Environment Analysis

National Information Exchange Model

July 31, 2020

TABLE OF CONTENTS

LIST OF TABLES

1. Introduction

1.1 Background

In January 2019, the U.S. Department of Defense (DoD) became the official government sponsor of the National Information Exchange Model (NIEM). NIEM is a common vocabulary that enables efficient information exchange across diverse public and private organizations. NIEM saves organizations time and money by providing consistent, reusable, and repeatable data terms, definitions, and processes.

The Information Exchange Package Documentation (IEPD) Life Cycle (IEPDLC) is the primary process for developing artifacts that define an information exchange specification. The IEPDLC provides a guide to understanding how IEPDs are built from NIEM and published. It is not intended to be prescriptive. IEPD builders may enter the life cycle at any step or adjust the scope of the life cycle to support the level of effort (LOE) required for their individual IEPD development.

Under the supervision of the DoD Joint Staff J6 Deputy Directorate for Command, Control, Computers, Communication and Cyber Integration (JS J6 DDC5I), the NIEM Management Office (NMO) aims to develop a set of tools to support the IEPDLC and needs to assess courses of action (COA) comprising hosting environment alternatives.

The requirement to support a Development, Security, and Operations (DevSecOps) Continuous Integration/Continuous Delivery (CI/CD) workflow in support of future NIEM development means automating as much as possible from build, test, deploy, to operations, enabling development teams to maximize their time on business impact. In a DevSecOps CI/CD pipeline, security is granted as much priority and automation as any aspect of development and is shifted to the left of the life cycle as much as possible (early and often).

Organizations embrace DevSecOps to continuously deliver high-quality and reliable software to their users. Culture and teamwork evolve with the intent to build better quality software faster. High-performing teams are needed to maintain balance in the opposing forces of throughput and stability, while both are amplified. DevSecOps realizes the Agile benefits of reducing risk, increasing velocity, and improving quality, but is scaled beyond the development life cycle to the product life cycle. DevSecOps increases resiliency, reduces unplanned downtime, and provides production metrics to close the feedback loop to adapt to users and fix software in a timely manner.

Industry views the DevSecOps 7 core practice areas as:

1. Continuous Integration (CI): Code is regularly delivered to a code repository, and builds and tests are automatically performed to find any issues. Alerts are sent if issues arise during the automated build process.
2. Configuration Management (CM): The tracking and controlling of changes to the software code base and archiving all file versions into a central CM database. Provides organization for the software build process by accounting for multiple environments.
3. Automated Testing: Automated tests for unit, functional, security, and performance. Testing occurs continuously throughout the development life cycle and provides insight into the current health of the software.
4. Continuous Delivery (CD): Code is continuously delivered to test environments and every software change is potentially deployable to production. Automated testing can drive the acceptance of software.
5. Continuous Deployment: All software changes that are accepted through automated testing are automatically deployed to production. These constant deployments do not impact the end user.
6. Infrastructure as Code: Using software to control the build, configuration, and deployment of the application. Additionally, software is used to control and provision the infrastructure of the system.
7. Continuous Monitoring: Ability to continuously monitor system/applications for issues and notify responsible parties in case of anomalies. Provide analytics gathering capabilities to ensure the application is performing at optimal levels and the system is secure.

1.2 Purpose

This document assesses hosting environment alternatives. The purpose of the analysis is two-fold:

- Identify a suitable COA for meeting NMO requirements and realizing operational efficiencies
- Recommend a course of action that considers technical, cost, and risk factors

NMO needs a hosting environment that meets the functional tool needs for the following user categories:

- Stakeholders or stakeholder communities with an interest in NIEM
- Practitioners, including IEPD developers and implementers such as NMO, technical assistance staff, content management staff, development staff, and government/contract/commercial tool developers

Additionally, the environment should realize the following efficiencies:

- Maximize information reuse
- Maximize tool interoperability
- Minimize the cost of using NIEM (particularly entry costs)
- Reduce time to develop IEPDs
- Minimize the cost of increasing automated support for NIEM
- Maximize consistency and quality of release products, IEPDs, and associated artifacts
- Maximize domain, developer, and user self-service

The recommendation accounts for findings gathered from NMO, technical assistance staff, development staff interviews, research into the current and emerging offerings throughout the DoD, and discussion with other Government entities that face or have overcome similar challenges.

1.3 Document Layout

The remainder of this document is constructed with the following sections:

- Section 2: Constraints, Limitations, and Assumptions – Describes guidance from NMO, study limitations, and statements related to the study taken to be true
- Section 3: Methodology – Describes the steps taken to solicit input on motivations, outcomes, and technical requirements that substantiate our evaluation and recommendation
- Section 4: Survey Results – Reports the responses from business and information technology (IT) stakeholders
- Section 5: COA – Identifies and evaluates COAs and recommends a solution based on NMO goals and validated requirements
- Section 6: Execution Approach – Recommends two critical steps once a decision has been made

2. Constraints, Limitations, and Assumptions

2.1 Constraints

In April 2020, NMO contracted Booz Allen Hamilton to operationally and technically assess hosting environment alternatives to enable new tool development and support the IEPDLC. NMO provided the following guidance:

- The assessment must be completed in three months from May 1, 2020 to July 31, 2020
- The assessment must include NIEM.gov, MAX.gov, Defense Intelligence Information Enterprise (DI2E), Warfighter Mission Area Architecture Federation and Integration Portal (WMAAFIP), Platform One, and should include at least one other alternative
- Booz Allen Hamilton must provide regular in-progress reviews to NMO

Additionally, Cloud Smart, the Government's new strategy to accelerate agency adoption of cloud-based solutions, provides the following guidance:

- All Federal agencies will rationalize their application portfolios to drive Federal cloud adoption
- To realize not only security benefits of cloud infrastructure but also its benefits related to scalability and speed-to-market, agencies should utilize mature agile development practices, including DevSecOps Continuous Integration/Continuous Deployment (CI/CD)

2.2 Limitations

In **Section 4**, we summarize business and technical input provided by the NIEM community given the following limitations:

- We compiled business and technical questions for NMO and development staff. We received two responses, which limited the input from the NIEM community to factor into the analysis.

