

Redesigning UK Defense Procurement for the AI Era

By Di Cooke

SEPTEMBER 2026

THE ISSUE

The United Kingdom is increasing defense spending at its fastest rate since the Cold War, naming AI a priority growth subsector. Yet the system built to buy ships, tanks, and aircraft was never designed for AI—a technology that can drift in behavior once delivered, hinges on rights to the data and models behind it, and takes specialist judgment to tell whether it works as intended. Recent reforms have made procurement faster, but that does not mean they address AI’s unique characteristics. This brief sets out six recommendations that would address these remaining procurement gaps by equipping the United Kingdom’s Ministry of Defence to be an intelligent customer of AI, redesigning contracts to align with how AI actually works, and growing a trusted supplier and assurance market. Together, they would turn strategic ambition into a procurement system that can buy, contract for, and sustain AI at the pace operations demand.

INTRODUCTION

As of 2026, artificial intelligence (AI) sits among the priority growth subsectors named in the United Kingdom’s largest sustained defense spending increase since the Cold War. Both the Strategic Defence Review and the Defence Industrial Strategy have centered AI as a core component of future warfighting, and a new UK Defence Innovation unit, backed by £400 million annually, has been established to fast-track innovation to the front line.¹

UK Defence and the wider government have already moved from intent to action on AI procurement.ⁱ The £900 million Digital Decision Accelerators for Defence

Open Framework have placed 26 suppliers under contracts to deliver AI decision support to the army’s ASGARD program, and the 2025 Spending Review earmarked £4 billion for autonomy.² A wider sovereign AI push has hardened in parallel, with the Defence Industrial Strategy 2025 framing UK sovereign capability as “the cornerstone of national security”; the Department for Science, Innovation and Technology (DSIT) launching the £500 million Sovereign AI Unit backing UK AI companies with investment, compute, and R&D funding to reduce reliance on foreign providers for security-critical AI; and a March 2026 cross-government directive classifying AI as a crit-

i “UK Defence” (often shortened to “Defence”) is the standard collective term for the entire UK defense enterprise, including the Ministry of Defence, the armed forces, and the MOD’s supporting agencies and bodies. It is used in this brief in that collective sense, rather than referring to the MOD head office alone.

ical element for national security, directing departments to prioritize UK suppliers.³

Process reform has also followed. The new segmented procurement model at the Ministry of Defence (MOD), which went live in April 2026, routes software, AI, and off-the-shelf capabilities through a new three-month fast lane, compared with a previous average of 6.5 years to award contracts worth more than £20 million.⁴ The recently published Defence Investment Plan set the overarching spending framework these reforms sit within, putting total planned defense spending on a path toward £298 billion, including ring-fencing £1.6 billion for UK Defence Innovation (UKDI) through 2030 and targeting 10 percent of the equipment budget on novel technologies, including AI.⁵ These measures are substantial, but none yet builds a procurement process able to deliver AI safely, securely, and responsibly, at the pace operations require.

The recommendations that follow address those gaps under three themes: (1) building an informed buyer base equips UK Defence with the skills, shared vocabulary, and testing capacity to act as an intelligent customer of AI; (2) designing contracts for how AI works in practice secures the data rights, continuity, and through-life assurance that AI systems need but standard defense contracts do not reach; and (3) developing an assurance-centered market open to specialist AI suppliers builds the trusted third-party assurance capacity, and the supplier depth, that is needed.

THE CHALLENGE OF AI PROCUREMENT DESIGN

AI procurement is hampered by two sources of friction: the technical characteristics of AI systems, which sit awkwardly with conventional procurement assumptions, and the structural features of the current reform program, which leave AI-specific design questions unaddressed.

Conventionally, defense procurement was designed with hardware in mind, and still runs software, IT, and AI through the same MOD equipment acquisition framework, CADMID, which was built for physical platforms. Recent reforms have begun to differentiate, with the segmented model's fast lane among them, but no separate software or AI acquisition pathway yet exists, so AI inherits assumptions designed for hardware. The friction that follows comes from AI's distinct technical nature.

First, AI systems are not static. A machine learning model trained on one dataset will drift in accuracy and behavior as the data environment shifts, as adversaries

adapt, or as the operational context changes. Research finds the more advanced the model, the higher the risk becomes.⁶ So a system that tested well can fail six months into operational use. JSP 936, the MOD's AI directive, requires performance to be monitored "at an appropriate rate," with continuing assurance whenever a model is modified; the 2024 Integrated Procurement Model already builds in iterative acquisition through its Spiral route.⁷ Neither yet translates into concrete contractual terms.

Altogether, AI-specific design questions sit one layer deeper than most reforms currently reach.

Second, data drives much of what AI systems do. Its provenance, quality, and representativeness determine how a system performs, and rights to it matter as much as rights to the hardware. JSP 936 directs that "contracting conditions should consider through-life support including access to data and algorithms as well as the resulting models," including "clear ownership of intellectual property."⁸ However, the standard contracting conditions (DEFCONs) that the MOD contracts use to handle intellectual property and technical data were built around patents, designs, and technical documentation, and were not designed for the training data, model weights, and configuration artifacts that AI systems depend on.⁹

Third, evaluating whether an AI model is reliable, secure, and operationally sound requires technical expertise that the procurement function has not historically been resourced for. The parliamentary Defence Committee's 2025 inquiry found AI expertise had limited reach into acquisition decisionmaking, further noting an AI workforce shortage.¹⁰ However, without technically capable buyers, the governance and assurance requirements set out by UK Defence cannot be meaningfully applied at the point of procurement. Altogether, AI-specific design questions sit one layer deeper than most access reforms currently reach.

