ASSESSMENT · SB-2026-02

The Export Rule Controls Your Data. It Never Tells You How to Protect It.

Where a cybersecurity obligation actually comes from when the regulation that controls your information does not contain one.

PUBLISHED	STATUS	REVISED
30 JULY 2026	PUBLISHED	30 JULY 2026
VERSION	AUTHOR	LICENSE
1.0	COLLIN B. GEORGE, CISSP	CC BY 4.0

Unclassified // Open Source

Analytic record

TYPE	Analysis — a structural account of how a cybersecurity obligation attaches to export-controlled information. Stable except where the underlying instruments change.
GOVERNING JUDGMENT	An export-control regulation can establish that information is controlled without prescribing any cybersecurity control set. The control set arrives through the Controlled Unclassified Information framework and becomes binding through a contract. Applicability is a contract question, not a question about the nature of the data.
PROBABILITY	That 10 CFR Part 810 prescribes no cybersecurity control set is assessed as certain; it rests on the text of the regulation. That CUI safeguarding obligations reach a non-federal entity only through a federal agreement is assessed as almost certain.
ANALYTIC CONFIDENCE	High for the regulatory analysis, which rests on published text in the Code of Federal Regulations and the CUI Registry. Moderate for the finding that Part 810 contains no encryption provision, which is an argument from the absence of a provision and is stated as such. These are separate axes and are not combined.
SUPERSESSION	Reassess on finalization of the FAR CUI rule (FAR Case 2017-016), on the CMMC Reform Task Force report expected mid-September 2026, or on any DOE guidance addressing information security under Part 810.
REVISION HISTORY	1.0, 30 July 2026 — first publication.

Executive summary

— 10 CFR Part 810 controls unclassified nuclear technology. Read it end to end and you will not find a cybersecurity requirement. No encryption. No access logging. No control set of any kind.

— That is not an oversight. Export rules say what is controlled and who may receive it. They do not say what to build.

— The control set comes from a different place — the Controlled Unclassified Information framework, which points to NIST SP 800-171.

— It becomes binding through a contract clause. Not through the export rule, and not because of what the data is. The same engineering file can carry a cybersecurity obligation at one company and none at another.

— ITAR and the EAR each give you an encryption safe harbor. Part 810 gives you nothing of the kind. Encrypting controlled nuclear technology is sound practice. It is not a regulatory answer.

IF YOU READ NOTHING ELSE

What to do	Pull the contract and read the clause list. If DFARS 252.204-7012 or an agency equivalent appears anywhere in your chain, NIST SP 800-171 Revision 2 is mandatory and your standard is settled. If no such clause appears, no federal cybersecurity standard is legally imposed on that information — whatever its export status.
Who this affects	Any firm holding export-controlled technical data. Your export-control obligation and your cybersecurity obligation come from different instruments and attach independently of one another. Having one does not establish the other.
What being wrong costs	Build more than you owe and you pay for an environment nothing required, every month, indefinitely. Build less than you owe and you face award ineligibility, contract action, and False Claims Act exposure at treble damages — with personal exposure for whoever signed the affirmation.

A question comes up early in almost every conversation about export-controlled engineering work: *we are subject to export controls, so which cybersecurity framework do we have to follow?* It is the right question. The difficulty is that the answer is not in the export regulation, and people go looking for it there.

10 CFR Part 810 is the clearest illustration available. It is the Department of Energy rule governing assistance to foreign atomic energy activities — the transfer of unclassified nuclear technology, whether abroad or to a foreign national standing in a room in the United States. It carries civil and criminal penalties. It is unambiguously a regulation about controlling sensitive information. And it contains no cybersecurity requirements at all.

What Part 810 Actually Says

Part 810 implements section 57 b.(2) of the Atomic Energy Act, codified at 42 U.S.C. 2077.[1] Its structure is straightforward. Section 810.2(b) lists the activities within scope. Section 810.6 makes certain activities generally authorized where the destination appears in Appendix A. Section 810.7 requires case-by-case authorization from the Secretary in three situations: activities with a country or entity not on the Appendix A list; the transfer of sensitive nuclear technology to any foreign country or entity at all; and a list of specified activities including uranium and plutonium isotope separation, heavy water production, production reactors, and reprocessing of irradiated fuel.[2]

