Westlaw Today
powered by Reuters

NISPOM creates new requirements for senior management officials

By Michael J. Montalbano, Esq., Blank Rome LLP*

JULY 5, 2022

In February 2021, the Department of Defense (DoD) promulgated 32 C.F.R. Part 117. This move converted the National Industrial Security Program Operating Manual (NISPOM) — the rules that govern personnel and facility security clearances — from DoD policy into federal law.

DoD embedded new requirements with potentially significant implications for cleared contractors and their senior management officials.

The move originally garnered little attention because the new regulations include virtually all requirements that were in the prior NISPOM.

DoD, however, embedded new requirements with potentially significant implications for cleared contractors and their senior management officials (SMO). And the Defense Counterintelligence and Security Agency (DCSA) is now signaling that it will hold SMOs accountable if they fail to meet these requirements.

A cleared contractor's SMO is the person "with ultimate authority over the facility's operations and the authority to direct actions necessary for the safeguarding of classified information in the facility."[1]

The SMO can no longer delegate responsibility over the contractor's industrial security program to another employee.

Typically, the SMO is the individual who holds the top position at a company, such as a chief executive officer or majority owner. Prior to the promulgation of Part 117, the SMO had discretion to delegate responsibility over the contractor's industrial security program to another employee. Section 117.7(b)(2) of the new NISPOM regulations has put an end to that practice.

Specifically, section 117.7(b)(2) of the NISPOM makes the SMO fully accountable for a cleared contractor's industrial security program, assigning the following new responsibilities to the SMO:

(1) Ensure the contractor maintains a system of security controls in accordance with the requirements of Part 117.

(2) Appoint a contractor employee or employees, in writing, as the Facility Security Officer (FSO) and Insider Threat Program Senior Official.

(3) Remain fully informed of the facility's classified operations.

(4) Make decisions based on classified threat reporting and the SMO's thorough knowledge, understanding, and appreciation of the threat information and the potential impacts caused by a loss of classified information.

(5) Retain accountability for the management and operations of the facility without delegating that accountability to a subordinate manager.

The SMO can no longer delegate responsibility over the contractor's industrial security program to another employee.

The SMO should engage with the organization's DCSA security representative whenever the representative visits or presents to the organization's personnel.

The SMO is now required to remain up to date on emerging threats to the contractor's industrial security program and ensure that the right personnel and controls are in place to protect the classified information that has been provided to the contractor. If these controls are not in place, the DCSA will hold the SMO accountable.

While DCSA has not yet provided guidance regarding what steps a SMO must take to ensure compliance with section 117(b)(2), SMOs should consider the following:

(1) **Size of organization**. The SMO of a smaller organization will have an easier time complying with section 117(b)(2) because there is a higher likelihood that the SMO's day-

to-day duties require attention to the industrial security program and the organization's classified work. The SMO of a larger organization, where the classified work is just a small component of the organization's project portfolio, might need to make a more concerted effort to understand the organization's industrial security program.

(2) **Engage the FSO**. While the SMO is accountable for the organization's industrial security program, the FSO is generally in charge of the day-to-day operations of the program. SMOs should leverage their FSOs by meeting with them regularly to keep up to date on the organization's industrial security program and any emerging threats.

(3) **Engage with DCSA**. DCSA should not have to seek out the SMO. Rather, the SMO should engage with the organization's DCSA security representative whenever the representative visits or presents to the organization's personnel. The SMO should also periodically request threat briefings from DCSA. These efforts will demonstrate to DCSA that the SMO is engaged with the organization's industrial security program, providing further evidence that the SMO is complying with 32 C.F.R. § 117(b)(2).

Notes

[1] § 117.3(b).

About the author

Michael J. Montalbano, a government contracts associate in **Blank Rome LLP**'s Philadelphia office, represents government contractors regarding bid protests, mergers and acquisitions, industrial security matters, audits, contract disputes, and federal regulatory requirements. He can be reached at michael.montalbano@blankrome.com.
This article was originally published June 16, 2022, on the firm's website. Republished with permission.

This article was published on Westlaw Today on July 5, 2022.