Meanwhile, the supplier base itself raises a separate question. Defense procurement has historically favored large prime contractors with the scale and clearance capacity to deliver complex platforms, with the MOD's top 10 suppliers accounting for 39 percent of the procurement budget.¹¹ Yet AI-native capability often sits elsewhere, such as in specialist firms grown up around civilian AI markets and in start-ups and small and medium enterprises (SMEs). Much of the United Kingdom's leading AI talent works in

those firms, which makes the supplier base question a talent access challenge as well. Whether the current level of concentration gives the right competitive pressure on AI quality, or whether primes' platform contracts insulate AI buying from direct competition through subcontracting, is therefore a question about capability sourcing as much as industrial structure. In addition, the United Kingdom's growing sovereign AI focus makes this a matter that extends beyond competitive concerns. The Defence Industrial Strategy 2025's framing of sovereign capability as central to national security is operationally credible only if a domestic specialist AI supplier base exists to draw on. UK Defence has begun to widen access at this segment of the market through standing up the Defence Office for Small Business Growth (DOSBG), as well as launching the SME Commercial Pathway, Enterprise Agreement Lite, and the £900 million Digital Decision Accelerators for Defence Open Framework, where half the named suppliers are UK SMEs.

UK Defence's AI procurement policy, guidance, and reforms have begun to reach into the AI-specific design layer, but they remain early stage, partial in scope, or not yet AI calibrated. The procurement practice, contract terms, and supplier and assurance market that AI procurement now requires still need building out; widening access is not the same as a supplier base Defence can evaluate, assure, and sustain.

RECOMMENDATIONS

The AI procurement decisions UK Defence makes in the upcoming years will shape its capability for decades. The six recommendations that follow address the design layer the current reforms have not yet reached, covering procurement literacy, frameworks for common understandings, the testing infrastructure to evaluate AI systems, contract design for systems whose behavior shifts over time, data rights and vendor dependencies, and the supplier-market structure on which sovereign AI capability depends. Framing is deliberately assurance-led, reflecting the direction that both Defence and the wider government have taken in making AI assurance a central component of their AI implementation strategy.

The AI procurement decisions UK Defence makes in the upcoming years will shape its capability for decades.

An implementation matrix following the six recommendations sets out the owning bodies and the lead time required for each recommendation, across quick wins, intermediate steps, and longer-term actions.

EQUIPPING THE MOD TO BE AN "INTELLIGENT AI CUSTOMER"

These recommendations cover the internal capabilities UK Defence needs to specify, evaluate, and assure the AI it buys, such as a tiered procurement skills pathway, a shared capability taxonomy, and permanent AI testing infrastructure. Part 1 of the AI Policy Directive, JSP 936, has laid out the goal for the MOD to become "an intelligent customer of AI," but the procurement workforce, common evaluation vocabulary, and testing capacity are not yet ready for the AI procurement that the sovereign AI growth push and the segmented model's rapid lane will generate.¹²

RECOMMENDATION 1: UPSKILL UK DEFENCE'S PROCUREMENT WORKFORCE AND DEVELOP DEDICATED AI TRAINING AND EDUCATION

Build a tiered AI procurement skills pathway that equips relevant procurement officers with foundational AI literacy, gives those managing AI programs specialist depth, and houses the function inside the Defence AI Skills Framework with certification, mandatory refreshers, and named pathway ownership. Together, these actions give Defence's procurement workforce a pathway to becoming the intelligent customer of AI required for the portfolio its operations will demand.

JSP 936 requires that "all staff working with AI are suitably qualified and experienced," while Laying the Groundwork, the MOD's report on the responsible AI senior officers' (RAISO) first year implementing the JSP 936 directive, frames building the MOD's AI expert workforce as a trifold task: external AI recruitment, intensive training for some existing personnel, and AI literacy for the rest.¹³ On the procurement side, Commercial X, part of the National Armaments Director (NAD) Group, has begun a Specialist Skills Development Programme for commercial officers buying experimental technologies, with first recruits joining March 2025, and has codeveloped a "How to buy AI" training package with the Defence Artificial Intelligence Centre (DAIC).¹⁴ Commercial X has done important early work, but current efforts cannot match the pace and volume of AI procurement ahead, and procurement staff need

continuous education to keep up with a fast-moving technology. This recommendation converts procurement-side AI training into a tiered, persona-defined skills pathway, with a structured route for closing the interim gap.