The definitions matter more than they usually do. Section 810.3 defines a foreign national as someone who is not a citizen or national of the United States, but *excludes* lawful permanent residents and protected individuals under 8 U.S.C. 1324b(a)(3). That is narrower than the phrase most companies use in practice, and an access rule written around “U.S. persons” will not match the regulation it is meant to

enforce. The same section defines technical data to include information recorded on disks, tapes, read-only memories, and computer codes — so there is no argument that the regulation was written for paper and never contemplated systems.[3]

Section 810.12 requires reports. Section 810.15 provides for penalties: criminal exposure under section 222 of the Atomic Energy Act, and, since a 2023 rulemaking, civil monetary penalties now set at $127,973 per violation, applied per day where a violation is a continuing one, and adjusted annually for inflation.[4]

Now the part that does not exist. Read the regulation in full, and read the 2015 final rule that produced its current form. The words *cybersecurity*, *information security*, and *encryption* do not appear. Not once, in either.[5]

What Part 810 says about protecting the technology it controls amounts to two things. Section 810.6(b) generally authorizes certain transfers to a foreign national where that person "executes a confidentiality agreement with the U.S. employer to safeguard the technology from unauthorized use or disclosure." And section 810.11(b) requires an applicant for specific authorization to describe "the applicant's technology control program" — a term the regulation uses and never defines. There is no list of elements. No requirement for access control, audit logging, encryption, network segmentation, or any other technical measure. DOE and NNSA guidance materials on Part 810 describe authorization mechanics and confidentiality agreements; they do not prescribe an information-security standard either.

> **A regulation can tell you that your information is controlled, that transferring it without permission is a crime, and that violations cost $127,973 apiece — and never once tell you what to build.**

WHY THIS MATTERS

You cannot discharge Part 810 by buying a security product, because there is no control set in the regulation to buy against. What the rule actually demands is that unauthorized people do not receive the technology, and that you can demonstrate it. That is an access-control and evidence problem, and it is the reason a "technology control program" and the systems enforcing it end up mattering more than any single tool.

Two Other Export Rules Address Encryption. This One Does Not.

This is worth dwelling on, because most firms handling controlled technical data have absorbed a rule of thumb from elsewhere in the export-control world, and it does not transfer.

The International Traffic in Arms Regulations contain section 120.54, which lists activities that are not exports. Among them: sending, taking, or storing technical data that is unclassified, secured end-to-end, and secured using cryptographic modules compliant with FIPS 140-2 or by other means providing security strength at least comparable to 128-bit AES — provided the data is not intentionally sent to or stored in a country listed in section 126.1, or in Russia. The provision goes further and says that the ability

to access technical data in encrypted form that meets those criteria does not constitute a release or export of that data.[6]

The Export Administration Regulations contain the same architecture at section 734.18, which was the earlier of the two and served as the model.[7]

Part 810 has no equivalent. There is no provision stating that encrypting controlled nuclear technology means a transfer has not occurred. There is no DOE guidance saying so either. The practical consequence is direct: a company can encrypt nuclear technology to a FIPS-validated standard, which is prudent and which will help it satisfy obligations that come from elsewhere, and it will not have earned the regulatory safe harbor that the same encryption would earn under the ITAR or the EAR. This finding rests on the absence of a provision rather than the presence of one, and it is stated on that basis.

> **WHY THIS MATTERS**
>
> If anyone on your team has been reasoning that encrypted data is not an export, find out where that came from. Under ITAR or the EAR it is a defensible position grounded in regulatory text. Applied to nuclear technology under Part 810, it is an assumption with nothing behind it. Encrypt anyway — it will help you satisfy obligations that come from elsewhere — but do not treat it as an authorization answer.

So Where Does the Control Set Come From?

Through the Controlled Unclassified Information framework, in five steps. Each step has an authority behind it.

One. Executive Order 13556 created a government-wide program for unclassified information that laws, regulations, and government-wide policies require to be protected.[8]

Two. The National Archives issued the implementing rule at 32 CFR Part 2002. It distinguishes CUI Basic, where the underlying authority sets no particular controls, from CUI Specified, where the authority prescribes its own. And it states that NIST SP 800-171 defines the requirements for protecting CUI Basic on non-federal information systems.[9]

Three. The CUI Registry contains a category called Export Controlled. Its description covers information whose export could reasonably be expected to affect national security and nonproliferation objectives — and it names, expressly, *sensitive nuclear technology information*. Among the authorities listed for that category is 42 U.S.C. 2077(a): the same statute Part 810 implements, designated as a Specified authority and carrying the marking CUI//SP-EXPT.[10]

Four. CUI Specified means you follow the safeguarding requirements the underlying law prescribes. Part 810 prescribes none.

