Request for Information (RFI) - Installation Operations Tool (IOT)
RFI #001A
Release Date: January 3, 2024

1) Executive Summary

Army installations need a networking and data brokering system capable of rapidly integrating diverse data sources and systems into a unified data mesh and Common Operating Picture (COP) dashboard. To meet these needs, US Ignite is managing an 'Installation Operations Tool' (IOT) project for the requirements development and live demonstration of a potential solution at Fort Moore, GA (formerly known as Fort Benning). This project is in support of the US Army Corps of Engineers, Engineer Research and Development Center (USACE-ERDC) and the Assistant Secretary of the Army for Installations, Energy and Environment (ASA IE&E).

As a part of the IOT project, US Ignite is releasing this Request for Information (RFI) to collect feedback from industry about the available technologies and key considerations for demonstrating an Installation Operations Tool live at Fort Moore, GA. Feedback received in response to this RFI will inform a subsequent solicitation(s) for the design, integration, and live demonstration of the Installation Operations Tool. The Installation Operations Tool is intended to become a foundational capability for securely and rapidly modernizing Army installations, so participation from industry partners is encouraged at this stage to ensure the best outcome for the future of Army installations and the servicemembers they support.

2) US Ignite Overview

US Ignite is a national nonprofit, a 501(c)(3), that is accelerating the smart city movement – and creating value for an entire ecosystem – by guiding communities into the connected future, creating a path for private sector growth, and advancing technology research that's at the heart of smart city development.

As a trusted partner, US Ignite brings this entire smart city ecosystem together, successfully pairing financial investment with technical and organizational expertise. Through the public-private partnership programs we run, US Ignite is a catalyst for communications network advancement, and for innovation in smart city services that are powered by a new generation of technologies. You can read more about US Ignite's programs on its website.

3) Installation Operations Tool Requirement and Anticipated Solution Overview

Summary of Need

The first major need Army installations have for an Installation Operations Tool is system and data integration, and interoperability. Information systems on Army installations are currently stove-piped, and breaking down those stovepipes creates multiple benefits. First, this allows for more rapid and effective Command and Control (C2) at the garrison and directorate levels, by making all necessary information on developing situations available within a single pane of glass. Second, this reduces the need for time-intensive, manual duplicate data entry in multiple systems with automatic system integration, saving time with limited manpower available. Finally, this allows for the enrichment for all connected business systems and business process

managers, by providing them access to data outside their domain or outside a given system.

The second major need Army installations have for an Installation Operations Tool is a new model for more rapidly and securely networking information systems. Currently, obtaining a new Authority to Operate (ATO's) for an information system can require between 6 and 18 months, with the potential of requiring even more time. Combined with the fact that systems need an ATO in order to communicate with other DoD systems, this dramatically inhibits Army installations' ability to experiment with and validate new capabilities in operational environments. Further, requiring every new system to obtain and maintain its own ATO raises the financial barrier to entry for new capabilities, and it creates a manpower constraint for Army risk assessors. If Army installations had a single hardened, zero trust, ATO'ed networking solution that could safely connect to external systems with just an interconnection agreement rather than an ATO, that would create substantial value for the Army. This Installation Operations Tool would allow for more rapid experimentation and modernization, it would reduce the proliferation and bottleneck-ing of Authorities to Operate, and it would reduce the financial barrier to capability development for both the Army and industry.

Summary of Major Subsystems of an Installation Operations Tool

This complex requirement would ideally be satisfied by one or a small few solution provider(s) or system integrator(s), but it is likely to require integration of multiple distinct technologies in harmony with one another. Below is a list of the different major subsystems understood to be required to create an Installation Operations Tool.