Action 1: Expand and build on Commercial X’s “How to buy AI” training across the wider MOD procurement workforce as a tiered Suitably Qualified and Experienced Personnel (SQEP) requirement. Laying the Groundwork recognizes the need for “SQEP to support robust assurance,” but it does not specify a procurement-focused track.¹⁵ This will be accomplished across two tiers: (1) foundational AI literacy for all procurement officers, and (2) specialist depth for those managing AI or AI-enabled procurement above a risk threshold as defined by JSP 936. The foundational tier matters because AI is increasingly embedded in vendor offerings whose primary purpose is not AI, meaning that officers across the wider workforce need to recognize AI components and apply the right scrutiny. The specialist tier, meanwhile, would cover AI’s differences from conventional software, evaluation, and assurance against JSP 936’s risk tiers, AI-specific data and IP issues, and life cycle implications.

Ownership: The NAD Group should hold the funding and mandate, while the Defence Commercial Function (DCF), the MOD’s cross-department commercial and procurement organization, should deliver the specialist tier through Commercial X, with DAIC providing AI content. Digital Skills for Defence (DS4D) should deliver the foundational tier while Defence Equipment and Support (DE&S) adopts the tiered SQEP requirement for its commercial and Future Capability Group staff. The AI Security Institute (AISI) and external academic partners should contribute curriculum content across both tiers.

Action 2: Add an AI procurement officer persona to the Defence AI Skills Framework, with certification, mandatory refreshers, and named pathway ownership. DAIC is building a Defence AI Skills Framework around five AI personas, with a planned head of AI profession post to own recruitment, retention, and career pathways. A procurement persona should be added. A defined persona keeps skills attention sustained as the technology, the MOD’s needs, and industry offerings change. Officers completing the appropriate tier would receive certification, with periodic refreshers required to maintain it.

Ownership: DAIC should own the framework and the head of AI profession should take ownership of the AI

procurement officer career pathway and SQEP standards, in coordination with the Pan Defence Skills Framework taxonomy. DE&S Future Capability Group’s program and procurement staff would be direct consumers, alongside Commercial X and the wider DCF.

Together, these actions give UK Defence’s procurement workforce a pathway to becoming the intelligent customer of AI required for the portfolio its operations will demand.

Action 3: Offer several supporting mechanisms to fill the interim skills gap and help shape the curriculum. Building an expanded training program takes time, and JSP 936 provides that “support from external organisations must be incorporated” where in-house competence falls short.¹⁶ Rather than a single route, UK Defence should draw on several mechanisms suited to different skill needs. A secondment program modeled on the Defence Finance Zig-Zag scheme announced in April 2026 would bring AI experts from academia and industry into MOD procurement on time-bound engagements. Such a “tour of duty” model would let specialists serve fixed terms inside the MOD while keeping their industry ties. In addition, an AI reservist pathway could also be extended to cover AI procurement talent specifically, mirroring the Joint Cyber Reserve Force. For both of these, the newly established AI Expert Advisory Group, which convenes industry and academic AI specialists, offers a ready channel for identifying suitable people and keeping the curriculum current.

Ownership: The NAD Group should own these mechanisms alongside the DCF, while DAIC and external expert partners coordinate AI content. The DE&S Future Capability Group and Commercial X would be the main destinations for secondees and other placements.

RECOMMENDATION 2: ESTABLISH A SHARED CAPABILITY FRAMEWORK FOR UK DEFENCE AI PROCUREMENT AND ASSURANCE

Develop and publish a UK Defence AI capability taxonomy that gives procurement teams, vendors, and assurance pro-

viders a shared vocabulary for describing AI systems, going beyond technical benchmarks to capture workflow positioning, authority delegation, and the organizational effects each system has on decisionmaking. Together, these measures turn per-system documentation into a cross-system framework for procurement, assurance, and downstream evaluation. They furthermore give Defence the shared vocabulary it needs to compare AI offerings consistently and condition assurance work on capability category.

Taxonomy foundations for AI procurement are forming. For instance, JSP 936 sets a five-level risk rating and requires definition of each system's operational design domain, while DAIC's AI Assurance Framework operationalizes that approach and supplies the DAIC AI model card as a per-system template now used across UK Defence.¹⁷ However, per-system documentation describes each AI offering on its own terms, leaving procurement teams without a common vocabulary for comparing offerings or mapping them onto consistent evaluation criteria. This recommendation sets out how to build it.

Action 1: Develop a classification taxonomy under DAIC and MOD leadership. A common language is the precondition for the process and measurement standards that sit above it. However, developing this will require dedicated research the MOD is not resourced to do in-house. The MOD should therefore commission an ad hoc research consortium to develop the initial operational taxonomy, drawing on the United Kingdom's AI governance research community and the DAIC AI Expert Group. Well-placed candidates include the Centre for the Governance of AI, the Institute for AI Policy and Strategy, the Centre for Emerging Technology and Security at the Alan Turing Institute, the Centre for Long-Term Resilience, and Apollo Research.

Ownership: DAIC, working under MOD direction, should be responsible for the definitional and technical work, while the AI Security Institute should support on capability evaluation domains, drawing on its existing structured work on AI model risks. Meanwhile, DSIT should support cross-government alignment, and the National Physical Laboratory (NPL) Centre for AI Measurement should support the technical-benchmark axis as its measurement work matures. A research consortium of AI governance experts, commissioned by the MOD, should produce the initial draft, and the AI Expert Advisory Group can provide further support.

