INSIDER THREAT PROGRAM DEVELOPMENT TRAINING (INSIDER THREAT SECURITY SPECIALIST COURSE)

Presented by: Jim Henderson, CISSP, CCISO

CEO, Insider Threat Defense, TopSecretProtection.com, Inc.

Counterespionage-Insider Threat Program Training Course Instructor
Cyber Security-Information System Security Program Management Training Course Instr.
Cyber Threat-Insider Threat Risk Analyst / Risk Mitigation Specialist
Founder / Chairman of The National Insider Threat Special Interest Group

Coordinating Sponsor/Hosts: **Scientific Research Corporation** is pleased to bring the **Insider Threat Program Development Training Course (Insider Threat Security Specialist Course)** to Greater Metro Atlanta, Georgia. SRC in cooperation with NCMS Georgia Chapter 16, has coordinated to have the ITPDT Course delivered to Defense Industry and Commercial Enterprise professionals in the Metro Atlanta region at a steeply discounted rate. Don't miss this opportunity to attain Insider Threat Security Specialist recognition and position your company to meet the requirements of the forthcoming Government mandates on Insider Threats common to all, but also **NISPOM Conforming Change #2 requirements** being levied on Cleared Defense Industry.

When: 12 – 14 January 2016

Agenda and Registration Information:
https://www.eventbrite.com/e/insider-threat-program-development-training-course-ncms-atlanta-ga-tickets-18047066261

Where: SRC Corporate Headquaters, 2300 Windy Ridge Parkway, Atlanta, GA. 30339
http://www.scires.com/about/location-atl.htm

Cost: Normal cost of attendance for this 3 day course is <u>$1395</u>, not including Travel, lodging and local transportation in the Maryland area. Scientific Research Corporation in partnership with NCMS Georgia Chapter 16, has negotiated a a steeply discounted rate of:
$795.00 = Huge Savings – 75 seats available; Don't Delay your registration

Who should attend and Why: Applicable to Corporate America, Mom & Pop Business USA, CI, SECURITY, CISO and IT Specialist alike. In addition to, the forthcoming NISPOM Conforming Change #2, Insider Threat Program requirements to be levied on Cleared Defense Industry; Every Business entity of 2 or more employee's is susceptible to an Insider Threat. This threat grows exponentially with the growth and diversity of the business itself. Insider Threats not only can lead to loss of technology, profitability and competitive market share, but can bring punitive damages depending upon the type and sensitivity of information lost.

The Insider Threat Development Program course will help the following individuals tasked with Identifying vulnerabilities, developing preventitive processes, deterance and mitigation response efforts that may become crucial to saving your critical data and business livelihood:

- Insider Threat Program Managers; Insider Threat Security Analysits; Insider Threat Program Support Personnel
- Facility Security Officers; Program Security Officers
- Counter-Intelligence Officers/Investigators
- Director of Security; Security Managers
- Physical Security Managers
- Human Resources – Personnel Security Specialists
- CIO; Information Technology (IT) / Network Administrators

Don't miss out – this training will be in very high demand at the start of 2016

Insider Threat Program Training Course Modules

MODULE 1-2 Overview Of Insider Threats / Espionage Corporate Espionage / Fraud / Theft Laws Related To Espionage-Insider Threat	MODULE 11 Information System Security Baseline Security Controls Secure Configuration Configuration Management
MODULE 3 Physical Security-Insider Threat Focus	MODULE 12 Developing, Implementing And Managing An Insider Threat Program Building An Insider Threat Program Risk Management Framework
MODULE 4 Data Security Lifecycle Data Loss Prevention-Protection	MODULE 13 Insider Threat Reporting And Investigations
MODULE 5 – Reference Only Protecting Classified Information SCI Security Requirements	MODULE 14 Creating An Insider Threat Awareness And Reporting Program
MODULE 6 Privacy Act Protecting Personally Identifiable Information (PII)	MODULE 15 Information Systems Auditing-Monitoring Insider Threat User Activity Monitoring Employee Monitoring Tools Data Loss Prevention Tools
MODULE 7 Personnel Security Program / Human Resources Behavioral Indicators Of Concern Continuous Evaluation Program	MODULE 16 Insider Threat Risk Management Insider Threat Vulnerability Assessments
MODULE 8 Security Policies And Procedures Building A Foundation / Culture Around Security	MODULE 17 Technical / Non-Technical Threats Common Sense Security Technology Threats Demonstration
MODULE 9 General User Security Requirements Security Responsibilities Briefings Acknowledgement Agreements	Insider Threat Program Policy Development Insider Threat Program Evaluation (Group Exercise-Discussion)
MODULE 10 Privileged User Security Requirements Security Responsibilities Briefings Acknowledgement Agreements Privileged User Monitoring	Insider Threat Security Specialist Exam Insider Threat Security Specialist Certificate

