

7.#	Section, Page	Solicitation Language	Question	Response
1	Section 6.0		Please confirm the definitive submission deadline for the Phase 1 Solution Brief. Section 6.0 states that submissions are due no later than August 27, 2026 at 1200 EDT, while other references identify September 1, 2026 at 1200 EDT.	Section 6.0 has been updated to show the Phase 1 submission date of 1 September 2026
2	Section 3.0 and 5.1		Section 3.0 states that "Proposers must demonstrate their commercial readiness and ability to execute these performance objectives during a physical, live-site demonstration phase." Section 5.1, Phase 2 states "No oral presentations or physical field deployments are required." Section 6.2 provides instructions for a Phase 2 written brief including a Title Page, Executive Summary, Technical Courses of Actions, and three Attachments – Schedule, Technical Architecture Diagrams, and Total Cost of Ownership. Can the Government please confirm instructions for Phase 2 and whether live-site demonstrations are required?	Section 3.0 has been updated to remove the reference to physical, live-site demonstration phase.
3	Section 6.1 and 7.1		Please confirm the page limits for the Phase 1 and Phase 2 briefings. Section 6.1, paragraph titled "Length" references a length that must not exceed 20 pages for the Technical Discussion and later states the Government will only evaluate the first 10 pages. Section 6.2 is titled "Solution Brief Content Structure" and provides instructions for both Phase 1 and Phase 2. Section 7.1 Gate A references a 20 page limit for the Solutions Brief. Please confirm the page limits for each Phase by section.	Section 6.1 have been update to reflect the twenty (20) page limitation. Section 6.3 and 6.4 have been added to clarify the requirement for Phase 2. Section 7.1 has been updated to clarify Gate Screening.
4	Section 7.1		Please provide instructions for satisfying Gate B: CHMC 2.0 / SPRS Compliance. In which Phase and which section should proposers include proof?	Section 7.1 has been updated to clarify Gate Screening.
5	Section 7.1		Please provide instructions for satisfying Gate C: Prohibited Sourcing Compliance: In which Phase and which section should proposers include certification of compliance?	Section 7.1 has been updated to clarify Gate Screening.
6	Overarching		If the scope is modified by mutual agreement during iterative prototyping, how will changes to milestone dates, deliverables, and completion expectations be documented and communicated to participating offerors?	Any changes to the requirements will be communicated to the iterative prototype awardees.
7	Overarching		Will a Security Clearance be required to perform any of the tasks? If so, what will be the highest level required and what position types will require it?	For the Solicitation and Evaluation Phases (Phase 1 & Phase 2): No Personnel Security Clearances (PCL) or Facility Security Clearances (FCL) (e.g., Secret or Top Secret) are required to participate or submit solutions. However, because the Government-Furnished Information (GFI) transmitted to down-selected offerors in Phase 2 contains Controlled Unclassified Information (CUI), offerors must successfully pass Gate B (CHMC 2.0 Level 2 / SPRS compliance) to receive the GFI and participate in Phase 2. All personnel accessing the CUI GFI must be U.S. citizens. For the Prototype Performance Phase (Post-Award): The baseline performance of this prototype involves the handling of CUI and is not anticipated to require a classified security clearance. Therefore, a DD Form 254 (Contract Security Classification Specification) is not anticipated at the time of award. However, if specific implementation tasks or site-specific Break/Fix/Repair (BFR) modernizations require physical or logical access to classified enclaves, secure command centers, or restricted areas at designated Army Materiel Command (AMC) installations, those specific personnel (e.g., Lead Systems Engineers, On-Site Cybersecurity Integrators) may be required to possess an active Secret security clearance. In such cases, the Government will coordinate and issue site-specific access or a DD Form 254 post-award as necessary.