Action 2: Publish an initial taxonomy as minimum viable product guidance and iterate it through real pro-

curement. The first published version should be framed as initial guidance, refined against live submissions, on the maturation pattern the DAIC AI Assurance Framework follows.

Ownership: DAIC should publish and maintain the taxonomy, while the AI Expert Advisory Group should convene industry and academic experts who could support the taxonomy's development and its regular review cycle, so it keeps pace with technical and operational change.

RECOMMENDATION 3: EXPAND THE AI MODEL ARENA'S TESTING INFRASTRUCTURE AND SCOPE

Establish the AI Model Arena as permanent testing infrastructure, fully integrated with the DAIC AI Assurance Framework and scaled to the rapid procurement lane. Permanent infrastructure and a wired-in connection to the DAIC Assurance Framework will give UK Defence the ongoing testing capacity to procure safe, secure, and reliable AI at the pace its expanding portfolio requires.

JSP 936 lays out Defence's requirement of verification and validation across the operational design domain, at boundary conditions, and against inputs outside design. The MOD's recently launched AI Model Arena evaluates models under such conditions, generating evidence in realistic mission contexts with varied inputs and adversarial conditions rather than against fixed benchmark datasets.¹⁸ The DAIC AI Assurance Framework also supplies the operational layer above it: a model card template, a risk assessment process aligned to JSP 936's five-level rating, and assurance question guidance. What the arena lacks is permanent footing, a published forward plan vendors can align with, and a defined route by which its outputs feed continuous assurance. The actions below would turn the arena from a working pilot into lasting testing infrastructure, integrated across the AI life cycle.

Action 1: Establish the AI Model Arena as a permanent testing and evaluation sandbox. Permanent operation requires ringfenced funding, expanded use case coverage, and capacity to test at the appropriate classification levels through secure facilities.

Ownership: DAIC would continue to be the operational owner, with the Defence Science and Technology Laboratory providing secure testing facilities and supporting on test design and adversarial conditions, and the DCF contracting for additional testing capacity where the current pilot configuration cannot meet classification or volume requirements.

Action 2: Wire the AI Model Arena into postdeployment life cycle assurance through the DAIC AI Assurance Framework. The framework already operationalizes JSP 936's through-life monitoring obligations, but no defined route yet exists for the arena's preprocurement evidence to feed the monitoring layer. DAIC should specify how arena outputs populate the model card and risk assessment templates, and how in-service monitoring against those baselines triggers re-evaluation. This converts the arena from a discrete preprocurement step into the entry point for continuous assurance, consistent with the sustainment provisions in Recommendation 5.

Ownership: DAIC should own the framework integration, while the DE&S Future Capability Group ensures programs consume the integrated evidence trail through contract and through-life management.

AI-RELEVANT CONTRACTUAL REDESIGN

These recommendations cover the contractual terms UK Defence needs to control the AI it buys and assure it across the life of the contract, such as clauses securing data rights, continuity and supply chain transparency, and a through-life assurance requirement built into every stage. These are the parts of the contract that existing instruments do not reach, and without them UK Defence cannot secure the freedom of action JSP 936 requires nor catch the unique failure modes AI systems can develop after deployment.

RECOMMENDATION 4: STRENGTHEN UK DEFENCE'S CONTRACTUAL CONTROL OVER AI SYSTEMS, DATA, AND SUPPLY CHAINS

Develop AI-specific contract clauses covering data rights, continuity, portability, and supply chain disclosure, so UK Defence retains the freedom of action JSP 936 requires across the AI life cycle. These provisions give UK Defence the foundations for sovereign AI capability: visibility into what its systems depend on, ownership of the data and models behind them, and freedom from lock-in to any single supplier or foreign jurisdiction.

UK Defence already has the policy basis and some contractual architecture to build on. JSP 936 requires contracting conditions to consider through-life access to data and algorithms, with clear ownership of intellectual property, and requires foreign export controls to be assessed so the

MOD keeps the “necessary Freedom of Action to maintain, modify, upgrade and operate the AI.”¹⁹ Existing contractual instruments cover software and technical data, but none reach the AI asset categories that AI capability turns on, including training data, model weights, evaluation datasets, and configuration artifacts. AI capability also moves faster than the lifespan of any single vendor relationship, so without rights over those assets and the means to move them, the MOD risks vendor lock-in, a dependence on a single supplier that both Knack et al. and Wright et al. identify as a core procurement risk.²⁰ The MOD's freedom of action therefore depends on data rights, portability, and supply chain transparency provisions secured at contract award, a contract design gap the measures below address.

These are the parts of the contract that existing instruments do not reach, and without them UK Defence cannot secure the freedom of action JSP 936 requires nor catch the unique failure modes AI systems can develop after deployment.

Action 1: Develop AI-specific standard contract clauses for training data, model weights, evaluation data, operational data, and configuration artifacts. Each category should carry specified rights for the MOD calibrated to mission need, complementing existing software and technical data instruments rather than replacing them. The same exercise should review contractor-owned background IP, assessing where existing mechanisms can disadvantage SMEs whose commercial viability depends on IP retention.

Ownership: The DCF, working with MOD commercial policy and legal bodies, should develop and issue the standard clauses and apply them across AI contracts, and DAIC should provide AI-specific input on asset categorization.