INSIDERTHREATDEFENSE.COM

Protecting Classified & Sensitive Information Is Our Business

NISPOM Conforming Change #2 And Insider Threat
What You Need To Know

Background

The NISP Operating Manual, also called NISPOM, establishes the standard procedures and requirements for government contractors interacting with classified information. The NISPOM was updated in March 2013 with the release of Conforming Change 1.

At the March 2014 meeting of NISPPAC, it was reported that the NISPOM conforming change #2 DoD formal coordination process was nearing completion. This change would incorporate the minimum standards for insider threat and the cyber intrusion reporting requirements. Once published, industry will have six months for implementation. The unofficial word is that the NISPOM Conforming Change #2 will be signed by December 2014.

NISPOM and Insider Threat

The new program requirements within NISPOM are based on the National Insider Threat Policy Minimum Standards. There are 6 key requirements that must be met. They include:

1. Establishment Of An Insider Threat Program
Contractors will establish and maintain an insider threat program that gathers, integrates and reports relevant and available information on potential or actual insider threat in accordance with E.O. 13587

2. Designation Of A Senior Contractor Official
The contractor will designate a U.S. citizen employee, who is a senior official and cleared in connection with the FCL, to establish and execute an insider threat program.

3. Reporting Indications Of An Insider Threat
Contractors will report all information specified in the "Minimum Reporting Requirements for Personnel with National Security Eligibility Determinations"

4. Providing Records Pertinent To Insider Threat
Per the National Insider Threat Policy, records pertinent to insider threat include but are not limited to:
A. Counterintelligence And Security Records. These records include personnel security files, polygraph examination reports, facility access records, security violation files, travel records, foreign contact reports, and financial disclosure filings.

B. Information Assurance. All relevant network data generated by IA elements including, usernames and aliases, levels of network access, audit data, unauthorized use of removable media, print logs, and other data needed for clarification or resolution of an insider threat concern.

C. Human Resources. Records that include: personnel files, payroll and voucher files, outside work and activities, disciplinary files, and personal contact records.

5. Insider Threat Training

The program must include Insider Threat Training. The Senior Contractor Official must ensure that the contractor program personnel assigned insider threat program responsibilities are trained, as well as all other cleared employees. The training must include:

A. Counterintelligence and security fundamentals including applicable legal issues.

B. Procedures for conducting insider threat response actions.

C. Laws and regulations on gathering, integration, retention, safeguarding and use of records and data and the consequences of misuse of such information.

D. Legal, civil liberties and privacy policies.

Specific insider threat related training must include:

A. The importance of detecting potential insider threats by cleared employees and reporting suspected activity to the insider threat program designee.

B. Methodologies that adversaries use to recruit trusted insiders.

C. Indicators of insider threat behavior and how to report such behavior.

D. Counterintelligence and security reporting requirements. Training must be satisfactorily completed within 30 days of initial employment or prior to being granted access to classified information, and annually thereafter. The contractor is responsible for establishing a system to validate and maintain records of all cleared employees who have completed the training.

6. Protection Measures Pertinent To User Activity Monitoring On Classified Networks.

The contractor must implement protection measures to monitor user activity on classified networks to detect activity indicative of insider threat behavior. The measures must be in accordance with guidance issued by the Cognizant Security Agency (CSA) and include the tools or capabilities that they require. In addition, the measures must adhere to Federal systems requirements as specified by FISMA, NIST, CNSS and others.