Five. Where a Specified authority is silent on safeguarding, the CUI Basic controls apply. Those controls are NIST SP 800-171 — 110 requirements across 14 families in Revision 2, which remains the revision the Department of Defense enforces.[11]

So the chain runs from a nuclear export regulation that says nothing about cybersecurity, through a records-management executive order, to a NIST publication. Nothing in that chain is obscure. It is simply spread across four documents that nobody reads together.

> **WHY THIS MATTERS**
>
> When a customer asks which standard you meet, the answer is NIST SP 800-171 Revision 2, and you should be able to say why in one sentence without reaching for counsel. Being able to explain the derivation is what separates a firm that has thought about its obligations from one repeating what a vendor told it.

The Part Most People Get Wrong

Here is where the common account fails. It is usually stated as: the data is export-controlled, therefore it is CUI, therefore 800-171 applies. Each arrow in that sentence is doing work the regulation does not support.

The CUI rule binds executive branch agencies. It reaches a company through an agreement — a contract, grant, licence, or similar instrument. And the definition is explicit about the boundary. CUI does not include information that a non-executive-branch entity "possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency."[9]

Read that against a real situation. A company designs equipment on its own money, for a commercial customer, using its own engineers. The design information is squarely export-controlled — Part 810 applies to it, and transferring it to a foreign national without authorization is unlawful. But it did not come from a federal agency and was not created for one. It is not CUI, and no federal cybersecurity standard is legally imposed on it.

Change one fact. The same company performs the same work under a subcontract to a national laboratory operator, and the prime flows down DFARS 252.204-7012 or an equivalent DOE clause. Now the information sits inside a federal agreement, the CUI framework reaches it, and NIST SP 800-171 is contractually mandatory.

Same engineering. Same file. Same server. Different obligation — because the contract changed, not because the data did.

> **Your export-control obligation follows the technology. Your cybersecurity obligation follows the contract. They are different questions with different answers, and conflating them produces error in both directions.**

Both directions is the point. Firms over-scope, building to a certification standard nothing in their contract requires, and paying for it. Firms under-scope, reasoning that they hold no direct federal contract and therefore owe nothing, and missing a flow-down sitting in a subcontract nobody read. The first mistake costs money. The second costs eligibility, and can cost considerably more than that.

> **WHY THIS MATTERS**
>
> This is the question to settle before authorizing spend, not after. The scope of what you must build is decided by a document you already hold. Two firms performing identical engineering can owe completely different things, and the only way to know which one you are is to read the clause list in your own contracts.

One further distinction is worth keeping straight, because the terms sound interchangeable and are not. The CUI Registry also carries nuclear-specific categories — Unclassified Controlled Nuclear Information under 42 U.S.C. 2168, and Naval Nuclear Propulsion Information — which rest on different statutes and protect different information, principally facility and material security data rather than design and manufacturing technology.[12] Sensitive nuclear technology under Part 810 travels through the Export Controlled category. Both are CUI. They arrive by different routes and can carry different handling requirements.

What This Looks Like Across the Regimes You Might Touch

Regime	What it controls	Prescribes a control set?	Where the control set comes from
10 CFR Part 810 DOE / NNSA	Transfer of unclassified nuclear technology and assistance, including to foreign nationals inside the U.S.	No	CUI framework plus a federal contract
ITAR State / DDTC	Defense articles and technical data on the U.S. Munitions List	No control set, but § 120.54 defines an encryption safe harbor	CUI framework plus a contract; encryption standard self-contained for the carve-out
EAR Commerce / BIS	Dual-use items and technology; nuclear end-use restrictions at § 744.2; 0-series ECCNs	No control set, but § 734.18 defines an encryption safe harbor	CUI framework plus a contract
10 CFR Part 110 NRC	Export and import of nuclear equipment and material — hardware, not technology	No	Not an information-security regime
DFARS 252.204-7012	Safeguarding covered defense information; 72-hour incident reporting	Yes, by reference	NIST SP 800-171, imposed by contract clause
FAR 52.204-21 now 52.240-93	Basic safeguarding of federal contract information	Yes	Fifteen requirements, self-contained

Regime	What it controls	Prescribes a control set?	Where the control set comes from
CMMC 32 CFR Part 170	Verification that a contractor meets 800-171	Adopts 800-171; adds assessment	NIST SP 800-171 — a verification layer, not the source of the duty
DOE contractor requirements	Protection of CUI and UCNI on contractor systems	Yes, by contract and directive	DEAR clauses and DOE orders

Read down the third column. Only the contract clauses prescribe anything. Every export regulation in the table controls information without specifying how to secure it.

