LrrK Letters

Vol. 1 · Issue 2 · January 2026

The Exception Architecture

Blue UAS, Domestic End Products, Conditional Approval, and the Administrative Production of Trust

Dateline: January 16, 2026

Abstract

January's drone exemptions reveal how a broad restriction becomes an operating policy. The FCC has removed specified Blue UAS systems and qualifying domestic end products from its production-based Covered List designation for a temporary period, while individualized applications now connect admission to disclosure and manufacturing commitments. These routes answer different questions about trust. They also distribute opportunity among agencies, producers and users with unequal resources. This essay examines their differences alongside new FAA test sites, event-security investment and the first announced Replicator 2 acquisition. Its argument is that an exception can be a serious instrument of transition without becoming proof of technical security or completed industrial capacity. A workable system needs timely decisions, bounded claims and a memory of changes, with public obligations proportionate to the access it grants.

The door inside the wall

The important development of this fortnight is a door. On January 7, the FCC modified its December restriction on foreign-produced drones and critical components. Systems and components included on the relevant Blue UAS lists, and those qualifying as domestic end products under the Buy American standard, received temporary exclusion from the production-based designation. An accompanying process invites other producers to seek individualized conditional approval. The original December determination had allowed favorable findings by the Department of War or Homeland Security. January supplies machinery through which some of that discretion can be exercised.[1][2]

This is an exception architecture because the routes are different. One recognizes an existing assessment process. Another recognizes a production standard. A third asks an agency to evaluate a particular application and its commitments. An operator may encounter all three as a simple distinction between available and unavailable equipment. For a producer, the route chosen determines which evidence must be assembled, which institution must be satisfied and how much uncertainty remains in the calendar. The design of those passages will help determine the market that emerges behind the December wall.

That is more interesting than a story in which an absolute ban has suddenly been abandoned. The initial restriction already preserved imports and sales of previously authorized models. Its exception power was present from the outset. What January demonstrates is the difficulty of governing a globally assembled machine through a sweeping production category. A country seeking independence still needs functioning aircraft, spare parts and an industry capable of learning. Immediate exclusion and eventual self-sufficiency run on different clocks. A temporary passage can connect them, provided its conditions bear some relationship to what industry can actually change.

The temporary exemptions run until January 1, 2027 unless superseded. That date matters in its present form. It is a deadline in this January record, not a promise that approval will last indefinitely or that a later government will necessarily extend it. The determination also excludes devices identified through section 1709 of the fiscal 2025 defense authorization act from its treatment of UAS and critical components. A reader should therefore resist interpreting the new categories as blanket relief for every product that could satisfy a manufacturing description. The precise legal route remains consequential.[1]

Temporary relief carries a particular emotional force. To an excluded producer it can look like permission to breathe. To a purchaser planning several years of service it can look like another approaching cliff. To an official responsible for an industrial transition it offers both continuity and pressure. None of these interpretations is absurd. Each measures the interval against a different obligation. The useful question is whether the state can make those obligations fit together without asking a buyer to mistake a conditional administrative status for a guarantee of future support.

Nor is a deadline automatically a defect. A permanent exception can harden a transition arrangement into an entitlement. Periodic review can make a company explain why promised changes have not occurred and whether the original justification remains sound. The problem begins when the review horizon is clear but the path through review is opaque. A date can discipline an applicant; it can also deter investment if the applicant cannot estimate the evidence, costs or decisions needed to survive it. Predictability is a productive resource, not merely a favor to regulated firms.