1. **Secure Networking (ZTNA, SASE, or others)** - an Installation Operations Tool needs to be able to rapidly, securely network with a large number of Army enterprise and installation-specific IT and OT systems/devices. To do this, it must include a Zero Trust Network Access (ZTNA) architecture, a Secure Access Service Edge (SASE) architecture, or other network security solution so that it can rapidly modify its authorization package to safely interface with information systems outside its accreditation boundary.
2. **Data Brokering/Mesh** - an Installation Operations Tool needs to be able to connect to, transmit, and receive data from a large variety of information systems, requiring a robust data brokering or data orchestration capability. This must include connectors to many different standard data sources, and support communication of many different structured and unstructured data formats and methods like batch, stream, trigger, etc.. To support a flexible installation Common Operating Picture, this data must be organized and managed in a data mesh architecture so that data products can be shared and discoverable across domains, while still ensuring proper access control among a diverse user base.
3. **Dashboard-of-Dashboards** - An Installation Operations Tool needs to bring each of the different system data and system interfaces into a common 'dashboard of dashboards'. In an enterprise as large as an Army installation there are 'Common Operating Pictures' (COPs) of multiple systems even just in a single directorate like emergency services or public works, and an Installation Operations Tool would need to inherit these systems' interfaces as part of its own, rather than become duplicative of them to avoid going unutilized. Further, an Installation Operations Tool needs to be configurable by user groups both horizontally across installation directorates and vertically within a mission

command, allowing each group to compose 'dashboards' of multiple 'views' of systems or visualizations relevant to them in a single pane of glass. However, an Installation Operations Tool could be enhanced by including domain-specific functionality off-the-shelf, like many emergency response operations center solutions or utility management solutions have available.

Anticipated Solution Requirements

The list of business and functional requirements below represents the complete picture of the end-state vision of the Installation Operations Tool. Recognizing that multiple capability development iterations would be required to reach a solution capable of meeting every one of these requirements, one objective of this RFI is understanding which of these requirements can be readily met through either commercial or government off-the-shelf (COTS/GOTS) solutions, and which of these would be unattainable with the time and resources available for the first iteration of the IOT project.

a. Installation management groups/components supported
    i. Primary user groups
        1. US Army Garrison, Fort Moore
            a. Garrison Command
            b. Resource Management Office
            c. Plans, Analysis, & Integration Office (PAIO)
            d. Directorate of Public Works (DPW)
                i. Energy & Utilities
                ii. Planning
                iii. Construction
                iv. Environmental Management
            e. Family, Morale, Welfare, and Readiness (DFMWR)
            f. Directorate of Plans, Training, Mobilization, and Security (DPTMS)
                i. Range Operations
                ii. Airfield Management
                iii. Emergency Operations Center
            g. Directorate of Emergency Services (DES)
                i. Access Control
                ii. Physical Security
                iii. Police
                iv. Fire
                v. Hunting Enforcement
                vi. Guards
    ii. Secondary user groups
        1. Higher leadership
            a. Headquarters Department of the Army (HQDA)
                i. DCS/G-9
            b. Army Materiel Command (AMC)
            c. Installation Management Command (IMCOM)

2. Training and Doctrine Command (TRADOC)
    a. Maneuver Center of Excellence
        i. Armor School
        ii. Infantry School

b. Example information systems integrated
    i. Enterprise Information Systems
        1. Training and range management systems
        2. Access control systems
        3. Financial management systems
        4. Real property and space utilization systems
        5. Army enterprise data lakes
        6. Work order management systems
        7. Metering systems
        8. Environmental/Meteorological forecasting and observational systems
        9. MS Teams
    ii. Installation Information Systems
        1. Smart Installation and Community Dashboard (SICD)
        2. Environmental/Meteorological Sensors
        3. Remote Surveillance systems
        4. CCTV's
        5. Computer Aided Dispatch (CAD) system
        6. Utility Monitoring and Control System (UMCS)
        7. Fleet vehicle tracking
        8. Smart Barracks
        9. Radio equipment
        10. Network equipment
        11. Social Media applications
        12. Cellular location data
        13. Hunting permitting applications
        14. Mission management software
    iii. Technical and identifying details on specific information systems that are available to be integrated with will be shared with successful awardees of a forthcoming solicitation.

