



LEGATE SOLUTIONS LLC

Federal AI Assurance & Cybersecurity Compliance

Primes bring us in when a solicitation puts real weight on AI governance, an authorization to operate (ATO), FedRAMP, logging maturity, or zero trust, and the team needs a cleared senior engineer who has already done that work in a federal environment. We take a defined work package, put a named principal on it, and we do not market to your customer.

UEI [UEI]
CAGE [CAGE]
SAM.GOV Active
SIZE Small business
SET-ASIDE [status as registered]
CLEARANCE Active Top Secret (DoD), SCI-eligible (lead principal)
CONTACT - partners@legatesolutions.com
legatesolutions.com

CORE COMPETENCIES

AI Governance and Compliance OMB M-25-21 / M-25-22

We support high-impact determinations, impact assessments, pre-deployment testing, monitoring plans, human oversight, appeal processes, and AI acquisition terms covering data rights and lock-in.

Secure AI Architecture and Deployment

We design secure AI deployments with grounded RAG, citation enforcement, hallucination and bias controls, human validation, multi-agent orchestration, and walled-garden or air-gapped inference for controlled unclassified information (CUI).

Zero Trust, Identity, and Privileged Access OMB M-22-09

Zero trust architecture, segmentation, enterprise IAM and PAM, TIC 3.0-aligned design, and cloud security across Azure, GCP, and AWS.

Authorization, FedRAMP, and Continuous Compliance

NIST SP 800-53 Rev. 5 control implementation, system security plans (SSPs), plans of action and milestones (POA&Ms), third-party assessment organization (3PAO) evidence, FedRAMP Moderate/High sustainment, continuous ATO (cATO) enablement, and automated FISMA reporting.

Continuous Monitoring, SIEM, and Incident Response OMB M-26-14

M-26-14 log coverage, SIEM and pipeline architecture, retention/searchability design, SOC enablement, threat intelligence integration, and incident response processes.

CAASM (Cyber Asset Attack Surface Management), Vulnerability and OT/IoT Visibility CISA BOD 26-04 / 23-01

Multi-tenant asset reconciliation, vulnerability management, ICS/SCADA and connected-device discovery, coverage metrics, and risk-based remediation prioritization.

Endpoint Security and Virtual Desktop Modernization

Enterprise EDR migration, multi-tenant policy architecture, detection tuning, secure AVD and VMware Horizon design, STRIDE modeling, and endpoint baselines.

Network Security and Secure Infrastructure

NGFW, micro-segmentation, SDN, TIC 3.0 patterns, directory services, data center and virtualization security, backed by expert IP/MPLS, BGP, IS-IS, and segment-routing engineering.

Security Automation, Test, and Validation

Automated STIG/SCAP scanning, IaC and container security gates, baselines, audit files, Python control-validation harnesses, test labs, and security-stack health checks.

WHY PRIMES BRING US ON

We have built federal AI systems.

Not slideware. Guardrails, grounding, citation enforcement, bias checks, and agentic asset enrichment — built, tested, and running in live federal environments.

We know what an evaluator marks down.

Our principals have written technical volumes and stood up in orals for federal cyber bids. We can write our own scope, map to your labor categories, and usually turn comments within 24 hours at no cost to the prime.

Cleared senior capacity.

Our lead principal holds an active Top Secret (DoD) clearance and is SCI-eligible. If your solicitation names a cleared senior security or AI architect, you can fill that slot without opening a recruiting cycle.

Depth at the network layer.

Two CCIEs and a JNCIE-SP between the principals, plus years designing and validating large IP/MPLS backbones.

Federal scale.

Our principals have delivered on DHS, CISA, DoD, DOE, and SEC programs, including security operations at multi-agency scale.

Three senior principals, no junior bench.

The person you meet is the person doing the work. We keep the scope tight, use firm-fixed pricing when it makes sense, and take ownership of our piece of the subcontract.

WHERE WE FIT

WORK PACKAGE	BEST FIT
AI assurance	High-impact determinations, impact assessments, guardrails, bias/hallucination testing, and secure CUI deployment.
ATO / FedRAMP	Control narratives, SSPs, POA&Ms, 3PAO evidence, cATO enablement, and continuous monitoring.
Visibility / zero trust	Logging maturity, SIEM, CAASM, endpoint modernization, segmentation, IAM, and privileged access.

