DCMA Blue List Basics for Thermal Imaging Users and Suppliers

Daniel Woosley

Director of UAS Business Development

Edgesource Corporation

Summary

Thermal imaging suppliers pursuing government contracts or contracts with critical infrastructure industries need to understand how their products are impacted by the US Government's push for a trusted supply chain. The Blue List provides a government review pathway for essential components of unmanned systems and the payloads they carry—including thermal imaging equipment. This article explains its purpose, the assessment process, and the implications for thermal manufacturers and integrators. It also describes how Recognized Assessors such as Edgesource help suppliers document their products and address assessment findings as customer requirements evolve.

Introduction

A thermal payload can meet the performance requirements for an unmanned aircraft system (UAS) or other unmanned system (UxS) but still be ineligible for a government or critical infrastructure customer purchase. The customer also needs to establish who made the hardware, where critical components originated, and what software controls them. A supplier that can answer those questions (and provide documentation) gives the customer a firmer basis for selecting its product.

The Blue List brings that review into a common government process. Managed by the Defense Contract Management Agency (DCMA) within the Department of War (DoW), it covers unmanned systems and components. The effort began as Blue UAS under the Defense Innovation Unit (DIU), which transferred management to DCMA on December 3, 2025. [1, 2]

Edgesource was selected by DIU as a Recognized Assessor. We help companies understand the applicable requirements and evaluate the evidence supporting their products. [3] For IRINFO readers who manufacture thermal cores, build camera modules, or integrate airborne payloads, the useful questions are practical: Does this pathway fit our product and customer? What will the assessment examine? What should we prepare before we begin?



What the Blue List Is For

The Blue List gives buyers a common catalog of vetted platforms, systems, and components approved for departmental purchase and use, subject to applicable requirements. DCMA manages it through its Unmanned Systems–Experimental organization, US-X. DIU remains involved in standards and checklists. [1, 2]

Its purpose follows from a specific purchasing problem. National Defense Authorization Act (NDAA) restrictions reach complete aircraft and specified onboard parts, including cameras, gimbals, flight controllers, and radios. A domestically assembled aircraft can therefore require examination of components supplied by several other companies. [4] Buyers need a dependable way to establish whether that equipment meets the applicable sourcing and security requirements.

The program developed two related listing categories: a Cleared List for aircraft and a Framework for components, subcomponents, modules, and software. Those terms still appear in government references. For a thermal supplier, the distinction matters because participation is possible without becoming an aircraft manufacturer. [5]

DCMA emphasizes establishing trust in components so that prior review can reduce repeated work when those parts enter other platforms. [6] For a component supplier, that review can have value beyond a single aircraft sale. The review can support subsequent integrations, although the customer must still check the listed configuration and requirements for the completed system. A component's status does not establish the suitability of every aircraft that uses it.

What Can Prevent Listing

A key baseline for Blue List assessment is Section 848 of the FY2020 NDAA, as amended. Subject to statutory exemptions and government waivers, it restricts defense procurement and operation of UAS and components manufactured in China, Russia, Iran, or North Korea, or by companies domiciled in those countries. [4, 5]

The restrictions also include flight controllers, radios, data-transmission devices, cameras, or gimbals manufactured in those countries or by companies domiciled there. It covers ground-control systems and operating software developed in those countries or by such companies, and network connectivity or data storage located there or administered by entities domiciled there. [4]

For a thermal supplier, the camera restriction is especially relevant. Purchasing a Chinese-manufactured camera through a U.S. distributor does not change its manufacturing source. Domestic assembly of the aircraft does not resolve that issue. Chinese-made integrated circuits within an otherwise non-Chinese component can also cause approval issues.

These categories do not constitute a blanket prohibition on every foreign-made component. Additional covered-entity, ownership, and security requirements must also be checked. [3, 5] A government exemption or waiver is separate from obtaining Blue List status. Missing origin records, meanwhile, call for more evidence: they neither prove that a source is prohibited nor establish compliance. The current government checklist governs the full assessment.

Why Thermal Components Belong in the Discussion

A camera assembly can contain a detector from one manufacturer, processing electronics from another, and firmware maintained by a third. The company selling the finished payload needs to understand those relationships.

Consider a camera module offered for integration into a government drone. Documentation for the detector may be complete, while the processor's manufacturing source or the origin of the firmware remains unresolved. The supplier should identify and close those gaps before treating the module's supply chain as established. The detector's documentation supports one part of the assembly; the assessor still needs evidence for the other relevant elements.

This example explains why thermal companies should understand the process even when they sell to an aircraft integrator rather than directly to the government. A core family can also serve several product lines, as the hypothetical arrangement in Figure 1 illustrates.