8	Overarching		Will this effort include the Operations and Maintenance (O&M) for complete lifecycle?	Scope of the Prototype OTA: The primary focus of this prototype effort is the planning, implementation, and validation of the Break/Fix/Repair (BFR) configurations at designated locations during the defined Period of Performance (PoP). It does not automatically guarantee or fund a pre-defined, global lifecycle O&M program. Required Lifecycle & Sustainment Planning: To enable accurate future planning, offerors are required to submit a 5-Year Total Cost of Ownership (TCO) Excel model (Attachment 3) in Phase 2, detailing the cost categories (licensing, software, hardware, and recurring maintenance) required to sustain their proposed solution. Operational Flexibility for Future Support: The requirement for complete lifecycle support, long-term O&M, and sustainment is highly scalable and contingent upon the specific needs of the Army Materiel Command (AMC). It depends entirely on the support required as installations or individual BFR tasks are formally assigned. The Government (the customer) will determine the appropriate level and scope of sustainment support required for any specific effort on a case-by-case basis. If successful, any potential follow-on production contract or transaction under 10 U.S.C. 14022(f) will be structured to allow the Government to dynamically order varying levels of lifecycle and sustainment support based on on-the-ground operational requirements.
9	1.0, page 3		Will we be using existing network infrastructure to secure and monitor OT/FRCS?	Leveraging Existing Infrastructure: Yes, where technically feasible, secure, and operationally viable, the prototype solution shall leverage existing physical network pathways and transport infrastructure to avoid unnecessary and costly "rip-and-replace" of functional network assets. Site-Specific Determinations: The determination to utilize existing network infrastructure versus deploying dedicated physical security boundaries or hardware will be made on a site-by-site (or BFR task-by-task) basis depending on the "as-found" operational environment.
10	Overarching		Is there an expectation to provide training to existing onsite personnel?	Task-Level Operational Hand-off: Yes. For any implemented Break/Fix/Repair (BFR) task, the successful offeror shall provide site-specific hand-off training and basic "over-the-shoulder" instruction to designated onsite Government personnel (e.g., Department of Public Works (DPW) technicians, local Network Enterprise Center (NEC) staff, or facility managers). Training Scope: This training is intended to be practical and operational, focusing on basic daily operations, user access administration, physical/logical security posture maintenance, backup/recovery procedures, and routine troubleshooting of the newly deployed or remediated solutions. As-Built Documentation Delivery: This training must be accompanied by the delivery of "as-built" technical documentation, network architecture configurations, basic system operating manuals, and other applicable documentation. No Formal Enterprise-Wide Curriculum Required: Offerors are not expected to design or deliver a formal, classroom-style global training program or enterprise-wide curriculum under this prototype OTA. Training expectations are strictly limited to localized, task-level hand-offs as individual installations are modernized.
11	Overarching		Will teaming agreements be required during Phase 1 efforts?	Teaming agreements will not be required during Phase 1 efforts. But should be provide if applicable in Phase 2.
12	Submission Instructions Table vs. 6.0		Submission instructions state Briefs are due 9/1/2026 / 6.0 states Phase 1 is due August 27, 2026. Please confirm the correct due date is 9/1/2026.	See the answer to question 1.
13	Section 7.1		Please confirm an acceptable verifiable proof of CHMC or active SPRS score is a screenshot from the SPRS system?	Yes an acceptable verifiable proof of CHMC or active SPRS score is a screenshot from the SPRS system

14	Section 6.0		The cover block directs the email subject line 'Call for Solution - [Your Company Name] - ATEC RIW26_005.' Section 6.0 directs 'Call for Solution - [Your Company Name] - ICED, RIW26_603.' Please confirm the correct subject line string for (a) questions and (b) the Phase 1 submission.	The Q&A response paragraph has been updated to clarify the naming convention. Sectio 6.0 has been updated to clarify the naming convention.
15	Section 3.0 and 7.2		Section 3.0 states offerors must demonstrate performance objectives 'during a physical, live-site demonstration phase,' and Section 7.2 states final selection is based on the written proposal 'and the live-site demonstration performance.' Section 5.1 states that for Phase 2 'no oral presentations or physical field deployments are required.' Please confirm that Phase 2 is a written submission only and that no physical or live-site demonstration will be required at any point prior to award	Section 3.0 and 7.2 has been updated to remove the reference to physical, live-site demonstration phase.
