Archimedes Products, Inc.

Precision Aerospace Manufacturing • Bohemia, New York • AS9100-Certified • Family-Owned Since 1959

August 14, 2026

CMMC Reform Task Force
Office of the DoD Chief Information Officer
Department of War
Submitted by electronic mail

Re: Reforming CMMC and Reducing Compliance Burden for the Defense Industrial Base (DIB) — Response to Request for Information, Notice ID 89ef9bfb0834473791e991c712698d94

To the Members of the CMMC Reform Task Force:

Archimedes Products, Inc. is a small, AS9100-certified precision manufacturer on Long Island. We build flight-critical parts for the F-16, the C-130, the Joint Strike Fighter, and commercial Airbus and Boeing programs. We are a Tier 2 and Tier 3 supplier. We handle Controlled Unclassified Information as a routine condition of doing this work, and we live the CMMC compliance problem every day.

Archimedes is a family business, and its story is an ordinary American one. It began in the basement of a New York City row house in 1959, started by my parents — immigrants who came to this country after the Second World War, my father from Poland and my mother from Germany — and it grew into the AS9100-certified shop we run today. I have owned and run it since 2010. We are seven people. Over the past ten years we have produced roughly eighty-five distinct part numbers, about half of them defense-related, for programs including the F-16, the C-130, and the F-35. We are exactly the kind of small, specialized manufacturer the defense industrial base depends on and cannot easily replace.

I write in two capacities. As the owner of Archimedes, I have direct, daily experience of what the current framework costs a shop of our size. As a systems engineer, I hold a Ph.D. in Mechanical Engineering from the California Institute of Technology, and in 1989 I founded Advanced Projects Research, Inc. (APRI), through which I have spent more than three decades taking hard defense problems from concept to validated hardware under DoD, DARPA, Navy, and NASA programs — work reflected in the public SBIR and DTIC record. I therefore speak not only to the burden, but to the feasibility of a better approach.

My concern is blunt. We cannot let the cost of handling CUI price American small manufacturers out of the global aerospace parts market. Our foreign competitors carry no comparable burden, and every recurring compliance dollar loads directly onto the price of every part we quote. A framework that quietly converts parts-makers into compliance departments — or drives them out of defense work entirely — weakens the very industrial base it was meant to protect.

There is a better way, and it is one my own industry already relies on. We do not independently invent and separately certify a unique design for every flight-critical part; we certify parts to an approved design. Medical devices and listed electrical equipment work the same way. A design-based certification pathway — adopt a pre-approved reference design, and demonstrate compliance by verifying conformance to it — would collapse the assessment burden without weakening the standard. The response that follows develops this recommendation and answers the RFI's seven questions from our direct experience.

These concepts were developed independently and privately; no Federal funding has touched them, and I am prepared to contribute the underlying reference designs in the public interest. I welcome the opportunity to support the Task Force's work.

Respectfully submitted,

Thomas H. Sobota, Ph.D.
President, Archimedes Products, Inc. • Founder, Advanced Projects Research, Inc.
21 Floyds Run, Bohemia, New York 11716 • thomas.sobota@archimedesproducts.com

Response to Request for Information

Reforming CMMC and Reducing Compliance Burden for the Defense Industrial Base (DIB)

Notice ID 89ef9bfb0834473791e991c712698d94 • Submitted by Archimedes Products, Inc. • August 14, 2026

Submission Information

Company: Archimedes Products, Inc. **CAGE Code:** 1BH94 **UEI:** EX8AB2JJY9H5 **DUNS:** 061965372

Point of Contact: Thomas H. Sobota, Ph.D., President — 21 Floyds Run, Bohemia, New York 11716 — Phone: 631-589 -1215 — Email: thomas.sobota@archimedesproducts.com — Fax: N/A

Proprietary information: This submission contains no proprietary or confidential business information and may be reproduced, quoted, and used by the Government without restriction.

Subject: Reforming CMMC and Reducing Compliance Burden for the DIB.