2.3 Assumptions

In **Section 5**, we assess each COA and provide a recommendation. The assessment and recommendation are supported by several assumptions. For clarity, we categorized the assumptions into five subsections: data, tools, tool infrastructure, business outcomes, and technical requirements. In each subsection, we enumerated the assumptions in the order we encountered

them. For example, we parsed the Tool Strategy Requirements Document (TSRD) before we participated in the NIEM Kickoff Meeting. Assumptions without a reference correspond to statements related to the study not explicitly stated in the TSRD, NIEM Kickoff Meeting minutes, and interview responses.

A fundamental assumption to this assessment is that a DevSecOps CI/CD pipeline will be essential to develop new tools that will be containerized and deployed to a web hosting site and available for download to users' machines for use independently. If separate DevSecOps CI/CD environment(s) are desired from the production hosting of the developed tool(s), then several additional options should be assessed as separate considerations.

2.3.1 Data

1. New NIEM tools should include the ability to upload static files/artifacts (e.g., UML diagrams, database schemas) used to support the Scenario Planning step in the IEPDLC. [Ref: TSRD-24.0]
2. New NIEM tools should include the ability to upload static files/artifacts (e.g., Word/Excel documents containing business rules) used to support the Analyze Requirements step in the IEPDLC. [Ref: TSRD-26.0]
3. New NIEM tools should store and leverage user custom data mappings for improved search support. [Ref: TSRD-78.0]
4. New NIEM tools will use both perishable and persistent data. [Ref: Interview]
5. All NIEM artifacts are and will be UNCLASSIFIED.

2.3.2 Tools

1. Developing and deploying new NIEM tools must not impact the NIEM release schedule. [Ref: TSRD-Assumptions]
2. The following tools must be maintained during new tool development: Schema Subset Generation Tool (SSGT), Conformance Testing Assistant (ConTesA), Movement, and Migration Assistance. [Ref: TSRD-Assumptions]
3. New NIEM tools (funded by government sponsors) must be government-owned/controlled and open-source to the NIEM user community. [Ref: TSRD-Assumptions]
4. New NIEM tools should be functional without dedicated accessibility to the Internet. [Ref: TSRD-6.0]

5. New NIEM tools should leverage industry-standard security measures for scanning any external files uploaded by an end user. [Ref: TSRD-14.0]
6. New NIEM tools should incorporate session management capabilities to keep track of a user's activity of interactions. [Ref: TSRD-33.0]
7. New NIEM tools should incorporate a user account registration and management capability. [Ref: TSRD-52.0]
8. New NIEM tools should include a webhook (or endpoint) for the Format Translator application programming interface (API) that SSGT can leverage to return a NIEM JavaScript Object Notation (JSON) Schema Subset. [Ref: TSRD-59.0]
9. New NIEM tools should address functional gaps rather than replace existing tools. [Ref: NIEM Kickoff Meeting]
10. New NIEM tools should be web-based. [Ref: NIEM Kickoff Meeting]

2.3.3 Tool Infrastructure

1. The environment should support containerization. [Ref: TSRD-3.0]
2. The environment should support a DevSecOps workflow. [Ref: TSRD-4.0]
3. The environment should support a collaborative authoring system for creating and maintaining linked collections of Web pages. [Ref: TSRD-4.0, TSRD-5.0]
4. The environment should support the ability to search and browse existing NIEM models. [Ref: TSRD-42.0]
5. The environment should support searching NIEM data components. [Ref: TSRD-45.0]
6. The environment should support the incorporation of machine learning algorithms to develop an intelligent search capability. [Ref: TSRD-66.0]
7. The environment should support the ability to identify related IEPDs found within a supported NIEM IEPD Registry and/or Repository. [Ref: TSRD-76.0]

2.3.4 Business Outcomes

1. NMO does not specify financial performance indicators, but the cost of the environment should be consistent with industry norms.
2. NMO does not specify user engagement metrics, but the environment should support user engagements.

3. NMO does not specify system performance metrics, but the environment's reliability should be consistent with industry norms.

2.3.5 Technical Requirements

1. New NIEM tools must serve technical documentation that outlines how third-party developers can interact with the software code base. [Ref: TSRD-106, Interview]
2. NIEM development staff do not prefer specific DevSecOps tools. [Ref: Interview]
3. New NIEM tools should support modular deployments. [Ref: Interview]
4. The environment needs an Impact Level (IL)-4 authorization to include, for example, data designated as Controlled Unclassified Information (CUI).
5. The environment must comprise distinct environments for development, quality assurance (QA), and production.
6. Current NIEM tools (e.g., SSGT, ConTesA, and Movement) will adapt to communicate via web services with new NIEM tools in the environment.
7. The environment will depend on access via web services to NIEM tools being maintained (e.g., SSGT, ConTesA, and Movement).

3. Methodology

New technology should support NMO's business needs, so we started by aligning business and IT stakeholders to create a clear and concise strategy for the environment.

First, we solicited input on the motivations for the hosting environment, categorizing questions along three dimensions: emergent business requirements, emergent business expectations, and aspirational business capabilities. **Section 4.1** lists the results of our survey.

Second, Cloud Smart encourages agencies to approach cloud adoption in terms of intended outcomes and capabilities, so we solicited input on the desired business outcomes for evaluating the environment. We categorized questions along three dimensions: financial management, user engagement, and system performance. **Section 4.2** lists the results of our survey.

Third, we solicited input on technical requirements given current configurations. **Section 4.3** lists the results of our survey.

