

Design Data Control for Aerospace and Defense

How SOS Enterprise Helps Enforce Export Control Obligations where Semiconductor Design Data is Created, Shared, and Reused.

Executive Summary

In most industries, a permission model on design data is a matter of good practice. In aerospace and defense, access to design data can become a regulated act with legal, operational, and contractual consequences. Granting an engineer access to a design file may itself trigger an obligation, and the system holding that file is where the control is either applied or merely asserted.

This paper sets out what United States export control and defense acquisition policy require of the system that holds integrated circuit design data, what those requirements imply for its architecture, and what SOS Enterprise provides against each. It is written for the program security or export control lead who has to defend the control, the design data or CAD manager who must operate it, and the engineering executive who carries the consequence when it fails.

Introduction

Under the deemed export rule, releasing technical data to a foreign person inside the United States is treated as an export to that person's country of citizenship or last permanent residence. Published guidance names the exposure directly: chip design intellectual property, fabrication process flows and electronic design automation systems are areas of particular risk, and giving a non-US person access to controlled drawings, CAD files, source code, test data or manufacturing instructions can create a violation (Buchalter, 2025; CTP, n.d.).

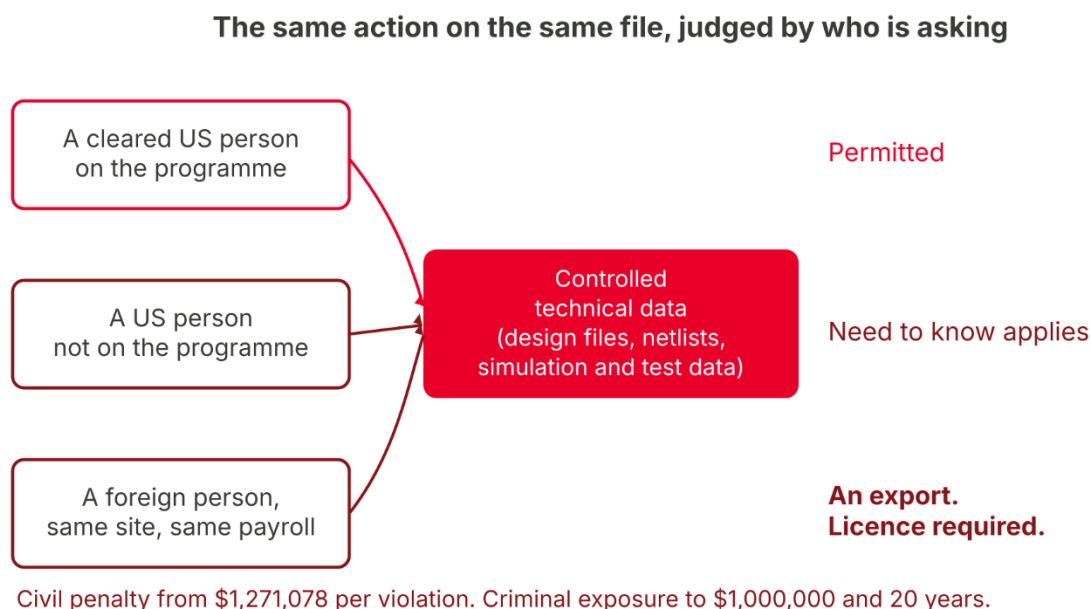


Figure 1. The legal character of an access decision depends on who is asking, not on what is being asked for.

The penalties are of a size that changes how the subject should be treated. The baseline civil penalty is \$1,271,078 per violation, or twice the value of the underlying transaction, whichever is

greater. Criminal exposure reaches \$1 million and 20 years of imprisonment per violation. Boeing agreed to pay a \$51 million administrative penalty for unauthorized transfers of defense technical data to foreign persons and related violations (Buchalter, 2025).

Three obligations follow, and all three fall on the system that holds the data. Access has to be decided per person and per object, not per network share. The decision must be enforced wherever the data can be reached, not only in the application a compliant user happens to open. And the organization needs to be able to show afterwards that the control was applied, to an auditor who was not present at the time.

Access as a Controlled Act

Deemed Export Risk in IC Design Environments

A conversation in a conference room, an email attachment and a granted file permission can all trigger the same licensing requirement as shipping hardware overseas (CTP, n.d.). For an integrated circuit design organization that means the controlled population is not a folder of documents. It is the working design data: schematics and layout, netlists, simulation results, test benches, characterization data and the scripts that produce them.