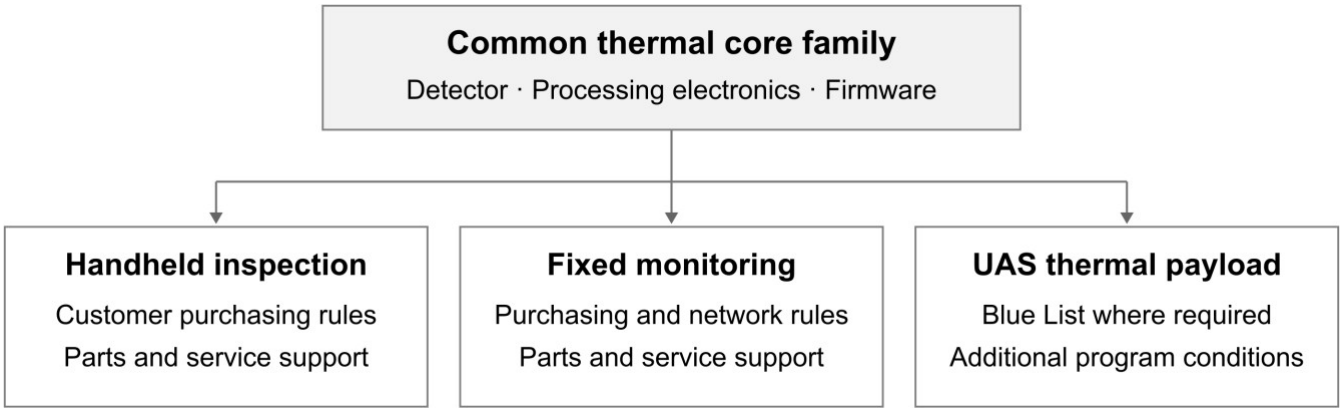


Figure 1. Shared thermal components can serve different markets. Purchasing eligibility depends on the requirements governing each product and customer.

For handheld and fixed-camera readers, the practical question is whether the supplier uses shared components and how it will support those products if the parts change. That connection makes sourcing and service plans worth discussing with the manufacturer. Sharing a core with a drone product does not by itself create a Blue List requirement for a handheld or fixed camera.

How the Assessment Works

DCMA describes a pathway in which the vendor submits a checklist packet through its portal and contracts with a Recognized Assessor. The assessor evaluates the company and relevant system or components, then reports the results for government consideration. [1] The following sequence explains that pathway and the preparation we recommend.

Define the product and the assessment. Establish whether the submission concerns a component, module, payload, or complete system. Identify the exact hardware and software versions and the intended government customer. Obtain the current submission requirements before agreeing on the assessment scope. This keeps the report tied to the hardware and software actually reviewed.

Examine the supporting evidence. Recognized Assessors review ownership interests, supply-chain provenance, country-of-origin records, component sourcing, and relevant hardware, software, and firmware evidence. Hardware is physically disassembled to verify whether the chips listed on the Bill of Materials (BOM) match what is physically observed in the device. Assessors work to a common standard and provide standardized reports. [3] At Edgesource, our work includes comparing the hardware bill of materials with the physical equipment, inspecting components, and analyzing software and firmware. The BOM is the product's parts inventory; checking it against the hardware helps establish what is actually present. [7]

Scope pic here

Address findings when needed. Missing records and a noncompliant component are different problems. One may require additional records; the other may require a product change. The supplier and assessor need to distinguish them clearly. DCMA's published Titan Dynamics pilot describes identifying noncompliant parts, replacing them, and resubmitting the product. [8] That example demonstrates a possible resolution, rather than a promise that every issue can be corrected in the same way or time.

Submit the report for a government decision. The assessor documents its findings and submits the report through the government process. The government determines whether the product will be listed. [1, 3] Edgesource can explain findings and assess the evidence supplied to address them. We do not make the listing decision or guarantee its outcome.

What Listing Changes for a Supplier

Listing provides a customer with an established government review to consider when selecting equipment. It can also support access to purchasing channels: the Defense Logistics Agency's FedMall Drone Corridor offers Blue List systems and related equipment. [9] Neither listing nor presence in a purchasing channel guarantees an order. The supplier must still satisfy the customer's performance, configuration, delivery, and contract requirements.

There is also a separate connection to Federal Communications Commission (FCC) equipment authorization. Qualifying Blue List aircraft and components currently have an exemption until January 1, 2028, from the FCC's Covered List restrictions on foreign-produced UAS and UAS critical components. For products requiring FCC authorization, that preserves a route to authorization; listing itself does not issue the FCC grant. Qualifying domestic end products and devices receiving conditional approval have separate routes. [10]

The consequence of remaining unlisted depends on the opportunity. Where a solicitation requires Blue List status, an unlisted product can be ineligible unless an expressly permitted alternative applies. Other customers may use different authorized routes. An unlisted part is not automatically barred from every government market.

Before committing to a delivery, establish whether the buyer needs the thermal component listed, needs evidence for an aircraft submission, or imposes further conditions. Make eligibility claims for that specific configuration and purchase.