PROOF POINTS: PLATFORMS, CERTIFICATIONS, AND CLEARANCES

AI & LLM: M365 Copilot, Copilot Studio, Azure OpenAI, Vertex AI, Claude, Bedrock, Ollama, RAG

Endpoint & EDR: CrowdStrike, Defender, Carbon Black, Tanium, Cylance, McAfee ePO, Intune, SCCM

Network & Perimeter: Palo Alto NGFW, VMware NSX, Cisco R&S, Juniper Junos (MX / PTX / ACX), Contrail, IP/MPLS, BGP, IS-IS, TIC 3.0, AD / DNS / DHCP

Virtual Desktop & Datacenter: Azure Virtual Desktop, VMware Horizon, vSphere, FlexPod, Veeam

Vulnerability & CAASM/CTEM: Tenable (Nessus, .sc, ACAS), Tripwire IP360, Axonius, Armis, ServiceNow HWAM

Identity & Privileged Access: CyberArk PAM and EPM, Venafi, Entra ID, HSM

SIEM, Data & GRC: Splunk, Elastic, Sentinel, Cribl, Databricks, RSA Archer, Phantom SOAR

Automation & Test: Ansible, OpenSCAP, STIG, GitLab CI/CD, Docker, Checkov, Prowler, Selenium, OWASP ZAP, IXIA/Keysight, Python

Certifications & clearances: CISSP, CISA (ISACA), CCSP, CDPSE, two CCIEs, JNCIE-SP, CyberArk, Splunk, Tenable, Palo Alto, VMware, NetApp, Microsoft, and DoD 8140 IAT III; active Top Secret DoD, SCI-eligible lead principal.

POLICY AND MANDATE COVERAGE

Legate Solutions LLC · UEI [UEI] · CAGE [CAGE] · nislam@legatesolutions.com · (646) 387-2448 · legatesolutions.com · Principal resumes, clearance verification, and references provided on request.

Experience described reflects work performed by Legate Solutions principals while employed by other organizations. It is provided to show individual qualifications and is not represented as corporate past performance of Legate Solutions LLC or as an endorsement by any agency named. Corporate past performance and references are available where applicable; where no relevant corporate record exists, Legate requests evaluation consistent with FAR 15.305(a)(2)(iv).

EXECUTIVE ORDERS

EO 14409 Advanced AI Innovation & Security (2026) · EO 14179 Removing Barriers to American Leadership in AI (2025) · America's AI Action Plan (2025) · EO 14306 Sustaining Select Cybersecurity Efforts (2025) · EO 14144 Strengthening and Promoting Innovation in the Nation's Cybersecurity (2025) · EO 14028 Improving the Nation's Cybersecurity (2021, as amended)

OMB MEMORANDA

M-25-21 Accelerating Federal Use of AI · M-25-22 Efficient Acquisition of AI · M-26-14 Logging & Network Visibility (rescinds M-21-31) · M-22-09 Federal Zero Trust Strategy · annual FISMA reporting guidance

NIST AND FRAMEWORKS

SP 800-53 Rev. 5 · SP 800-171 · SP 800-207 Zero Trust · Cybersecurity Framework · AI Risk Management Framework (AI RMF) · RMF and cATO · FedRAMP (Rev. 5, 20x) · FISMA · CMMC · MITRE ATT&CK · ISO 27001 · SOC 2

CISA DIRECTIVES AND PROGRAMS

BOD 26-04 Risk-Based Vulnerability Remediation · BOD 23-01 Asset Visibility · Continuous Diagnostics & Mitigation (CDM) · Secure by Design · Deploying AI Systems Securely · agentic AI security guidance

NAICS 541512 Computer Systems Design · 541519 Other Computer Related Services · 541690 Scientific & Technical Consulting · 541611 Management Consulting · 541715 R&D in Engineering **PSC** D310 Cyber Security · D302 Systems Development · R425 Engineering Services

If that is the gap on your team, page two covers how we engage: proposal support, scoped work packages, and named cleared personnel.

