



IA-CND TRAINING



SGIS – Cyber Security Solutions (CSS), in partnership with Cyber Defense Solutions (CDS) (an SDVOB) and AFCEA Educational Foundation's Professional Development Center (PDC), provides IA-CND training capabilities. We supply tailored network intrusion analysis and incident response training for the Department of Defense, Law Enforcement and federal intelligence and counterintelligence organizations responsible for ensuring the defense of national information systems.



The Certified Network Intrusion Analyst - Networks™ Certification (CNIA-N™) Prep Course covers network forensics and incident response. This course approaches network intrusion investigations from an IA-CND perspective instead of the traditional law enforcement perspective. This course provides the necessary training for Government IT and IA professionals to perform incident handling and network forensics, particularly for analyzing incident-related data and determining the appropriate response to each incident.

The Certified Network Intrusion Analyst - Systems™ Certification (CNIA-S™) Prep Course covers system forensics and incident response. This course provides the necessary training for Government IT and IA professionals to perform incident handling and system forensics, particularly for analyzing incident-related data and determining the appropriate response for each incident.

The Certified Network Intrusion Analyst - Malware™ Certification (CNIA-M™) Prep Course covers malware forensics, reverse engineering, and incident response. This course provides the necessary training for Government IT and IA professionals to perform incident handling and malware forensics and reverse engineering, particularly for analyzing incident-related data and determining the appropriate response.

WHO SHOULD ATTEND?

- Information technology staff.
- Information security staff.
- Cyber Law Enforcement Investigators.
- Cyber Counterintelligence Investigators.
- Cyber Intelligence Analysts.
- CND and IA Analysts assigned to analyze, investigate and/or respond to security events or incidents.