What It Costs to Get This Wrong, in Both Directions

Scoping error is not a one-sided risk, and the two failure modes have different costs and different time horizons.

If you build more than you owe	If you build less than you owe
A government-cloud environment, licensing, and managed services no contract required — a recurring cost with no termination date.	**Loss of award eligibility. Where a contract requires a current score or status, a lapse costs a renewal without anyone alleging anything.**
Engineering workflow constrained for no regulatory reason: split tenants, restricted collaboration, slower work on non-controlled projects.	Contract action — cure notices, withheld payment, termination.
Compliance effort spent on requirement families that were never triggered, displacing work on obligations that were.	False Claims Act exposure. Damages are trebled, with a penalty per claim submitted, and cases can be brought by a private whistleblower.
A credibility cost with customers when the posture cannot be explained by reference to any clause.	Personal exposure for the person who signed. Reckless disregard suffices; the statute does not require an intent to deceive.

The asymmetry is worth stating plainly. Over-building is expensive and recoverable. Under-building is comparatively cheap right up to the point at which it is not, and the consequence arrives attached to a representation someone already made in writing.

The July Suspension Proved the Point

On 13 July 2026 the Department of War suspended CMMC Phase II, the third-party certification layer that was to begin appearing in contracts on 10 November 2026.[13] The suspension was announced alongside a sixty-day review, and it changed nothing about what contractors owe. DFARS 252.204-7012 continued. NIST SP 800-171 Revision 2 continued. Self-assessment and SPRS scoring continued. The annual affirmation at 32 CFR 170.22 continued.[14] That was the subject of the companion assessment in this series.[15]

Set against the structure described above, the reason is plain rather than surprising. CMMC was never the source of the obligation. It was a mechanism for checking whether the obligation had been met. The duty itself sits in the contract clause, and behind the clause in the CUI framework, and behind that in a NIST publication. Removing the verification layer left the obligation layer untouched because they were never the same layer.

The same logic runs one step further. A regulation that never prescribed a control set cannot lose one when a certification program pauses. Whatever the Task Force recommends in September will change what contracts require going forward. It will not change what Part 810 says, because Part 810 never said anything on the subject.

Nobody Has Ever Been Fined Under Part 810

There is an asymmetry here that is worth stating plainly, because it runs against intuition.

Part 810 carries real penalties. DOE finalized the civil penalty procedures in a rule effective February 2023, and the maximum now stands at $127,973 per violation.[4] Yet no assessed civil penalty under Part 810 appears anywhere in the public record — not in DOE or NNSA announcements, not in the Federal Register, not in the trackers that law firms maintain for exactly this purpose. The leading criminal matter under section 57 predates the civil penalty rule: Szuhsiung Ho pleaded guilty in 2017 and received twenty-four months.[16] Part 810 enforcement records are not always public, so absence of a published penalty is strong evidence rather than proof.

Now look at the other side. In fiscal year 2025 the Department of Justice reported more than $52 million recovered across nine cybersecurity settlements under the False Claims Act, and has settled fifteen such matters since the Civil Cyber-Fraud Initiative began in 2021.[17] Georgia Tech Research Corporation paid $875,000 in September 2025 over an allegedly fictitious assessment environment and a campus-wide score DOJ called false.[18] In June 2026 a Huntsville contractor paid $507,144 after self-reporting a perfect score of 110 and later being assessed by the government at negative 170.[19]

So the export regulation that controls nuclear technology and carries six-figure penalties has, so far as the public record shows, never assessed one. The contract clause that says nothing about nuclear technology at all is where the enforcement actually happens. If you are budgeting attention by where the risk has historically landed, it lands on the representation you made in a federal contract — not on the export rule that made your data sensitive in the first place.

> **WHY THIS MATTERS**
>
> The exposure that has actually cost companies money is not a Department of Energy penalty. It is the score and the affirmation sitting in a federal database with a named official attached to them. If you are deciding where to direct scarce attention, direct it at whether those statements can be substantiated — not at the export regulation, which for all its severity has no visible enforcement record.