Respondent Profile

Respondent: Archimedes Products, Inc., Bohemia, New York — an AS9100-certified precision aerospace machine shop and a seven-person, family-owned small business (founded 1959). Over the past decade we have produced roughly 85 distinct part numbers, about half of them defense-related. **Role in the supply chain:** Tier 2 / Tier 3 subcontractor producing flight-critical machined parts for F-16, C-130, and F-35 (JSF) programs, and for commercial Airbus and Boeing work. **CUI posture:** We receive and generate CUI (technical drawings, specifications, and program data) as a routine condition of contract performance. **Target level:** CMMC Level 2 / NIST SP 800-171 Rev. 2. **Author:** Thomas H. Sobota, Ph.D. (Caltech), President of Archimedes and founder of Advanced Projects Research, Inc. (APRI, est. 1989), a systems-engineering firm with a multi-decade record of competitively awarded DoD, DARPA, Navy, and NASA research.

We answer the questions on which we have direct experience and concentrate our recommendations on Questions 6 and 7, where we offer a specific, buildable structural reform.

Question 1 — Top cost drivers, administrative burdens, and operational challenges

For a shop of our size, the dominant burden is structural: every small contractor must independently design, document, implement, and individually certify a unique compliance architecture. That root cause produces five specific, prohibitive drivers:

1. **Bespoke architecture and one-off assessment.** Each contractor stands up a unique environment that must then be evaluated against 110 controls and 320 assessment objectives (NIST SP 800-171A). The figures the Department itself has cited — roughly $593,800 for a third-party certification and $388,600 for a self-assessment cycle — are consistent with what a firm our size faces. For a seven-person shop, that is the same infrastructure investment demanded of a company ten times our size, to protect a handful of endpoints.
2. **The subscription tax.** The path of least resistance to "compliance" has become migration into the Microsoft and Google cloud ecosystems (e.g., GCC High). For a small business this is a perpetual, per-seat tax that recurs forever and grows with headcount — paid for capabilities that could instead run in-house on a single, one-time-purchased appliance. We are, in effect, renting our own compliance in perpetuity.
3. **Outside expertise and documentation.** Because the standard is written for IT specialists, we must buy a consultant to author the System Security Plan and a recurring MSSP contract for monitoring — expertise we cannot staff internally. The SSP and POA&M are living documents that consume owner and engineering time, most of it spent documenting a custom design that a reference design would render unnecessary.
4. **Complexity is itself the cost — and the risk.** The printout of the common settings on a single pfSense firewall runs about twenty pages of rules. No one — not the owner, often not the consultant — can look at that ruleset and tell which line someone once added to "make something work" that quietly opened a hole in security. When the security of the enterprise depends on hand-configured devices no human fully understands, complexity has become the vulnerability, and auditing it becomes a specialized, expensive, never-finished exercise.

5. **Assessor scarcity and schedule risk.** With roughly one hundred authorized assessors for a base of well over one hundred thousand firms, the queue itself is a barrier. Schedule uncertainty translates directly into contract risk for a small supplier that cannot afford to sit out award cycles.

The stakes are larger than any invoice. Every recurring compliance dollar is priced into every part we quote, against foreign competitors who bear no such cost. The burden is already pushing owners to divert engineering time from production to paperwork — and, at the margin, to weigh whether to remain in defense work at all. When a precision shop shifts its effort from making aircraft parts to managing cybersecurity documentation, the nation does not gain security; it loses manufacturing capacity it cannot quickly rebuild.

Question 2 — Controls that deliver meaningful cybersecurity improvement

The controls that measurably reduce real risk are the ones that limit the blast radius of an inevitable compromise, not the ones that generate paperwork. The highest-value controls for a small manufacturer are:

- **Multifactor authentication (3.5.3)** — the single highest-leverage control against credential theft and phishing.
- **Least privilege and access enforcement (3.1.1, 3.1.2, 3.1.5)** — confining who can reach CUI at all.
- **Boundary protection and CUI separation / enclaving (3.13.1, 3.13.2)** — keeping CUI off the general business and shop-floor networks. This boundary is where protection belongs, a point we develop under Question 6.
- **Encryption of CUI at rest and in transit (3.8.6, 3.13.11, 3.13.16)** — protecting data when a device or channel is lost.
- **Removable-media and media protection (3.8.7) and physical protection (3.10 family)** — realistic, inspectable defenses a small business can actually own.