16	Page 9, Section 6.1		The solicitation documents states "Length: The Technical Discussion section must not exceed twenty (20) pages," and "The Government will only evaluate the first ten pages of any technical discussion; content beyond page 10 will be discarded."	See the answer to question 3.
17	Page 9, Section 6.1,		Section 6.1 states the Technical Discussion must not exceed twenty (20) pages, but also that the Government will only evaluate the first ten (10) pages. Could the Government please confirm the page limit for Technical Discussion section is 20 pages?	See the answer to question 3.
18	Page 9, Section 6.1 / Page 11, Section 6.2		Page 9 of the solicitation states "Cost and Total Cost of Ownership (TCO) estimates must be provided in Microsoft Excel (.xlsx)," and on page 11, The list of Phase 1 submission contents does not include a TCO estimate, but the list of Phase 2 contents explicitly requires it as "Attachment 3 - Total Cost of Ownership (TCO)." The formatting instructions for Phase 1 in Section 6.1 mention a TCO estimate, but the content requirements for Phase 1 do not. The TCO is explicitly required in Phase 2. Could the Government please clarify if a TCO estimate is required with the Phase 1 submission? If so, what level of detail is expected?	No TCO is required with the Phase 1 submission. The estimate should provide a breakdown of cost categories, detailing licensing, software, hardware, recurring maintenance costs and their basis of estimate.
19	Overall		Can an offeror include anticipated teammates in Phase 2 that are not mentioned in Phase 1?	Yes n offeror include anticipated teammates in Phase 2 that are not mentioned in Phase I
20	Section 6.0		When is the Phase 1 proposal due? Table states 1 Sept 1200 EDT, but Section 6 states 27 Aug 1200 EDT	See the answer to question 1.
21	Page 9, Section 6.1,		Section 6.1 states Length to be no more than 20 pages, but later states that "content beyond 10 pages will be ignored". Is this a typo? Will 20 pages or 10 pages be considered?	See the answer to question 3.
22			Are Service Levels to be defined later? Or, negotiated per event?	High-Level Framework in Base Agreement: The baseline Model Agreement will establish a high-level framework for Service Levels, categorizing task and system urgency (e.g., Critical, Urgent, Routine) with corresponding standardized physical and logical response window targets. Negotiated and Defined Per Event: The specific, binding Service Level Agreements (SLAs)—including exact operational response times, physical remediation on-site arrival targets, backup-recovery parameters, and system uptime metrics—will be negotiated and defined on a per-event or task-by-task basis as individual installations or Break/Fix/Repair (BFR) tasks are formally assigned. Customer-Driven Criticality Scalability: This hybrid model allows the Government (the customer) to dynamically scale operational service levels and cost parameters depending on the specific mission criticality of the target system (e.g., a critical utility grid or manufacturing line at an Organic Industrial Base vs. an auxiliary administrative building sensor).
23			Funding profile, FFP or CP or T&M?	The Funding profile will be CPFF.
24			In Section 3.0 in the table for Telemetry & Data Integration Remediation it speaks to "authorized repositories". What will be considered an "authorized repository"? Will the Offeror need to provide a plan to provide these repositories or will these be pre-established sites the team will be directed to use?	Government-Furnished Baseline: Yes, the Government will direct the successful offeror to utilize pre-established, Government-furnished authorized repositories, databases, or enterprise data lakes. The offeror is not required to host or provide these database or storage platforms.
25			Is there a NOC/SOC service expected? Or, just a Help Desk ticket input service?	No Independent NOC/SOC Required: There is no requirement or expectation for the successful offeror to establish, operate, or maintain a Network Operations Center (NOC) or Security Operations Center (SOC). Integration with Existing Government Security Centers: Enterprise-level security and network monitoring remain the responsibility of the Government (e.g., Regional Cyber Centers (RCCs), local Network Enterprise Centers (NECs), and authorized Cyber Security Service Providers (CSSPs)). On-Demand Ticket & Dispatch Service: Post-award support is focused on an on-demand, event-driven Break/Fix/Repair (BFR) model. The contractor shall provide a Help Desk or ticket input service to receive, track, prioritize, and log technical discrepancy reports from authorized Government representatives. The contractor will utilize this ticket intake to coordinate and dispatch resources for remote troubleshooting or physical, on-site remediation as required.
