

FINAL RULE CODIFIES NISPOM WITH UPDATES INTO CFR

Recent actions of the U.S. government focus on protecting U.S. national security through safeguarding U.S.-based technologies and information from foreign misappropriation. For instance, a recent number of U.S. policies and regulations have sought to deny China access to U.S. export-controlled items and technologies. Please see [here](#) and [here](#) for analysis of recent U.S. export restrictions towards China. Additionally, legislative and regulatory changes that expand the type of transactions under the jurisdiction of the U.S. Committee on Foreign Investment in the United States ("CFIUS"), are also designed to protect national security sensitive U.S. businesses and technologies from foreign exploitation. Please see [here](#) and [here](#) for analysis of recent updates to CFIUS.

A final rule effective as of February 24, 2021, also seeks to deter the foreign diversion of U.S. technologies by making certain changes to the National Industrial Security Program Operating Manual ("NISPOM") regarding the handling of classified materials by U.S. government contractors. This rule includes several substantive changes to the NISPOM, including the incorporation of reporting requirements under Security Executive Agent Directive ("SEAD") 3, a counterintelligence program designed to secure U.S. classified materials handled by employees of U.S. government contractors from foreign espionage. Additionally, the rule eliminates preconditions for certain government contractors operating under a Special Security Agreement ("SSA") to obtain a National Interest Determination ("NID") for access to classified information. The rule also codifies the NISPOM into the U.S. Code of Federal Regulations ("CFR") at [32 CFR 117](#). Prior to this final rule, the NISPOM existed as a manual within the Department of Defense.

Contractors will have six months from February 24, 2021 to comply with these changes.

Key issues

- A final rule effective as of February 24, 2021 codifies the NISPOM into the CFR and imposes changes on U.S. government contractors engaged in classified contracts.
- The updates impose new reporting requirements on U.S. government contractors with respect to activities of employees.
- The rule implements a new, limited exception to NID requirements for U.S. government contractors whose parent entities are incorporated in either the UK, Canada, or Australia.

NISPOM Fundamentals

As the Department of Defense is the Executive Agent of the National Industrial Security Program ("NISP"), which the NISPOM implements, the department has taken the lead in coordinating with other designated departments and agencies under the NISP that establish NISP-related security requirements (the Department of Energy, the Nuclear Regulatory Commission, the Office of the Director of National Intelligence, and the Department of Homeland Security) in the codification of the manual into the CFR, along with establishing updates. The NISP seeks to protect classified information released to U.S. government contractors and applies to all contractors working for executive branch departments and agencies that require access to classified information. To ensure that classified information provided to U.S. government contractors is properly secured, the NISPOM defines the restrictions, requirements and safeguards that contractors must follow based on the standards outlined in the NISP. The NISPOM also specifies the various mechanisms used to mitigate foreign ownership, control, or influence ("FOCI").

New Reporting Requirements

Among the changes to the NISPOM in the final rule, under implementation of SEAD 3, contractors must now report specific foreign activities of their cleared employees to the U.S. government agencies with which they contract for classified projects. Overseas travel and foreign contacts are specific examples of foreign activities which now must be reported. Further, the NISPOM now requires contractors to provide briefings to their employees before and after such travel to warn them of foreign espionage.

The NISPOM also places obligations on government agencies. Specifically, the NISPOM directs government agencies to analyze the reported activities of government contractor employees to determine their continued eligibility for dealing in classified material. The addition of SEAD 3's reporting requirements for U.S. government contractors dealing with sensitive or classified information into the NISPOM will now provide for a single, nation-wide implementation plan of the directive, while allowing individual government agencies to collect further information that they deem necessary.

Elimination of NID Requirement for Certain Entities

The final rule also eliminates certain requirements for particular U.S. government contractors whose parent entities are incorporated in either the United Kingdom, Canada, or Australia (referred to as "covered National Technology and Industrial Base ("NTIB") entities") that enter into SSAs with U.S. government agencies. Specifically, those entities will no longer be required to obtain a NID for access to Top Secret and other classified information. NIDs are required in advance to confirm that the release of classified information to the contractor will not harm U.S. national security.

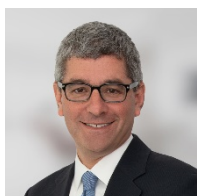
The practical effect of eliminating the NID requirement is limited in scope, as only certain cleared entities (those operating under an SSA) whose parent entities are incorporated in just three countries are eligible to avail themselves of the elimination of the NID requirement. For eligible entities, however, the change is likely welcome, as NIDs are both costly and time consuming to obtain. This

change allows for quicker response times for covered NTIB entities to begin performing on classified contracts without the delays associated with waiting for an NID.

* * *

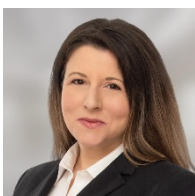
All U.S. government contractors will have six months from the effective date (until August 24, 2021) to review the NISPOM changes addressed above and take appropriate measures to update their existing compliance programs. Failure to integrate such changes into compliance regimens could result in significant consequences, including the loss of the ability to handle classified material if found to have not reported relevant foreign activities to required U.S. agencies. The loss of such clearances would greatly impact the ability of U.S. government contractors to work on U.S. national security-related projects. Furthermore, contractors who do not review the requirements for NTIB entities and do not take advantage of this exception could needlessly be adding costs and time to U.S. government contracts which they are working. Reviewing and establishing the appropriate changes now will help ensure continued access to U.S. classified material and avert any unnecessary complications to completing projects under certain U.S. government contracts.

CONTACTS



Joshua Berman
Partner

T +1 202 912 5174
E joshua.berman
@cliffordchance.com



Renée Latour
Partner

T +1 202 912 5509
E renee.latour
@cliffordchance.com



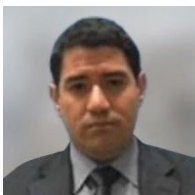
Holly Bauer
Associate

T +1 202 912 5132
E holly.bauer
@cliffordchance.com



Laurence Hull
Associate

T +1 202 912 5560
E laurence.hull
@cliffordchance.com



Michael Press
Associate

T +1 202 912 5214
E michael.press
@cliffordchance.com

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

© Clifford Chance 2021

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.