INFORMATION SYSTEMS SECURITY PROGRAM MANAGEMENT

TRAINING COURSE

Developing, Implementing & Managing

FISMA / Department Of Defense / Intelligence Community

Information Systems Security Program

VERSION 1

LAST UPDATE 2/22/10

MODULE 1

INTRODUCTION TO INFORMATION SECURITY MANAGEMENT

INTRODUCTION TO INFORMATION SYSTEMS SECURITY MANAGEMENT

REVIEW

Presentation: Information Security Governance.pdf
Effective Versus In-Effective Security Governance.pdf
Information Security Terminology.pdf
Data Lifecycle Security.pdf
Information Technology / Information Security Essential Body Of Knowledge.pdf

MODULE 2A

FISMA / FEDERAL INFORMATION SECURITY MANAGEMENT ACT

REVIEW

Presentation: FISMA Overview.pdf
Presentation: FISMA Implementation Project.pdf
FISMA Security Controls Overview.pdf
FISMA Steps.pdf
FY 2008 FISMA Reporting FAQ.pdf

OMB/NIST Guidance On New FISMA Metrics

OMB/NIST Release Draft Of New FISMA Metrics.url
OMB-FY2010 Security Metrics.pdf
FISMA Reporting For 2010.url

MODULE 2B

NATIONAL SECURITY SYSTEMS

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY AGENCIES

REVIEW

Department Of Defense And Intelligence Community Agencies Regulations.url

MODULE 3

NIST SPECIAL PUBLICATIONS

REVIEW

Presentation: NIST Special Publications.pdf
FIPS-NIST Publications Overview.pdf
NIST Special Publications.url
NIST Special Publications Mailing List.url

MODULE 4

SECURITY CATEGORIZATION

FEDERAL INFORMATION / FEDERAL INFORMATION SYSTEMS

REVIEW

Presentation: Security Categorization Of Information Systems.pdf
FIPS-PUB-199: Standards for Security Categorization of Federal Information and Information Systems.pdf
NIST FAQ: For Security Categorization Standards For Information And Information Systems.pdf
CNSS 1253: Security Categorization And Control Selection For National Security Systems.pdf

MODULE 5

BASELINE SECURITY CONTROLS

FEDERAL INFORMATION / FEDERAL INFORMATION SYSTEMS

REVIEW

SECURITY CONTROLS

Presentation: Baseline Security Controls.pdf
FISMA Security Controls Overview.pdf
FIPS-200: Minimum Security Requirements for Federal Information and Information Systems.pdf
NIST SP 800-53R3: Recommended Security Controls For Federal Information Systems.pdf
NIST SP 800-53R3: Appendix G: Information Security Program Controls.pdf
NIST SP 800-53R3: Appendix D: Security Controls Summary Listing For L-M-H Baselines.pdf
NIST SP 800-53R3: Appendix F: Security Control Catalog.pdf
NIST SP 800-53: NIST To DCID 6/3 Security Controls Mappings.pdf

CONSENUS AUDIT GUIDELINES **(20 Specific Security Controls That Are Essential For Blocking Known High-Priority Attacks)**

Consensus Audit Guidelines No Substitute For FISMA Guidance.url
Consensus Audit Guidelines Overview.url
Consensus Audit Guidelines / Description Of Controls.url

SECURITY CONTROLS DATABASE

NIST SP 800-53: Security Controls Database Application Overview.pdf
NIST SP 800-53: Security Controls Database Application.url
NIST SP 800-53: Security Controls Database Quick Reference Guide.pdf

SECURITY CONTROLS ASSESSMENTS AND CHECKLISTS

NIST SP 800-53A: Presentation On Assessment Procedures-1.pdf
NIST SP 800-53A: Guide for Assessing the Security Controls in Federal Information Systems.pdf
NIST SP 800-53A: Security Control Assessment Process Chart.pdf
NIST SP 800-53A: Appendix D-- Assessment Method Descriptions.pdf
NIST SP 800-53A: Appendix E-- Assessment Expectations.pdf
NIST SP 800-53: Security Controls Assessment Form.pdf
NIST SP 800-53A: Appendix F-- Security Control Assessment Procedures.pdf
NIST SP 800-53A: Appendix I-- Security Assessment Reports.pdf