c. Business requirements supported
    i. Data brokerage
        1. Incorporating data from multiple information systems into single tools, including
            a. Business intelligence platforms
            b. Geospatial visualization platforms
                i. Illustrative examples and potential solutions include TAK, C2IMERA, Thingsboard, or similar.
            c. Self-serve analytics and application development environments
        2. Sharing data from one information system to another to enrich that information system's performance
        3. Inheriting multiple interfaces or data visualizations from one or more information systems as views or widgets in a single large-form dashboard

display.
    a. This pattern is desired to avoid imposing additional systems on top of what operators and garrison commanders already use
    b. The 'Army Materiel Command Knowledge Management Portal' (AKMP) is one example of such an interface that may be extended to meet this requirement.
4. Data discoverability of all permitted data products throughout the views described in each of the above requirements
5. Data product management for domain data product owners

ii. Command and Control
1. Pushing or sharing views with selected groups or individuals - either up to command for situational awareness/decision-making, or between situational responders
2. Flexible command process flow configuration (configuring the process, actions taken and roles in a command process, and the groups or individuals that support each role or step in the process)
3. Mobile accessibility - the Installation Operations Tool should be accessible by cell phone, tablet, or small form figure laptop so that it can be accessible by responders and technicians in their vehicle or at a field location.

iii. Example installation management use cases benefiting from data mesh and fusion
1. Situational Deconfliction
    a. When requested to deploy emergency response assets, having visibility of the upcoming missions and implied demand for those assets to better predict the ability to meet all requirements
2. Emergency Response
    a. Emergency Medical Services vehicle/asset stationing based on locations of planned training activities.
    b. Providing fire with visibility of FRCS data like CO2 sensors, so that if multiple concurrent emergencies are reported they can understand the likelihood of a false fire alarm and prioritize the size of response sent to each emergency accordingly
3. Public Works
    a. Building fault detection, fusing FRCS data with weather sensor, publicly available weather API, and meter consumption data
    b. HVAC-control modifications predicted based on troop schedules, HVAC trends, weather, and occupancy patterns.
    c. Fusing cellular location data with floor plan and stationing information systems to understand observable facility under and overutilization
4. Physical Security
    a. Comprehensive, layered physical security including access control, remote surveillance systems, CCTV's, and other assets
    b. Search and traceability of one individual or vehicle between multiple security camera systems
5. Public Affairs

        a. Having visibility of emergency services information in order to respond in a timely manner to information requests regarding emergency events
    6. Range Management
        a. Automating the integration between ISportsman requests to hunt on installation and Range Facility Management Support System (RFMSS)
    7. Resource Management
        a. Continuously updated analytics on status of funds available between directorates
    8. Human Resources
        a. Data and Application Integration between each of the necessary human resource systems necessary for onboarding new soldiers to an installation

iv. Risk Management
    1. Expedite the RMF update process to take between 30 and 90 days to incorporate new interfaces and associated interconnection agreements with information systems outside the Installation Operations Tool's authorization boundary

v. Cybersecurity
    1. Establish zero trust network access (ZTNA), Secure Access Service Edge (SASE), or similar cloud/network security architecture

d. Operational Environment
    i. A central server is anticipated to be deployed in a data center at a remote ERDC-controlled location until authorization to deploy in the Fort Moore data center is approved.
    ii. The Installation Operations Tool will likely have access to a research network capable of providing the transport layer from Fort Moore to a remote ERDC-controlled location, if additional hardware deployment is beneficial. The research network has the ability to provide access to NIPR users and access NIPR resources.
    iii. Once authorized, the Installation Operations Tool will have the ability to use the base network for transport to information systems. However, not all information systems may be accessible via the base network due to lack of physical proximity, and new vendor-proposed transport mechanisms like commercial or private 4G/5G or commercial fiber may be proposed.
e. Architecture
    i. On-premise or hybrid architecture, with non-mission-critical reporting or non-time sensitive applications being able to run in the cloud but mission critical functions being able to operate in a disconnected state on-premise to avoid disruptions due to lack of connectivity.
    ii. A unified user access control system for controlling access to both data and networked resources. The access control system must support authorization of external identities through SAML2.0 or OpenID Connect. The access control system must support on-premise user authorization when operating in a disconnected state.