We then used responses from business and IT stakeholders to compile assumptions (tagged in **Section 2.3** as "Ref: Interview") and priorities.

Finally, we assessed several alternatives in a comprehensive way, measuring compute resourcing, storage, etc. Our recommendation considers NMO objectives (**Section 1.2**), business and IT stakeholders' priorities (**Section 4**), and the systematic assessment for each alternative (**Section 5**).

4. Survey Results

We started aligning business and IT stakeholders by compiling business and technical questions on and around business motivations (**Section 4.1**), business outcomes (**Section 4.2**), and technical requirements (**Section 4.3**). From these different points of view, our questions were targeted at characterizing the needs, expectations, and aspirations of the NIEM community to provide a recommendation that was not simply focused on the best technology specification. Rather, our questions were aimed at documenting business concerns with technical concerns to support NMO with informed tradeoffs. Our questions were specific because the cloud service market is very competitive, and without understanding the nuances of client-specific objectives and workloads, distinguishing cloud service providers can be difficult, if not impossible.

4.1 Business Motivations

4.1.1 Emergent Business Requirements

Emergent business requirements comprise business necessities coming into existence.

The business stakeholder asserted that reducing capital expenses (i.e., funds used to acquire, upgrade, or maintain assets such as technology or equipment) was not a business driver, which shapes decisions on environment costs.

The business stakeholder asserted that end of support (i.e., vendors ceasing support for products or services) for mission-critical technologies was not a business driver, which shapes decisions on environment procurements.

The business stakeholder asserted that responding to regulatory compliance (i.e., laws, regulations, guidelines, or specifications relevant to business processes) changes was not a business driver, which shapes decisions on scheduling workload migration tasks.

The business stakeholder asserted that improving IT stability was a low priority business driver, which shapes decisions on environment procurements.

The IT stakeholder did not provide input for any of the emergent business requirements questions.

Findings:

- NMO asserted that neither reducing capital expenses, upgrading/migrating mission-critical technologies reaching end of support, nor regulatory compliance changes were business drivers for the environment
- NMO deemed improving IT stability to be a low priority business driver

4.1.2 Emergent Business Expectations

Emergent business expectations measure how business necessities come into existence.

The business stakeholder asserted that saving cost was a medium priority business driver, which shapes decisions on environment costs.

The business stakeholder asserted that reducing vendor/technical complexity was a high priority business driver, which shapes decisions on environment products and services.

Both the business stakeholder and the IT stakeholder indicated that optimizing internal operations was a medium priority business driver, which shapes decisions on environment products and services.

Findings:

- NMO asserted that reducing vendor/technical complexity was a high priority business driver
- NMO asserted that saving cost and optimizing internal operations were medium priority business drivers

4.1.3 Aspirational Business Capabilities

Aspirational business capabilities measure long-term business goals.

Both the business stakeholder and IT stakeholder indicated that preparing for new technical capabilities and building new technical capabilities were high priority business drivers, which shapes decisions on environment products and services.

The business stakeholder asserted that scaling to meet market demands and geographic demands were high priority business drivers, which shapes decisions on environment procurements.

Both the business stakeholder and IT stakeholder indicated that improving customer experiences and engagements was a high priority business driver, which shapes decisions on environment products and services.

The IT stakeholder provided the following rationale: “NIEM has provided a couple of tools to assist users as they build IEPDs or otherwise search, build, or use NIEM content. Some gaps are better addressed outside of NIEM using existing tools (e.g., model requirements in a spreadsheet or UML tool). But there are definitely places where we can provide additional support to the users to make it easier and quicker to build NIEM content.”

Findings:

- NMO and IT stakeholders rated each aspirational business capability (preparing for new technical capabilities, building new technical capabilities, scaling to meet market/geographic demands, and improving user engagement) as a high priority business driver.

4.2 Business Outcomes

4.2.1 Financial Management

Since the business stakeholder asserted that saving cost was a business driver, we asked questions on financial management such as reducing capital expenses for hardware and software and avoiding capital/operating expenses in a future budget.

We added assumptions on financial management outcomes (**Section 2.3.4**).

4.2.2 User Engagement

Since the business stakeholder asserted that improving user engagement was a business driver, we asked questions on user engagement such as reaching new user/domain segments (quickly) and enabling easy self-service provisioning to support operations.

We added assumptions on user engagement outcomes (**Section 2.3.4**).

Parenthetically, the IT stakeholder provided the following general comment related to user engagement: “I think the key business outcome is to lower the barrier / increase NIEM adoption and usage by providing tools that make NIEM easier for exchange developers to use. Another important outcome is to improve the quality of the NIEM exchanges and content that are built by having helpful user interfaces that provide guidance to users as they develop content, and

integrated NIEM [Naming and Design Rules] NDR and QA testing to help users identify and correct conformance issues during development."

4.2.3 System Performance

Since the business stakeholder asserted that IT stability was a business driver, we asked questions on system performance such as meeting service level agreements and meeting recovery point objectives and recovery time objectives to support operations.

We added assumptions on system performance (**Section 2.3.4**).

4.3 Technical Requirements

The IT stakeholder asserted there are no special security considerations for any of the IT assets, and no software in use has special processing unit requirements such as graphics processing units or tensor processing units.

The IT stakeholder asserted that the volume of content to be stored is less than 100GB, and there are no requirements on data retention.

The IT stakeholder reported user statistics for January 2020 (356 users and 713 sessions) and asserted there are web services for search and schema subset generation provided by SSGT.

The IT stakeholder asserted that no executable code will be uploaded.

Since references such as the TSRD suggest the NMO wants to pursue modern software delivery mechanisms, we asked questions on DevSecOps tooling support, supporting modular deployments, and serving technical documentation. We added assumptions on these technical requirements (**Section 2.3.5**).