COMMITTEE ON NATIONAL SECURITY SYSTEMS/CNSS

CNSS 1253: Security Categorization And Control Selection For National Security Systems.pdf
Overview of NIST SP 800-53 Rev. 3 and CNSSI 1253.ppt
CNSS Instruction 1253 Security Control Mapping Table.pdf
CNSS Instruction 1253 MappingTo DOD 8500.2.xls

MODULE 6

SECURE CONFIGURATION OF INFORMATION SYSTEMS

HARDWARE / OPERATING SYSTEMS / SOFTWARE APPLICATIONS

REVIEW

Presentation: Secure Configuration Information Systems.pdf
Federal Desktop Core Configuration/FDCC FAQ.pdf
Federal Desktop Core Configuration Training.url
Best Practices For Hardening Host Systems-Video Based.url **(27 Minutes)**

MODULE 7

INTER-CONNECTING INFORMATION SYSTEMS

REVIEW

Presentation: Inter-Connecting Information Systems.pdf
NIST SP 800-100: Chapter 6 Overview Inter-Connecting Systems.pdf
NIST SP 800-47: Sample Memo of Understanding-Interconnection Security Agreement.pdf

MODULE 8

PRIVACY

PERSONALLY IDENTIFIABLE INFORMATION / PII PROTECTION

PRIVACY IMPACT ASSESSMENTS / PIA

REVIEW

PRIVACY REQUIREMENTS AND PRIVACY BRIEFINGS

OMB Privacy Memo Summaries.pdf
Presentation: Privacy Act Training 2006.pdf
National Institutes of Health Privacy Awareness Training.url

PRIVACY IMPACT ASSESSMENTS

Privacy Impact Assessments Overview.pdf
Privacy Impact Assessment Training.url
Privacy Impact Assessment Guidance From OMB.url (Conducting Privacy Impact Assessments / Privacy Policies on Websites)
Privacy Impact Assessments On Systems Containing Federal Employees-Contractors PII.pdf

PRIVACY AND DATA BREACHES

OMB Memo: Recommendations for Identity Theft Related Data Breach Notification.pdf

MODULE 9

MOBILE DEVICE SECURITY

REVIEW

PED & Removable Storage Media Training.url
OMB Memo 06-16: Protection Sensitive Information-Removed From/Accessed From Outside Agency.pdf

MODULE 10

SECURITY SERVICES AND PRODUCT ACQUISITION

REVIEW

NIST SP 800-100: Chapter 12 Security Services and Products Acquisition.pdf
Dept. Of Commerce Training Video: Effectively Integrating IT Security Into The Acquisition Process.url

MODULE 11

SECURITY POLICIES AND PROCEDURES

REVIEW

Presentation: Security Policies And Procedures.pdf
Recommended Security Policies.pdf

MODULE 12

INFORMATION SECURITY AWARENESS / EDUCATION / TRAINING

REVIEW

Presentation: Information Security Awareness-Training-Education.pdf
MANDATORY TRAINING FOR FEDERAL GOVERNMENT, DEPARTMENT OF DEFENSE AND INTELLIGENCE COMMUNITY
Federal Information Systems Security Awareness Training.url
Intelligence Community Information Assurance Awareness Training.url

DOD Information Assurance Awareness Training.url

MODULE 13

ACCESS CONTROL LIFECYCLE

IDENTIFICATION / AUTHENTICATION / AUTHORIZATION / TERMINATION

REVIEW

Presentation: Access Control-Identification-Authentication.pdf
Access Controls Lifecycle Checklist.pdf
Network Access Request And Authorization Form.pdf

MODULE 14

GENERAL USERS SECURITY REQUIREMENTS

RULES OF BEHAVIOR FOR COMPUTER SYSTEMS / NETWORK ACCESS

INFORMATION SYSTEMS SECURITY BRIEFINGS

REVIEW

Presentation: Generals Users Security Requirements.pdf
DOD/IC Rules Of Behavior Briefing And Acknowledgement Agreement.doc **(Use For New Hire Briefings & Security Education Awareness)**

