



## Request for Information (RFI) - Installation Operations Tool (IOT)

### RFI #001A

### Questions and Answers

1. Will there be a draft RFP so we have a chance to review the terms and conditions prior to the final RFP?
  - a. No, the RFP will only be available for review once it is released.
2. Who would own the IP? US Ignite or Fort Moore? That's a big legal question as it looks like US Ignite is acting as a SETA contractor for the Army.
  - a. US Ignite would own the IP, and has granted ERDC a royalty-free, non-exclusive, worldwide, irrevocable license to the deliverables.
3. What's driving the schedule? This seems very aggressive and doesn't reflect a normal application development (depending on the design and total number of systems, the dashboards could take months, system integration/data integration could take months for automated data access) and it doesn't look like test and validation are on the schedule. Data architecture and design seem to be missing as well.
  - a. The schedule is motivated by the desire to demonstrate the value of the IOT capability before future programming decisions about the capability need to be made.
  - b. The project team recognizes the level of ambition of the schedule. To minimize schedule risk, the project team anticipates minimizing the scope necessary during the initial configuration/demonstration phase, and encourages vendors to consider capabilities that require as little new development or customization as possible to demonstrate functionality.
  - c. Below are the windows in the schedule shown in the '*Integrated Master Plan/Schedule Delivery*' section of Addendum A corresponding to each of the project phases described in this question.
    - i. Dashboarding, system integration and data integration - 6/21-8/9
    - ii. Test and validation - this can be considered during the installation/integration period from 9/9/24-12/9/24
    - iii. Data architecture/design - 5/10/24-6/20/24
4. Are they looking for custom app dev or integrated COTS solutions?
  - a. The project team is looking for mature, maintainable (e.g. COTS, GOTS) cost effective solutions.
5. Will the selected vendor have an opportunity to validate the use cases/design requirements?
  - a. Unless the anticipated RFP structure changes, yes. The first 1.5 months of the first post-award phase are reserved for discovery and design, to include validation of the list of use cases and design considerations previously developed by the project team. Although subject to change, the project team anticipates providing the IOT vendor(s) flexibility in the use case(s) satisfied during the initial configuration/ demonstration phase of the project.
6. Who's driving user acceptance testing and what's the acceptance criteria?
  - a. As the client for the IOT vendor, US Ignite will serve as the final authority for user acceptance testing, with input from ERDC and FMGA.



- b. Criteria for selection of an IOT vendor(s) are expected to be those below
    - i. Value - Price for assessed quality of capabilities provided
    - ii. Experience - Demonstrated experience delivering capabilities similar to those required under IOT
    - iii. Schedule - Ability to demonstrate a functional capability within the schedule required, as evaluated by the level of new development or configuration proposed.
    - iv. Capability - Assessed evaluation of the requirements met and benefits provided by the proposed demonstration capability.
  - c. Criteria for acceptance of the initial configuration/demonstration phase are anticipated to be those below.
    - i. Ability for the demonstrated capability to satisfy one or more use cases developed by the project team, which are expected to be articulated in the RFP.
    - ii. Ability for the demonstrated capability to meet a minimum set of functional and technical requirements to be articulated in the RFP.
  - d. Criteria for acceptance to proceed to phase 2 'operational capability delivery' are anticipated to be those below.
    - i. Determination of whether the budget in the proposal developed during phase 1 is within the budget available for phase 2, which is anticipated to be defined within the upcoming solicitation.
    - ii. Value - price for assessed quality of deliverables proposed for phase 2
    - iii. Schedule - demonstrated ability to deliver the scope in the proposal developed during phase 1, in the schedule available for phase 2
    - iv. Capability - Assessed evaluation of the requirements met and benefits provided by the capability defined in the proposal developed during phase 1.
  - e. Criteria for acceptance of the operational capability are anticipated to be defined by the scope, schedule, and budget defined in the proposal developed during phase 1.
7. What's the level of documentation expected?
- a. The levels of documentation expected at the end of each phase in the project are provided below.
    - i. RFI responses - there are no mandatory requirements for documentation provided in response to this RFI. This flexibility is provided to reduce the barrier to entry for vendors to respond to the RFI. See section 5 'Response Content Guidance' of the RFI for documentation that would be beneficial to submit in response to the RFI.
    - ii. RFP submissions - the submission requirements are anticipated to include the below.
      - 1. Work Breakdown Structure (WBS), minimally at level 2
      - 2. Integrated Master Schedule
      - 3. System architecture diagram
      - 4. Anticipated hardware and software list, with flexibility
      - 5. Fixed price cost proposal for phase 1
      - 6. Minimum capability delivered during phase 1