5. COA

With NMO's guidance, we identified seven alternatives for hosting environments. We assessed each alternative using the same set of dimensions: compute and networking, storage and content delivery, deployment and management, app services, risks, and costs. We summarize the pros and cons for each alternative and conclude this section with a recommendation.

5.1 NIEM.gov

Currently, NIEM.gov is operated by the Department of Homeland Security (DHS) Platforms and Solutions Division, Solutions Development Directorate (SDD). DHS provides an enterprise

content delivery network, web hosting/content management services, web development services, and/or custom services for the NIEM.gov website. [Ref: Memorandum of Understanding between DHS, OCIO, IS2O, and NMO]

5.1.1 Compute and Networking

Pro: Existing web presence.

Con: The environment is a highly customized, tightly controlled Amazon Web Services (AWS)/CGI Federal hybrid cloud, but DHS representatives indicated they "do not have the capability to expand" now.

5.1.2 Storage and Content Delivery

Pro: The environment uses AWS-based storage: MariaDB and MySQL. The environment uses Drupal 7 for content management, but DHS plans to migrate to Drupal 9 by November 2021.

Con: DHS representatives indicated they will consider containerization post-Drupal 9 upgrade late 2021, but containerization services are not available now.

5.1.3 Deployment and Management

Pro: The environment uses Drupal DevSecOps tools

Con: Containerization services are not available.

5.1.4 App Services

Pro: The Web Content Management tools and support services include JIRA, Confluence, Bitbucket, Bamboo, Akamai, New Relic, Code Dx, Entrust, Splunk, and Zenoss.

Con: Containerization services are not available.

5.1.5 Risks

Based on feedback from the DHS SDD Project Manager, the environment does not support containerization and will not support containerization for approximately 1.5 years. And the environment is undergoing an authority to operate (ATO) review, which could impact the roadmap for migrating to Drupal 9.

5.1.6 Costs

The NIEM.gov web site support is provided as a no cost agreement as part of DHS's contribution to the NIEM.gov program. [Ref: Memorandum of Understanding between DHS, OCIO, IS2O, and NMO]

5.1.7 Summary of Pros and Cons

The environment is backed by a robust commercial cloud service provider (CSP) with the resources to support IT stability (**Section 4.1.1**) and the tools to support new capability development (**Section 4.1.3**). However, DHS does not have the capability to accommodate new workloads and the environment does not support containerization.

5.2 MAX.gov

MAX.gov is a government-wide suite of advanced collaboration, information sharing, data collection, publishing, business intelligence, and authentication tools and services used to facilitate knowledge management. MAX.gov tools include MAX Community, MAX Collect, MAX Survey, MAX A-11, MAX Analytics, and MAX Authentication, among others.

MAX.gov is Federal Risk and Authorization Management Program (FedRAMP) authorized to process and store information up to Federal Information Security Management Act of 2002 (FISMA) Moderate, and user access permissions can be customized for each workflow stage and page. MAX.gov is registered with FedRAMP as an Agency Authorized Software as a Service (SaaS) provider.

The MAX.gov ATO was signed on November 1, 2018 by the Office of Management and Budget (OMB) Authorizing Official (AO) Kelly Kinneen, Assistant Director for Budget. The 2018 ATO package is under review with FedRAMP and includes the assessment results from the FedRAMP-approved third party assessor (3PAO), which was completed in October 2018. Detailed information from this security assessment, and all relevant Assessment and Authorization (A&A) documentation is located in the FedRAMP repository, and per OMB circular A-130 Appendix I, Section J, can be used by any agency that has reviewed the documentation and determined that the protections are sufficient for the agency's security needs.

5.2.1 Compute and Networking

Pro: None.

Con: MAX.gov does not offer customizable or configurable hosting solutions as an independent service.

5.2.2 Storage and Content Delivery

Pro: None.

Con: The environment does not offer customizable or configurable database solutions.

Storage and content delivery services are limited to the MAX.gov service catalog, which includes PostgreSQL and DB2. However, the environment does not offer these platforms as a service to third-party applications.

5.2.3 Deployment and Management

Pro: None.

Con: The environment does not offer customizable or configurable application, tool, or code deployment/management tools.

5.2.4 App Services

Pro: None.

Con: App services are limited to the existing data services offered as part of the MAX.gov service catalog, e.g., Elasticsearch, WordPress, Pentaho, Adobe, Apache Solr, OpenLDAP, and Atlassian Tools.

5.2.5 Risks

The environment is not capable of supporting the containerization service requirement. External services/tools would not be capable of communicating with services in the environment.

5.2.6 Costs

The approximate cost-per-year to host a MAX.gov website, development environment, and authentication services for up to 500 users would be $185,000 [Ref: MAX.gov pricing guide]. Additional fees are associated with adding applications ($5,000 per application for authentication service).

5.2.7 Summary of Pros and Cons

This environment is not a viable alternative because it does not support containerization, DevSecOps workflows, machine learning algorithms, nor communication with external tools (e.g.,

SSGT, ConTesA, and Movement). Indeed, MAX.gov representatives asserted they "have some hosting partners but not something we are looking to continue" and they "are much more of a SaaS platform."

5.3 DI2E

The DI2E Developer Tools provide an open development environment for the defense and intelligence community, offering a full suite of popular, widely used development tools. Project teams can establish cross-team efforts to support development, integration, and test needs. The tools support software development life-cycle activities by providing issue tracking, project collaboration, documentation, and design artifact hosting.

Aligning with Office of Acquisition, Technology, and Logistics (AT&L) Open Systems Architecture guidance, the DI2E Developer Tools provide ready access and accessibility to government-owned capabilities.

5.3.1 Compute and Networking

Pro: None.

Con: DI2E does not offer customizable or configurable hosting solutions as an independent service.