Whether a release requires a license depends on both the classification of the technology and the country of citizenship of the person receiving it. A single design object can therefore be freely available to one engineer, available to a second only on a need-to-know basis, and unavailable to a third sitting at the next desk on the same payroll.

Need-to-Know is Written into Policy

The Program Protection Plan is the single source document used to coordinate and integrate all protection efforts on a defense program. Its stated purpose is to deny access to Critical Program Information to anyone not authorized or without a need to know, and to prevent inadvertent disclosure of leading-edge technology to foreign interests (AcqNotes, n.d.; Defense Acquisition University, 2019).

Two phrases in that sentence are engineering requirements rather than policy language:

Need to know means authorization is per person and per object, and cannot be satisfied by a role held across a whole program.

Inadvertent disclosure means the control has to continue even when nobody is paying attention, which is a statement about defaults and about enforcement points.

Hardware assurance measures under the same policy are intended to reduce the likelihood that an adversary can exploit vulnerabilities built into microelectronics, insert malicious logic during development and fabrication, or introduce counterfeit parts (Defense Acquisition University, 2019). Each of those depends on knowing what was in a design at each point, and who could have changed it.

Compliance Is Now a Contractual Requirement

Cybersecurity Maturity Model Certification requirements became effective on 10 November 2025, following publication of the final rule in the Federal Register on 10 September 2025, and began appearing in new Department of Defense contracts from that date. Level 2—the level that applies to most contractors handling Controlled Unclassified Information—aligns with the 110 controls of NIST Special Publication 800-171. From 10 November 2028 the Department intends to include requirements at every level in all applicable solicitations and contracts, including option periods on contracts awarded earlier (Crowell & Moring, 2025; Secureframe, n.d.).

The effect is that access control on design data moves from something a program can assert to something a contract can be lost over, on a published timetable.

System Requirements for Controlled Design Data

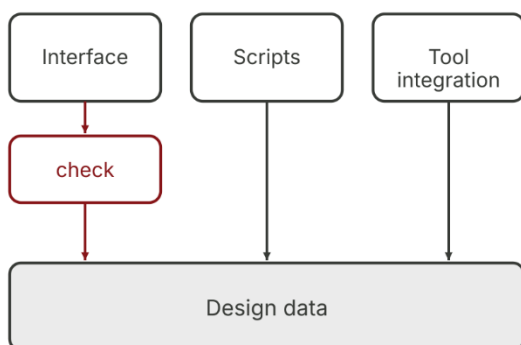
Enforcement at the Data Layer

Published practice for managing releasability across multinational programs is explicit about where enforcement belongs. Releasability markings are attached to every data object and evaluated on every query, with enforcement at the interface layer and at the data layer, never at the user interface alone (Corvus Intelligence, n.d.).

The reason is that a design environment is reached by many routes. Engineers use the application, but they also use command line tools, scripts, batch flows, continuous integration jobs and the design tools themselves. A check applied in only one of those routes is not sufficient as a control; it becomes a convention that other routes may bypass.

Checks held in the interface

every other route reaches the data unchecked



One mediated path

no route reaches the data without passing the same point

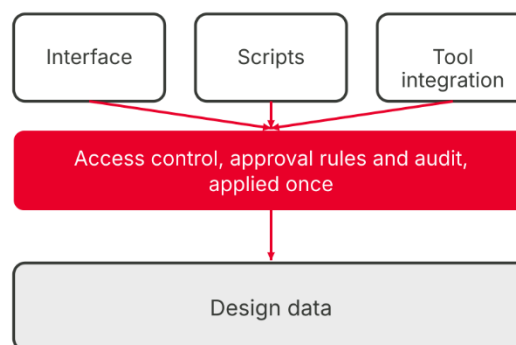


Figure 2. A control applied in one client is a convention. A control applied at the single point every client must pass is a mechanism.

Program and Site-Level Separation

The recommended pattern is to maintain distinct working environments for controlled and uncontrolled programs, with different access rules, supplier populations and data handling policies, giving an architectural separation equivalent to the physical separation defense contractors already maintain between classified and unclassified work areas (PreVeil, n.d.).