- iii. Initial configuration/demonstration phase
    1. Process flow of use case(s) enabled by the demonstrated capability, with development support from US Ignite
    2. Network architecture diagram for demonstration configuration
    3. System architecture diagram for demonstration configuration
    4. Hardware and software list in demonstration configuration
    5. API documentation (OpenAPI specification or similar), interface design document, or similar for interfaces exposed from IOT
    6. Proposal for phase 2, anticipated to include similar artifacts as those required by the RFP.
  - iv. Operational capability phase
    1. Phase 1 artifacts, updated to include the configuration of the operational capability developed during phase 2.
    2. Source code for operational capabilities.
8. Is system training required/expected?
    - a. Informal system training reviewing functionality and use, with recording for future use, will be required during phase 1. Formal training may be required in phase 2.
  9. Who's driving the change management process?
    - a. For assets managed by the Fort Moore, GA Network Enterprise Center (FMGA NEC), the FMGA NEC will facilitate the change management process with approval from the South East Region Network Enterprise Center. For all assets deployed at Fort Moore, GA, the FMGA S6 and system owners will participate in the change management process. US Ignite anticipates that assets managed by the FMGA Network Enterprise Center (NEC) will be managed by the NEC, but will confirm prior to releasing the RFP.
    - b. For assets managed within the VTIME environment, USACE-ERDC will facilitate the change management process.
  10. What type of contract are they planning to release? FFP, T&M?
    - a. US Ignite plans to award a Firm Fixed Price (FFP) contract if a vendor(s) is selected under the anticipated RFP.
  11. What network and/or location will the pre-authorized IOT (Installation Operations Tool) need to be deployed at?
    - a. The project team anticipates providing flexibility in the network for the pre-authorized IOT to be deployed in, to be defined during the design period of the demonstration phase.
    - b. US Ignite anticipates that dark fiber and conduit will be made available at the NEC data center, along with the locations of assets to be integrated with as available on base. US Ignite will confirm this prior to releasing the RFP.
    - c. The pre-authorized IOT will be permitted to network between local and cloud environments through commercial or private cellular networking, as required by the vendor's proposed solution.
    - d. A network access point is anticipated to be made available to the Research and Development Environment (RDE) network, with access to the Virtual Toolbox for Installation Mission Effectiveness (VTIME) environment deployed in Azure Government Cloud, although this is not guaranteed.