These controls share a decisive property: their effect is concrete, and their presence can be verified by inspection rather than by reading configuration files. That is the principle the standard should reward.

Question 3 — Requirements with high burden and least measurable improvement

The lowest-value burden is the requirement that each unique implementation be independently assessed. Beyond that, three categories impose enterprise-scale cost with limited marginal benefit at our scale:

- **Implicit cloud mandates.** Requirements that, in practice, steer small firms into subscription cloud ecosystems, when a ground-based, on-premises design provides equal or better protection at far lower lifetime cost and with a smaller external attack surface. The Department should be indifferent to cloud versus ground; today the framework is not.
- **Enterprise monitoring applied to tiny networks (the 3.3 audit family).** SIEM licensing, log retention, and continuous-monitoring infrastructure sized for large enterprises but applied to a shop with a handful of endpoints — largely to satisfy an assessor rather than to reduce a real risk.
- **Documentation of bespoke designs (the 3.12 family).** Much of the SSP/POA&M volume exists only because every environment is unique. Standardize the design and most of it disappears.

The theme is consistent: the burden concentrates in requirements whose cost scales with the size and uniqueness of the architecture, while their security value does not. Remove the uniqueness and most of the waste goes with it.

A concrete measure of that detachment, from our own shop. We are entirely ground-based and self-hosted, and we estimate that replacing our whole IT infrastructure — both mail servers (we already run internal and external mail separately), every home-run hardwired drop, every office and shop-floor computer, and the dashboard kiosks — would cost substantially less than a single third-party assessment cycle. When assessing a system costs more than building the secure system itself, the burden has plainly detached from the security it is meant to deliver.

Question 4 — Use of commercial cybersecurity capabilities, and how the Department can better accept them

Small manufacturers already run capable commercial tooling. The problem is not availability; it is that the Department re-assesses each deployment from scratch, at each contractor, and that the easiest compliant path pushes us toward perpetual cloud subscriptions we do not need.

Ground-based capability is real and dramatically cheaper. A dedicated in-house mail server and video-conferencing system can run on a computer the size of a paperback book, using open-source and perpetually-licensed software, giving a contractor sovereign control of its CUI with no recurring per-seat cost and no dependence on a third party's cloud. This is not a downgrade; for a single-site small business it is a smaller attack surface and a lower lifetime cost than the subscription alternative.

Recommendation: The Department should (a) accept validated commercial and open-source reference configurations — specific software in specific, documented setups — as presumptively conformant, so a contractor who adopts an approved configuration verifies conformance rather than commissioning a fresh assessment; and (b) place ground-based, on-premises reference designs on fully equal footing with cloud, ending the implicit push into subscription ecosystems. Both can be issued as guidance, without rulemaking.

Question 5 — Challenges with Phase I self-assessment, and streamlining

Phase I self-assessment is hard for small firms for three reasons. First, translating 110 controls and 320 objectives into concrete actions requires expertise we do not have on staff, so even the self-assessment drives consulting cost. Second, the SPRS scoring methodology and the SSP/POA&M expectations are unfamiliar and ambiguous, particularly around scoping which systems fall inside the CUI boundary. Third — and this genuinely chills honest reporting — owners fear False Claims Act exposure from a good-faith self-assessment that a later reviewer second-guesses.

Streamlining: (a) provide a plain-language, guided self-assessment tied to an approved reference design, so a small firm answers "am I using the approved design as issued?" rather than interpreting 320 objectives in the abstract; (b) publish a simple CUI-scoping tool so firms draw the boundary correctly; and (c) establish a good-faith safe harbor for firms that self-attest to conformance with an approved design. Together these turn self-assessment from an expert exercise into a verification checklist.