This has to hold at two levels. A program boundary separates one body of work from another. A need to know boundary operates inside a program, because not everyone cleared for a program is entitled to every part of it.

Limiting Copies of Controlled Technical Data

Every full copy of controlled technical data held outside the managed environment is a copy that has to be protected, backed up, accounted for in an audit and removed when a person leaves. Conventional design flows produce these copies routinely, because each engineer populates a working area with the part of the design they need.

The number of copies is therefore an export control variable and not only a storage cost.

Auditable Records of Access Decisions

An assessor arriving after the fact asks who had access to a given body of design data during a given period, who authorized it, on what basis, and what was done with it. Answering from directory permissions alone reconstructs the present state and says nothing about the past.

How SOS Enterprise Addresses These Requirements

These requirements point to a clear architectural pattern: controls must sit where the data lives, be evaluated on every request, and leave behind evidence that can be reviewed later. SOS Enterprise is designed around that pattern.

SOS Enterprise brings design data management, IP lifecycle management and governance together in one platform for semiconductor design organizations. The governance model is the part that matters most in this setting, and the architecture underneath it is what makes the model enforceable.

Server-Enforced Access through a Single Path

There is no direct access to the underlying store. Every request passes through the server, which is the single place where access control, automation rules and audit are applied. A script, a design tool integration, a continuous integration job and a person at a browser are subject to the same decision, because they arrive at the same point.

This is the property that makes the remaining controls meaningful. A permission model matters in proportion to the number of ways it can be bypassed.

Four Decisions before Anything is Returned

Four decisions, applied in order, before anything is returned

the last one is applied without a marker, so an unauthorised reader does not learn that a field exists

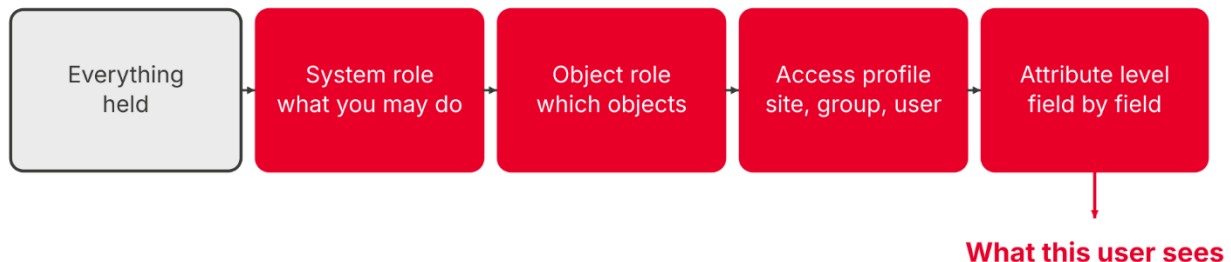


Figure 3. Access is narrowed four times, and the last narrowing leaves no trace that something was withheld.

Access is decided in four layers:

System role determines what a user may do at all, using built in roles or roles defined by the organization.

Object role and object permissions determine which objects they may do it to, assigned per object rather than inherited from a position in a directory tree.

Access profiles restrict search and view access, and are built from sites, groups and individual users. The site dimension matters here, because geography and the population at a location are often the terms in which an export control decision is actually written.

Attribute access levels operate field by field, at public, protected or private, enforced on the server. This is the level at which need to know inside a program becomes practical, because a single IP can carry both a technical description that a wide population may read and conditions of use that only a few may read.

The last of those is enforced silently. An unauthorized reader does not see a redaction marker, because a redaction marker is itself a disclosure that something exists.

Program and Site-Level Governance

A program is held as a project with its own membership, its own roles and its own approval rules. Groups carry their own attributes and classes, and are the unit used in access profiles, so a population defined once can be applied consistently across the objects a program contains.

Design data is replicated between sites over encrypted connections, with each site running a service that coordinates with the others. Which sites participate is an administrative decision, which is the point at which the geography of a program is set.

Reducing Copies through Linked Work Areas

Working areas can be populated with links into a single managed copy rather than with duplicates of the design. A project of 100 gigabytes yields working areas of approximately 50 megabytes. An engineer holds a real, editable copy only of the files they have actively checked out, and the copy becomes a link again when the work is checked in.

Controlled technical data held on engineer workstations, for a 100 GB design and 20 engineers

Full copy in every work area



Work areas holding links into one managed copy



Figure 4. Reducing the number of copies of controlled technical data reduces the amount of it that has to be protected, audited and removed.

