IA2 Information Assurance Associates, Inc.

Information Assurance Officer (IAO) Training (CNSS-4014)

IAO Course Overview:

Information Assurance Associates (*IA2*) is formally accredited by the Committee on National Security Systems (CNSS), which operates under the National Security Agency (NSA), to provide comprehensive certification training for Information Assurance Officers (IAOs). This course curriculum was specifically designed for IAOs that exercise system level security control over Department of Defense (DOD), Combatant Command, Service or Agency (CC/S/A), Intelligence Community (IC) and federal critical information infrastructures. The IAO course provides three days of comprehensive, non-technical, entry level professional training necessary to achieve the fundamental knowledge, skills, and abilities necessary to facilitate and integrate requisite system level security policies, processes, practices, procedures and protocols within DoD, CC/S/A, IC and federally controlled information systems and networks. This training focuses on planning, identifying, implementing, enforcing and maintaining data center security as well as integrating technical and non-technical solutions for securing critical information infrastructures and establishing standards necessary to help protect the confidentiality, maintain the integrity and ensure the availability of sensitive data and critical organizational computing resources.

Instructor Qualifications:

The *IA2* award winning instructor staff are all Fully Qualified Navy Certification Agents, Certified Information System Security Professionals (CISSPs), Certified Information Security Managers (CISMs) and Master Training Specialists. Additionally, each instructor has a minimum of fifteen years experience as a functional DOD, Intelligence Community or federal information system security professional. For national intelligence applications, *IA2* instructor staff members have been certified as NSA Adjunct Faculty and as NSA Accreditation Action Officers (AAOs), additionally each instructor holds a security clearance for access to SI/SCI data.

References:

- DoD Directive 8500.1, "Information Assurance" October 24, 2002.
- DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003
- DoD Directive 8570.1-M (Draft), DoD IA Training, Certification and Workforce Management. December 17, 2003
- DoDI 5200.40 DoD Information Technology Security Certification and Accreditation Process (DITSCAP)
- DoD 8510.1-M, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Manual, July 2000.
- Director Central Intelligence Directive (DCID) 6/3 – Protecting Sensitive Compartmented Information Within Information Systems.
- Director Central Intelligence Directive (DCID) 6/9 – Physical Security Standards for Sensitive Compartmented Information (SCI) Facilities.
- Joint DODIIS/Cryptologic SCI Information System Security Standards (JDCSISSS)
- CJCSI 6510.01b "Defensive Implementation Operations" Aug 1997
- CJCSM 6510.01 "Defense-in-Depth: Information Assurance and Computer Network Defense (CND)" December 2002
- Public Law 100-235 Computer Security Act of 1987
- OMB Circular A130
- CNSS 4014/4009
- Various Combatant Command, Service and Agency Directives

IAO Course Content

Information System Security Planning and Organization.

This lesson focuses on the security planning and administrative security procedures for systems that process sensitive, classified and national intelligence data. This lesson establishes individual roles, responsibilities and obligations and defines special requirements consistent with maintaining a secure network centric environment. Special emphasis is placed in the following areas:

- Individual responsibilities and special obligations associated with Information Assurance (IA) and secure network operations; including

specific responsibilities of the PAA, DAA, DAA Rep, Certifier, ISSM, ISSO, SA, NSO and User.

- The requirement to maintain and enhance information system security within a controlled environment including; the significance of facility planning and management; and the construction and implementation of user focused policies and Standard Operating Procedures (SOPs).
- The need to establish effective Information Security (INFOSEC) program planning including;
  - ✓ Describing and defining user based policies and procedures;
  - ✓ Establishing and enforcing system contingency, continuity and emergency plans;
  - ✓ Implementing, monitoring, analyzing and reporting unusual system activities;
- Implementation and enforcement of user based access controls including;
  - ✓ Password maintenance, management and administration;
  - ✓ Rule and Role based access controls.
- Integration of administrative security measures including preparatory actions, implementation responsibilities, and reporting requirements.
- The requirement and occasions for Security Awareness, Training, and Education (SATE)

Implementation and Enforcement of Information System Security Policies and Practices.

This lesson discusses a myriad of issues that relate directly to the operation, use, maintenance, disposition and control of information systems consistent with federal laws, national standards and organizations policies, practices and procedures. Special focus is placed on:

- Laws, regulations and other public policies. Emphasis is placed on their relevance to users and ways to ensure user understanding and compliance. Documents reviewed include:
  - ✓ PL 100-235 (Computer Security Act);
  - ✓ PL 99-474 (Computer Fraud and Abuse Act);
  - ✓ PL 93-579 (Copyright Act);
  - ✓ PL 99-508 (ECPA);
  - ✓ PL 93-579 (Privacy Act);
  - ✓ PL 107-56 (The Patriots Act);
  - ✓ PL 97-255 (FMFIA);

- ✓ PL 104-231 (FOIA);
- ✓ E.O. 12333
- ✓ OMB Circular A-130;
- ✓ NTISSD-600;
- ✓ PL-104-208 The Information Technology Management Act of 1996 (Clinger-Cohen Act)
- ✓ FIPS/NSTISSI/NIST/DCID/DODIIS Publications, as well as ISO/IEEE Standards, and;
- ✓ DOD, Joint and CC/S/A Directives, Instructions, Regulations and Guidelines.