Action 2: Apply standard continuity-of-operations and portability provisions to AI contracts above a defined threshold. JSP 936's right of access to model weights, training data, and evaluation code depends on supplier cooperation, which offers no protection if a supplier fails, exits the market, or refuses to comply. Conse-

quently, continuity provisions should cover: (1) escrow of training data, model weights, and configuration artifacts with a neutral third party, so the MOD can recover them if the supplier fails or refuses access; (2) exit arrangements; (3) step-in rights; (4) named-successor arrangements identified in advance; and (5) minimum notice periods before a vendor can terminate, withdraw, or materially change the service. In addition, portability provisions should require vendors to supply migration tools, including export utilities, common API support, and the documentation needed to operate the model in an alternative environment, so capability can move to an alternative provider without bespoke rebuilding.

Ownership: The DCF, working with MOD commercial policy and legal bodies, should draft the continuity and portability provisions alongside the data rights clauses and issue them as standardized, reusable clauses written into AI contracts at award, on a do-once, use-many basis.

Action 3: Require vendors above the threshold to disclose upstream supply chains for any system offered, at award and on material change. Disclosures should cover foundation models incorporated, third-party components used, and the jurisdictions in which compute, hosting, and inference operate. Without this visibility, neither security assurance nor sovereign control can be meaningful. Undisclosed foreign dependencies expose deployed AI to supply chain compromise and conflicting export control regimes, and opaque upstream components make it impossible to confirm whether the MOD retains the control the rest of this recommendation seeks to protect.

Ownership: The DCF should draft the disclosure clause as part of the AI clause package and write it into AI contracts above the threshold, while DAIC should receive and assess the disclosures as part of the assurance process.

RECOMMENDATION 5: EMBED THE THROUGH-LIFE ASSURANCE REQUIREMENT IN UK DEFENCE AI PROCUREMENT CONTRACTS

Ensure UK Defence AI procurement contracts carry the through-life assurance requirement at every stage of the contract's life, from rapid-lane development iteration through operational sustainment. This preserves the assurance bar JSP 936 sets, while accounting for the AI-specific reality that a system performing well at delivery may degrade undetected.

MOD policy already recognizes the need to monitor AI systems continuously against unique failure modes, with

JSP 936 codifying it as a through-life assurance requirement and the DAIC AI Assurance Framework operationalizing those obligations through standardized guidance materials. Meanwhile, procurement structure is moving in the same direction: The newly established segmented procurement model runs a three-month rapid lane for software and AI on the Accelerating Commercial Pathway, Commercial X has shown that pace and rigor can run together at scale, and component organizations are formalizing coordination groups to maintain oversight as AI capabilities transfer from acquisition into operations. Nonetheless, these directions do not yet meet at the contract level. This recommendation suggests four measures to close that gap, with two for the development stage and two for the postdeployment stage.

Action 1: Specify assurance evidence at each rapid-lane contract iteration, carried by DAIC Framework artifacts. Each iteration on the segmented model's rapid lane should produce assurance evidence proportionate to the JSP 936 risk rating of the iteration, with the substantive evidence content carried by the DAIC AI Assurance Framework's materials and evolving along with the framework's offerings. This anchors progression between contract phases on substantive AI-specific evidence rather than on generic deliverable completion and gives both the contracting body and the supplier the same standardized vocabulary for what constitutes adequate evidence at each iteration.

Ownership: DE&S should write the evidence requirement into rapid-lane contracts at award, applying the standard templates the DCF maintains, while DAIC maintains the framework artifacts that define what evidence each risk level requires.

Action 2: Establish a defense-specific accelerated requalification route for midcontract AI model updates. The European Defence Agency noted in 2025 that defense AI use cases require model updates at a pace incompatible with running the full qualification cycle each time, and that new approaches are needed to formalize the trade-off between safety and operational tempo.²¹ To address this, the UK procurement-side route should distinguish routine midcontract updates, such as retraining on fresh operational data within the same operational domain, from material changes, such as architectural shifts, new operational domains, or changes to the risk profile. This would help prevent a routine model refresh from triggering a full requalification cycle that the contracting timeline cannot absorb, without weakening assurance for substantive changes.

Ownership: DAIC should publish the criteria distinguishing routine updates from material changes against the JSP 936 risk rating, the program's technical and assurance authority authorizes the accelerated route on each contract where the supplier meets those criteria, and DE&S should make the corresponding contractual change.

Action 3: Carry funded sustainment provisions across operational life. Keeping an AI system safe and effective after delivery is continuous work, but contracts too often treat it as an optional extra. Left unfunded, the through-life monitoring this recommendation depends on slips from obligation to goodwill, and systems degrade undetected. AI procurement contracts should therefore carry standardized, funded sustainment provisions covering monitoring, performance evaluation, retraining, and updating across operational life. Treating sustainment as a funded deliverable, not an optional add-on, turns that obligation into enforceable practice.

Ownership: DAIC should publish the standard sustainment clause and the minimum content required and DE&S should write the clause into all AI contracts at award, with the sustainment budget ringfenced rather than negotiated midlife.