Dynamic posture, or compliance exercise? Candidly, at our scale the self-assessment today is performed largely for compliance. The controls that genuinely improved our posture — multifactor authentication, least privilege, and boundary separation — we would run regardless; the documentation-heavy remainder produces paperwork, not security. Tying self-assessment to an approved design changes that, because confirming "we are running the approved design" is a live, repeatable posture check rather than a one-time paperwork exercise.

Question 6 — Specific, actionable reforms to reduce cost and barriers to entry for small, medium, and non-traditional businesses, recommendable within 60 days, without degrading protection of federal data

This is the heart of our response, and it answers the question as asked: a specific, actionable reform the Task Force can recommend within 60 days that drastically reduces cost and barriers to entry, and that does not degrade the protection of federal data — because the approved design must meet or exceed NIST SP 800-171. It requires no new legislation and no new hardware, only a change in how NIST and the Department recognize compliance, adoptable as guidance rather than rulemaking.

Recognize a design-based certification pathway. Allow a contractor to demonstrate compliance by adopting a pre-approved, system-level reference design that meets or exceeds current requirements. Compliance is then shown by verifying conformance to the approved design, not by a full independent evaluation of a one-off implementation. The assessment burden drops from "evaluate this unique system against 320 objectives" to "confirm this contractor is using the approved design as issued." This is exactly how aircraft parts, medical devices, and listed electrical equipment are already certified: the hard engineering is done once, reviewed once, and adopted many times, and safety is demonstrated by conformance. CUI-handling infrastructure is the anomaly, and ending that anomaly is the single highest-leverage move available to this Task Force. It also directly lowers the barrier to entry: a new or non-traditional firm can enter the DIB by adopting an approved design, rather than funding a six-figure compliance project before it can place a first bid.

Protect at the boundary so innovation can move freely inside. A tiered secure-subnet architecture places the guarantee against CUI escape at the boundary of the secure subnet — not on every file, tool, or program within it. That distinction has enormous practical value. Consider a machinist who writes a useful program at home and wants to run it at work. Under today's regime, installing it can trigger a ten-day security review of the code. Under a boundary-protected enclave, he can install and use it inside the subnet freely, because the assurance the Department actually cares about — that CUI cannot leave — is enforced at the perimeter, not by auditing every line of code.

Security that lives at the boundary preserves the productivity and shop-floor innovation that make a small manufacturer valuable in the first place.

Companion actions, all within near-term reach:

- **Keep the standard open and implementation-agnostic.** Write it as a requirements standard — what must be true — that any qualified provider can certify against, not a single prescribed design. This drives competition, multiple qualified sources, and continuous innovation rather than vendor lock-in, and it is the same discipline the Department already applies through performance-based specifications.
- **Publish reference designs for small-business CUI handling.** Begin with a dedicated, pre-configured CUI workstation — plug-in ready, pre-approved, no custom architecture and no independent assessment required. A small contractor buys it, installs it, and is compliant by conformance.
- **Right-size requirements by blast radius.** Scale expectations to the size of the environment and the amount of CUI at stake, so a seven-person shop like ours is not held to infrastructure designed for a prime.
- **Establish the good-faith safe harbor.** Pair the pathway with protection for firms that adopt and self-attest to an approved design, so adoption is not a legal risk.

Stop-gap measures deployable inside the 60-day window. The reforms above are recommendations the Task Force can issue now; full implementation will realistically take a year or more. Two interim measures require no rulemaking and can be recognized immediately:

- **Authorize a controlled air-gapped ("sneaker-net") transfer mode.** Recognize as presumptively compliant a small-business enclave that is physically air-gapped, in which a single designated custodian controls all CUI moving in and out on encrypted physical media under a simple log. The custodian is the runner; protection lives at the boundary; there is no cloud and no external attack surface to audit. It is the certified-mail model in physical form, and a seven-person shop can stand it up in days.
- **Recognize existing free DoD training as meeting the awareness requirement.** DoD already funds cybersecurity training for exactly this workforce — the DoD Cyber Awareness Challenge (cyber.mil) and Project Spectrum (DoD Office of Small Business Programs, delivered through the APEX Accelerators). Directing small firms to these and accepting their completion as satisfying the awareness controls (3.2 family) is a zero-cost reform available today.