MODULE 15

PRIVILEGED USERS SECURITY REQUIREMENTS

NETWORK AND SYSTEM ADMINISTRATORS

REVIEW

Presentation: Privileged Users Security Requirements.pdf
Privileged Users: Network And Systems Administrators Security Responsibilities Acknowledge Agreement.pdf

MODULE 16

RISK MANAGEMENT

REVIEW

RISK MANAGEMENT OVERVIEW

Presentation: NIST Risk Management Framework.pdf
Presentation: Continuous Monitoring Program Overview.pdf
Presentation: Continuous Monitoring Program.pdf **(From Compliance to Risk Management)**
CNSS Policy No. 22: Information Assurance Risk Management Policy For National Security Systems.pdf
NIST FAQ'S On Continuous Monitoring.pdf
Continuous Monitoring Plan Template.doc

RISK ASSESSMENT AND SECURITY INSPECTION CHECKLISTS

NIST SP 800-53: Security Controls Assessment Form.pdf
Dept. Of Justice IT Security: Risk Assessment Worksheets And Questions.pdf
Dept. Of Justice IT Security Risk Assessment Tool.xls

MODULE 17

CERTIFICATION AND ACCREDITATION / C&A

REVIEW

OVERVIEW OF CERTIFICATION AND ACCREDITATION

DNI ICD 503: IT Systems Security Risk Management And Certification-Accreditation.pdf
DNI ICD 503 Questions To DNI: Responses And Clarifications.pdf
DNI Presentation: Certification And Accreditation Transformation Overview.pdf
DOD-IC Agreement Related To ICD 503.pdf

NIST Presentation: Risk Management / Certification And Accreditation.pdf
NIST SP 800-100: Chapter 11 Certification And Accreditation.pdf
NEW- NIST SP 800-37 Rev. 1-- DRAFT Guide for Applying The Risk Management Framework To Federal Information Systems.pdf
OLD- NIST SP 800-37: Guide For Security Certification-Accreditation Of Federal Information Systems.pdf
NIST SP 800-37: Certification And Accreditation Process Chart.pdf
Department of Energy Certification-Accreditation Guidance.pdf **(Excellent Overview Of The C&A Process)**
Certification and Accreditation Group Exercise.pdf

SYSTEM SECURITY PLANS / SSP

Housing And Urban Development SSP Template.doc

SECURITY TEST AND EVALUATION / ST&E

Presentation: Systems Security Certification Testing.pdf
HHS Security Test And Evaluation Guide.pdf

MODULE 18

SECURITY VULNERABILITY TESTING OF INFORMATION SYSTEMS AND NETWORKS

SECURITY VULNERABILITY DATABASES AND ALERTS

REVIEW

Video: CERT-Best Practices For Security Vulnerability Assessment.url
Video: On-Screen Demonstrations Of Security Tools.url
Guidelines For Developing Penetration Testing Rules Of Behavior.pdf
ISSM Approval To Conduct Network Testing.pdf

SECURITY VULNERABILITY DATABASES

National Vulnerability Database Search.url
US-CERT Vulnerability Notes Database.url

SECURITY ALERTS

US-CERT Federal Knowledge Base System For Vulnerabilities Alerts.url
US-CERT Technical Cyber Security Alerts.url
KBAlertz.com - Knowledge Base Alerts.url

MODULE 19

CONFIGURATION MANAGEMENT

REVIEW

Presentation: Configuration Management.pdf
Configuration Management Examples Of Security Significant Changes.pdf

CONFIGURATION MANAGEMENT POLICIES

Configuration Change Management Policy.pdf
Configuration Change Request Form.pdf
Configuration Management Hardware-Software Implementation Checklist.pdf
Information Systems Maintenance Policy.pdf
Information Systems-Network Equipment Maintenance Log.pdf

CHANGE MANAGEMENT SOFTWARE

Xacta IA Manager Continuous Assessment.url
ECORA Configuration and Change Management Software.url
Belarc BelManage Enterprise Configuration Management Software.url
Tripwire Configuration Change Management Software.url
Open Source Tripwire For Linux And Unix.url
InstallWatch Change Mangement Software.url
Windows XP Change Analysis Diagnostic Tool.url
Whats Running System Information Utility.url