- The concept and fundamental differences between Information System, Threat and COMSEC Monitoring including;
  - ✓ Special emphasis is placed on the control and protection of "Incidental Information";
  - ✓ The restrictions associated with e-mail content monitoring and keystroke monitoring;
  - ✓ The COMSEC monitoring implications within system auditing;
  - ✓ Federal as well as IC and CC/S/A COMSEC standards.
  - ✓ Intelligence Oversight with regards to computer applications.
- Evaluating protection requirements and determining information protection levels including Modes of Operation, Protection Level, Certification Level, Mission Assurance Categories (MAC), Classification Levels (CL), Robustness and Security Levels of Concern (LOC).
- Information Assurance Vulnerability Management (IAVM) reporting and compliance standards including;
  - ✓ Information Assurance Vulnerability Alert (IAVA) reporting methods and compliance requirements;
  - ✓ Information Assurance Vulnerability Bulletin (IAVB) reporting and compliance requirements and;
  - ✓ Information Assurance Vulnerability Technical Advisories and Task Orders (IAV-TA/TO) reporting and compliance requirements.
- Defining requirements and ensuring that Telecommunications Electronics Material Protected from Emanating Spurious Transmissions (TEMPEST) standards are identified and satisfied for all network configurations that process classified or national intelligence data.
- Describing and implementing Operations Security (OPSEC) processes including establishing OPSEC objectives, outlining OPSEC threats and determining OPSEC Essential Elements of Friendly Information (EEFI).

- Individual Standards of Conduct including computer ethics; fraud, waste and abuse actions; and a review of the concept of due-care, best business/ security practice, and reasonable and customary;
- Implementation of requisite electronic records management including maintenance, management and retention requirements as they relate to hardware and software assets.
- The principals and requirements for defining a Concept of Operations (CONOP) and establishing Mission Requirements.

Data Encryption (Cryptology).

This lesson provides a basic overview of data encryption including the integration and application of encryption philosophies and standards. The lesson focuses on:

- The purpose, the different types and the various applications of Data Encryption Standards (DES) including the unique security concerns associated with data encryption;
  - ✓ Symmetric and asymmetric key streams
  - ✓ Public and private cryptology.
  - ✓ The RSA algorithm.
  - ✓ Maintaining Confidentiality, Integrity, Authentication, and non-repudiation
- Communications Security (COMSEC) requirements including the basic principals of COMSEC, the uses of COMSEC technologies, and the application of appropriate COMSEC measures;
- An overview of Digital Signatures characteristics, issues, concerns and requirements including;
  - ✓ Key management (EKMS);
  - ✓ Key generation;
  - ✓ Key distribution;
  - ✓ Key installation and;
  - ✓ Key storage, recover, change and disposal.
- A basic overview of Public Key Encryption (PKE) and the Public Key Infrastructure (PKI) concept including a review of critical components, digital certificates and essential processes including;
  - ✓ Certification Authority, Registration Authority and Local Registration Authority requirements and responsibilities;
  - ✓ Identification of PKI enabled system components and services;

Physical, System and Data Access Control.

This lesson focuses on issues, concerns and requirements that determine the administration and management of physical, system and data access controls based on the sensitivity of the data processed and the corresponding authorization requirements of individual users. Discussions center on:

- Identifying the best, most cost effective, least intrusive, and least disruptive types of access controls necessary to satisfy specific organizational security concerns, specifically;
  - ✓ Identifying and determining physical access control methods and procedures;
  - ✓ Defining system access control requirements including identification and authentication methods and management controls.
  - ✓ Implementing biometric controls including establishing characteristics as well as identifying complications and concerns;
- Enforcing rule based, role based or content based access controls that facilitate data access requirements and accommodate data access controls that are consistent with the established DoD trusted criteria and DCID Protection Level standards.
- Defining data security models significant to maintaining confidential and integrity (e.g.Bell-LaPadula/Clark-Wilson/Biba) as well as the assurance level framework for expressing information security;
- Defining standards and requirements specific to the international Common Criteria, determining Evaluation Assurance Level (EAL) conditions and facilitating NIAP compliance.
- Establishing protective, detective and corrective access restrictions that facilitate physical, technical and administrative control measures for the three states of information including defining organizational requirements specific to the Defense in Depth (DiD) philosophy;
  - ✓ Network Intrusion Detection Systems;
  - ✓ System and Network Auditing;
  - ✓ Network firewalls;
  - ✓ Vendor requirements (HW/SW/FW)
  - ✓ Information systems security requirements and models
  - ✓ System and network architecture