Three ways to be trusted

The Blue UAS route and the domestic-product route should not be collapsed into one security claim. In the January determination, DoW describes the Blue process as including cyber and hardware assessments, supply-chain compliance, data-privacy requirements and penetration testing. Those are the department's account of the assessment supporting its conclusion. Recognition by the FCC removes a particular authorization obstacle for qualifying equipment. It does not create a new independent measurement of every configuration an operator might assemble after purchase.[1]

The domestic-end-product route uses a different argument. The determination invokes manufacture in the United States and a domestic-content cost threshold, linking qualification to the objective of a stronger domestic industrial base. It identifies that production as supporting the administration's security imperative. This makes industrial resilience part of the meaning of acceptable risk. It does not mean that the same kind of technical test has been performed for every product entering through this route. A procurement-derived production standard and a cybersecurity assessment can both be useful while establishing different things.

That difference is a feature to make visible, rather than an embarrassment to conceal. Geographic production can affect the reach of law, the reliability of replenishment, access to manufacturing knowledge and exposure to export restrictions. Hardware and software assessment can investigate behavior that a factory address does not disclose. One cannot substitute completely for the other. If public communication presents both routes with the same undifferentiated badge of trust, it invites buyers to infer equivalence where the policy has actually accepted different grounds for admission.

Consider two hypothetical suppliers. One assembles domestically and meets the applicable content test but depends on a proprietary maintenance service whose operating terms a buyer has barely examined. Another has undergone extensive security assessment but relies on an overseas input that could become hard to replace. These examples describe possible dependencies, not defects established in any named product. They show why an

approval category is the beginning of a purchasing inquiry. The buyer still has to ask what matters for the intended mission, and which unanswered question would make service fail.

The individualized route makes the bargain more explicit. January 7 guidance requests corporate ownership and control information, detailed component and country-of-origin disclosures, manufacturing and testing locations, software and firmware origin, supply-chain concentration and single points of failure. It also requests a time-bound American manufacturing plan, investment and staffing information, a responsible contact and quarterly progress updates. Applicants must certify completeness and accuracy and disclose material changes. The original guidance says conditional approvals may run for up to twelve months and that submission does not guarantee acceptance.[2]

These requests are substantial because they reach beyond the finished airframe. They ask a producer to explain the organization and supply network behind it. They may reveal a domestic brand's dependence on a foreign manufacturing bottleneck or a foreign company's concrete ability to establish production here. In principle, such inquiry can be more discriminating than a flag on a box. Its quality will depend on whether the information is tested, updated and used to reach consistent decisions. A long application can describe a complicated business without necessarily making that business more secure.

The guidance attaches consequences to misrepresentation and knowing violations of conditions, including termination and exclusion from reapplication. It says decisions can be adjusted at the agencies' discretion. That is real leverage. The public should nevertheless distinguish the loss of an exception from the direct performance of a manufacturing promise. A regulator can remove access quickly; it cannot make a delayed production line function by signing a termination notice. Good conditions must help officials identify progress early enough to protect continuity, rather than reveal failure only when permission ends.

The people who can get through

An application is work. A producer needs component records from suppliers, an understanding of ownership relationships, a defensible production plan and people able to answer follow-up questions. Those capabilities are unevenly distributed. A small engineering firm may understand its aircraft better than it understands federal process. A large firm may be better at organizing an application than at repairing a subtle weakness in a delivered system. Administrative competence is necessary to a regulated market, but it should not silently become the main measure of technical merit.

This creates a political economy inside the exception. Scarce review capacity can become a source of competitive advantage. A firm that obtains a decision early can plan orders while a rival waits. A component supplier can become difficult to substitute if its paperwork travels more easily through procurement than another supplier's evidence. These are structural possibilities, not findings of favoritism in January's process. They warrant attention precisely because no corrupt intention is required for them to arise. A rational system can still favor organizations best equipped to navigate it.

The answer is not to abolish disclosure. Without it, officials would be asked to accept industrial promises on the applicant's authority. A sensible response is to make the burden proportional and the decision path legible. Applicants should know which information is indispensable, which uncertainty can be resolved through a bounded trial, and what a request for more information is intended to establish. Public reporting can describe processing time and decision categories without exposing sensitive designs or supplier contracts. Consistency is easier to assess when the categories of decision are visible.