Three Questions That Settle It for Your Company

None of these requires counsel to answer, though the answers may send you to counsel.

One. Where did this information come from? Did it originate with a federal agency, or was it created for one under a contract, grant, or other agreement? If neither — if your engineers made it on company money for a commercial customer — it may be export-controlled without being CUI, and no federal cybersecurity standard is legally imposed on it.

Two. If there is a federal agreement, what clause is in it? Not what your customer said on a call. The clause list in the contract. Look for DFARS 252.204-7012, for FAR 52.204-21 or its renumbered form at 52.240-93, and for DOE equivalents. The clause is what creates the obligation, and it is a document you already hold.[20]

Three. If a customer is asking you to become compliant, what exactly are they citing? Get it in writing. A customer requirement that names NIST SP 800-171 Revision 2 sets a different target than one demanding a government-cloud environment or third-party certification. Building to the wrong assumption is expensive, and the language costs nothing to obtain.

If those three answers are clear and consistent, the framework question resolves itself. If they conflict — a prime demanding certification under a contract carrying no such clause, say — that conflict is the finding, and it is better identified before an environment is built around it.

When This Stops Being a Technical Question

Whether particular technology falls within Part 810's scope, whether a transfer requires specific authorization, and who a company designates as its empowered official are legal determinations. So is any conclusion that a representation already made to the government may have been inaccurate. Those belong with export-control counsel, and the second belongs there immediately.

What is engineering, and what this assessment addresses, is the question of which control set a system should be built to and why. That question has an answer, and the answer is not in the export regulation.

This assessment is not legal advice and is not a substitute for counsel.

LIMITATIONS

What this assessment does not establish

This assessment addresses how a cybersecurity obligation attaches to export-controlled information. It does not determine whether any particular technology is within Part 810's scope,

whether any particular firm holds CUI, or which framework binds any particular contract. Those are determinations that depend on facts and instruments not in the public record.

The finding that Part 810 contains no cybersecurity provision rests on full-text review of the regulation and its 2015 final rule. It is an argument from the absence of a provision. DOE could address information security through guidance without codifying it, and the review conducted here found no such guidance; that is not the same as proving none exists.

The absence of any assessed civil penalty under Part 810 rests on published records. The civil penalty rule permits but does not require publication of notices of violation, so non-public enforcement cannot be excluded.

Two matters material to the analysis are unresolved. The FAR CUI rule proposed in January 2025 has not been finalized, and its final form would affect how CUI obligations reach civilian-agency contractors. The CMMC Reform Task Force has not reported. Neither is treated here as settled.

An assessment that cannot state what would change it should not be published. This one would change if DOE issued guidance prescribing information-security requirements under Part 810; if the National Archives or a court held that CUI status attaches to information by subject matter alone, without a federal agreement; or if an enforcement action imposed 800-171-type obligations on a firm directly under an export regulation rather than through a contract.

SOURCES

Primary sources

Every factual assertion traces to a primary regulatory, statutory, or Department of Justice record. Where the public record does not settle a question, the text says so rather than resolving it by inference.

1. 10 CFR Part 810, *Assistance to Foreign Atomic Energy Activities*, eCFR, Title 10, retrieved 30 July 2026. Authority: Atomic Energy Act § 57 b.(2), 42 U.S.C. 2077. `https://www.ecfr.gov/current/title-10/chapter-III/part-810`
2. 10 CFR 810.6 (generally authorized activities and Appendix A destinations); 10 CFR 810.7(a), (b), (c) (activities requiring specific authorization, including the transfer of sensitive nuclear technology to any foreign country or entity).
3. 10 CFR 810.3 (definitions of foreign national, sensitive nuclear technology, and technical data).
4. 10 CFR 810.15; civil penalty procedures final rule, 88 FR 1979 (12 January 2023), implementing the amendment to Atomic Energy Act § 234A by section 3116(b) of the FY2019 National Defense Authorization Act; penalty amount as adjusted, 89 FR 105406 (27 December 2024).
5. Department of Energy, *Assistance to Foreign Atomic Energy Activities*, final rule, 80 FR 9359 (23 February 2015). Full-text review of the rule and preamble, including the discussion of public comments, identifies no reference to cybersecurity, information security, or encryption.
6. 22 CFR 120.54 (ITAR, activities that are not exports, reexports, retransfers, or temporary imports), added at 84 FR 70887 (26 December 2019).
7. 15 CFR 734.18 (EAR, activities that are not exports, reexports, or transfers), added at 81 FR 35604 (3 June 2016).

