of the course focuses primarily on the Information Assurance mechanisms used in Microsoft® Windows® Server 2003. The course describes file systems, some administrative procedures, server management, and folder and file permissions. Topics on security policy, archiving, logs, host- and network-based intrusion detection, as well as third-party tools are provided. A module on Response presents information about preparation, reaction, notification, recovery options, and working with law enforcement. (5 hrs)



### **Windows Server 2003 Incident Preparation & Response (IP&R): Part II**

**Date 10/07 – Ver 1.1**

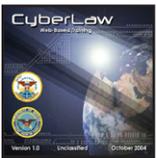
This course is designed for individuals who are identified by DoD 8570.01-M, Information Assurance Improvement Program, as IAT or IAM Level II. IAT and IAM Level I personnel who are preparing for the responsibilities of Level II may also find this courseware useful. The course addresses automated check procedures (Gold Disk), checking for IAVM compliance, Windows Active Directory, implementation of IA Policy through checklists and security readiness reviews, and includes an introduction to cyber forensics. (2 hrs)



**UNIX Security for System Administrators**  
**Date 12/04 – Ver 2.0**

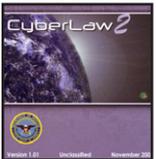
This course provides an overview of UNIX security basics for Systems Administrators (SAs) and Information Assurance Officers (IAOs). Topics covered include: network terminology, a framework of UNIX security relating to SA duties, security tools and commands, and reporting mechanisms. The course can be used to provide a conceptual UNIX Security foundation supporting Department of Defense Technical and Management Level I Information Assurance Certifications. It is also appropriate as a refresher for Technical and Management Level II. The course is designed to help beginning to intermediate System Administrators and Information Assurance Officers understand their roles in keeping their system secure; understand vulnerabilities and threats in terms of their origins, methods, and damage capabilities; identify, classify, and use system commands and other tools to assist in keeping the system secure. Because of the wide variety of system configurations, variations among local policies, and rapid technological changes, task specifics are not emphasized in this course. (10.5 hrs)

**CyberLaw**



**CyberLaw I**  
**Date 10/04 – Ver 1.0**

CyberLaw I is a web-based training product for DoD lawyers who need to understand the legal and policy issues, both current and emerging, associated with IA and Critical Infrastructure Protection (CIP). DoD lawyers will gain an increased ability to recognize and properly analyze legal issues in Cyberspace. The presentation begins with an introduction to the internet. The second module, "Law in Cyberspace," defines computer crime, discusses the First and Fourth Amendments, and presents statutory considerations to be applied during investigations. This module also discusses the four distinct roles or "lanes of the road" pertinent to Computer Network Defense. References are provided throughout the course for lawyers to follow evolving areas of the law in Cyberspace. (6 hrs)



**CyberLaw 2**  
**Date 11/06 – Ver 1.01**

This product is the second installment in the DoD CyberLaw training suite of products. This course is designed to aid the DoD attorney in keeping abreast of policies and laws that pertain to cybercrime. This course is divided into three sections. The first section discusses issues relating to investigating crime, including the applicability of the Fourth Amendment, honeypots, honeynets, honeygrids, transborder issues, statutory issues, and online undercover operations. The second section addresses issues related to prosecuting crimes and electronic evidence. The third section of this training product addresses post-trial issues and the disposition of evidence. (5.5 hrs)

**IA Simulations**



**CyberProtect**  
**Date 03/10 – Ver 2.0**

CyberProtect is a web-based, interactive computer network defensive exercise with a video game look and feel. It is intended to familiarize players with information assurance security terminology, concepts, and policy. Players learn about defensive security tools, which must be judiciously deployed on a simulated network. The player then faces 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 quarters of 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. (2 hrs)