There is also a question of whose continuity the process protects. A producer wants permission to sell. An operator wants equipment that can be maintained through a budget cycle. A component manufacturer wants demand stable

enough to justify tooling. Those needs can reinforce one another, but they are not identical. An approval that enables a new product launch near a deadline may help the producer without giving a buyer much confidence about later revisions. A manufacturing plan may create useful domestic capacity while leaving a mission-specific payload unsupported. The same decision can distribute security unevenly.

For that reason, the object of review should remain close to the product that enters use. Model names are convenient handles for machines whose components and services can change. A revised radio, an outsourced repair arrangement or an update server moved to a new operator may alter the relevant dependencies. This is not an argument that every alteration must restart an entire review. It is an argument for explaining which changes matter, who must report them and how a prior conclusion survives reassessment. Permission should have a memory.

The material-change disclosure in the January guidance provides a starting point. Its value depends on interpretation. Too narrow an interpretation leaves important changes invisible; too broad an interpretation can bury reviewers in notifications. The agencies need a distinction between ordinary maintenance and a change that affects the grounds for approval. Industry needs confidence that candid reporting will lead to a proportionate response. Otherwise the incentive can become defensive silence or unhelpful overreporting, neither of which helps a decision-maker understand the actual machine.

Users have a corresponding claim to usable information. They need not receive a company's full confidential application. They should be able to learn the scope of approval, the supported configuration, its relevant conditions and the expected support period. A public buyer should not discover after acquisition that the approval it relied upon covered a different variant. Nor should a purchaser be expected to infer a service commitment from a place on a list. Access, support and assurance are promises made by different actors. Procurement must bring them into the same conversation.

A test site is another kind of passage

On January 8 the FAA announced two additional UAS test sites: the Choctaw Nation of Oklahoma and the Indiana Economic Development Corporation. They become the eighth and ninth designated sites. The agency describes their role in evaluating emerging aircraft, supporting beyond-visual-line-of-sight and more autonomous operations, and collecting evidence for integration into national airspace. This is another way of opening a door, though it answers an aviation question rather than the FCC's production-based market restriction.[3]

Test infrastructure matters because a regulator and a buyer cannot responsibly learn everything from a supplier's showroom. Conditions must be created in which aircraft can be operated, failure can be observed and a proposed use can be compared with a requirement. A test site offers airspace, facilities and an institutional relationship through which that learning can occur. Its location can also change who is able to participate. Travel, specialized staff and the cost of repeating an evaluation affect which organizations get to turn a promising design into credible evidence.

Adding sites can improve access without automatically producing comparable results. An aircraft tested in one environment has encountered that environment, with its operators, weather, traffic assumptions and mission profile. Another site's success may answer a different question. This variation can be valuable; diverse conditions expose different weaknesses. The problem is not that every site must imitate every other. It is that the resulting evidence must describe its own limits clearly enough for a later reviewer to understand what can travel and what needs to be repeated.

An illustrative delivery trial makes the distinction plain. A route completed with favorable visibility, a prepared landing location and a technical team standing by may establish a useful milestone. It does not establish the same

service with tired staff, an altered loading procedure or unexpected ground activity. A demanding trial can still be economical if it identifies which conditions break the result. A polished demonstration becomes expensive when its omissions surface only after procurement. The purpose of a testing network should include discovering those omissions before they become operational surprises.

The relationship between approval routes becomes crucial here. Security assessment, domestic-content qualification, equipment authorization and operational aviation permission cannot simply be stacked as if each added the same kind of assurance. One concerns production and supply exposure. Another concerns radio and equipment rules. A flight evaluation addresses behavior under stated conditions. The operator must eventually assemble a coherent case from all of them. If the institutions exchange only final badges, the work of reconciling their assumptions falls on a buyer who may have the least capacity to do it.