Two further properties matter in this setting. Files in the managed copy are stored with obfuscated names, so it is not a browsable representation of the design to anyone who reaches the file system. And a working area can be populated sparsely, covering only the part of the design hierarchy a person is working on, so the controlled population a given engineer holds is smaller again.

Recorded Approval Workflows

Requests to view the details of an IP, to download it, to upload a new IP or revision, and to join a project are handled as approval tasks. The request, the approver and the outcome are recorded. The approval flow is defined by the organization, so the sequence of authorizations a program requires can be encoded rather than remembered.

An event driven automation layer allows conditions to be attached to those decisions, so that access to a designated body of work requires a particular approval, and the people who depend on an object are notified when it changes.

The result is that the question in section 3.4 is answered from a record of decisions rather than from an inspection of current permissions.

Revision History and Design Assurance Evidence

Design assurance for airborne electronic hardware under DO-254 assigns a Design Assurance Level from A to E according to the severity of the failure condition the hardware contributes to. For the higher levels the guidance calls for full bidirectional traceability across requirements, design, implementation and test results, and traceability is among the first things certification authorities

examine. The Hardware Configuration Management Plan specifies version control and change management procedures for the program (Jama Software, n.d.; Visure Solutions, n.d.).

SOS Enterprise records every change to a design object as a revision, and a snapshot captures the revision of every file in every library at a single moment as an immutable record. Two levels of version are maintained, so the versions released for reuse are recorded separately from the daily working history and do not have to be inferred from it. Each IP carries a hierarchical bill of materials resolved on the server and a record of its consumers, so the composition of a delivered design and the reach of any part of it are both retrievable. Documents attach to the specific IP or project revision they describe, which is what keeps a verification report bound to the version it verified.

Requirements Mapped to SOS Enterprise Mechanisms

Requirement	What Meets It
Decide access per person and per object	System role, object role and object permissions, access profiles built from sites, groups and users
Apply need to know inside a cleared program	Attribute access levels enforced on the server, applied without a marker
Enforce wherever the data is reachable	One mediated path, with access control, automation and audit applied at the server
Separate controlled from uncontrolled work	Projects with their own membership, roles and approval rules; administrative control of which sites participate
Limit the spread of controlled data	Working areas populated with links into one managed copy, sparse population, obfuscated storage
Show that control was applied	Approval tasks recording request, approver and outcome; event driven rules; revision and snapshot history
Support design assurance evidence	Immutable snapshots, two levels of version, resolved bill of materials, documents bound to revisions

Allied and Partner Program Collaboration

These control questions become more complex when design data crosses organizational or national boundaries. Allied and partner programs require shared visibility without assuming shared entitlement.

Co-production and co-development arrangements transfer proprietary technology, manufacturing processes and technical data between parties, and require documentation, program protection, differential capability, encryption and access controls to protect what is shared (Defense Trade Solutions, n.d.). Release of controlled technical data to a foreign partner without an approved agreement is limited in scope (Defense Security Cooperation Agency, n.d.).

Two consequences follow for a design data environment supporting such a program.

The first is that releasability is a property of the object rather than of the person. In a multinational setting one item may be releasable to one group of partners and not to another, and the same holds for design artifacts inside a jointly developed device. Holding that as a structured attribute,

with access enforced at the field level, is closer to the shape of the obligation than holding it as a folder.

The second is that a shared catalogue and shared visibility are different things. A partner may need to know that an IP exists, its interfaces and its version, without being entitled to its implementation. Access profiles and attribute access levels together allow the catalogue to be common while the contents are not, which is what makes a jointly developed program workable without creating a second, divergent copy of the record for each participant.

The pattern is consistent across domestic, multinational, and partner environments: access decisions must be made at the level of the design object, enforced by the system of record, and retained as evidence.

Best Practices Before Tool Selection

The following hold whatever system an organization uses.

Write the control at the object level, not the share level. A network share is a boundary that cannot express need to know, and it is the boundary most inadvertent disclosures cross.

Decide where enforcement lives before selecting a tool. A control applied by one client is bypassed by every other client. Establish which point every route must pass and confirm that the decision is made there.

Hold releasability and classification as structured data. A marking that exists only in a document header cannot be evaluated on a query and cannot be reported against.