26			In section 6.1 TCO is requested in phase 1, in section 6.2 TCO is requested for Phase 2. Will a TCO need to be provided for each phase and a detailed cost proposal in phase 3? Or is a TCO only needed for Phase 1?	See the answer to question 18
27	Header table / Section 6.0	Header table: "Solution Briefs due date/time" = September 1, 2026, 1200 EDT. Section 6.0: "Offerors must submit their Phase 1 package via email to the Agreements Officer and Specialist listed in the header block no later than August 27, 2026, at 1200 EDT."	Can the government please confirm the controlling due date/time for the Phase 1 Solution Brief submission is September 1, 2026, 1200 EDT?	See the answer to question 1.
28	Header table / Section 6.0	Header: "Call for Solution - [Your Company Name] - ATEC RIW26_005" (Example: Call for Solution - ABC Corp ATEC, RIW26_005). Section 6.0: "The email subject line must strictly read: Call for Solution - [Your Company Name] - ICED, RIW26_603."	Can the government please confirm the correct solicitation/call reference number to use in submission subject lines: ATEC RIW26_005 or ICED, RIW26_603?	See the answer to question 14.
29	Section 6.1	Section 6.1: "The Technical Discussion section must not exceed twenty (20) pages. Title pages, table of contents, and disclosures do not count against this limit. The Government will only evaluate the first ten pages of any technical discussion; content beyond page 10 will be discarded."	Can the Government confirm whether white paper submissions in Phase 1 shouldn't exceed 10 or 20 pages?	See the answer to question 3.
30	Section 3.0 / Section 5.1	Section 3.0: "Proposers must demonstrate their commercial readiness and ability to execute these performance objectives during a physical, live-site demonstration phase." Section 5.1: "No oral presentations or physical field deployments are required."	Can the government please clarify the expectations for Phase 2 and reconcile the "physical, live-site demonstration" language in Section 3.0 with the Section 5.1 statement that no oral presentations or physical field deployments are required?	See the answer to question 2.
31	Section 6.1 & 6.2	Section 6.1 "Format: Microsoft Word (.docx) file, Cost and Total Cost of Ownership (TCO) estimates must be provided in Microsoft Excel (.xlsx)." Section 6.2 "At a minimum, the Phase 2 Demonstrate Technical Courses of Actions must include the following sections: Attachment 3 - Total Cost of Ownership (TCO): The Offeror shall provide an estimate of the Government's total cost of ownership (TCO) for the proposed solution over the next five (5) fiscal years."	Section 6.1 and Gate A (Section 7.1) require a TCO in Microsoft Excel format as part of Phase 1, and Gate A ties pass/fail to its submission. However, the Phase 1 content structure in Section 6.2 does not list a TCO as a required deliverable — it appears only as Attachment 3 (which was not included with the solicitation) under Phase 2. Is a TCO required at Phase 1, or only at Phase 2?	See the answer to question 18
32	Section 6.1 & 6.2	Section 6.2, Attachment 3: "The Offeror shall provide an estimate of the Government's total cost of ownership (TCO) for the proposed solution over the next five (5) fiscal years. The estimate should provide a breakdown of cost categories, detailing licensing, software, hardware, recurring maintenance costs and their basis of estimate."	Can the government please provide an updated TCO Excel file? The Excel attached to the solicitation appears to be a list of geographic sites as opposed to the TCO template.	The Offeror is to provide their own Attachment 3.

