DoD Update

Insider Threat and the NISP

Steve Lewis
Valerie Heil

May 19, 2015

AGENDA

- Continuous Evaluation
- IMESA
- Insider Threat
- NISPOM Change 2
- SAP Policy Issuances
- NISPOM Rewrite
- Questions

Why Continuous Evaluation

- Early detection and mitigation of potential insider threats
- Reduce cost of performing traditional background investigations
- Response to multiple unauthorized disclosures of classified information and shooting incidents involving trusted insiders
- Secretary of Defense approved CE implementation as one of four key Washington Navy Yard recommendations
- Authorized by Executive Order 13467 (Reforming Processes…) and individually on the SF 86 release (2010 version)

DoD CE Way Ahead

- DoD actively consulting, collaborating, and coordinating with DNI and other Performance Accountability Council principals on its CE efforts.

- Goal is to develop CE processes that provide the same or more information than that developed by Tier 3 (Secret &below) investigations at greater frequency and at substantially less cost.

- CE will be a critical feed into DoD Insider Threat Program capabilities at all levels

Identity Matching Engine for Security and Analysis (IMESA)

Validates Credentials (e.g. CACs)/ Checks NCIC wanted persons file

5M	**The approximate number of persons registered**
2.5 – 3M	**The approximate number of swipe transactions per week**
200K	**The approximate number of persons registered each month**
> 1,000	**The approximate number of person matches with open active warrants**
126	**The number of installations connected**

NISPOM Change #2

New NISPOM 1-202 Insider Threat Program

- Establish and Maintain Insider Threat program
- Designate Insider Threat Senior Official
  - Must be cleared in connection with facility clearance
  - Establish and execute an insider threat program
  - May be FSO, but also has to be a Senior Official
  - FSO must be integral member of contractor’s program
- Gather, Integrate and Report
  - As required by Cognizant Security Agency (CSA)
  - Relevant and available information indicative of a potential or actual insider threat
- Clarification will be by Industrial Security Letter

NISPOM Change #2

New NISPOM 3-103: Insider Threat Training

- Considered appropriate by the CSA
  - Personnel with insider threat program responsibilities
    - Counterintelligence and security fundamentals
    - Procedures for conducting insider threat response actions
    - Applicable laws related to use (or misuse of records and data)
  - All other cleared personnel
    - Insider threat awareness training
- Required training before being granted access to classified information
- Establish and maintain a record of all cleared employees who have completed the initial and annual training

NISPOM Change #2

Chapter 8: Revisions

- ISSM role includes insider threat awareness
- User activities on contractor's classified systems are subject to monitoring
  - Banners on all classified information systems (ISs)
    - Activity on classified network is subject to monitoring
    - Could be used in criminal, security or administrative actions
- Security awareness training for all users (initial and refresher) (chp 3)
- CSA guidance will be based on guidance for Federal ISs
  - Terminology updates to synchronize to NIST 800-37
    - e.g., Assessment and Authorization instead of Certification and Accreditation

Other Major Changes in NISPOM Change #2

- New 1-401: Report cyber intrusions into cleared defense contractors (CDCs) classified information systems to DoD (section 941, FY13, NDAA)

- New Appendix D: NISPOM Supplement: will cancel 1995 NISPOM Supplement 1
  - No gap in guidance, since DoD will not publish NISPOM change #2 until DoD SAP volumes are published.

NISPOM Change #2

Progress toward publication

- Required concurrence by DOE, NRC, ODNI and DHS
- Received:
  - NRC and ODNI concurrence in March 2015
  - DOE concur with comments on April 1, 2015
  - DHS concur on May 11, 2015
- Resolved DOE comments as of May 11, 2015
- Now in DoD pre-signature edit and then legal sufficiency review
- Goal remains to publish by July 31, 2015
- Implementation no later than 6 months from publication (NISPOM paragraph 1-102c)

DoD SAP Manual

- DoDM 5205.07 Vol 1, “General Procedures”
- DoDM 5205.07 Vol 2, “Personnel Security”
- DoDM O-5205.07 Vol 3, “Physical Security”
- DoDM 5205.07 Vol 4, “Marking”

- Status
  - Volumes 3 and 4 published.
  - Volume 1 has completed legal review and is ready for signature.
  - Volume 2 in legal review.

Note: DoD Issuance Website: http://www.dtic.mil/whs/directives/index.html

NISPOM Rewrite

Will replace 2006 NISPOM and its two conforming changes

- Planning process started with CSAs: DOE, NRC, ODNI and DHS
- NISPPAC NISPOM ad hoc Working Group reestablished

- Series of workshops planned through the summer
  - NISPOM topics divided into six working “buckets”
  - CSA workshop for each bucket - followed by -
  - NISPPAC NISPOM ad hoc WG workshop

- May 20 – CSA workshop for bucket #1
  (Responsibilities, General Information, Reporting Requirements)
- June 2 – NISPPAC NISPOM ad hoc WG for bucket #1

Questions?