Record the grant, not only the state. Current permissions describe today. An assessment is about a period, and only a record of decisions covers it.

Count the copies. Establish how many complete copies of controlled design data exist outside the managed environment, on workstations, on shared drives and in personal archives. The number is usually higher than expected, and reducing it is the least disruptive improvement available.

Test removal. Take a person who left the program six months ago and establish what they could have reached, when authorization was withdrawn, and whether any copy they held still exists.

Where to start

The exercises above are worth running before any tooling decision, because they convert a general concern into a measured one. Counting copies and testing removal both take days rather than weeks, and both produce a number a program review can act on.

From there the sequence is usually to express program boundaries as projects with explicit membership, to move the markings that govern release from document headers into structured attributes, and to route access grants through a recorded approval rather than a request to an administrator.

SOS Enterprise supports each of those steps directly. Program separation is expressed as project membership with its own roles and approval rules. Markings held as attributes are enforced on the server, field by field, without revealing what was withheld. Grants are recorded as approval tasks carrying the request, the approver and the outcome. And working areas built from links rather than copies reduce the controlled population that has to be protected in the first place.

By reducing uncontrolled copies, recording access decisions, and enforcing permissions at the data layer, SOS Enterprise helps turn export control from a policy assertion into an operating control. The design data management, IP lifecycle management and governance capabilities described in section 4 are the three parts of that control.

Export control obligations are enforced against what an organization can demonstrate, and a program demonstrates control with the records its systems kept while nobody was watching.

For more information or to book your SOS Enterprise demo, visit the webpage: [SOS Enterprise | Keysight](#)

References

AcqNotes. (n.d.). Program protection plan (PPP).

<https://acqnotes.com/acqnote/careerfields/program-protection-plan>

Buchalter. (2025). Foreign talent, domestic risk: Deemed export issues in tech hiring.

<https://www.buchalter.com/insights/foreign-talent-domestic-risk-deemed-export-issues-in-tech-hiring/>

Corvus Intelligence. (n.d.). Complete guide to NATO interoperability for defense software.

<https://corvusintell.com/blog/interoperability/complete-guide-to-nato-interoperability/>

Crowell & Moring. (2025). Finally, the CMMC final rule: DoD completes CMMC rulemaking,

ushering in new era in DoD cybersecurity. <https://www.crowell.com/en/insights/client-alerts/finally-the-cmmc-final-rule-dod-completes-cmmc-rulemaking-ushering-in-new-era-in-dod-cybersecurity>

CTP, Inc. (n.d.). Deemed exports in U.S. export control compliance. <https://www.ctp-inc.com/articles/deemed-exports-in-u-s-export-control-compliance>

Defense Acquisition University. (2019). Defense acquisition guidebook, chapter 9: Program protection.

<https://www.dau.mil/guidebooks/Shared%20Documents%20HTML/Chapter%209%20Program%20Protection.aspx>

Defense Security Cooperation Agency. (n.d.). Security assistance management manual, chapter 3.

<https://samm.dsca.mil/chapter/chapter-3>

Defense Trade Solutions. (n.d.). Decoding co-production and co-development in ITAR.

<https://defense-trade.com/decoding-co-production-and-co-development-in-itar-a-comprehensive-guide/>

Jama Software. (n.d.). What is DO-254? A complete guide to airborne hardware design assurance.

<https://www.jamasoftware.com/requirements-management-guide/aerospace-and-defense/do-254/>

PreVeil. (n.d.). PreVeil for international defense suppliers: The practical path to CMMC, DFARS,

and ITAR compliance. <https://www.preveil.com/resources/preveil-for-international-suppliers-seeking-cmmc-dfars-and-itar-compliance/>

Secureframe. (n.d.). The CMMC 2.0 timeline: Key dates, deadlines and the current phase.

<https://secureframe.com/hub/cmmc/proposed-final-rule>

Visure Solutions. (n.d.). DO-254 explained: Design assurance guidance for airborne electronic

hardware. <https://visuresolutions.com/aerospace-and-defense/do-254/>

As a mission-critical design enablement partner, Keysight connects design, emulation, and test so customers can solve the world's most complex engineering challenges. Accelerate innovation at www.keysight.com.



This information is subject to change without notice. © Keysight Technologies, 2026, Published in USA, October 7, 2026, 3126-1790.EN