33	Section 7.1, Gate A	Section 7.1, Gate A Submission formatting and completeness: Pass: The Solution Brief (White Paper) is submitted as a Microsoft Word file (.docx) and the TCO is submitted as a Microsoft Excel file (.xlsx) with active formulas intact. The Solutions Brief utilizes Arial or Times New Roman 11pt or 12pt font with 1-inch margins (headers and footers may be outside margins). The Solutions Brief does not exceed the twenty (20) page limit excluding diagrams. The submission includes clear, comprehensive details that support an initial compliance review with all required criteria (section 2 and 3); no essential elements are missing or unclear. Fail: The Solutions Brief exceeds the twenty (20) page limit. The submission is not provided in the specified file format or does not adhere to the required font and margin specifications. The submission is missing detail or clarity to determine compliance with basic mandatory requirements; key elements are missing, incomplete, or ambiguous.	Can the government please confirm whether diagrams / figures are excluded from the page count for both the 20-page limit and any 10-page evaluation cutoff?	Diagrams / figures are excluded from the 20 page page count
34	Section 5.2	Phase 2 submissions will be evaluated. The Source Selection Authority (SSA) reviews and signs the Selection Memo.	Milestone 5 (Final Evaluation & Selection) has a target completion of September 18, 2026. Milestone 6 (Negotiations & Award) is listed as a 5-day duration but shows a target completion of September 25, 2026 – a 7-day span rather than 5. Please confirm the correct duration or target date for Negotiations & Award.	Section 5.2 Milestone 6 duration has been corrected to 7 days.
35	N/A	The deadline to submit questions for Phase 1 is 19 August 2026 at 1500 EDT.	Given the compressed 15-day Phase 1 window and the inconsistencies noted above in previous questions, when will the Government provide a solicitation amendment incorporating the answers to these questions?	Responses and revised ICED-603 Call for Solutions Enterprise OT/ICS/FRCS Modernization Rev01 are provided before 20 August 2026.
36	Section 3.0		Regarding full-lifecycle approach to cyber resilience for Operational Technology (OT), should offerors assume integration with existing Army enterprise network (domain joined) or assume closed-restricted and stand-alone networks. Is the authorization boundary at the enterprise level or site/system level?	Assumed Network Posture (Closed-Restricted/Enclave). Offerors should assume that OT/ICS/FRCS networks are operated as closed-restricted, enclave-isolated, or stand-alone networks. They are not to be domain-joined to the standard, administrative Army enterprise IT network (e.g., NIPRNet Active Directory). However, secure egress telemetry pathways (such as through firewall-restricted demilitarized zones or secure gateways) will be established to forward system health and monitoring data to authorized enterprise repositories as directed. Site-Level Authorization Boundary: The Risk Management Framework (RMF) authorization boundary is established at the site or system level (e.g., local utility plant SCADA boundary or building/facility-control enclave boundary), not as a single global enterprise boundary.
37	Section 7.3		The CIS identifies interoperability with legacy protocols such as Modbus, BACnet, and LonWorks while minimizing unnecessary physical hardware replacement. Does the Government have a preferred approach for normalizing and integrating legacy protocols, or is the Government seeking offeror-proposed approaches provided the solution remains vendor-agnostic and satisfies cybersecurity requirements?	Offeror-Proposed Approaches: The Government does not mandate or prescribe a single preferred technical mechanism, brand, or approach for protocol normalization and integration. Offerors shall propose and justify their engineering approaches to ingest legacy field protocols and securely translate them to meet the open standards and cybersecurity requirements defined in the CIS.
38	Section 6.1	Evaluated Page Count	Section 6.1 states: Length: The Technical Discussion section must not exceed twenty (20) pages. Title pages, table of contents, and disclosures do not count against this limit. The Government will only evaluate the first ten pages of any technical discussion; content beyond page 10 will be discarded. Question: There appears to be a conflict between Technical Discussion section page count and evaluated page count, please clarify page count.	See the answer to question 3.
39	Section 6.1	Solution Brief Submission Requirements (Phase 1)	Section 6.1, under Format, states "Cost and Total Cost of Ownership (TCO) estimates must be provided in Microsoft Excel (.xlsx)". However, according to Section 6.2 Solution Brief Content Structure, cost estimates are part of Phase 2, not Phase 1. Question: Would the government confirm that cost estimates are NOT to be submitted as part of the Phase 1 Solution Brief.	See the answer to question 18
40	Sections 5.2 & 6.0	Due Date	Section 5.2 refers to a 15 day response window with a completion date of September 1, 2026. Section 6.0 states: Offerors must submit their Phase 1 package via email to the Agreements Officer and Specialist listed in the header block no later than August 27, 2026, at 1200 EDT. Question: Would the government clarify the due date?	See the answer to question 1.