- e. The project team anticipates a vendor cloud-based solution to be the most rapidly networkable solution, although a required network or location will not be imposed.
12. Will this network already have direct access to AWS GovCloud or other DoD approved cloud providers?
- a. Per point d in the response to question 11 above, a network access point may be made available to the Azure Government Cloud hosting VTIME, although this is not guaranteed.
13. Are there existing Army ATO's that the IOT can inherit controls from to, or will the RMF process start from scratch?
- a. The project team may need this question to be re-framed, in order to provide the right response.
  - b. The project team expects that the IOT capability would inherit controls in place within the capability proposed by the IOT vendor.
  - c. If the IOT capability is deployed within the authorization boundary of VTIME in a subsequent project it may then inherit controls from VTIME, although that is not anticipated under the scope of this project.
  - d. If the IOT is deployed into an operational DoDIN network like the Installation Campus Area Network (ICAN), it would likely inherit controls from that network.
14. Similarly, are there existing authorized systems that will need an interconnect for the IOT to function as intended?
- a. The list of potential systems for the IOT vendor to propose interconnecting with, including authorization status of each system, is anticipated to be provided as an addendum to the forthcoming solicitation.
15. Does the Army already have an existing Secure Networking architecture that is already ATO'ed?
- a. The project team may need this question to be re-framed, in order to provide the right response.
  - b. The Fort Moore Installation Campus Area Network (ICAN) is ATO'ed network.
  - c. The DoD cybersecurity reference architecture can be found [here](#).
16. What are the existing COPs in use at an Army installation that the IOT would integrate? Is there a preference for one COP or dashboard tool over another?
- a. The full list of information systems in use at Fort Moore is anticipated to be released as part of the upcoming solicitation.
  - b. Some personnel consider the following as COPs, though these are largely more domain-centered than the Garrison-level COP requested; Hexagon CAD; WebEOC; PSIF; various UMCS e.g. Niagara; the AMC Knowledge Management Portal (AKMP)
17. Are the EIS and IIS systems well understood and documented in terms of process/policies to gain access?
- a. The IIS systems that will be viable to gain access to during the demonstration period of the project will be well understood, with documentation anticipated to be available on both network, API, and authorization access concerns.
  - b. The EIS systems to be accessed either during the operational period or in a subsequent project are notionally understood and some will have data samples made available through Army Vantage, but the process/policies for accessing



these systems will need to be developed as part of the operational period or post-operational period roadmap to be developed.

18. Are the EIS and IIS systems modernized and well documented in terms of API interfaces?
  - a. Given the volume of EIS used at Fort Moore the level of modernization that can be expected to be available for each has not been thoroughly evaluated.
  - b. There is at least one IIS that is anticipated to have API interfaces created in support of this project, in advance of an IOT vendor(s) being awarded. Additionally, there are multiple IIS that are already modernized, with thorough API documentation.
19. Is there existing documentation of which data is a priority for which of the end users at Ft. Moore and their corresponding use cases?
  - a. This has not yet been documented. US Ignite will make efforts to collect this information prior to awarding a contract to an IOT vendor(s).
20. Why is FedRAMP medium a requirement as well as an ATO?
  - a. Either FedRAMP medium or ATO may be required, depending on the architecture of the proposed solution. In its end state an edge component of the IOT capability would be beneficial, which is expected to require ATO. If, however, a purely cloud solution is proposed in the time available, FedRAMP medium would likely be sufficient.
21. Who are the self-service data lake users?
  - a. There are two classes of expected self-service data lake users - installation business units that require visibility to data in information systems they've not previously had access to, to improve their processes; along with developers of future capabilities enabled by access to the data lake.
22. How are you normalizing data, assuming that each facility has its own data schema? It is our experience that data from individual critical infrastructure systems does not apply to any standard data model.
  - a. The normalization approach will need to be defined by the IOT vendor(s).
23. Is a partial RFI response to only specific areas that the responders' products can deliver relevant & compliant capabilities a valid response? In other words, can responses address only certain portions of the RFI relevant to the responder's technology offerings or must they address each element of the RFI?
  - a. Yes, we encourage responders to articulate which portions of the RFI are relevant to the responders' technology offerings. Indicating which requirements have technologies readily available to meet them will help the project team understand which requirements may be impractical given the schedule and budget available for the project.
  - b. Responders' capabilities are not required to be able to address all requirements in the RFI.
24. Is there a standard DoD base CI/CD tooling, processes and procedures to manage both the development, testing and deployment of base level platforms? Does it address the full lifecycle maintenance process for either release or problem repairs to the systems that will be integrated with the Installation Operations Tool (IOT)?
  - a. The answer to the above parent question is provided below, while the answers to the sub-questions below are addressed in each subsequent sub-bullet.