A useful public investment would therefore make test conclusions easier to carry between institutions. That can mean a clear description of the aircraft and software tested, environmental conditions, unsuccessful attempts, operator preparation and changes made afterward. It does not require one giant database containing every sensitive fact. It requires enough shared meaning that one office's result does not become another office's slogan. Faster decisions are possible when a reviewer can reuse a sound piece of evidence instead of either trusting it blindly or recreating it from scratch.

The FAA's announcement establishes expanded designated infrastructure and an intended program of work. Its success should be judged later through the quality and usefulness of that work, including the opportunities available to smaller participants. Counting sites is easy. Understanding whether a test prevented a bad purchase, supported a safe operation or exposed an unresolved failure takes more effort. That effort is where the national value of the designation will be made. The productive asset is a capacity to learn, rather than the number on the map alone.

Buying time before the crowd arrives

The World Cup introduces a less forgiving clock. Reuters reported on January 12 that DHS would invest $115 million in counter-drone measures for the tournament and America's 250th anniversary celebrations. The report distinguishes this announcement from earlier FEMA grants of $250 million to eleven host states. The figures describe different public funding actions; they should not be casually added into a claim of equipment already installed. The report also says DHS did not specify which technologies would be deployed at venues.[4]

The article's limited technology detail is analytically important. A protection program must eventually decide which hazards it is addressing, where it can observe them and what lawful response is available. An instrument that detects a transmission may not detect a different kind of flight. An alert can be technically accurate yet operationally ambiguous. A venue can need the FAA, police, federal authorities and infrastructure operators to agree on what happens next. Public investment becomes protection only when those relationships work within the time allowed by the event.

This is where administrative speed can be a safety capability. A responder cannot always pause to resolve an organizational dispute while an aircraft approaches a crowd. Responsibilities need to be established before the incident. Speed also makes error more consequential. A system that turns every uncertain observation into an urgent threat can consume attention and interfere with legitimate operations. The choice is not between caution and action. It is between procedures that make uncertainty usable and procedures that either suppress it or allow it to paralyze a decision.

The January 13 War Department account supplies a more specific procurement event. JIATF 401 announced its first Replicator 2 acquisition on January 11: a contract for two DroneHunter F700 systems, expected for delivery

by April. The account describes a reusable interceptor using a net and presents the purchase as a step toward protecting military installations and infrastructure. Two systems are a concrete acquisition. Expected April delivery is a schedule. Neither should be expanded into an assertion that the resulting protection is already operational nationwide.[5]

The small initial quantity can be understood as a chance to learn. Operators can investigate integration, training, maintenance and the consequences of using the system in a particular setting. A reusable interceptor has its own replenishment and recovery demands even when it does not consume an expensive missile with each attempt. Questions about the safe handling of a captured aircraft remain operational questions, not benefits that can be inferred from a product description. A procurement can be sensible precisely because it creates a bounded opportunity to answer them.

This sequence connects capital to authority without making them interchangeable. Federal demand can reassure investors that a market exists. Investors can help a supplier expand before every later order is certain. Public agencies may benefit from that willingness to absorb risk. They should also guard against the return journey, when expectations amplified in capital markets begin to stand in for evidence of capability. A named acquisition is a reason to investigate the product's progress. It is not a substitute for acceptance records, training outcomes or performance under the conditions where it will be used.

The public has paid for more than hardware when it funds an early deployment. It has helped buy information about whether the arrangement works. Some of that information may properly remain protected, especially where it describes defensive coverage. Yet confidentiality should not erase internal accountability or prevent aggregate lessons from improving the next purchase. The lesson from two systems may be more valuable than a premature claim of scale. A program should be able to say what it learned without requiring its first announcement to have been a declaration of final success.

Keeping the exception from becoming the product

Taken together, the January developments suggest a government trying to build several kinds of trust at once. It is recognizing assessment lists, defining domestic production, inviting manufacturing commitments, expanding aviation testing and financing protection for concrete events and installations. These actions do not form one legal approval. They create an institutional environment in which different organizations will decide which aircraft and defenses may be supplied, tested, bought and used. Their coherence will depend on how well those decisions refer to one another.