iii. A data lake or data mesh capable of storing and querying both structured and unstructured data. The Data lake or Data Mesh must be capable of being deployed in a hybrid model where data is synchronized between on-premise and cloud data lake or data mesh instances.

iv. A Zero Trust networking tool made up of two parts.
    1. Hardware - at each interface with external systems, a secure gateway device is expected to be deployed to create a trustless network peer between the Installation Operations Tool and the external system. This may be a head server for external systems if creating a single interface with that system, or with each device on that system if the Installation Operations Tool is expected to securely network that system.
    2. A software defined network capable of configuring communication between On-Premise and Cloud Network Resources within or peered to the IOT Project.

v. Bi-directional data flows with Army 'Virtual Toolbox for Installation Mission Effectiveness' (VTIME) running in Azure GovCloud, currently on the ERDC research network.

vi. Ability to network with external information systems using secure connections over installation NIPR network, and ideally commercial or private cellular as well.

vii. Interoperability of data, networks, and applications will be beneficial through containerization and adherence to industry and DoD standards, to avoid environment and vendor lock-in.

f. Security

i. Ability to undergo Risk Management Framework (RMF) process defined by DoDI 8510.01/8500.01 and obtain Authority to Operate (ATO).

ii. Any implementation or integration with Facility-Related Control Systems (FRCS) shall conform to UFC 4-010-06 cybersecurity requirements.

iii. Ability to rapidly iterate the authorization package of the IOT capability to incorporate interfaces with new systems more quickly than conventional ATO's, potentially by achieving cATO.

iv. Compliance with Zero Trust design principles
    1. Software defined networking and perimeter
    2. Attribute-based access control, least-privileged access, continuous multifactor authentication and behavioral biometric risk scores
    3. Infrastructure, API, and process segmentation
    4. Data encryption in transit and at rest
    5. Dynamic policy enforcement, data rights management, loss prevention, and dynamic data discovery, classification and tagging
    6. Dynamic device status scans, instrumentation, service updates and inventorying

v. Secure software supply chain including pre-STIG'ed containers and services

vi. Adherence to DevSecOps best practices

vii. Analytics for cyber anomaly detection and deep packet sniffing

viii. Compliance with NIST 800-171 controls

ix. Minimally FedRAMP medium for the cloud portion of any hybrid solutions

g. Governance
    i. Dynamic policy management/automation
    ii. Interoperability policy
    iii. Documentation policy
    iv. Privacy policy
    v. Access control policies
    vi. Security policies
    vii. API management
h. Data lake/mesh capabilities
    i. Self-service data platform
        1. Storage/query engine
        2. Data contract management
        3. Monitoring
        4. Data product catalog
    ii. Policy automation (lifecycle management, terms of use, etc.)
i. Developer support
    i. Provide deployable industry standard development services within Installation Operations Tool architecture like DevSecOps and version control tools, pre-STIG'ed container images, SQL and NoSQL-based database and data factory tools, application development tools, and more.
    ii. These standard resources are desired so that existing capabilities may be refactored into the Installation Operations Tool boundary, and so that new capabilities can be built using it.
    iii. This potential requirement of the Installation Operations Tool could be satisfied by Government Off the Shelf Solutions, including but not limited to OSD Advana Edge.
j. Relevant DoD and other executive orders, memos, guides, strategies, and policies
    i. Army Installations Strategy, 2020
    ii. Army Data Plan, 2022
    iii. Army Cloud Plan, 2022
    iv. DoD Cloud Computing Security Requirements Guide, 2022
    v. NIST SP 800-171
    vi. FedRAMP
    vii. DoD Digital Modernization Strategy, 2019
    viii. Executive Order on Improving the Nation's Cybersecurity, 2021
    ix. DoD Zero Trust Reference Architecture
    x. DoD Cybersecurity Reference Architecture
    xi. DoD Zero Trust Strategy

4) Q&A and Office Hours

Any requests, questions, or other communications about this RFI must be made by email to sayed.elhamz@us-ignite.org, RFI Coordinator. Communications made to other US Ignite personnel or attempts to ask questions by phone or in person will not be allowed or recognized as valid and may disqualify respondents from any future related solicitations. Any questions must be submitted by January 19, 2024 8:00 PM ET. Respondents are encouraged to submit questions

as early as possible, to support time for dialogue and address. US Ignite will endeavor to respond to all parties no later than January 26, 2024 8:00 PM ET.

