THE GOVERNMENT CONTRACTOR®

Information and Analysis on Legal Aspects of Procurement

JANUARY 14, 2026 | VOLUME 68 | ISSUE 2

¶ 8 FEATURE COMMENT: Supply Chain Hide-And-Seek: How And Why The FY 2026 NDAA BIOSECURE Act Could Apply To You (Yes, You)

When "We Don't Do Biotech" Stops Being the Right Answer

If the BIOSECURE Act had a soundtrack, many companies would be humming a familiar early-2000s refrain from *It Wasn't Me* by Shaggy, along with articulating variants on the same theme:

"We don't do biotech."

"That system isn't ours."

"That vendor is far too downstream in the supply chain to actually matter."

While those reactions are understandable, they're also insufficient if your organization sells goods or services to the U.S. Department of Defense.

The BIOSECURE Act, enacted in Section 851 of the Fiscal Year 2026 National Defense Authorization Act (P.L. 119-60) (NDAA), is ***not*** limited to entities that identify as biotechnology firms. Instead, it reaches a large swath of companies (*and* research institutions … *and* healthcare systems … *and* software manufacturers … *and* …) that *use* biotechnology tools, services, software, or data in the performance of federal work if the ultimate end-user is the U.S. Government.

In many cases, those tools are embedded quietly in automated systems and/or outsourced systems—and they rarely attract attention until someone starts asking pointed questions. As reflected in other recent regulatory activity designed to target vulnerabilities in supply chains (e.g., prohibitions on Kaspersky, Huawei, and ZTE equipment; Buy American Act enforcement; CMMC and attendant cyber requirements) federal procurement policy is swinging away from a narrow focus on final deliverables. Therefore, it comes as no real surprise that the FY 2026 NDAA emphasizes supply-chain visibility, industrial base resilience, and foreign influence risk across multiple provisions. Now more than ever, Uncle Sam is examining precisely how work is performed and the inputs a company is using to make that work possible.

That is precisely where the BIOSECURE Act focuses its attention. The statute is designed around the concept that supply-chain risk does not announce itself. Rather, it hides in routine vendor relationships and embedded systems. For that reason, the BIOSECURE Act is already relevant to companies across a much

wider swath of industries than many expect. And thus, that is where the game of supply-chain hide-and-seek begins.

Why This Is Not Just a Biotech Issue Anymore—Sure, some companies will immediately recognize themselves as operating in the biotechnology space. Many others will not. That distinction is increasingly irrelevant today, as biotechnology is no longer confined to lab benches or research pipelines. Rather, biotech is embedded in analytic platforms that process biological data, automated diagnostic and testing systems, AI-enabled research tools, outsourced sequencing and analysis services, and specialized software that supports biological workflows. Many/most of these tools were adopted "back-in-the-day" for speed, scale, or efficiency, not with federal procurement compliance in mind. As a result, they likely sit several layers removed from teams that manage contracts, grants, or regulatory risk. Over time, those tools become background infrastructure, rarely questioned and seldom revisited.

The breadth of the statute reinforces this point. Section 851(k)(2) defines "biotechnology equipment or service" to include not only physical equipment and instruments, but also software and services used to research, develop, analyze, manufacture, detect, or process biological material or biological data. That scope is intentionally broad. For many organizations, the real challenge is not whether biotechnology is involved at all, but whether anyone has ever mapped where it appears in the supply chain. A subcontractor's testing platform, a third-party analytics service, a quality-control system, or a cloud-based biological data processor can all create exposure under the statute. The risk does not arise from malintent on behalf of the organization. It arises from blind spots that no one knew to check before the FY 2026 NDAA was passed.

Industries Most Likely Impacted by the BIOSECURE Act—In practice, BIOSECURE Act exposure will not announce itself loudly. Instead, it will surface through routine choices made years ago and never revisited. For example, a defense contractor may rely on a third-party lab to support medical readiness testing. Or a software company may process biological data for a customer's federally funded research program using a specialized analytics platform. Maybe a manufacturer outsources quality control or validation work to a vendor selected for speed and cost, not ownership structure. In each case, biotechnology is not the business, but it is part of how the business gets done. That is exactly where Section 851 focuses attention. Here's how it could impact specific sectors of industry:

- **Biotechnology and Life Sciences**: *A no-brainer here*. Companies involved in genomics, proteomics, synthetic biology, cell and gene therapy, biologics manufacturing, or molecular diagnostics, including those relying on third-party sequencing, bioinformatics platforms, or laboratory automation.
- **Pharmaceutical and Drug Manufacturing**: *Yep, them too.* Drug manufacturers using external biotech services for discovery, clinical trials, manufacturing analytics, quality control, or biologically derived inputs, even where biotech is not the core business.
- **Medical Devices and Diagnostics**: *Of course they are.* Device manufacturers and testing companies that integrate biological analysis, reagents, sensors, or biological data-processing software into product design, validation, or performance.
- **Healthcare and Research Institutions**: *Makes sense, huh?* Hospitals, academic research centers, federally funded laboratories, and contract research organizations using covered biotechnology equipment or services in grant-funded or cooperative research.
- **Agriculture and Food Technology**: *We can kinda see it.* Agtech firms using genetic analysis, bioengineered inputs, biological monitoring, or biotechnology-enabled production methods, particularly in federally funded programs.
- **Contract Manufacturers and Specialized Suppliers**: *Ok…Maybe.* Providers of reagents, laboratory instruments, automation systems, sensors, or specialized platforms supporting

biotech and pharma customers, including firms affected indirectly through customer compliance requirements.

- **Defense and Aerospace Contractors**: *Wait, what now?* Contractors supporting programs involving medical readiness, human performance, biodefense, environmental monitoring, or bio-enabled materials, even where biotechnology is secondary to the mission.

- **Data Analytics, AI, and Software Providers**: *OK … what … how?* Companies developing or operating software, analytics platforms, or AI tools used to analyze biological material or biological data, including cloud-based or outsourced solutions.

As can be seen when working through the above list, the common thread is not industry classification. It's ***whether biotechnology tools or services appear anywhere in the supply chain supporting the ultimate federal work***.

Impacts to Federal Assistance More Broadly—A key aspect of the BIOSECURE Act that a fast pass may overlook is that it is not limited to traditional procurement contracts. It also applies to federal grants and loans (and other federal assistance arrangements, depending on how an agency structures and implements the funding). Obviously, this is an important distinction due to the focus of the BIOSECURE Act because many organizations receive federal funding who don't view themselves as "federal contractors." Entities like research institutions, healthcare systems, technology companies supporting federally funded programs, and commercial entities participating in cost-shared or pass-through funding arrangements are likely to find BIOSECURE Act questions bubbling up in grant terms, subaward requirements, or funding certifications, not just in Federal Acquisition Regulation clauses. For organizations that do not routinely track acquisition rulemaking, this can be where the statute—and its risk—first makes itself known.

What the BIOSECURE Act Is and Where It Lives in the NDAA—The BIOSECURE Act, codified in Section 851 of the FY 2026 NDAA, titled "*Prohibition on Contracting with Certain Biotechnology Providers,*" establishes a Government-wide framework that, once implemented:

> Prohibits executive agencies from procuring biotechnology equipment or services from entities designated as *biotechnology companies of concern* (Section 851(a));
>
> Bars agencies from awarding or renewing contracts, grants, or loans to entities that use covered biotechnology equipment or services in performance (Section 851(b)); and
>
> Directs implementation through an Office of Management and Budget-led designation process and subsequent FAR rulemaking, rather than immediate statutory contract clauses (Sections 851(f) and 851(h)).

Notably, rather than naming prohibited companies directly in the statute, Section 851(f) takes an approach that will feel familiar to many federal contractors. It directs the OMB to develop and publish a Government-wide list of "biotechnology companies of concern" through an interagency process. Importantly, Congress did not ask OMB to start from a blank slate. The statute requires that the list include, at a minimum, any entities identified by the Department of Defense under Section 1260H of the FY 2021 NDAA (P.L. 116-283; 10 USCA 113 note) where those entities are involved in biotechnology activities; thus building on pre-existing China-focused supply-chain and national security frameworks contractors (*should*) have been navigating for years.

Section 851(h) then empowers the Federal Acquisition Regulatory Council with effective dates that are deliberately phased, as set out in Section 851(c) and keyed to the timing of the FAR revisions. Applying phased effective dates, the FAR Council must amend the FAR to implement the BIOSECURE Act's prohibitions in harmony with OMB publishing the list of biotechnology companies of concern and when the final implementing regulations are issued. What this means in practical terms is that while the law sets the policy direction now, the real compliance obligations are going to arrive later. This will happen by way of new FAR clauses, representations, and certifications that

contractors will begin to see in future solicitations and contracts.

Waiting for the FAR Clause Misses the Point—While the enforcement promised in Section 851 will be delayed until OMB completes the designation process and the FAR is revised, *this is not a grace period.* It is an opportunity to prepare. The statute itself explains why waiting can feel rational and why that instinct can be misleading where, in Section 851(c), it makes clear that the BIOSECURE Act's prohibitions are triggered by implementation milestones, most notably the revision of the FAR pursuant to Section 851(h). Once the FAR is amended, it's "go time" and the restrictions begin taking effect on a staggered basis, generally 60 or 90 days later depending on the category of biotechnology entity involved as specified in Section 851(f)(2).