The danger is that the exception becomes the product: a status easier to communicate than the machine's actual limitations. A company can sell reassurance through an official name. A buyer can simplify an uncomfortable decision by pointing to that name. An official can report approval throughput as if it measured security delivered. None of these shortcuts requires dishonesty. Each offers relief from complexity. Together they can leave the operational system less understood than the paperwork suggests, particularly after maintenance and software changes have accumulated.

The opposite danger is a process so elaborate that it cannot admit useful equipment at the pace public missions require. Every unresolved uncertainty cannot become a reason for indefinite delay. An aircraft protecting a dangerous facility or supporting emergency work may be valuable before all questions are closed. The state needs a way to authorize bounded use, collect evidence and revise a conclusion. Conditional admission is suited to that task when its limits are specific and its reviews are timely. It fails when conditions become a permanent fog around an otherwise ordinary purchase.

The reciprocal obligation is straightforward. A producer receiving temporary access should provide candid information and make observable progress on the commitments supporting it. An agency imposing conditions should explain its judgments and act within a calendar on which others can plan. A public buyer should specify the capability it needs and retain the evidence generated by early use. These are different responsibilities. Conflating them lets each institution imagine that another has answered the difficult question. Separating them clearly allows the overall system to move with greater confidence.

The practical contract between buyer and supplier can help carry that discipline. A purchaser might arrange for spare parts, access to maintenance records and an agreed response when a software service ends. It might specify which substitution requires consent and how a performance problem will be reported. Such provisions do not confer a regulatory exemption, and they cannot insure against every political change. They can keep an institutional decision from becoming a private mystery at the moment equipment fails. The buyer then has something more usable than a marketing claim about an official list: an account of what another party has undertaken to do.

There is a cost to maintaining that account. Engineers must document changes, purchasers must read conditions, and agencies must preserve the staff needed to make decisions. Those costs should enter the argument about efficiency. A process can appear cheap because it transfers work to an operator who encounters it later as downtime. It can appear slow because it performs work that prevents a much larger interruption. Neither speed nor volume is a complete measure. The relevant comparison is the burden of reaching and sustaining a useful decision, including the failures the process helps people avoid.

January's architecture is promising because it admits that a national category is too coarse to carry every decision. It is demanding because the exceptions must now bear the practical weight. The coming year will test whether they can support investment without rewarding empty plans, accelerate learning without diluting review, and preserve continuity without extending every arrangement by habit. That outcome is still open. A door in the wall is useful when people can understand where it leads, what they must carry through it and who remains responsible once the machine is on the other side.

Notes and sources

1. FCC, DA 26-22, January 7, 2026, including its attached DoW determination. Establishes the initial January 1, 2027 horizon, Blue UAS and domestic-end-product categories, and the section 1709 limitation. The department's descriptions of security testing are attributed to it. Original notice.
2. DoW and DHS, January 7, 2026, guidance for individualized UAS conditional approvals. Supports the requested disclosures, material-change certification, quarterly manufacturing updates, initially twelve-month maximum and consequences for knowing violations or misrepresentation. Original guidance.
3. FAA, January 8, 2026, announcement designating Choctaw Nation and Indiana Economic Development Corporation as the eighth and ninth UAS test sites. Establishes designations and intended work, rather than measured safety or decision-time outcomes. Agency announcement.
4. David Jeans, Reuters, January 12, 2026, report of DHS's planned $115 million counter-drone investment and the separate earlier FEMA grants. Used for the announced spending and limited public technology detail, not proof of installed capability. Contemporaneous report.
5. War Department, January 13, 2026, account of JIATF 401's January 11 announcement of its first Replicator 2 acquisition: two DroneHunter F700 systems, expected by April. System descriptions are the department's account; delivery and operational outcomes remain prospective. Acquisition account.