ASSOCIATION OF OLD CROWS

Operations Manual

OpMan 52 – Insider Threat Program

Effective: March 19, 2017
Admin Review: February 23, 2021

1. **PURPOSE:** To establish policy and assign responsibilities for the Insider Threat Program (ITP). The ITP will seek to establish a secure operating environment for personnel, facilities, information, equipment, networks, or systems from insider threats.

2. **INSIDER THREAT DEFINITION:** An insider threat is defined as the likelihood, risk or potential that an insider will use his or her authorized access, wittingly or unwittingly to do harm to the security of the United States. Insider threats may include harm to contractor or program information to the extent that the information impacts the contractor or agency's obligations to protect classified national security information.

3. **INSIDER THREAT PROGRAM:** The program will gather, integrate, and report relevant and credible information covered by the 13 personnel security adjudicative guidelines (see list below) that may be indicative of a potential or actual insider threat to deter all contractor employees granted personnel clearances (PCLs) and all employees being processed for PCLs, from becoming insider threats; detect any cleared person with authorized access to any government or contractor resources to include personnel, facilities, information, equipment, networks, or systems, who pose a risk to classified information; and mitigate the risk of an insider threat as defined above.

   Personnel Security Adjudicative Guidelines
   (1) Guideline A: Allegiance to the United States
   (2) Guideline B: Foreign Influence
   (3) Guideline C: Foreign Preference
   (4) Guideline D: Sexual Behavior
   (5) Guideline E: Personal Conduct
   (6) Guideline F: Financial Considerations
   (7) Guideline G: Alcohol Consumption
   (8) Guideline H: Drug Involvement
   (9) Guideline I: Psychological Conditions
   (10) Guideline J: Criminal Conduct
   (11) Guideline K: Handling Protected Information
   (12) Guideline L: Outside Activities
   (13) Guideline M: Use of Information Technology Systems

4. **SCOPE AND APPLICABILITY:** This ITP applies to all AOC staff offices and personnel with access to any government or contractor resources to include personnel, facilities, information, equipment, networks, or systems.

5. **GUIDING PRINCIPLES:**
   a. The Association of Old Crows is subject to insider threats and will take actions to mitigate or eliminate those threats.
   b. The Association of Old Crows will continually identify and assess threats to the organization and its personnel and institute programs to defeat the threats.

6. POLICY:

a. The ITP will be established to protect personnel, facilities, and automated systems from insider threats in compliance with DoD 5220.22-M Change 2 of the "National Industrial Security Program Operating Manual (NISPOM). This program will seek to prevent espionage, violent acts against the Nation or the unauthorized disclosure of classified information; deter cleared employees from becoming insider threats; detect employees who pose a risk to classified information systems and classified information; and mitigate the risks to the security of classified information through administrative, investigative, or other responses.

b. The ITP will meet or exceed the minimum standards for such programs, as defined in paragraph 1- 202, DoD 5220.22-M Change 2 of the "National Industrial Security Program Operating Manual (NISPOM) with additional guidance provided in Industrial Security Letter (ISL) 2016-02 and Defense Security Service (DSS) ODAA Process Manual for Certification and Accreditation of Classified Systems under the NISPOM."

c. The responsibilities outlined below are designed to enable the ITP to gather, integrate, centrally analyze, and respond appropriately to key threat-related information. The ITP will consult with records management, legal counsel, and civil liberties and privacy officials to ensure any legal, privacy, civil rights, and civil liberties issues (including, but not limited to, the use of personally identifiable information) are appropriately addressed.

7. RESPONSIBILITIES:

a. Insider Threat Program Senior Official (ITPSO), will be designated in writing and will act as the company's representative for ITP implementing activities. The designated ITPSO will be cleared in connection with the facility clearance, be a United States citizen, and will be designated as Key Management Personnel (KMP) in the National Industrial Security System (NISS) in accordance with Cognizant Security Agency (CSA) guidance and in accordance with NISPOM 1-202b.

b. The ITPSO will be responsible for daily operations, management, and ensuring compliance with the minimum standards derived from Change 2 to DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)." Responsibilities include:

