wiley

ALERT

DoD Proposes Amendments to National Industrial Security Program Operating Manual (NISPOM)

December 18, 2023

WHAT: On December 13, 2023, the Department of Defense (DoD) proposed amendments to the National Industrial Security Program Operating Manual (NISPOM) that seek to address the public comments it received in response to its previous rule in December 2020 that codified the NISPOM in the Code of Federal Regulations. Comments are due by **February 12, 2024**.

WHAT THIS MEANS FOR INDUSTRY: Although DoD's proposed amendments "create no additional requirements to current NISP policy," they provide some helpful clarification, including, for example, that the NISP and the evolving requirements for safeguarding Controlled Unclassified Information (CUI) are distinct. DoD also proposed to revise the rules covering open storage areas and highlighted the role of Industrial Security Letters (ISLs) that provide DoD-specific guidance. Wiley will continue to monitor this space and provide further updates as additional guidance is issued.

The NISPOM serves as the "single, integrated cohesive industrial security program" for the protection of classified information for all non-governmental entities granted access to classified information, including government contractors. The NISPOM provides overarching guidance on the standards to which contractors must adhere, including the procedures and criteria for obtaining personnel and facility clearances, requirements for implementing security measures, reporting requirements for security breaches and other suspicious activities, requirements for establishing an insider threat program, and other ongoing compliance requirements. As a reminder, and as discussed in our previous alert, DoD's December 2020 rule made

Authors

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Tessa Capeloto
Partner
202.719.7586
tcapeloto@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Christopher B. Weld
Partner
202.719.4651
cweld@wiley.law

Vaibhavi Patria
Associate
202.719.4667
vpatria@wiley.law

Lisa Rechden
Associate
202.719.4269
lrechden@wiley.law

Practice Areas

Government Contracts

National Security

three important changes:

1. The rule codified the NISPOM in Title 32 of the Code of Federal Regulations. Previously, DoD maintained the NISPOM as a DoD Manual.
2. The rule incorporated the requirements of Security Executive Agent Directive (SEAD) 3 by requiring cleared contractor personnel to provide ongoing reports to the government on specific information and activities that may adversely impact their clearance eligibility, including foreign contacts and foreign travel.
3. The rule implemented provisions of Section 842 of the 2019 National Defense Authorization Act (NDAA) that removed the requirement for U.S.-cleared companies owned by Australia, Canada, and the United Kingdom to obtain a national interest determination before accessing classified information.

Proposed Amendments: DoD's proposed rule addresses six overarching issues.

Controlled Unclassified Information.

Because the CUI Program borrows some processes from the requirements governing classified information, some have conflated the programs for safeguarding classified information and CUI. In its December 2020 rule, DoD emphasized that "compliance with CUI requirements is ***outside the scope of the NISP and this rule***." In response to the December 2020 proposed rule, the confusion appears to have continued as DoD received "seven comments on CUI." In response, DoD has again reiterated that "compliance with CUI is outside the scope of the NISP." DCSA's website also confirms that "DCSA will ***not*** assess contractor compliance with established CUI system requirements within DoD classified contracts associated with the NISP."

Safeguarding Classified Information.

DoD proposed updating the NISPOM to clarify procedures for leaving an open storage area unattended during business hours, requirements for the reproduction of classified information – including accountability, control, and marking requirements of the reproduced classified information, and procedures for waste products resulting from reproductions. DoD also proposed allowing delegation of approval authority to Facility Security Officers (FSO) if agreed to by the Cognizant Security Agency. More guidance on safeguarding will be provided via forthcoming ISLs.

SEAD 3 Implementation Guidance and Costs.

Several comments raised concerns that the reporting requirements and processes created by Security Executive Agent Directive 3 (SEAD 3) were not clear, particularly on how information systems will be used to report foreign travel, when reporting foreign travel is required, and details on who approves the foreign travel requests. DoD previously attempted to clarify some of these issues in ISL 2021-02. In response to concerns that it would be especially burdensome for contractors to submit individual foreign travel reports, DoD also proposed modifying its systems to be capable of receiving multiple foreign travel reports in a single submission. DoD also acknowledged the original rule underestimated the cost for implementing SEAD 3 and

updated its cost estimates accordingly.

National Interest Determination (NID) Requirements for Certain Contractors.

DoD received comments requesting clarity on which entities qualify as National Technology and Industrial Base entities, which some commenters recommending that NIDs be eliminated. The final rule reflects language taken directly Public Law 115–232, which eliminated the NID requirement for U.S.-cleared companies owned by Australia, Canada, and the United Kingdom. DoD declined to make any additional rule changes because it considered doing so to be outside the scope of this rule.

Personnel and Facility Security Clearances.

DoD proposed clarifying that the only exception to the general rule requiring FSOs to be U.S. citizens may apply to the Senior Management Official or Insider Threat Program Senior Official if the entity has a limited entity eligibility determination due to foreign ownership, control, or influence. DoD also proposed addressing comments concerning the frequency of security review cycles by modifying the text to provide that security reviews will only occur once every 12 months unless special circumstances warranted otherwise. Responding to concerns regarding unannounced reviews without specific guidelines, DoD proposed to clarify that unannounced security reviews will be conducted only if there is a possibility of imminent loss or compromise of classified information.

Industrial Security Letters

DoD explained that many of the remaining comments it received deal with issues specific to contractors under DoD security cognizance. DoD generally addresses these issues through separate Industrial Security Letters (ISLs). In response to these questions, DoD committed to re-issuing any previous ISLs that are still needed. Once DoD completes this process, it should clarify what guidance remains effective today.