- i. For information security purposes, the configuration management and CI/CD tooling used by the Fort Moore Network Enterprise Center (NEC) to manage the lifecycle of base information systems will not be released until an IOT vendor(s) has been awarded. Collectively, the tools used by the NEC address the full lifecycle maintenance process for base systems that the IOT will integrate with.
    - b. Is there a standard CI/CD Orchestrator that must be incorporated into the Installation Operations Tool deployment into production?
      - i. No, the IOT vendor will have flexibility in choosing the CI/CD orchestrator and associated tools they're experienced using to manage the DevOps lifecycle of their system.
      - ii. Vendors are not likely to be able to expect CI/CD deployment support within the ERDC RDE and VTIME environments. Vendors may be able to use Army CREATE or PlatformOne.
    - c. Is there a current deployment manager that can support container code deployments, virtual machines and multiple OS environments (Linux, Android, Apple IOS, Windows, etc.) or does one need to be supplied?
      - i. The Fort Moore Network Enterprise Center is anticipated to be able to support these deployment and resource provisioning actions for information systems it manages, though this will be confirmed prior to releasing the RFP. However, the IOT vendor(s) will be responsible for such actions as they relate to the IOT capability.
25. Support of the OSD Advana Edge platform is identified as an example GOTS to include in the Installation Operations Tool (IOT) but is that a requirement? If a requirement specifically to include, who will be responsible to support these GOTS components and their inclusion with the Installation Operations Tool?
  - a. <https://www.acq.osd.mil/asda/ae/ada/data-analytics.html>
  - b. OSD Advana Edge is not strictly a requirement, it is merely a potential solution responders may consider as part of their proposed capability. If personnel have CAC access and can access Ironbank, they may be able to use similar pre-hardened libraries as those available within Advana Edge.
26. VTIME is identified as a specific system to integrate with, but the RFI also requires the solution needs to be capable of mission critical functions being able to operate in a disconnected state on-premises. Since VTIME is currently a centrally platform running at an ERDC site, is it planned to be provided as an on-premise platform that can provide central dashboard and digital twin capabilities for operational inclusion into a base level dashboard as well as the dashboard-of-dashboards operational readiness view?
  - a. The answer to this parent question is provided below, in advance of addressing the additional sub-questions in points b and c.
    - i. Given VTIME's current deployment at both the ERDC site and Azure Government cloud, and given the schedule available for the IOT project, it is not anticipated to be a strict requirement for the demonstration IOT capability to integrate with VTIME.
    - ii. The demonstration capability is anticipated to be a base-level (Fort Moore-specific) dashboard-of-dashboards with operational readiness view, which may be deployed either on-premise or in a commercial or



- government cloud.
  - b. VTIME was to present a consolidated view across DoD so is it expected to provide the dashboard-of-dashboards or a view only into the Installation Operations Tool?
    - i. Army Vantage and OSD Advana are current Data Platforms applicable across DoD. Final VTIME requirements are not yet available. The Installation Operations Tool is focused at the installation level, and can inform the requirements for an edge, on-base capability to address installation-level decision making.
  - c. Is an alternative on-premises VTIME functionality inclusion that can still transmit relevant information to a central VTIME when available a positive extension to the architecture solution response?
    - i. Deploying an on-premise dashboard-of-dashboard functionality with the ability to transmit information to a central VTIME when available would be a positive extension of the architecture solution response.
27. The architecture description is a combination of on-premises and hybrid cloud availability with a unified user access control to accessing data and networking resources. The description doesn't describe any edge computing functionality which brings the value of movement of computing closer to data generation and both timely analysis and identification and only transmission of relevant and that data to be externalized for better Readiness visibility and necessary immediate actions.
- a. Is the inclusion and value of edge computing solutions in the overall architecture a positive extension to the architecture response?
    - i. The inclusion and value of edge computing solutions in the overall architecture is a positive extension to the architecture response.
    - ii. The anticipated benefits of moving the computing to the edge/closer to data generation are below
      - 1. Be able to maintain critical operations in the event of a disconnection to external network availability.
      - 2. Reduce costs associated with over-the-air data transmission costs, and cloud storage costs for non-reporting data
28. Zero Trust Network Access (ZTNA) architecture seems to be following the NIST standard but doesn't explicitly state the NIST SP 800-207 Zero Trust Architecture
- a. Is the Zero Trust solution proposal limited to the described architecture or will a more secure solution proposal be accepted for review in the RFI solution response?
    - i. The Zero Trust solution proposal is not limited to the described architecture, and a more secure solution proposal will be accepted for review.
  - b. Should an assumption be made that Zero Trust must be able to support containerized code that when executing on a cluster and new instances are spun up can support an embedded Zero Trust activation, authentication & authorization with the containerized instance of the software?
    - i. Such an implementation would be beneficial, but is not anticipated to be strictly required.
29. The RFI is focused on data brokering/mesh to be able to connect to, transmit, and receive



