

Fasoo Enhances ITAR Compliance with Data-Centric Security Controls

SEOUL, SOUTH KOREA, January 27, 2026 /EINPresswire.com/ --

— [Fasoo](#), the leader in data-centric security, highlights the growing challenges organizations face in maintaining compliance with the [International Traffic in Arms](#)

[Regulations \(ITAR\)](#) as defense

manufacturers and suppliers increasingly rely on global collaboration.

“The challenge is no longer limited to controlling physical exports alone. It lies in governing how sensitive technical data is accessed, shared, and reused across distributed teams, cloud platforms, and complex supplier networks,” said [Jason Sohn, Executive Managing Director](#) at Fasoo. “As collaboration becomes more global and digital, organizations need controls that move with the data itself to maintain compliance and control.”

Under the ITAR, an export can occur not only when controlled data leaves the United States, but also when it is disclosed to a foreign person within U.S. borders. This concept of “deemed export” means that access to controlled data may constitute a regulated event. In today’s digital engineering environments, where CAD files, design drawings, specifications, and reports move across systems and partners, maintaining compliance depends on controlling how data is accessed and used throughout its lifecycle.

Many organizations continue to rely on repository-level controls, network boundaries, or manual processes to manage ITAR obligations. However, these approaches often break down once technical data is downloaded, copied, or shared externally. Without controls that travel with the data, companies face increased risks of unauthorized access, untracked retransfers, and insufficient audit trails, which can lead to severe regulatory penalties and loss of export privileges.

Fasoo addresses these challenges by enabling a data-centric approach to ITAR compliance, one that governs technical data directly and continuously, regardless of where it travels. Instead of attempting to secure every system or collaboration tool, Fasoo focuses on embedding persistent protection, access control, and traceability into the files themselves.



With file-level encryption, ITAR-controlled technical data remains secure after download or transfer, ensuring that only authorized individuals can access sensitive content. Eligibility-based granular access controls allow organizations to align data access with citizenship, role, and project context, reducing the risks of unauthorized disclosure to foreign persons.

At the same time, comprehensive file activity logs provide end-to-end visibility into how export-controlled data is accessed, modified, shared, or retransferred.

This approach is particularly critical in multi-tier defense supply chains, where authorized partners may further share data with subcontractors or affiliates. By maintaining control and visibility beyond organizational boundaries, Fasoo helps organizations prevent hidden export violations while preserving efficient collaboration across engineering and manufacturing ecosystems.

By shifting ITAR compliance from a reactive, system-based process to a proactive, data-centric security embedded in data itself, organizations can reduce regulatory risks, strengthen audit controls, and build trust across defense supply chains.

For more information, visit <https://en.fasoo.com/insight/itar-compliance/>.

About Fasoo:

Fasoo provides unstructured data security, privacy, and enterprise content platforms that securely protect, control, trace, analyze, and share critical business information while enhancing productivity. Fasoo's continuous focus on customer innovation and creativity provides market-leading solutions to the challenges faced by organizations of all sizes and industries. For more information, visit <https://en.fasoo.com/>.

Jungyeon Lim

Fasoo

jungyeon@fasoo.com

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[YouTube](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/885067926>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable

in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.