Action 4: Decide when to retrain an AI model using pre-agreed triggers, with a named owner for each decision. AI models need periodic retraining as the data and threat environment shifts, and leaving the timing to case-by-case judgment invites delay and inconsistency. Contracts should set out in advance the conditions that prompt a retraining decision and name who is responsible for making it. These include signs that a model's performance is drifting, incident reports from operators using it, significant changes in the operational environment, and updates to UK defense policy. Fixing the triggers and the owner at contract award turns retraining from an ad hoc reaction into a planned, accountable step.

Ownership: The RAISO would hold routine retraining decisions against the criteria DAIC publishes and escalate material changes through the JSP 936 risk-based approval chain.

BUILDING A CAPABLE AI VENDOR MARKET

RECOMMENDATION 6: BUILD A DEFENSE-READY UK AI ASSURANCE MARKET

This final recommendation builds a defense-ready AI assurance market on foundations already forming in the civil-

ian sector. That market is maturing fast, but it is not yet calibrated to defense needs, and without the defense-side measures to make it usable, the assurance bar JSP 936 sets will outstrip the external capacity AI procurement now depends on.

UK Defence does not have to build this market alone, as substantial civilian infrastructure is already forming around DSIT's Trusted Third-Party AI Assurance Roadmap, a phased route to professional certification supported by an £11 million Innovation Fund opening in spring 2026 and a new £10.5 million Centre for AI Measurement at the National Physical Laboratory, all underpinned by a sizable and growing AI assurance sector.²² Defense-specific assurance infrastructure is at an earlier stage but moving in the same direction, with DAIC's AI Assurance Framework operationalizing JSP 936 through live projects developing standardized documentation, an aligned risk assessment process, and assurance question guidance. What is missing are the defense-side measures to make it usable.

Action 1: Establish and publish guidance on what constitutes adequate assurance at each JSP 936 risk level. DAIC should publish clear minimum assurance thresholds against the five-level risk rating, evolving alongside the AI Assurance Framework as it moves from minimum viable product to operational maturity. Published thresholds inform the growing assurance market of the requirements certified providers will need to evaluate against and signal to AI vendors how to align their offerings with the assurance bar they will face in defense procurement.

Ownership: DAIC should publish and maintain the thresholds.

Action 2: Build a defense-specific certification overlay on civilian assurance foundations. Once the DSIT scheme is formalized, qualifying civilian assurance certification could count as prequalification for defense work, with a defense overlay added on top. The Cyber Essentials certification scheme, required for in-scope MOD contracts, provides a precedent.²³ The overlay should cover the unique requirements arising from the defense-specific operational, legal, and security environment.

Ownership: DAIC should set the overlay criteria, and DSIT should be engaged early to ensure the civilian scheme accommodates a defense overlay.

Action 3: Make AI assurance a procurable capability in its own right. As AI procurement scales, the MOD's in-house assurance capacity risks struggling to keep pace.

The DCF should therefore establish a parallel commercial pathway for assurance-as-a-service contracts, allowing the MOD to procure system testing, model validation, and post-deployment monitoring directly from trusted and accredited third-party providers, independently of the AI system being assured. This adds a second route by which the maturing third-party assurance market reaches UK Defence

and reduces single-point dependency on the MOD's own assurance personnel.

Ownership: The DCF should establish the assurance-as-a-service pathway. The DAIC should specify the work and act as the technical buyer, while DOSBG should signpost SME providers into the pathway.

Table 1: Phased Implementation Matrix

This matrix summarizes the sequencing of all six recommendations across three phases, identifying the specific actions and owning bodies at each stage.

Recommendation	Quick Wins (< 6 months)	Intermediate Steps (< 1 year)	Longer-Term Actions (< 2 years)	Owning Bodies
Rec 1: Equip UK Defence's procurement workforce to act as an intelligent customer of AI	Stand up an interim skills menu: secondments (Zig-Zag model), tour-of-duty placements, and an AI procurement reservist stream, with the AI Expert Advisory Group sourcing people.	Scale Commercial X's "How to buy AI" training across the workforce via DS4D as a tiered SQEP requirement (foundational literacy first, specialist depth to follow).	Embed an AI procurement officer persona in the Defence AI Skills Framework, with certification, refreshers, and pathway ownership under the head of AI profession.	<i>NAD Group; DCF (Commercial X); DAIC; DS4D; DE&S; AISI; AI Expert Advisory Group</i>
Rec 2: Establish a shared capability framework for UK Defence AI procurement and assurance	DAIC and MOD scope the taxonomy and commission a research consortium (GovAI, IAPS, CETaS, CLTR, Apollo Research) to produce the initial draft.	Publish a minimum viable product taxonomy as initial guidance and require structured capability submissions from vendors against it.	Iterate the taxonomy through the AI Expert Advisory Group's review cycle against live submissions until it shapes assurance decisions consistently.	<i>DAIC; commissioned research consortium; AI Expert Advisory Group; AISI; DSIT; NPL Centre for AI Measurement</i>
Rec 3: Expand the AI Model Arena's testing infrastructure and scope	DAIC publishes a forward use case roadmap so vendors and procurement teams can align to the arena's expanding scope.	NAD Group ringfences funding to convert the arena from pilot to permanent infrastructure, with expanded use case coverage and additional secure testing facilities commissioned where the current configuration cannot meet classification or volume needs.	DAIC specifies how arena outputs feed into the AI Assurance Framework's monitoring layer, converting the arena from a discrete preprocurement step into the entry point for continuous life cycle assurance.	<i>DAIC; Defence Science and Technology Laboratory; DCF; DE&S Future Capability Group</i>
Rec 4: Strengthen UK Defence's contractual control over AI systems, data, and supply chains	The DCF, with MOD commercial policy and legal, publishes a first AI clause package covering data rights, continuity, portability, and supply chain disclosure.	The DCF writes the clauses into above-threshold AI contracts at award; DAIC assesses supply chain disclosures as part of assurance.	The clause package iterates through use in live contracts, reviewed periodically by the DCF to keep pace with technology and vendor practice.	<i>DCF; MOD commercial policy and legal bodies; DAIC</i>

