CLIENT ALERT

Department of Defense Adds New Requirements to National Industrial Security Program Operating Manual

Jun.03.2016

On May 18, 2016, the Department of Defense (DoD) approved Change 2 to the National Industrial Security Program Operating Manual (NISPOM), which prescribes requirements, restrictions, and other safeguards to prevent unauthorized disclosures of classified information. Change 2 modifies the NISPOM in several main areas. Relevant highlights from Change 2 include the following:

- **Insider Threat Program**. Change 2 requires contractors holding facility clearances to establish and maintain an insider threat program that will gather, integrate, and report relevant and available information indicative of a potential or actual insider threat. Insider threats may include harm to the contractor or program information, to the extent that the information impacts the contractor or the agency's obligations to protect classified national security information. According to Industrial Security Letter 2016-02, contractors must have a written insider threat program in place no later than November 30, 2016. As part of its insider threat program, the contractor must:
    - Appoint an Insider Threat Program Senior Official (ITPSO) who is a senior official and a U.S. citizen with appropriate clearance. The ITPSO may also be the company's Facility Security Officer. A corporate family may establish a corporate-wide insider threat program with a corporate-wide ITPSO; however, each legal entity must also have its own designated ITPSO.
    - Ensure that contractor program personnel assigned insider threat program responsibilities complete training in counterintelligence and security fundamentals, procedures for conducting insider threat response actions, applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information, and applicable legal civil liberties, and privacy policies.
    - Ensure that all cleared employees are trained before being granted access to classified information, and annually thereafter, on the importance of detecting potential insider threats and the reporting of suspected activity; methodologies of adversaries to recruit trusted insiders and collect classified information, in particular within information systems; indicators of insider threat behavior and procedures to report such behavior; and counterintelligence and security reporting requirements.
    - Review, among other things, the contractor's insider threat program, during its self-inspections.
    - Report information that may indicate an employee poses an insider threat.
    - Implement security protection measures for contractor information systems that are used to capture, create, store, process, or distribute classified information, in accordance with guidance issued by the cognizant security agency, including tools or capabilities to monitor user activity on classified information systems in order to detect activity indicative of insider threat behavior. In addition the measures must adhere to Federal systems requirements as specified by the Federal Information Security Management Act, the National Institute of Standards and Technology, the Committee on National Security Systems, and others.

- **Self-Inspections**. Change 2 also bolsters requirements pertaining to contractor self-inspections. In addition to requiring contractors to perform periodic self-inspections of their overall security program including the insider threat program, the revised NISPOM requires contractors to prepare a formal report describing the self-inspection, its findings, and the resolution of any issues found. The revised NISPOM also requires a senior management official at each cleared facility to annually certify that a self-inspection has been performed, that senior management has been briefed on the results, that corrective action has been taken, and that management fully supports the cleared facility's security program.
- **Reporting of Cyber Incidents**. Change 2 requires Cleared Defense Contractors to report immediately any cyber incident involving their covered information systems that have been approved to process classified information.
    - Cyber incidents are defined as: actions taken through the use of computer networks that result in an *actual or potentially adverse effect* on *an Information System or the information residing therein*.
    - Cyber incident reports must include, at a minimum, a description of the technique or method used in the cyber incident; a sample of the malicious software, if discovered and isolated by the contractor, involved in the cyber incident; and a summary of information in connection with any DoD program that has been potentially compromised due to the cyber incident. DoD has indicated that it will later provide detailed reporting instructions via the issuance of an Industrial Security Letter.
    - Change 2 also informs contractors that DoD may be required to obtain access to the contractor's equipment or information so that it may conduct forensic analysis.
- **Information System Security Program**. Change 2 requires contractors to maintain a classified information system security program that incorporates a risk-based set of management, operational, and technical controls and to certify that the information systems to be used for processing classified information include such a program. This program must include, at a minimum:
    - Policies and procedures that reduce information security risks to an acceptable level and address information security throughout the information system life cycle.
    - Plans for providing adequate information security for data resident in the information system or on the networks, facilities, or groups of information systems.
    - Training for all classified information system users on the security risks associated with their activities and responsibilities under the National Industrial Security Program.
    - Testing and evaluation of information security policies, procedures, practices, and security control implementation.
    - A process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies in the contractor's information security policies, procedures, and practices.
    - Procedures for detecting, reporting, and responding to security incidents, and events.
    - Plans and procedures for information system continuity of operations when required by contract.
    - A self-inspection program.

  Additionally, Change 2 requires all information users to comply with the requirements of the information security program, be accountable for their actions, not share and protect any authentication mechanisms issued for control of their access to an information system, and be subject to monitoring of their activity on any classified network.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

David Z. Bodenheimer
Partner – Washington, D.C.
Phone: +1 202.624.2713
Email: dbodenheimer@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Maida Oringher Lerner
Senior Counsel – Washington, D.C.
Phone: +1 202.624.2596
Email: mlerner@crowell.com

Mark A. Ries
Senior Counsel – Washington, D.C.
Phone: +1 202.624.2794
Email: mries@crowell.com

Jonathan M. Baker
Partner – Washington, D.C.
Phone: +1 202.624.2641
Email: jbaker@crowell.com