MODULE 20

PLAN OF ACTION AND MILESTONES / POA&MS

REVIEW

Presentation: Plan Of Action And Milestones-POA&MS.pdf
OMB Guidelines For Preparing And Submitting Plan Of Actions And Milestones.pdf

MODULE 21

INFORMATION SYSTEMS AUDITING / LOGGING, MONITORING AND REPORTING

REVIEW

Presentation: Information Systems Security Audit Requirements Overview.pdf

Windows Operating System Auditing Overview.pdf

Windows Operating System Event Logs Overview.pdf

Microsoft Events And Errors Message Center Advanced Search.url

WINDOWS OPERATING SYSTEM / ACTIVE DIRECTORY AUDITING

Windows & Active Directory Auditing.url

USB PORT AUDITING

USBDeview - View Installed-Previously Connected USB Devices On System.url

LINUX SECURITY

Linux Security Administrator's Guide: User, System, and Process Accounting.url

ROUTER SECURITY AUDIT LOGS

Cisco Router Security Audit Logs.url

MODULE 22

INCIDENT RESPONSE AND REPORTING

REVIEW

Presentation: Incident Response And Reporting.pdf

Computer Incident Reporting Policy.pdf

Computer Incident Reporting Form.pdf

COMPUTER SECURITY INCIDENT RESPONSE TEAMS

CMU CERT: Creating a Computer Security Incident Response Team A Process for Getting Started.url

MODULE 23

DOCUMENT SECURITY

METADATA PROBLEMS IN MICROSOFT OFFICE DOCUMENTS / PDF FILES

REVIEW

Presentation: SRS Electronic Document Security Introduction.pps

Presentation: SRS TopTen Hidden Data Issues.wmv

SOFTWARE TO REMOVE METADATA

Document Detetctive Metadata Removal Software.url **(Reviewed And Recommended)**

IC Clear **(Located On JWICS: http://icclear.csp.ic.gov/MainPage.htm)**

REDACTION

NSA: How To Safely Publish Sanitized Reports Converted From A Word Document To PDF Document.pdf

MODULE 24

THREATS AND VULNERABILITIES

REVIEW

Presentation: Overview Of Threats.pdf

Air Force Presentation: Threats From Electronic Devices.pdf

Steganography Overview: More Then Meets The Eye.pdf

Inside Job: 8 Companies That Got Burned by Rogue IT Workers.url

10 Top Spy Gadgets.url

MODULE 25

ELECTRONIC COMPUTER STORAGE MEDIA

CLEARING / SANITIZING / DESTRUCTION

REVIEW

Presentation: Clearing, Sanitizing, Destruction Of Computer Media.pdf
Computer Media Clearing-Sanitization-Destruction Policy.pdf
Computer Media Clearing-Sanitization-Destruction Form.pdf
NSA Procedures For Destruction Of Classified Material At NSA/CMC Facility.url

DISK WIPING SOFTWARE

Active Kill Disk Hard Drives Eraser.url
BCWipe For Windows.url
BCWipePD.url
Darik's Boot and Nuke.url

MODULE 26

IT CONTINUITY PLANNING

REVIEW

NIST SP 800-100: Chapter 9 Information Technology Contingency Planning.pdf
Information Systems Contingency Plan Template.pdf

FEDERAL REGULATIONS AND GUIDANCE

PUBLICS LAWS

Federal Information Security Management Act/FISMA.url
Appendix III to OMB Circular No. A-130: Security of Federal Automated Information Resources.url
Applicable Laws And Guidance For US Government Information-Information Systems.pdf
IT Security Laws And Federal Regulations.pdf
NIST Laws, Regulations, And Directives.url
Public Laws - Library of Congress.url
Computer Fraud and Abuse Act.url
Code of Federal Regulations.url

GENERAL SERVICES ADMINISTRATION (GSA)

GSA Reporting For Contractors.url
GSA Online Form For Government Contractors To Submit Evidence Of Possible Criminal Activities.url

OFFICE OF MANAGEMENT AND BUDGET (OMB)

OMB Circulars.url
OMB Memoranda.url

WHITE HOUSE

Presidential Executive Orders.url
National Security.url
Homeland Security.url