Malicious Logic/MALWARE - Prevention, Detection, Reaction, Recovery and Reporting

This lesson addresses the threat posed by malicious software as well as the proper methods for downgrading, declassifying and/or destroying hardware, software and memory components used to process sensitive, classified or national intelligence data. Specifically, this lesson focuses on:

- The technical and non-technical impact malicious logic has on an organization and internal measures necessary to;
  - ✓ Identify malicious logic events;
  - ✓ Enforce methods necessary to prevent infection or introduction of malicious software;
  - ✓ Enforce actions required to prevent recurrence and;
  - ✓ Facilitate organizational reporting requirements and responsibilities.
- Methods and control procedures necessary to ensure the secure and proper disposition of hardware, software, memory components and recordable information storage media. This includes discussions on;
  - ✓ Overwriting processes and procedures;
  - ✓ Sanitizing processes and procedures;
  - ✓ Degaussing processes and procedures;
  - ✓ Destruction processes and procedures;
  - ✓ Clearing processes and procedures;
  - ✓ Declassification processes and procedures.

Configuration Management, Contingency Planning and Disaster Recovery.

This lesson topic focuses on protecting the integrity of "trusted" computing baselines as well as enforcing changes through the implementation of control measures that manage enhancements or modifications to system hardware, software, firmware, and documentation throughout its operational life-cycle. This lesson also addresses contingency planning actions, Defense in depth, and recovery processes necessary to ensure availability of critical information infrastructures. Special emphasis is placed on;

- The need to ensure the effective implementation of configuration controls and contingency actions. Including the requirement to;
  - ✓ Control changes to the trusted hardware and software baseline.

- ✓ Implement emergency response procedures as well as emergency destruction and emergency action planning.
- ✓ Perform backup procedures and system restoration and recovery processes for critical information infrastructures.
- ✓ Enforce Contingency Planning, preparatory and execution activities and;
- ✓ Identify appropriate and functional emergency response protocols.

- Enforcement of a comprehensive Consequence Management Plan, Disaster Recovery Plan and Continuity of Operations Plan (COOP).

Threat and Vulnerability Assessment; Risk Response and Recovery Actions.

This lesson focuses on the identification, analysis, assessment and evaluation of information system threats and vulnerabilities and their impact on an organization's critical information infrastructures. Specific discussions focus on:

- The concept of threat analysis as well as the potential impact of common technical and non-technical (administrative) vulnerabilities and their corresponding relationship with identified threats; as well as unique concerns posed by the intentional/unintentional, employee, and insider/outsider threats;
- Countermeasure analysis that outlines ways to integrate reasonable, cost-effective controls necessary to mitigate the threat/vulnerability risk potential to an acceptable level;
- Risk assessment discussions that center on the resulting impact or harm to an organizations efficiency, functionality, reputation and mission;
- Special risk analysis, risk assessment, and risk management techniques as well as risk calculation and measurement methods;
- Individual actions and activities that facilitate the identification control, measurement and mitigation of individual risk factors to satisfy Information System Security certification and accreditation.
- Evaluating and mitigating network and System Security Architecture security issues and concerns.

Information System and Network Security Certification and Accreditation (C&A).

This lesson offers comprehensive discussions that center on the DOD Information Assurance Certification and Accreditation Process (DIACAP),

process, and the NSA Information Security Certification and Accreditation Process (NISCAP). This lesson also provides a contrast and comparison review between DIACAP, DITSCAP, NISCAP and NIACAP. Special emphasis is placed on the DIACAP concept of certification and accreditation including:

- The various phases and activities associated with the DIACAP C&A process as well as the characteristics of the various phase activities associated with the DIACAP C&A process.
- The format and content of the DIACAP Implementation Plan and the associated Security Implementation Plan as well as special requirements including IA Control evaluation and required risk evaluation strategies.
- The format, structure and content of all requisite documentation to support DITSCAP C&A requirements.
- The different classes of accreditation including "Type", ATO, IATO, Denial, and Joint.

Student Progress Checks:

Student comprehension is measured by administering a cumulative progress check at the end of the last day of training. Topical reviews are conducted at the beginning and end of each training day to help to reinforce key learning objectives, reiterate essential subject areas and respond to individual student questions. Satisfactory completion and remedial requirements will be consistent with each customer training standards.