WHAT PRIMES ASK US FIRST

How many people can you put on?	Three senior principals today. If the requirement runs bigger than that, we can bring in additional cleared senior people we have worked with before. What we will not do is claim a bench we do not have — we would rather be one focused subcontractor on your team than your whole staffing plan.
Do you have corporate past performance?	Not under the Legate Solutions LLC name yet, and we would rather tell you that up front than bury it. The delivery history sits with our principals. Where the RFP allows it, we ask for a neutral rating and let the key personnel and the technical approach do the work.
Can you take cost-reimbursable work?	Fixed price is usually the easiest path. For T&M, we work under your awarded labor categories at agreed rates. If the requirement needs a DCAA-approved accounting system, flag it early so we can structure the role correctly.
How fast can you support a proposal?	Quickly. We can usually return comments within 24 hours and draft a scoped technical section within three business days once the assignment is clear. Resumes and commitment letters can follow your format.
Will you go around us to the customer?	No. For a named opportunity, we can sign exclusivity and will not market around you or team with a competitor on the same requirement. We are not trying to build a prime business.
What do you cost?	We usually price by work package after a short no-cost scoping call. If you need labor-category ranges for bid shaping, we can typically provide them within 48 hours of RFP release.

WHAT YOU CAN ASSIGN US

OFFERING	DELIVERABLES	WEEKS	COMPLIANCE DRIVER
High-Impact AI Determination and Impact Assessment	Use-case inventory; high-impact determination memo; AI impact assessment; pre-deployment test report; monitoring plan; human oversight, appeal and feedback process design.	4–6	OMB M-25-21 \$4(b), recurring for every new high-impact deployment
AI Guardrail and Assurance Engineering	Grounding and citation enforcement; hallucination, bias and prompt-injection test harness; red-team findings; evaluation baseline; drift monitoring; human validation workflow.	6–8	OMB M-25-21; NIST AI RMF; CISA secure AI and agentic AI guidance
Secure AI Architecture for CUI and Sensitive Data	Walled-garden or air-gapped inference design; private networking and service controls; model/data portability; authorization-aligned architecture and control mapping.	6–10	OMB M-25-22 acquisition terms; FedRAMP; ATO prior to deployment
ATO and FedRAMP Readiness Sprint	NIST SP 800-53 Rev. 5 gap matrix; SSP narratives; POA&M sequencing; 3PAO evidence prep; Rev. 5 transition and key-security-indicator assessment.	6–10	FedRAMP consolidated 2026 rules; Rev. 5 closes to new applications in 2027
Logging and Continuous Event Monitoring Readiness	IT, OT, and IoT asset reconciliation; M-26-14 logging maturity gap analysis; draft agency logging plan; SIEM and pipeline architecture; retention and searchability design.	4–8	OMB M-26-14, with maturity milestones running from late 2026 through 2027
CAASM and Vulnerability Data Reconciliation	EDR, CMDB, cloud and scanner reconciliation; duplicate and identity conflict resolution; coverage metrics; risk-based remediation mapping; executive dashboarding.	4–6	CISA BOD 26-04 risk-based remediation; BOD 23-01; CDM reporting
Endpoint and Virtual Desktop Security Modernization	EDR migration; multi-tenant policy architecture; detection tuning; secure AVD or VMware Horizon design; STRIDE threat modeling; endpoint baseline and coverage assurance.	6–10	Zero trust device pillar (OMB M-22-09); FISMA continuous monitoring
Security Control Validation and STIG Automation	Automated STIG/SCAP scanning; custom audit files and baselines; IaC and container security gates; security-stack health checks; control-validation evidence pipeline.	4–6	NIST SP 800-53 Rev. 5 assessment; DoD STIG compliance; cATO evidence automation

Also available: fractional AI security architect or chief cyber architect support, named cleared key personnel, and no-cost technical volume or orals help on teamed bids.

Pricing: Usually firm-fixed-price after a brief scoping call. Labor-category ranges are available to support bid shaping when needed.

HOW WE CONTRACT

Firm-Fixed-Price Work Package Discrete deliverable, fixed price. No approved accounting system required from us.	T&M Subcontract Negotiated hourly rates against your awarded labor categories.	Key-Personnel Placement Named cleared senior resource with letter of commitment.	Advisory Retainer Set days per month for senior architecture and governance support.
--	--	--	--