5.3.2 Storage and Content Delivery

Pro: None.

Con: The environment does not offer customizable or configurable database solutions.

Storage and content delivery services are limited to the DI2E service catalog, which includes Bitbucket, a distributed version control system.

5.3.3 Deployment and Management

Pro: None.

Con: The environment does not provide Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) that allow projects to host their services or applications. The environment does allow projects to store build artifacts and binaries but does not allow any run-time hosting of them.

5.3.4 App Services

Pro: DevOps tools available for utilization, e.g., Atlassian Tools, Bitbucket, Jenkins, Nexus, SonarQube, Fortify, TestRail, and FileSend.

Con: App services are limited to the existing data services offered as part of the service catalog.

5.3.5 Risks

The environment does not provide hosting services for any external projects, nor is it capable of supporting the containerization service requirement. External services/tools would not be capable of communicating with services in the environment.

5.3.6 Costs

The DI2E Developer Tools are available at no cost to any Intel-related project in the DoD or Intelligence Community (IC).

5.3.7 Summary of Pros and Cons

This environment is not a viable alternative because DI2E does not provide hosting services for any external projects to host services or applications.

5.4 WMAAFIP

WMAAFIP is a central, federated hub for discovery, accessibility, understandability, and reusability of Warfighter Mission Area (WMA), DoD Chief Information Officer (CIO) Information Enterprise (IE), and Joint Information Environment (JIE) architectures. The portal is designed to:

- Provide a common context (federated environment) for sharing WMA architectures, mission threads, and other related joint capability integration information between various authoritative repositories to increase the effectiveness and efficiency of decision-making in a dynamic environment by our customers
- Maximize limited resources and eliminate/reduce duplicative efforts
- Improve the speed of development for architecture products by reusability
- Share data between various organizations, tools, and environments

5.4.1 Compute and Networking

WMAAFIP is hosted in the Defense Information Systems Agency (DISA) Defense Enterprise Computing Center (DECC) as part of the DISA milCloud and milSuite catalog of service offerings.

Pro: None.

Con: WMAAFIP does not offer independent compute resources, however, WMAAFIP representatives asserted that if a new project joins WMAAFIP, then compute resources in the DECC would be adjusted accordingly. In this sense, WMAAFIP acts as a cloud broker in dealing with DISA milCloud procurement for the new project team, but the project must align with the WMAAFIP mission.

5.4.2 Storage and Content Delivery

Pro: None.

Con: WMAAFIP is a collection of Staging and Production hosting environments specifically managed for WMAAFIP custom code hosting.

5.4.3 Deployment and Management

Pro: None.

Con: Deployment and management services are not provided outside of WMAAFIP updates, which are tested and promoted through staging (both NIPR and SIPR) prior to releasing the build to production.

5.4.4 App Services

Pro: None.

Con: App services other than customized WMAAFIP MVC application on .NET Framework are not provided as part of the WMAAFIP offering. Continuous Integration/Continuous Delivery (CI/CD) pipeline services such as container registry, code repository, and code deployment/execution are not offered.

5.4.5 Risks

If containerization services become a “must-have” rather than “nice-to-have,” then the environment is not capable of supporting this requirement. If NIEM workloads do not align with the WMAAFIP mission, the environment will not host the application.

5.4.6 Costs

Not assessed.

5.4.7 Summary of Pros and Cons

This environment is not a viable alternative because it does not provide support for hosting containerized workloads and has extremely limited product and service support. Moreover, NMO would need to demonstrate NIEM's applicability to the WMAAFIP mission.

5.5 Platform One

Platform One is the centralized team providing DevSecOps/Software Factory managed services with baked-in security to DoD programs. Platform One services/capabilities provide the following:

- Manage software factories for development teams so they can focus on building mission applications
- Decouple development teams from factory teams with DevSecOps and site reliability engineer (SRE) expertise
- Help instantiate DevSecOps CI/CD pipelines in days at various classification levels
- Build and leverage the DoD hardened containers while avoiding one-size-fits-all architectures
- Compliance with the DoD Enterprise DevSecOps Initiative (DSOP)
- Centralizing the container hardening of 172 enterprise containers (databases, development tools, CI/CD tools, cybersecurity tools, etc.)
- Provide DevSecOps managed services with collaboration tools, cybersecurity tools, source code repositories, artifact repositories, development tools, DevSecOps as a Service, etc. These services are managed on Cloud One by the SRE team, so development teams can simply use those tools and pay per use at scale with bulk licenses.

The Party Bus service offering comprises multi-tenant environments for development, QA, and production in a "one-stop-shop" for DevSecOps. IL-2, IL-5, Secret, and TS/SCI environments exist or are in development. Specifically, Platform One will be supporting the following environments:

- AWS IL-2, IL-5, S (when available), S-SAP (when available), TS/SCI, TS-SAP (FENCES), and AWS Outpost.
- Azure IL-2, IL-5, S (when available), S-SAP (when available), and Azure Stack.
- On-premise/Edge VMWare vSphere.

Moreover, Platform One's offerings will continue to expand upon customer requests.

5.5.1 Compute and Networking

Pro: The Cloud Native Access Point is available on Cloud One to provide access to development, QA, and production enclaves at IL-2, IL-4, and IL-5 that use Platform One DevSecOps environments by using an internet-facing, cloud-native zero trust environment.

Con: Lack of Service Level Agreement (SLA). SLAs are planned.

5.5.2 Storage and Content Delivery

Pro: Storage services are bundled into capability packages. Separate database offerings are not available "á la carte."

Repo One—the DoD Centralized Container Source Code Repository (DCCSCR)—is the central repository for source code to create hardened and evaluated containers for the DoD. It also includes various source code open-source products and infrastructure as code used to harden Kubernetes distributions. All DoD activities that are creating containers that could benefit the DoD at an enterprise scale should publish their containers' source code in the DCCSCR by following the DoD Enterprise DevSecOps Reference Design, Container On-boarding Guide, and Container Hardening Guide requirements. All programs should evaluate any existing containers for reuse before creating a new container image.

