National Insider Threat Special Interest Group (NITSIG)

Protecting Information Is Our Mission

Serving As A Premier Trusted Partner To The
U.S. Government, Department of Defense, Intelligence Community Agencies,
Defense Industrial Base Contractors, Private-Sector Businesses / Organizations
For Insider Threat Mitigation

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.

The National Insider Threat Special Interest Group

The NITSIG and supporting partners will provide individuals working for government and businesses with a **central source** for insider threat awareness training, insider threat program development training and insider threat risk mitigation.

Websites:
http://www.nationalinsiderthreatsig.org
http://www.insiderthreatdefense.com

Jim Henderson / CISSP, CCISO
Co-Founder / Chairman Of The National Insider Threat Special Interest Group (NITSIG)
Counterespionage-Insider Threat Program Training Course Instructor
Cyber Threat-Insider Threat Risk Assessment Auditor / Analyst
Phone:
561-809-6800 / 888-363-7241
E-Mail:
jimhenderson@nationalinsiderthreatsig.org
jimhenderson@insiderthreatdefense.com
Connect With Me On LinkedIn:
http://www.linkedin.com/in/isspm