Recommendation	Quick Wins (< 6 months)	Intermediate Steps (< 1 year)	Longer-Term Actions (< 2 years)	Owning Bodies
Rec 5: Embed the through-life assurance requirement in UK Defence AI procurement contracts	DAIC publishes criteria separating routine updates from material changes; DE&S writes the iteration-evidence requirement and accelerated requalification route into rapid-lane templates.	DAIC publishes the standard funded sustainment clause; DE&S writes it into all AI contracts at award, with budgets ringfenced, not negotiated midlife.	Retraining runs on pre-agreed triggers and named ownership, with each program's senior responsible owner holding routine decisions against DAIC criteria and escalating material changes.	DAIC; DE&S
Rec 6: Build a defense-ready UK AI assurance market	DAIC publishes minimum assurance thresholds against JSP 936's five-level risk rating, signaling to the market and to vendors what providers must evaluate against.	DAIC engages DSIT so the Trusted Third-Party AI Assurance scheme can carry a defense overlay once formalized, with overlay criteria set in parallel.	The defense overlay launches, civilian certification counts as prequalification, and the DCF stands up an assurance-as-a-service pathway.	DAIC; DSIT; DCF; DOSBG

Source: CSIS.

CONCLUSION

The United Kingdom has set its strategic direction and built real reform momentum, but what remains missing is a procurement system designed for the technology it is already buying. Policy and best-practice materials such as JSP 936, the DAIC AI Assurance Framework, and Laying the Groundwork have set the direction, and initiatives like the AI Model Arena, the segmented procurement model, Commercial X, and the Accelerating Commercial Pathways program have begun to put reform into operation. The recommendations here address the next step: a procurement system that can buy, contract for, and sustain AI at the pace that faster procurement and a growing sovereign AI portfolio now demand.

The United Kingdom has set its strategic direction and built real reform momentum, but what remains missing is a procurement system designed for the technology it is already buying.

The three pillars work as a single loop: Skilled buyers with shared vocabulary and testing capacity are the precondition for AI-calibrated contracts that hold data rights, continuity, and through-life assurance, and those contracts

are enforceable only against a credible supplier market deep enough to meet them. The window to accomplish this rapidly is narrowing, as the AI portfolio entering operational service this decade will be shaped by procurement decisions taken in the next few years. Delays carry identifiable costs, ranging from foreign export controls binding Defence to dependencies it cannot exit, AI systems degrading undetected after delivery, and specialist firms holding the United Kingdom's leading AI capability priced out by conventional procurement structures.

Procurement design built for AI is the foundation UK Defence needs to convert its ambition into capability for the decade ahead. ■

DiCooke is a non-resident adjunct fellow with the Intelligence, National Security, and Technology Program at the Center for Strategic and International Studies in Washington, D.C.

This brief is made possible by general support to CSIS. No direct sponsorship contributed to this brief.

CSIS BRIEFS are produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s). © 2026 by the Center for Strategic and International Studies. All rights reserved.