data from various information systems. The focus of the requirements is on connectors for the data flows while including a Zero Trust to securely network these connections and data flows. The Zero Trust seems to be only outbound in its protection.

- a. Is a solution that allows the data to remain resident at the generation point that can be securely (encrypted) connected to by only pre-authorized systems (external or local) or individuals an accepted RFI solution response?
  - i. Yes. The RFI is not intended to impose a particular Zero Trust design, and vendors are encouraged to propose recommended designs, including those that are more than just outbound in their protection.
30. Is there an assumption that the proposed RFI solution brings the necessary SDKs for future customization and functionality that can be used by DoD directly with their integration with any standard DoD base CI/CD processes and procedures?
  - a. Providing an SDK to support future customization and functionality for use by DoD directly would be beneficial, but is not strictly required.
31. Are there any technologies, portlets/widgets/etc, not to be used in the dashboard-of-dashboards implementation?
  - a. Technologies to be used in the dashboard-of-dashboards implementation must be compliant with the National Defense Authorization Act (NDAA), which provides provisions for articulating prohibited technologies.
32. If customization work for a base platform must be done to expose data required for the Installation Operations Tool is defined, will the owning platform team be responsible to both develop and support that integration for sustained availability of the data access or interactions to the system?
  - a. Yes. In advance of the anticipated award of an IOT vendor(s), US Ignite anticipates securing integration support relationships with the system owners for several installation platforms/information systems.
  - b. The FMGA S6 will help foster relationships with system owners, vendors, and US Ignite across the project.
33. We license our solutions based on user count. This is solely the number of employees that would need to be covered by the solution. Can you provide an approximate user count?
  - a. We anticipate there being multiple 'phases' of the Installation Operation Tool's maturity, with each phase having different estimated user counts below.
    - i. At initial demonstration of a single business capability, we expect 5-20 users.
    - ii. Once we reach complete coverage of one installation, we anticipate 100-1000 users.
    - iii. If this becomes an installations enterprise capability, we may have as many as 1000-5000 users.
  - b. We would be interested in the licensing considerations at each of these scales, to inform our growth strategy for the capability.
34. Question 10 (below) is asking for a ROM on schedule and cost for the full scope. Could you share the details of the full scope? Without scope details we are unable to provide the ROMs.
  - a. (Question 10 in RFI) Rough Order of Magnitude (ROM) schedule and cost requirements for your solution.
    - i. Given the potential for multiple awards for multiple subsystems to be





necessary to satisfy the full scope, as well as the 1-n unknown number of potential systems to be integrated with as part of the project, respondents are encouraged to briefly summarize what scope their ROM may cover in an appropriate format.

- b. See the addendum A released in support of this RFI for details on the anticipated scope and schedule.
  - c. Given that the objective of this RFI is to inform what scope is reasonable to require given the time and budget resources available, we're unable to articulate the full scope until responses are analyzed.
  - d. That being said, responders are encouraged to provide typical deployment costs, the basis for estimating costs, and/or the approximate costs for meeting specific requirements, as practical.
35. Question 12 asks "which of these requirements is your anticipated solution(s) capable of meeting off the shelf, or with customization?"
- a. Does this apply to all components under 'Anticipated Solution Requirements as listed in the outline in Section 3 (i.e., a. Through j.)?'
    - i. Yes.
36. Is the end user for this RFI Fort Moore, or any specific division in Fort Moore?
- a. See subsection a '*Installation management groups/components supported*' of the RFI for the list of primary and secondary user groups.