This means that while Congress gave agencies and contractors time to adjust, it's not an open-ended safe harbor. The effective-date framework creates a rolling compliance horizon in which obligations can attach quickly once the regulatory process is complete. By the time a clause appears, the window for thoughtful planning may already be closing.

For contractors, this matters most when BIOSECURE Act compliance moves from theory to representation. Once FAR clauses and related representations are implemented under Section 851(h), companies likely will be required to affirmatively certify that covered biotechnology equipment or services tied to a biotechnology company of concern are not used in performance of the contract. At that point, the question is no longer whether a company intended to rely on such tools, but whether it can substantiate what it is representing.

As with other areas of federal contracting, such as cybersecurity requirements or domestic preference regimes, certifications made without a clear understanding of vendor relationships, subcontractor workflows, and embedded systems tend to surface later as performance issues, audit findings, or proposal risks. Companies that treat Section 851 as an early signal rather than a future inconvenience are typically far better positioned when implementation accelerates.

When the List Changes Mid-Stream—Another area that seems to have escaped some scrutiny is what happens if a vendor or service provider is designated as a biotechnology company of concern ***after*** a contract or award is already underway? While Section 851's phased implementation provides some transition protection, it doesn't eliminate judgment calls and the associated risk of getting them wrong. As with all things supply chain, companies will need to evaluate whether alternative suppliers are available, whether continued use is permissible during a transition period, how to document the analysis, and when to engage the contracting officer or grants official. But don't let this checklist-styled grouping dupe you. Each requires balancing contractual obligations, regulatory expectations, and business continuity, and all on compressed timelines.

When "It Wasn't Me" Stops Working—There is a reason supply-chain discussions default to "it wasn't us": modern operations are layered; vendors are outsourced; responsibility is distributed. But the BIOSECURE Act is expressly designed to collapse that distance. Once compliance obligations attach, plausible deniability gives way to required clarity. The expectation will be visibility, documentation, and the ability to explain how biotechnology-related supply-chain risk is identified and managed. And, at that point, the *Shaggy* chorus no longer works.

In order to address and avoid these issues, here are 10 things federal contractors should be doing right now:

1. **Confirm whether biotechnology touches your business at all**—including through software, analytics, testing, validation, quality control, or outsourced services, not just core products or R&D.

2. **Map biotechnology-related vendors and subcontractors**—focusing on where biological material or biological data is analyzed, processed, stored, or validated, even if those functions sit several tiers removed from prime contract performance.

3. **Evaluate vendor foreign ownership, control, and influence risks**—using the same lens already applied to China-related sourcing restrictions and other national security frameworks.

4. **Identify where BIOSECURE Act issues could surface contractually**—including FAR-based procurements, grants, cooperative agreements, subawards, and customer flowdowns, rather than assuming this will appear only in solicitations.

5. **Pressure-test your ability to make representations and certifications**—asking whether you could confidently support a statement today that no covered biotechnology equipment or services tied to a company of concern are used in performance.

6. **Plan for the "vendor gets listed mid-performance" scenario**—including how decisions would be documented, when escalation would occur, and how continuity of performance would be balanced against emerging compliance obligations.

7. **Coordinate procurement, compliance, IT, research, and legal perspectives**—ensuring supply-chain decisions are evaluated holistically rather than through isolated operational silos.

8. **Monitor OMB designation activity and FAR Council rulemaking**—understanding how phased implementation timelines could affect upcoming bids, renewals, and funding opportunities.

9. **Assess downstream exposure**—including how customers, primes, or funding agencies may begin pushing BIOSECURE Act-related representations and audit rights into teaming agreements and supplier contracts.

10. **Validate your approach before it is tested externally**—avoiding encountering issues when responding to a solicitation, audit, grant certification, or contracting officer inquiry.

The BIOSECURE Act is not intended to catch companies off guard; it's intended to reveal what's been hiding in plain sight. The organizations that fare best are not the ones that guess correctly, but the ones that took the necessary time to understand what they were being asked to stand behind. As the FY 2026 NDAA continues Congress's push toward deeper supply-chain visibility and national-security-driven procurement, organizations that uncover and address blind spots early will be far better positioned than those still insisting, too late, that they do not do biotech.

♦

The Feature Comment was written for THE GOVERNMENT CONTRACTOR by* Alex Major *and* Franklin Turner. *Mr. Turner and Mr. Major are Partners in the Washington, D.C. office of McCarter & English, LLP, where they serve as Co-Leaders of the Government Contracts Practice Group. The authors routinely teach courses on a variety of Government contracts issues and can be reached at amajor@mccarter.com and fturner@mccarter.com.