41	Section 3.0	Telemetry & Data Integration	Does the Government envision a single enterprise supervisory platform, or is interoperability between multiple existing platforms considered acceptable provided enterprise visibility is achieved?	Interoperability and Multi-Platform Acceptability: The Government does not mandate or require a single, proprietary enterprise-wide supervisory platform. Interoperability between multiple existing, legacy, or newly modernized platforms is fully acceptable, provided that normalized enterprise-level visibility, secure telemetry data flow, and consolidated monitoring are successfully achieved.
42	Section 3.0	Cybersecurity & Resilience	Is there a minimum Level where data should be encrypted or secured? I.e. Level 0, 1, 2, 3, 4	Encryption in Transit (Level 2 and Above): Yes. Secure, encrypted transport (utilizing government-approved cryptographic standards such as AES 256 or TLS 1.3) is expected for all data in transit starting at Level 2 (Supervisory Control) and above. Encryption is a mandatory requirement for any telemetry or management data traversing network segments between local site enclaves and the enterprise repositories (Level 3 to Level 4). Level 0 / Level 1 Encryption Constraints (Legacy Reality): The Government recognizes that legacy, operational field devices at Level 0 (sensors/actuators) and Level 1 (PLCs, RTUs, DDC controllers) frequently utilize legacy serial or unencrypted IP protocols (e.g., standard Modbus RTU/TCP or BACnet MS/TP) that cannot natively support cryptographic encryption or signatures. There is no requirement to force native, device-level encryption at Level 0 or Level 1 where legacy hardware constraints prevent it. Boundary Protection Requirement: Where Level 0 or Level 1 devices cannot natively secure or encrypt their data, the proposed solution should implement secure physical or logical boundary protections as close to the Level 1 boundary as technically feasible. Site-Specific Implementation Variability: The exact implementation of encryption and boundary protection controls is highly site-specific and contingent on the unique physical, hardware, and firmware capabilities of the target environments assigned under each individual Break/Fix/Repair (BFR) task. The Government expects the contractor to dynamically adapt encryption and boundary protection strategies to match the technical and fiscal realities of each unique installation, rather than proposing a rigid, one-size-fits-all model.
43	Section 3.0	Unified Control System Integration	Can the solution have GovCloud components or will it be restricted to only the Army's network and servers?	On-Premise Baseline Priority (Core Prototype Solution): The primary prototype solution shall be architected as a local, on-premise, or enclave-isolated solution utilizing the Army's physical networks and any applicable garrison servers. It should be capable of fully executing all Break/Fix/Repair (BFR) remediation and monitoring capabilities without assuming active cloud connectivity. This is to ensure alignment with current AMC boundaries and prevent execution delays. GovCloud Permissible ONLY as a Separate, Optional COA: The Government is open to evaluating GovCloud integration (e.g., DoD Impact Level 4/5 or cArmy) as a separate, optional Course of Action (COA) within the Phase 2 submission.
44		General IT	Is solution allowed to have control of network segmentation or will NEC provide all of those functions?	Government Control and Management: The contractor's solution is not authorized to independently manage, configure, or control any portion of the Army's network infrastructure, whether physical or logical. All network administrative control, logical segmentation enforcement, and firewall/routing policy management remain the sole responsibility of the Government (e.g., the local Network Enterprise Center (NEC) or the target environment's Government owner). Contractor Support Role: The contractor's role is to provide, engineer, and deliver the technical capability and recommend configuration policies and rulesets. All proposed logical segmentation rules, virtual boundaries, and gateway policies must be submitted to the Government network authorities for review, approval, and execution. No Direct Modification of Network Assets: Under no circumstances shall the contractor have direct administrative or configuration write-access to core NEC-owned switches, routers, firewalls, or logical overlay controllers. Any required physical port assignments, VLAN configurations, or routing policy changes must be submitted as technical requests to the NEC or authorized Government network engineers for implementation.