Iron Bank—the DoD Centralized Artifacts Repository (DCAR)—is the DoD repository of digitally signed, binary container images that have been hardened according to the Container Hardening Guide coming from Iron Bank. Containers accredited in Iron Bank have DoD-wide reciprocity across classifications. Prior to creating a new container image, DoD programs should check if new container images already exist in DCAR and use the DoD signed containers whenever possible.

Platform One dedicated DevSecOps environment enable developers to build and deliver new hardened containers as needed for program-specific software (pay per use/container). Custom development services enable developers to build and deliver new and accredited custom software applications (microservices) by leveraging the Platform One pipeline and following Platform One's DoD Continuous Authority to Operate (cATO) (pay per app).

Con: Lack of SLA.

5.5.3 Deployment and Management

Pro: The Party Bus service offering includes a DevSecOps Platform, which is a collection of approved, hardened Cloud Native Computer Foundation (CNCF)-compliant Kubernetes distributions, infrastructure as code playbooks, and hardened containers that implement a DevSecOps platform compliant with the DoD Enterprise DevSecOps Reference Design, and its source code is hosted on Repo One.

The DevSecOps Platform includes the various mandated containers of the Reference Design including Elasticsearch, Fluentd, and Kibana (EFK), Sidecar Container Security Stack (SCSS), etc. Teams should leverage the Infrastructure as Code (IaC) available on the DCCSCR whenever possible and contribute back their code improvements to the DCCSCR whenever applicable.

Con: Lack of SLA.

5.5.4 App Services

Pro: Platform One provides pay-per-use services (e.g., Platform One Enterprise Chat for connecting developer teams and Platform One Exchange, a knowledge sharing service for software developers and engineers) and contract vehicles to facilitate teams' adoption and move to DevSecOps. The list of services will continuously evolve.

Con: Lack of SLA.

5.5.5 Risks

If there are no established SLAs, then application availability thresholds may not be met consistently.

5.5.6 Costs

The general cost is $2,000 per developer per month. This does not include special workload requirements such as support for artificial intelligence and machine learning services, and there is an additional cost if the project becomes a "mass consumer."

5.5.7 Summary of Pros and Cons

Platform One provides a wide range of products and services. Their approved ATO and the speed at which they can onboard a new project would be a benefit to NMO. However, Platform One does not appear to have any type of service level agreement with their tenants, leaving applications susceptible to downtime and performance issues without clear resolution procedures.

5.6 AWS GovCloud

AWS GovCloud comprises Amazon's regions designed to host sensitive data, regulated workloads, and address the most stringent Government security and compliance requirements. Amazon advertises AWS GovCloud as giving government customers and their partners the flexibility to architect secure cloud solutions that comply with the FedRAMP High baseline; the DOJ's Criminal Justice Information Systems (CJIS) Security Policy; U.S. International Traffic in Arms Regulations (ITAR); Export Administration Regulations (EAR); DoD Cloud Computing Security Requirements Guide (SRG) for IL-2/4/5; FIPS 140-2; IRS-1075; and other compliance regimes.

5.6.1 Compute and Networking

Pro: Amazon's Elastic Container Service enables customers to spin up containers as needed. These containers will then request a certain amount of CPU and memory, which is charged on a monthly bill. Notional rates are $0.0486/vCPU per hour (CPU) and $0.0053/GB per hour (memory).

Con: Higher level of technical knowledge required for managing instances required to avoid over-spending on non-essential resource utilization.

5.6.2 Storage and Content Delivery

Pro: Amazon offers many storage options that support different data access patterns. For example, assuming NIEM's storage requirement does not exceed 100GB, the monthly (Elastic Block Storage) cost would be on the order of $10 per month. AWS will charge ($0.15 per GB for first 10TB per month) for sending data outside its region. We were not provided usage statistics to estimate this cost.

Amazon's Relational Database Service (RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It is available on several database instance types, including PostgreSQL, MySQL, MariaDB, and SQL Server. Costs vary by instance type.

Con: Higher level of technical knowledge required for managing instances to avoid over-spending on non-essential resource utilization.

5.6.3 Deployment and Management

Pro: AWS has an extensive suite of tools for deploying and managing services from developing, building, and testing to deploying and monitoring. Everything is added to a monthly bill and allows an administrator to deploy services as needed. Services are controlled and managed in an access-controlled management portal.

Con: Higher level of technical knowledge required for managing instances required to avoid over-spending on non-essential resource utilization.

5.6.4 App Services

Pro: AWS has several relevant services to support user account registration and management, DevSecOps pipelines, monitoring apps in production, machine learning applications, etc. Examples of some relevant services and their notional costs include the following:

- API as a service
    - HTTP APIs $1.00 for the first 300 million
    - Caching starts at $0.02 per hour
    - WebSocket APIs $1.20 for the first billion
- AWS Lambda (used in CI/CD to run code without provisioning dedicated servers)
    - Requests $0.20 per million
    - Duration $0.0000166667 for every GB-second
- AWS CodeBuild (service that compiles and tests source code)
    - Linux price per build minuet starts at $0.005
    - Windows platform not available
- AWS Elastic Container Registry (managed Docker container registry)
    - Storage: $0.10 per GB-month
    - Data Transfer In: FREE
    - Data Transfer Out: up to 9.999TB per month and $0.155 per GB

Notably, these services are only indicative of one way to build a CI/CD pipeline. AWS offers several services that will allow NIEM to customize a CI/CD pipeline.

Con: Higher level of technical knowledge required for managing instances required to avoid over-spending on non-essential resource utilization.

