SHIN&KIM
법무법인(유) 세종

Searches and Seizures Involving Military Secrets: What Defense Companies in Korea Need to Know

2026.11.25

For defense contractors and other companies operating in Korea's defense sector, a criminal investigation can have consequences far beyond the individuals involved. Where employees of private-sector defense companies are suspected of disclosing military secrets in the course of their duties, they may be subject to investigations by military investigative authorities and proceedings before military courts, notwithstanding their civilian status (Articles 3(2) and 44 of the Military Court Act). If a disclosure of military secret or security breach is established, the consequences may extend beyond criminal penalties to administrative sanctions, including debarment from public procurement, and adverse contractual consequences, potentially including contract cancellation.

Searches and seizures present an additional challenge. A company's servers and premises may hold classified information and trade secrets relating to multiple defense projects, many of which have no connection to the investigation. The priority is therefore not simply to cooperate with investigators, but to ensure that the investigative measures do not unnecessarily expose sensitive information from unrelated projects.

An effective response begins with understanding who has authority to investigate, what the search warrant permits, and how to protect sensitive information throughout the process. This newsletter explains the legal framework governing searches and seizures involving military secrets in Korea and the practical steps defense companies should consider before, during and after a search.

1. Know Who Is Authorized to Investigate

Korea's military investigative framework changed on July 31, 2026, when the Defense Counterintelligence Command was abolished and its national security-related investigative functions were transferred to the Ministry of National Defense's Criminal Investigation Command (CIC). Under Article 3 of the Decree on the Criminal Investigation Command, the CIC oversees military police activities relating to the investigation and prevention of offenses under the Military Secret Protection Act, together with related criminal intelligence functions.

Military police have primary responsibility for investigating national security-related offenses, including the

unauthorized disclosure of military secrets. Military prosecutors handle supplementary and direct investigations and are responsible for initiating and conducting prosecutions.

For defense companies, the immediate concern is whether the officials seeking access to information or personnel have the legal authority to do so. When military personnel visit company premises or request documents, ask employees to appear for questioning, or seek other cooperation, companies should verify the personnel's identity and agency, the purpose and legal basis of the investigation, and the scope of their investigative powers. This includes confirming whether the matter falls within the jurisdiction of military investigative authorities and whether the specific requests are legally authorized.

Where an investigation or request for cooperation lacks a legal basis, companies should take appropriate legal action, including raising objections.

2. Review the Warrant Before the Search Begins

A search warrant does not give investigators unrestricted access to a company's premises or information. The warrant defines the permissible scope of the search and seizure, and companies should ensure that investigators remain within those limits.

Consider a search involving the suspected disclosure of military secrets relating to Project A. Even if classified materials concerning Projects B and C are stored on the same server, they do not automatically fall within the scope of the seizure.

Before investigators begin, companies should review the warrant to establish:

- The alleged offense and the persons identified in the warrant, including the suspect or any person identified as a witness;
- The locations authorized for search; and
- The materials subject to seizure and their connection to the alleged offense.

If investigators attempt to search or seize materials beyond the authorized scope, companies should take appropriate action, including raising objections.

- Request a Copy of the Warrant: Article 159 of the Military Court Act requires investigators to present a search warrant. Unlike Articles 118 and 219 of the Criminal Procedure Act, however, it does not expressly require them to provide a copy. Companies should nevertheless request a copy to safeguard their defense rights and verify the alleged offense and the authorized scope of the search and seizure. In practice, a copy is often provided upon request.
- Limits on the Scope of a Search and Seizure: The search and seizure by the investigators should be confined to the persons, locations, and materials specified in the warrant.

In this regard, it is notable that the Supreme Court has held that materials not expressly identified in a warrant cannot automatically be considered relevant to an alleged offense merely because they are of the same or a similar nature as those specified in the warrant (Supreme Court Judgment No. 2021*Do*8284 dated February 27, 2025; Supreme Court

Judgment No. 2018*Do*18866 dated June 1, 2023).

3. Searches at Locations Requiring Military Security: Consent and Security Measures Required

Under Article 150 of the Military Court Act, searches and seizures at locations requiring military secrecy cannot be conducted without the consent of the person in charge or their representative. This requirement may apply to private-sector facilities as well as military installations.

However, the consent right does not give companies an unrestricted right to refuse a search. Under the same provision, consent may be withheld only where granting it would seriously prejudice important national interests. The Supreme Court has further held that refusal must be supported by specific, objective grounds indicating a serious risk to national security, national defense, or similar interests (Supreme Court Judgment No. 2026*Do*6500 dated July 9, 2026).

Rather than seeking to prevent a search solely because the location requires military security, companies should focus on appropriate safeguards that protect sensitive materials while allowing lawful investigative measures to proceed. Depending on the circumstances, companies should request:

- The presence of company security personnel during the search;
- Separation of areas covered by the search from those outside its scope;
- Measures to limit unnecessary photography and access to areas outside the authorized search scope; and
- Separate identification and handling of classified materials relevant to the investigation.

These measures can help prevent the unnecessary exposure of military secrets unrelated to the investigation and reduce the risk of a search extending beyond its authorized scope.