(1) Self-certify the Insider Threat Program Plan in writing to DSS no later than 6 months from the issue date of Change 2 to DoD 5220.22-M, NISPOM.
(2) Provide copies of the Insider Threat Plan upon request and will make the plan available to the DSS during the Security Vulnerability Assessments (SVA).
(3) Establish an Insider Threat Program based on the organization's size and operations.
(4) Provide Insider Threat training for Insider Threat Program personnel and awareness for cleared employees.
(5) Establish user activity monitoring on classified information systems in order to detect activity indicative of insider threat behavior. These monitoring activities will be based on Federal requirements and standards (Federal Information Security Management Act, National Institute of Standards and Technology, and Committee for National Security Systems) and in accordance with NISPOM 8-100d.
(6) Establish procedures in accordance with NISPOM, paragraph 1-202b and 1-300, to access, gather, integrate, and provide for reporting of relevant and credible information across the contractor facility (e.g., human resources, security, information assurance, and legal review) covered by the 13 personnel security adjudicative guidelines that may be indicative of a potential or actual insider threat to

deter employees from becoming insider threats; detecting insiders who pose a risk to classified information; and mitigating the risk of an insider threat.
(7) Establish a system or process to identify patterns of negligence or carelessness in handling classified information, in accordance with NISPOM 1-304c, even for incidents that do not warrant a culpability or incident report.
(8) Conduct self-inspections of the Insider Threat Program in accordance with NISPOM 1-207b.
(9) Oversee the collection, analysis, and reporting of information across the company to support the identification and assessment of insider threats.
(10) Establish and manage all implementation and reporting requirements, to include self-assessments and independent assessments, the results of which shall be reported to the Senior Management.

8. INSIDER TREAT TRAINING:

a. Insider Threat Program Senior Official (ITPSO) Training

(1) ITPSO training will be completed by November 30, 2016.
(2) If a new ITPSO is appointed after the 6-month implementation period, the new ITPSO will complete the required training within 30-days of being assigned ITPSO responsibilities.

b. ITP Personnel Training

(1) All personnel assigned duties related to insider threat program management will attend the training outlined in NISPOM 3-103a.
(2) After initial implementation of this plan and completion of the required training, all new contractor personnel assigned duties related to the insider threat program management will complete the above training within 30-days of being assigned duties and refresher training annually thereafter.

c. Employee Insider Threat Awareness Training

(1) Training on insider threat awareness in accordance with NISPOM 3-103b will be required for all cleared employees before being granted access to classified information and annually thereafter in accordance with NISPOM 3-103b.
(2) Cleared employees already in access will complete insider threat awareness training no later than May annually in accordance with NISPOM 3-103b.
(3) All cleared employees who are not currently in access will complete insider threat awareness training prior to being granted access and annually thereafter in accordance with NISPOM 3-103b.

d. Insider Threat Training Records Management

(1) Insider Threat Training Records will consist of training attendance records, certificates, or other documentation verifying that personnel completed the training requirements in accordance with NISPOM 3- 103c.
(2) Insider Threat Training Records will maintain records of all employee insider threat awareness or program initial and refresher training in accordance with NISPOM 3-103c.
(3) Insider Threat Training Records will be available for review during DSS security vulnerability assessments.
(4) Insider Threat Awareness will be included in annual refresher training to reinforce and update cleared employees on the information provided in initial training in accordance with NISPOM 3-108.

9. **INSIDER THREAT REPORTING REQUIREMENTS:** All credible Insider Threat Information will be coordinated and shared with the ITPSO, which will then take action as directed in NISPOM, paragraph 1-300, “Reporting Requirements.” The following information will be reported:

a. Information regarding cleared employees, to include information indicative of a potential or actual insider threat and which falls into one of the 13 adjudicative guidelines, which must be reported when that information constitutes adverse information, in accordance with NISPOM 1-302a, ISL 2006-02 and ISL 2011-4.
b. Incidents that constitute suspicious contacts, in accordance with NISPOM 1-302b (Suspicious Contacts) and ISL 2006-02.
c. Information coming to the ITP's attention concerning actual, probable or possible espionage, sabotage, terrorism, or subversive activities at any of its locations must to be reported to the nearest Federal Bureau of Investigation (FBI), with a copy to the CSA, in accordance with NISPOM 1-301, and ISLs 2006-02 and 2013-05.
d. Information determined to be any possible or potential successful penetration of a classified information system must be reported immediately to the CSA per NISPOM 1-401.