5.6.5 Risks

If the system is assessed to be higher than IL-4, some services may not be offered. When the system is architected, the architecture should consider the cost to transmit data (between regions and/or zones) to avoid incurring outgoing data costs, and additional configuration and work may be needed to allow NIEM to work across platforms. If building a new environment, cyber authorization efforts (ATO) will be required at additional time and cost.

5.6.6 Costs

Notional costs are embedded in the sections above. Specific costs are dependent upon which services are utilized and at what level. Notional scenario used to compare this option against other COAs can be found in **Section 5.8**.

5.6.7 Summary of Pros and Cons

AWS offers one of the most comprehensive set of service offerings available. NIEM should have no problem finding all the services and resources needed to deploy a CI/CD pipeline and run containerized workloads. However, the lack of a platform with an already approved ATO means NIEM may need to go through an ATO process, which can take 6-12 months on average.

5.7 Azure Government

Azure Government comprises Microsoft's regions for hosting sensitive data, regulated workloads, etc. Microsoft advertises Azure Government as providing unparalleled flexibility and breakthrough innovation for U.S. government agencies and their partners by providing world-class security, protection, and compliance; modernizing legacy infrastructure to a flexible, hybrid environment; providing capacity when and where you need it; and enabling efficiencies and cost savings across departments.

5.7.1 Compute and Networking

Pro: Azure's Container Service enables customers to spin up containers as needed. These containers will then request a certain amount of CPU and memory, which is charged on a monthly bill. Notional rates are $0.0486/vCPU per hour (CPU) and $0.0054/GB per hour (memory).

Con: Higher level of technical knowledge required for managing instances required to avoid over-spending on non-essential resource utilization.

5.7.2 Storage and Content Delivery

Pro: Microsoft offers many storage options that support different data access patterns. For Block Storage, Azure only gives customers the option to choose predefined disk sizes, so the notional cost would be $19.71 per month for 128GB. For Object Storage, Azure Blob offers several Blob Storage tiers, with the Premium (first 50TB $0.188 per GB) and Hot (first 50TB $0.0296 per GB) tiers being the most practical options, considering the latency of the other tiers. Azure will charge ($0.109 per GB for first 10GB per month) for sending data outside its region. We were not provided usage statistics to estimate this cost.

Microsoft makes it easy to set up, operate, and scale a relational database in the cloud. It is available on different database instance types, e.g., PostgreSQL, MySQL, and SQL Server. Costs vary by instance type.

Con: Higher level of technical knowledge required for managing instances required to avoid over-spending on non-essential resource utilization.

5.7.3 Deployment and Management

Pro: Azure has an extensive suite of tools for deploying and managing services from developing, building, and testing to deploying and monitoring. Everything is added to a monthly bill and allows an administrator to deploy services as needed. Services are controlled and managed in an access-controlled management portal.

Con: Higher level of technical knowledge required for managing instances required to avoid over-spending on non-essential resource utilization.

5.7.4 App Services

Pro: AWS has several relevant services to support user account registration and management, DevSecOps pipelines, monitoring apps in production, machine learning applications, etc. Examples of some relevant services and their notional costs include the following:

- API Management starts at $0.26 per hour (Basic 1,000 requests/second)
- Azure Functions
    - Execution time $0.000016/GB-s after first 400,000 GB-s
    - Total Executions $0.20 per million executions after first one million executions
- Azure Pipelines

    - One Microsoft-hosted job with 1,800 minutes per month for CI/CD and one self-hosted job with unlimited minutes per month
    - $40 per extra Microsoft-hosted CI/CD parallel job and $15 per extra self-hosted CI/CD parallel job with unlimited minutes
- Azure Container Registry (Basic $0.208 per day)
    - 10GB Storage
    - Two web hooks
    - Geo Replication not supported

Notably, these services are only indicative of one way to build a CI/CD pipeline. Azure offers several services that will allow NIEM to customize a CI/CD pipeline.

Con: Higher level of technical knowledge required for managing instances required to avoid over-spending on non-essential resource utilization.

5.7.5 Risks

If the system is assessed to be higher than IL-4, some services may not be offered. When the system is architected, the architecture should consider the cost to transmit data (between regions and/or zones) to avoid incurring outgoing data costs, and additional configuration and work may be needed to allow NIEM to work across platforms. If building a new environment, cyber authorization efforts (ATO) will be required at additional time and cost.

5.7.6 Costs

Notional costs are embedded in the sections above. Specific costs are dependent upon which services are utilized and at what level. Notional scenario used to compare this option against other COAs can be found in **Section 5.8**.

5.7.7 Summary of Pros and Cons

Azure offers one of the most comprehensive set of service offerings available. NIEM should have no problem finding all the services and resources needed to deploy a CI/CD pipeline and run containerized workloads. However, the lack of a platform with an already approved ATO means NIEM may need to go through an ATO process, which can take 6-12 months on average.

5.8 Recommendation

Disclosure: Booz Allen Hamilton maintains strategic relationships with leading cloud service providers, including AWS and Microsoft Azure. Additionally, Booz Allen Hamilton provides programmatic and engineering contract support to the Air Force Cloud One and Platform One service offerings.

This environment analysis was based on several key dimensions (compute and networking, storage and content delivery, deployment and management, etc.). Based on these dimensions and the assumptions (**Section 2.3**), we determined MAX.gov, DI2E, and WMAAFIP are not viable alternatives. NIEM.gov may be a viable alternative as soon as November 2021, subject to several unknowns. Summarily, these environments lacked the ability to host containerized workloads or were not willing/able to provide hosting services. **Table 1** provides a comparison of the dimensions compared for viable hosting services and providers based on the following technical scenario.