4. Electronic Data Seizures: Why Participation Matters

Electronic data requires particular attention during searches of defense companies. Computers and servers often contain information relating to multiple projects, including military secrets, defense technologies, and trade secrets that may have no connection to the alleged offense.

Two procedural safeguards are especially important:

(1) Review and Collect Relevant Data On Site

As a general rule, investigators should identify electronic data relevant to the alleged offense at the search location and seize it by printing or copying the selected information.

Removal of the storage device itself should be considered only in exceptional circumstances, such as where selecting relevant data on site is impossible or would make it substantially difficult to achieve the purpose of the seizure. Companies should seek legal advice before consenting to removal.

(2) Participation Rights in Subsequent Data Reviews

Participation should not end when investigators leave the premises.

The Supreme Court has held that the examination, printing, or copying of electronic data after a storage device has been removed remains part of the execution of the search warrant (Supreme Court Decision No. 2009*Mo*1190 dated May 26, 2011).

Defense companies should exercise their right to participate in the search and seizure process with legal counsel, including any subsequent review and selection of electronic data. Continued participation is important to prevent unrelated information from being unnecessarily examined, disclosed, or seized.

5. Preserve Evidence, but Recognize Statutory Deletion Requirements

Companies must distinguish between unauthorized deletion of investigative materials and deletion required by law.

When a search and seizure is anticipated or underway, materials relevant to the investigation should be preserved. Companies must not delete, alter or relocate such materials on their own initiative.

The Military Secret Protection Act, however, establishes a separate rule for certain military secrets remaining on electronic storage devices.

Under Article 16(3) of the Military Secret Protection Act, where military secrets subject to seizure have been submitted by printing or copying data from an electronic storage device, a prosecutor or military prosecutor may require the person in possession of the original device to delete any such military secrets remaining on it. A judicial police officer or military judicial police officer acting under the direction of a prosecutor or military prosecutor may also make such a request.

Failure to comply immediately with such a request may result in imprisonment for up to two years or a fine of up to KRW 20 million.

The following points are particularly important:

- Confirm the requesting official's authority, the information subject to deletion, and the scope of the request, and document the measures taken;
- Comply with separate obligations under Article 16 of the Military Secret Protection Act to report the loss or theft of military secrets and respond to requests for their submission by investigative authorities or military units; and
- Address any orders concerning the deletion, destruction, or vesting in the National Treasury of seized military

secrets, which may be issued by a prosecutor or military prosecutor even where the case concludes without prosecution, pursuant to Article 20-2 of the Military Secret Protection Act.

6. Prepare for a Search: Why Early Response Matters

In cases involving suspected violations of the Military Secret Protection Act, searches and seizures typically take place early in an investigation to identify how military secrets may have been disclosed. Evidence obtained at this stage can significantly shape the direction and scope of subsequent proceedings. Early legal involvement and a coordinated response are therefore critical.

When investigators arrive at company premises, the company should promptly contact legal counsel and communicate its intention to participate in the search. Where appropriate, it should request a reasonable delay to allow counsel to arrive, review the warrant and its scope, and participate in the process.

Companies should also be prepared for searches conducted without advance notice. Under Articles 122 and 219 of the Criminal Procedure Act, investigators may dispense with prior notice in urgent circumstances, including where there is a risk of evidence destruction.

An established internal response protocol can help companies address these situations promptly while protecting sensitive information and complying with lawful investigative requirements.

Practical Search and Seizure Checklist

For defense companies facing an investigation involving military secrets, the following measures should form the basis of an effective response:

1. **Prepare an internal response protocol.** Establish procedures in advance and arrange for legal counsel to participate from the outset.
2. **Verify the investigators' authority.** Confirm their identity, agency, and legal basis for the investigation and review the warrant.
3. **Check the scope and relevance of the search.** Confirm the persons, locations, and materials covered by the warrant and assess whether the materials sought are relevant to the alleged offense.
4. **Protect locations requiring military security.** Confirm applicable consent requirements and request appropriate security safeguards.
5. **Participate throughout the process.** Exercise participation rights during on-site searches and seizures, as well as subsequent selection of electronic data.
6. **Review the seizure inventory and follow-up requirements.** Confirm what has been seized and address any applicable obligations concerning the deletion or other disposition of military secrets.

How Shin & Kim Can Help

Shin & Kim LLC's Defense Industry & National Defense Team advises defense companies on matters involving military secrets, defense industry laws and regulations, and military investigative procedures.

The team provides advice throughout the investigation process, from developing search and seizure response protocols and assisting with on-site searches to advising on investigations involving company personnel and post-search procedures.

Key Contacts

Young-Hoon Kim
Partner

+82-2-316-2862
yhoonkim@shinkim.com

Seongjin Kim
Partner

+82-2-316-1843
sjinkim@shinkim.com

Jin Han-ock
Associate

+82-2-316-4647
hojin@shinkim.com

Donghyun Kim
Advisor

+82-2-316-2864
dhkim@shinkim.com

Sejin Kim
Senior Foreign Attorney

+82-2-316-7270
sejinkim@shinkim.com

Copyright SHIN & KIM LLC. All rights reserved.