8. Executive Order 13556, *Controlled Unclassified Information* (4 November 2010).

9. 32 CFR Part 2002, particularly § 2002.4 (definitions of CUI, CUI Basic, and CUI Specified, and the exclusion of information a non-executive branch entity possesses in its own systems absent a federal origin), § 2002.14 (safeguarding; designation of NIST SP 800-171 for non-federal systems), and § 2002.16 (agreements and arrangements). Final rule at 81 FR 63324 (14 September 2016).

10. National Archives and Records Administration, CUI Registry, category *Export Controlled* (marking EXPT; banner CUI//SP-EXPT where a specified authority applies), listing 42 U.S.C. 2077(a) among its authorities and naming sensitive nuclear technology information in the category description. **https://www.archives.gov/cui/registry/category-detail/export-control**

11. NIST Special Publication 800-171, Revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* — 110 requirements in 14 families.

12. NARA CUI Registry, categories *Unclassified Controlled Nuclear Information — Energy* (42 U.S.C. 2168) and *Naval Nuclear Propulsion Information*.

13. Department of War, *Forging the Arsenal of Freedom: Department of War Suspends CMMC Phase II Requirements* (13 July 2026); suspension memorandum signed 10 July 2026 by DoW Chief Information Officer Kirsten A. Davies, with a separate memorandum from the Under Secretary of Defense for Acquisition and Sustainment directing removal of third-party certification requirements from active solicitations.

14. DFARS 252.204-7012; 32 CFR 170.22 (annual affirmation); 48 CFR 204.7501. The 32 CFR program rule took effect 16 December 2024; the 48 CFR acquisition rule took effect 10 November 2025.

15. George, Collin B., *The Deadline Went Away. The Obligations Did Not.* Assessment SB-2026-01, Sanctir LLC, 20 July 2026.

16. *United States v. Szuhsiung Ho*, E.D. Tenn., guilty plea January 2017; twenty-four month sentence for conspiracy to unlawfully engage in the production of special nuclear material outside the United States without Department of Energy authorization.

17. U.S. Department of Justice, *Fact Sheet: False Claims Act Settlements and Judgments, Fiscal Year 2025* (16 January 2026). **https://www.justice.gov/opa/media/1424126/dl**

18. U.S. Department of Justice, settlement with Georgia Tech Research Corporation (30 September 2025).

19. Settlement agreement, *United States v. LOGZONE, Inc.* (June 2026); Department of Justice release of 18 June 2026. **https://www.justice.gov/opa/media/1446716/dl**

20. Class Deviation 2026-O0025, *Revolutionary FAR Overhaul — FAR Part 40, DFARS Part 240*, Defense Acquisition Regulations System, effective 1 February 2026; Revision 2 issued 16 July 2026, effect not yet established in the public record.

21. FAR CUI proposed rule, FAR Case 2017-016, 90 FR 4278 (15 January 2025); not finalized as at the date of this assessment.

SUGGESTED CITATION

> George, Collin B. *The Export Rule Controls Your Data. It Never Tells You How to Protect It.* Assessment SB-2026-02, version 1.0. Sanctir LLC, 30 July 2026.

METHOD

Method note

This assessment is independent open-source analysis. Its findings trace to primary sources: the text of 10 CFR Part 810 and its 2015 final rule; the ITAR and EAR provisions cited; Executive Order 13556 and 32

CFR Part 2002; the NARA CUI Registry; NIST SP 800-171; the DFARS and FAR clauses cited; and Department of Justice settlement announcements. Where the public record does not settle a question — including whether non-public Part 810 enforcement exists, and the final form of the FAR CUI rule — that is stated rather than resolved by inference.

The central negative finding, that Part 810 contains no cybersecurity control set, was tested by full-text review of the regulation and the preamble to the rule that produced its current form, and by review of DOE and NNSA program guidance. Sanctir is a solo practice; this work was subjected to adversarial self-review, not external peer review.

AUTHOR

About the author

Collin B. George, CISSP, is the principal of Sanctir LLC, an independent research and advisory practice working on CMMC and NIST SP 800-171, export controls, sanctions, and defense industrial base risk.

Sanctir is a solo practice. This assessment was subjected to adversarial self-review rather than external peer review, and is not affiliated with any government agency, academic institution, or defense contractor.

ORCID 0009-0007-8162-6839 · Full background · Contact