Cover Photo: Ian Forsyth/Getty Images

ENDNOTES

1. Ministry of Defence, *Strategic Defence Review 2025: Making Britain Safer: secure at home, strong abroad* (London, UK: Ministry of Defence, June 2025), 16, <https://www.gov.uk/government/publications/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad>.
2. “Digital Decision Accelerators for Defence (DDAD) Open Framework,” Ministry of Defence, <https://www.find-tender.service.gov.uk/Notice/049782-2025>; and HM Treasury, *Spending Review 2025* (London, UK: HM Treasury, 2025), CP 1336, <https://www.gov.uk/government/publications/spending-review-2025-document/spending-review-2025-html#executive-summary>.
3. Ministry of Defence, *Defence Industrial Strategy 2025: Making Defence an Engine for Growth* (London, UK: Ministry of Defence, September 2025), 9, <https://www.gov.uk/government/publications/defence-industrial-strategy-2025-making-defence-an-engine-for-growth>; and Press Office, UK Government’s Department for Science, Innovation and Technology, “AI Firms Pioneering Drug Discovery, Cheaper Supercomputing and More Get First Backing through UK’s Sovereign AI,” press release, April 16, 2026, <https://www.gov.uk/government/news/ai-firms-pioneering-drug-discovery-cheaper-supercomputing-and-more-get-first-backing-through-uks-sovereign-ai>.
4. Ministry of Defence, *Strategic Defence Review 2025: Making Britain Safer: secure at home, strong abroad* (London, UK: Ministry of Defence, June 2025), <https://www.gov.uk/government/publications/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad>.
5. Ministry of Defence, *The Defence Investment Plan: Equipping our Forces, Defending our Future* (London, UK: Ministry of Defence, July 2026), https://assets.publishing.service.gov.uk/media/6a44e989167a99cf0018da38/The_Defence_Investment_Plan.pdf.
6. Ulysse Richard, Heather Frase, Sarah Cao, Di Cooke, Sebastian Kwon, and Adrianna Tan, *Testing and Evaluation of Agentic AI Systems In Military Command and Control* (London, UK: Arcadia Impact, August 2026), <https://doi.org/10.48550/arXiv.2608.20597>.
7. Ministry of Defence, *JSP 936 V1.1 Dependable Artificial Intelligence (AI) in Defence* (London, UK: Ministry of Defence, November 2024), 27, https://assets.publishing.service.gov.uk/media/6735fc89f6920bfb5abc7b62/JSP936_Part1.pdf; and Ministry of Defence, *Integrated Procurement Model: Driving Pace in the Delivery of Military Capability* (London, UK: Ministry of Defence, February 2024), <https://www.gov.uk/government/publications/integrated-procurement-model-driving-pace-in-the-delivery-of-military-capability>.
8. Ministry of Defence, *Dependable Artificial Intelligence*, 30.
9. Ministry of Defence, *Guidelines for Industry No. 10: The Intellectual Property Rights (IPR) DEFCONs*, Commercial Toolkit (London: Ministry of Defence), <https://www.gov.uk/guidance/knowledge-in-defence-kid>.
10. House of Commons Defence Committee, *Developing AI Capacity and Expertise in UK Defence* (London, UK: House of Commons, January 2025), HC 590, <https://publications.parliament.uk/pa/cm5901/cmselect/cmdfence/590/report.html>.
11. Imogen Squire and Simon Brawley, *Research and Development (R&D) for UK Defence* (London, UK: Parliamentary Office of Science and Technology, April 2026), POSTnote 766, 21, <https://doi.org/10.58248/PN766>.
12. Ministry of Defence, *Laying the Groundwork: Responsible AI Senior Officers’ Report 2025* (London, UK: Ministry of Defence, October 2025), 7, <https://www.gov.uk/government/publications/laying-the-groundwork-responsible-ai-senior-officers-report-2025>.
13. Ministry of Defence, *Dependable Artificial Intelligence*, vi; and Ministry of Defence, *Laying the Groundwork*, vi.
14. “Ministry of Defence - Commercial X,” Ministry of Defence, last modified January 26, 2026, <https://www.gov.uk/guidance/ministry-of-defence-commercial-commercial-x>.
15. Ministry of Defence, *Laying the Groundwork*, 9.
16. Ministry of Defence, *Dependable Artificial Intelligence*, 28.
17. Ministry of Defence, “The Defence AI Centre (DAIC) AI Assurance Framework,” *AI Practitioner’s Handbook*, last modified February 27, 2026, <https://www.digital.mod.uk/policy-rules-standards-and-guidance/aiph/the-defence-ai-centre-ai-assurance-framework>.
18. Press Office, Ministry of Defence, “Launching the AI Model Arena,” press release, November 10, 2025, <https://www.gov.uk/government/news/launching-the-ai-model-arena>; and “The AI Model Arena: Redefining How the UK Evaluates AI,” Advai, November 24, 2025, <https://www.advai.com/journal/the-ai-model-arena-redefining-how-the-uk-evaluates-ai>.
19. Ministry of Defence, *Dependable Artificial Intelligence*, 30.
20. Anna Knack et al., *Defence AI Assurance: Identifying Promising Practice and a System Card Template for Defence* (London, UK: The Alan Turing Institute, September 2025), <https://www.turing.ac.uk/news/publications/defence-ai-assurance-identifying-promising-practice-and-system-card-template>; and Jared Wright, Benedict Macon-Cooney, and Kevin Luca Zanderemann, *Reimagining Procurement for the AI Era* (London, UK: Tony Blair Institute for Global Change, August 2024), <https://institute.global/insights/public-services/reimagining-procurement-for-the-ai-era>.
21. European Defence Agency, “Trustworthiness for AI in Defence,” European Defence Agency TAID Working Group, White Paper, May 2025, <https://eda.europa.eu/docs/default-source/brochures/taid-white-paper-final-09052025.pdf>.
22. Department for Science, Innovation and Technology, *Trusted Third-Party AI Assurance Roadmap* (London, UK: Department for Science, Innovation and Technology, September 2025), <https://www.gov.uk/government/publications/trusted-third-party-ai-assurance-roadmap>; and National Physical Laboratory, “NPL to Establish New Centre for AI Measurement,” press release, January 29, 2026, <https://www.npl.co.uk/news/npl-to-establish-new-centre-for-ai-measurement>.
23. “Cyber Essentials,” National Cyber Security Centre, <https://www.ncsc.gov.uk/cyberessentials/overview>.