The scenario is assumed for comparison purposes only and actual costs will vary based on number of users, services provisioned, and data storage required:

- (2) developers
- 100 Gb of data storage required
- IL4 controls/protections required for CUI information
- DevSecOps CI/CD pipeline required
- Assumes 24/7 operations (AWS and Azure bill in 15 minute or less increments)
    - Assume (4) vCPU's utilized 24 hours daily by up to 2 Dev's
    - Assume 30 GB RAM utilized 24 hours daily by up to 2 Dev's
- Costs not captured in this scenario:
    - Data leaving AWS & Azure
    - API service usage
    - Identity management if needed
    - Logging capabilities if needed
    - Container registry usage
    - AWS Lambda - variables
    - AWS CodeBuild – variables

	Platform One (RECOMMENDED)	AWS GovCloud	Azure Government
Compute and Networking	Cloud Native Access Point on AF Cloud One for IL-2/4/5 (Built on AWS, with Azure planned)	Elastic Container Service (Rates are $0.0486/vCPU per hour (CPU) and $0.0053/GB per hour (memory))	Azure Container Service (rates are $0.0486/vCPU per hour (CPU) and $0.0054/GB per hour (memory))
Storage and Content Delivery	Bundled into capability packages (Party Bus, Repo One, Iron Bank)	Elastic Block Storage ($10 /month up to 100 Gb)	• Block Storage ($19.71 /month up to 128 Gb) • Object Storage (Azure Blob) ($0.188 per Gb)
Deployment and Management	Fully DevSecOps CI/CD platform, CNCF-compliant Kubernetes and hardened containers	Extensive suite of tools for deploying and managing services from developing, building, and testing to deploying and monitoring. Pay for what tools/services are utilized.	Extensive suite of tools for deploying and managing services from developing, building, and testing to deploying and monitoring. Pay for what tools/services are utilized.

App Services	Pay-per-use, fully managed by Platform One administrators (Full list of services available, but Party Bus bundle meets initial NMO requirements)	• API as a service
		  ○ HTTP APIs $1.00 for the first 300 million
		  ○ Caching starts at $0.02 per hour
		  ○ WebSocket APIs $1.20 for the first billion
		• AWS Lambda (used in CI/CD to run code without provisioning dedicated servers)
		  ○ Requests $0.20 per million
		  ○ Duration $0.0000166667 for every GB-second
		• AWS CodeBuild (service that compiles and tests source code)
		  ○ Linux price per build minute starts at $0.005
		  ○ Windows platform not available
		• AWS Elastic Container Registry (managed Docker container registry)
		  ○ Storage: $0.10 per GB-month
		  ○ Data Transfer In: FREE
		  ○ Data Transfer Out: up to 9.999TB per month and $0.155 per GB
			• API Management starts at $0.26 per hour (Basic 1,000 requests/second)
			• Azure Functions
			  ○ Execution time $0.000016/GB-s after first 400,000 GB-s
			  ○ Total Executions $0.20 per million executions after first one million executions
			• Azure Pipelines
			  ○ One Microsoft-hosted job with 1,800 minutes per month for CI/CD and one self-hosted job with unlimited minutes per month
			  ○ $40 per extra Microsoft-hosted CI/CD parallel job and $15 per extra self-hosted CI/CD parallel job with unlimited minutes
			• Azure Container Registry (Basic $0.208 per day)
			  ○ 10GB Storage
			  ○ Two web hooks
			  ○ Geo Replication not supported

	Platform One (RECOMMENDED)	AWS GovCloud	Azure Government
Risks	Lack of SLAs	• If the system is assessed to be higher than IL-4, then some services may not be offered. • If building new environment, cyber authorization efforts (ATO) will be required at additional time and cost.	• If the system is assessed to be higher than IL-4, then some services may not be offered. • If building new environment, cyber authorization efforts (ATO) will be required at additional time and cost.
Estimated Costs to Sustain NIEM	$4K /month for Party Bus – Platform One	$1-4K /month for chosen AWS-native services	$1-4K /month for chosen Azure-native services
DevSecOps Pipeline	• Minimal labor cost associated with NMO onboarding into Platform One. • No cost associated with cyber authorization effort (Platform One-managed)	• $$$ for NMO management of DevSecOps tool suite, cyber authorization efforts (ATO), and process workflows	• $$$ for NMO management of DevSecOps tool suite, cyber authorization efforts (ATO), and process workflows

Table 1: Viable NIEM Hosting Environments

Platform One, AWS GovCloud, and Azure Government all offer a wide variety of hosting solutions. AWS and Azure offer the most comprehensive list of services and hosting solutions. With either AWS or Azure, NMO could host their entire DecSevOps pipeline and the containerized workloads required to serve new NIEM tools.

AWS and Azure offer expansive app suites and the most control over configuring and managing environments. The expansive app suites would give NMO the support to improve IT stability (**Section 4.1.1**), reduce complexity (**Section 4.1.2**) by relying on services, build new technical capabilities (**Section 4.1.3**), and scale to meet demands (**Section 4.1.3**). The control would give NMO the ability to highly customize the environment and optimize costs (**Section 4.1.2**). However, Platform One offers an authorized platform that NMO could use to build a DevSecOps pipeline and host applications.

If NMO prefers to have complete control over the environment, then AWS or Azure are suitable choices. If NMO does not require complete control and prefers to use an environment that is already authorized, then Platform One is a suitable choice, but stakeholders should establish service level agreements. In any case (Platform One, AWS, Azure), legacy tools such as SSGT need to be adapted to communicate with new tools via web services.

6. Execution Approach

NIEM will need to adapt its legacy tools to enable them to communicate with new containerized tools. The environment architecture should rely on a design that is as cloud agnostic as possible and rely on open source development.

NIEM will need to engage their cloud provider of choice (e.g., Platform One, AWS, Azure) to begin the onboarding process and to review the available products and services. The products and services provided by each of these providers would enable NMO to implement a CI/CD pipeline and serve new tools that support the NIEM community.