Preparing for Requirements Beyond Listing

Some defense purchasing programs impose additional sourcing conditions and verification beyond baseline NDAA compliance. Drone Dominance, which aims to expand the industrial base producing attack and surveillance drones through phased competitions, provides a concrete example. Its Phase 3 solicitation expressly requires a supply-chain framework more restrictive than NDAA compliance. Selected vendors must provide equipment for DCMA inspection and updated BOMs with technical contacts for their component suppliers. [11]

The framework's imaging requirements tighten across phases. Phase III calls for camera or sensor assembly and circuit boards from non-covered countries, with firmware repositories neither hosted nor administered from a covered country. Phase IV adds a non-covered-country image sensor and a repository hosted and controlled by a U.S. entity and available for audit. Covered countries here are China, Russia, Iran, and North Korea. [11]

These are requirements for that program, rather than universal Blue List conditions. For a thermal supplier supporting a participating aircraft manufacturer, they create specific questions about assembly, detector sourcing, and firmware control. Review the customer's next delivery requirements while selecting suppliers and planning product changes. A previous assessment should be checked against the new requirement and the configuration now being offered.

Getting Ready for an Assessment

Preparation starts with organizing information the company should be able to retrieve and explain. We recommend assembling:

1. A clear product description with model numbers, hardware revisions, firmware versions, and the intended customer or program.
2. A current bill of materials identifying the relevant original manufacturers, part numbers, and supplier contacts, with supporting origin records.
3. Company ownership information and an explanation of who develops, supplies, and maintains the product's software and firmware.
4. A record of substitutions or planned changes, together with the person responsible for keeping the product documentation current.

These are preparation recommendations, not a substitute for the current government checklist. Identify missing records openly. If an upstream supplier considers its information proprietary, establish an acceptable disclosure arrangement with that supplier and the assessor rather than substituting an unsupported assurance.

Edgesource can explain the assessment scope and identify unresolved sourcing questions. Our hardware, software, and supply-chain analysis gives suppliers a concrete basis for responding to findings. [7] To discuss an assessment with Edgesource, bring the exact product, its intended customer, and the documentation already available.

Conclusion

Thermal suppliers pursuing government drone opportunities should understand the Blue List before the customer needs an approval or supporting evidence. Preparation means knowing the offered configuration, supporting its sourcing claims, and checking the next customer's requirements.

References

Sources reviewed October 8, 2026. Consult current program materials and the applicable solicitation for subsequent changes.

1. Defense Contract Management Agency. DCMA accelerates Blue List process. July 27, 2026.

2. Defense Innovation Unit. DIU's Blue UAS List To Transition to DCMA. December 3, 2025.

3. Defense Innovation Unit. DIU Announces Recognized Assessors to Support Blue UAS NDAA Compliance Certification. September 19, 2025.

4. U.S. Code. Section 848 of Public Law 116-92, as amended, statutory note under 10 U.S.C. 4871. See subsections (a)(1), (c)–(e) for sourcing restrictions, exemptions, waivers, and covered countries.

5. Defense Innovation Unit. Blue UAS Refresh List, Framework Platforms and Capabilities Selected. February 14, 2025. System and component listing categories.

6. Defense Contract Management Agency. Army-made motors power historic Game of Drones flight. September 4, 2026. Component review and reuse.

7. Edgesource Corporation. Blue UAS Recognized Assessor services. Assessment methods and supplier assistance.

8. Defense Contract Management Agency. DCMA champions Drone Dominance objectives. September 29, 2025. Titan Dynamics pilot.

9. Defense Logistics Agency. Troop Support plays key role in DoW's drone strategy, bolstering national, event security. January 30, 2026; republished on DVIDS February 3, 2026.

10. Federal Communications Commission. DA 26-957, Appendix A, September 9, 2026 (current exemptions, including the January 1, 2028 expiration); UAS Covered List FAQs, January 7, 2026 (background guidance on equipment-authorization scope; its original exemption date has been superseded).

11. Drone Dominance Program. Supply Chain Framework Version 2, July 23, 2026, pages 1–4; Phase 3 Request for Solutions, Revision 3, sections 5.5 and 5.7. Documents linked from the current program website.

12. Edgesource Corporation. UAS and counter-UAS capabilities, company background, and mission capabilities.

About Edgesource

Edgesource Corporation is a Recognized Assessor for the Blue List, originally selected by DIU under Blue UAS. Its assessment services combine hardware inspection, software and firmware analysis, and verification of component sourcing. More information about assessment services: www.edgesource.com/blue-uas

Edgesource conducts research, development, test and evaluation in cybersecurity, UAS, and counter-UAS technologies, hardware and software exploitation, and national-security applications. Its Windtalker(TM) and Dowding(TM) capabilities support drone detection and situational awareness.

Founded in 1997, Edgesource serves Intelligence, Defense, and other national-security customers through software and systems engineering, data engineering, secure cloud integration, cybersecurity, and applied artificial intelligence. Its capabilities include cleared professionals, an accredited Sensitive Compartmented Information Facility (SCIF), CMMI Maturity Level 3 appraised processes, and ISO 9001 and ISO 27001 certifications.

About the Author

Daniel Woosley is the Director of UAS Business Development at Edgesource Corporation. With a background in federal law enforcement and protection of federal facilities and high-value targets, he helps organizations and equipment manufacturers navigate supply chain and cybersecurity threats that can put lives and property as risk. In collaboration with Edgesource's UxS lab, he researches and writes about emerging technology and policy implications of unmanned systems. He can be reached for follow-up questions at dwoosley@edgesource.com.