The reference designs contemplated here require some purpose-built, system-level hardware whose security function is fixed at manufacture. This is buildable today. As a systems-engineering firm that has repeatedly taken defense problems from concept to validated hardware, APRI's experience informs our confidence that these designs are practical, not aspirational; we offer them in the public interest and no Federal funding has touched them.

Question 7 — Reforms that strengthen actual operational resilience

Resilience should be measured by how small the damage is when — not if — something is compromised. Four reforms would move the framework from documentation compliance toward demonstrable resilience:

1. Reward blast-radius limitation and visual inspectability. Explicit trust zones with default-deny between them contain a breach to a single zone. Where zone boundaries are made physically and visually inspectable, an assessor can walk a facility and see a violation without privileged system access, and verification becomes fast, cheap, and honest — far more resilient than a well-documented flat network.

2. Prefer fixed-function hardware over configurable complexity. The twenty-page firewall ruleset no one fully understands is the opposite of resilient. Critical security functions should live in simple, non-configurable, inspectable devices whose behavior is fixed at manufacture and cannot be silently altered by a well-meaning change that punches a hole. Unalterability is the feature, not a limitation: a device that cannot be reconfigured cannot be misconfigured.

3. Provide a secure, segregated transport for organizational mail. Before email, companies ran internal inter-office memo systems for fluid internal communication and used the U.S. Postal Service for anything leaving the building. The same discipline can be restored digitally: intra-company mail flows freely inside the enclave, while any message crossing to another organization passes through a sealed, fixed-function transport appliance at the network boundary — modeled on certified mail, where the relay never sees the contents and simply confirms that a sealed packet moved from one registered address to another. Internal communication becomes fluid again, with no chance of escape, and no new national identity system is created.

4. Recognize that the same solution protects commercial competitiveness. The escape of a controlled drawing is not only a defense problem. Boeing, Airbus, and any company with valuable product designs face the same risk of losing proprietary IP. Infrastructure built to protect CUI protects commercial designs equally well, which multiplies the return on the Department's investment and widens the base of firms that will adopt — and help sustain — these standards.

Feasibility, Risks, and Innovations

Feasibility. The design-based pathway is administratively feasible now — it is a recognition of conformance, adoptable as NIST/DoD guidance without new statute. The reference designs are technically feasible now: a ground-based, self-hosted CUI enclave and a fixed-function boundary appliance are buildable from existing components. As a firm that has repeatedly taken defense hardware from concept to validation, APRI regards them as engineering, not research.

Risks and challenges. The principal risk is capture — a standard written around a single vendor's product. The mitigation is to keep it an open, implementation-agnostic requirements standard that any qualified provider can certify against. A second risk is under-scoping the CUI boundary, which a plain-language scoping tool addresses. A third is transition friction, which the interim stop-gap measures above are designed to absorb.

Innovations. Three elements are, to our knowledge, novel in this context: certifying CUI infrastructure to an approved design rather than assessing each unique implementation; visual, physical inspectability of trust-zone boundaries so compliance can be verified without privileged access; and a sealed, fixed-function transport appliance modeled on certified mail, in which the relay never sees content and unalterability is itself the security feature.

Closing and Offer to Contribute

The Task Force's two goals — lowering barriers for small and non-traditional businesses and genuinely improving security — are not in tension. The way to serve both is to stop requiring every small firm to independently invent, document, and separately certify a unique architecture, and instead let them adopt pre-approved designs and demonstrate compliance by conformance, exactly as we already certify the flight-critical parts we build. Do this, and small manufacturers stay in the fight, American parts stay competitive in the global market, and security improves because good designs are adopted widely instead of poor ones being improvised individually.

As a working Tier 2/3 manufacturer and a systems engineer, I am prepared to contribute reference designs in the public interest and to participate in the standards review. I welcome any follow-up the Task Force finds useful.

Respectfully submitted — Thomas H. Sobota, Ph.D., President, Archimedes Products, Inc.; Founder, Advanced Projects Research, Inc.