Respondents are permitted and encouraged to request office hours with US Ignite staff, either to raise clarifying questions or to brief and seek feedback on related solutions. Respondents wishing to request office hours may do so by emailing sayed.elhamz@us-ignite.org. Office hours used to gain additional information about this project or RFI will be recorded and published for equal access on US Ignite's website. Office hours used to discuss vendor capabilities will not be recorded and will be treated as confidential.

5) Response Content Guidance

There are no mandatory requirements for content submitted in response to this RFI. US Ignite recommends respondents re-use, to the greatest extent practical standard, existing materials available within respondents' organizations to avoid significant time being necessary to respond. Below is a list of types of information that would be beneficial to US Ignite.

1. Company overview
2. List of relevant products/solutions
3. Boilerplate overview materials on relevant products/solutions
4. List and details of related deployments in communities or DoD installations
5. Compliance with DoD policies and industry standards including but not limited to FedRAMP, NIST SP 800-171, NIST SP 800-53
6. Any active relevant Authority to Operate (ATO)
7. Solution architecture and related technical documentation
8. Potential ecosystem partners expected to have interest/relevance to the scope of the Installation Operations Tool
9. Key challenges or opportunities perceived by respondents
10. Rough Order of Magnitude (ROM) schedule and cost requirements for your solution
    a. 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
11. Is your organization able to deliver one, multiple, or all of the major subsystems described in section 3, either individually or by obtaining government off-the-shelf solutions and/or working with established channel partners?
12. Which of these requirements is your anticipated solution(s) capable of meeting off the shelf, or with customization?

13. Are there any requirements in section 3 that impose particular schedule, technical, or budget risk for your organization relative to the rest of the requirements?

14. Given the summary of needs and business requirements, are there any alternative architectures or approaches your organization would recommend considering as anticipated solutions?

15. Would your organization be more likely to respond to a solicitation for just one or two of the major subsystems described in section 3, relative to a solicitation for the complete solution?

16. If your organization were interested in bidding just to satisfy one or two of the major subsystem requirements, would you be open to being paired with another performer bidding to provide the remainder of the solution?

6) Submission Instructions

All RFI responses should be submitted by February 2, 2024, 8:00 PM Eastern Time. Responses should be submitted via email to sayed.elhamz@us-ignite.org and should conform with the required guidelines described in section 5 'Response Content' above. Respondents will receive an email from US Ignite confirming receipt of their response. Respondents are encouraged to submit information as early as practicable, and may provide multiple responses to this RFI.

7) Disclaimers

- This RFI does not constitute a solicitation.
- Information received in response to this RFI will be used by US Ignite to develop the scope of a future solicitation.
- The ability for respondents to request office hours with US Ignite does not obligate US Ignite to a certain time period of responsiveness, and it does not commit US Ignite to make a certain amount of time available for office hours.
- All information received in response to this RFI will be considered confidential, and will not be shared with anyone other than USACE-ERDC or Fort Moore, GA without prior consent from the respondent.
- Respondents wishing to submit responses containing controlled unclassified information (CUI) may indicate as such to the RFI coordinator listed above, and will be provided instructions for doing so.
- Information classified as Secret or Top Secret is not to be submitted in response to this RFI.
- Submission of information in response to this RFI is purely voluntary; US Ignite assumes no financial responsibility for any costs incurred.
- US Ignite reserves the right to request follow-on discussions with respondents to understand the details of responses received.