45	Section 3.0	Cybersecurity & Resilience	How does the Government define success for identity-based microsegmentation in OT environments?	Government Response: Offeror-Proposed Success Framework: The Government does not prescribe or pre-determine the specific technical metrics, testing protocols, or validation formulas used to define success for identity-based microsegmentation. Offerors are expected to propose their own success validation and measurement plan within their Phase 1 and Phase 2 Technical solution or Courses of Action (COAs).
46	Section 3.0	Cybersecurity & Resilience	What security categorization levels apply to the majority of OT/ICS/FRCS environments?	Standard DoD Baseline (CNSSI 1253 / UFC 4-010-06): In accordance with CNSSI 1253 and UFC 4-010-06 (Cybersecurity of Facility-Related Control Systems), the baseline security categorization for the majority of standard Army OT/ICS/FRCS environments is established as Low Confidentiality, Moderate Integrity, and Moderate Availability (L-M-M). Site-Specific and Mission-Critical Variability: While L-M-M represents the typical baseline, security categorizations are site-specific and contingent on the mission-criticality of the local target environment.

47		Niagara as a Unified Integration Layer:	Would the Government view a vendor-neutral middleware approach, such as Niagara Framework functioning as the enterprise integration layer across multiple legacy systems, as meeting the intent of vendor-agnostic integration?	No Brand Pre-Approval: The Government does not endorse or pre-approve specific commercial brand-name products, proprietary middleware frameworks, or software suites.
48		Preservation of Existing Investments	To what extent does the Government prioritize preservation of existing BAS/SCADA investments versus replacement with solutions?	Proposed Solutions: It is the offeror's responsibility to propose and justify the their solution and approach for a given site, balancing the preservation of existing operational infrastructure with the need to achieve the security and interoperability requirements defined in the CIS.
49		Legacy Protocol Integration	Can the Government provide an estimated breakdown of installed protocols across representative AMC facilities, including BACnet/IP, BACnet MS/TP, Modbus TCP, Modbus RTU, LonWorks, OPC, DNP3, SNMP, OPC-UA, and proprietary protocols?	No Centralized Protocol Inventory: Due to the decentralized and varied developmental history of legacy systems across Army Materiel Command (AMC) garrisons, the Government does not possess a centralized, exhaustive, or guaranteed statistical percentage breakdown of installed protocols. Break/Fix/Repair (BFR): Performing physical and logical discovery of deviating "as-found" site networks and protocols is the responsibility of the successful offeror.
50		Legacy Protocol Integration	Given the large installed base of legacy LonWorks systems throughout Federal facilities, should responders assume LonWorks integration remains a mandatory capability?	Technical Capability: LonWorks is identified in the CIS as a legacy protocol on the ground. The technical capability to ingest, normalize, and secure legacy protocol traffic is a requirement of the overall proposed solution. However, the physical deployment of this is determine by the site-specific requirements and GFI or possibly as an "as-found" of the target environment of an assigned Break/Fix/Repair (BFR) task.
51		Enterprise Data Integration	What, if any, enterprise data repositories being considered for normalized data streams and site-to-site comparisons?	The specific enterprise data repositories are To Be Determined (TBD). However, the proposed solution must be capable of transmitting normalized data streams to Government-designated endpoint(s) using standard, open APIs and transport protocols.
52		Enterprise Data Integration	Does the Government anticipate implementation of a common tagging strategy, such as Haystack, Brick Schema, Niagara tagging, or another standard to normalize enterprise telemetry?	No Prescribed Tagging Standard: The Government does not prescribe a specific commercial semantic modeling standard as the exclusive enterprise solution at this time. However, to satisfy the telemetry normalization requirements of the CIS the proposed solution shall utilize a standardized, fully documented, and open metadata tagging or semantic schema.
53		Cybersecurity & Resilience	How does the Government define success for identity-based microsegmentation in OT environments?	See Q&A #45