Managing Contracts as a Prime Contractor Involving Large IT Applications

Department of Homeland Security (DHS) Immigration and Customs Enforcement (ICE)

Contract Name: Enforcement Systems Operations and Maintenance Support Services (ESOMSS)

Contract #: W52P1J18DA062 / 70CTD021FR0000226 Contract Type: FFP & T&M

Date of Award: 09/24/2021 Period of Performance: 02/01/2022-01/31/2027

Point of Contact: Name, Phone, Email: Kapilesh “Bobby” Jerath, 202-732-7336, Kapilesh.Jerath@ice.dhs.gov

Covers TAs: 1, 3, 4, 5, 7, 8, 9, 10 Total Contract Value: $75,335,658.63

Project Overview and Complexity: Harmonia as the prime is responsible for more than 40 named complex applications critical for enforcement operations at the Southwest Border under the ICE Enforcement and Removal Operations (ERO) division that interface with other DHS and Law Enforcement branches, such as Customs and Border Protection (CBP), Cybersecurity and Infrastructure Security Agency (CISA), and Federal Bureau of Investigation. We created a state-of-the-art AWS architecture for the applications, using cloud native services, event-driven architecture, and serverless lambda functions to optimize cloud costs. ICE desires a culture of innovation, where ideas can be realized by field operators and quickly implemented in a matter of weeks, applying Agile, AWS cloud hosting, and DevSecOps (setting up Functional Quality Testing (FQT), UAT, and QA envs.). We support a complex environment with over 7.9k+ Law Enforcement Officers and ERO employee users in 200 domestic and 25 overseas locations. The applications we support use biometrics as the primary identification means during the booking process to reduce errors with person and encounter linking. To receive consistent reporting information, we are redesigning an event-centric processing model that uses events from the initial subject encounter and significant manipulation of database outputs. We are modernizing the EAGLE and Notice to Appear (NTA) systems that use biometric data – including ICE’s most crucial database, the Enforcement Integrated Database (EID) which is Salso a DHS-shared repository. This tool provides a person-centric data view in Alien Files using Biometric Identity Management to accurately link records to people. We integrate with multiple biometric exchanges: Integrated Automated Fingerprint Identification System (IAFIS), Automated Biometric Identification System (ABIS), National Crime Information Center (NCIC), and National Law Enforcement Telecommunications System (NLETS). The technology stack includes Java Platform Enterprise Edition and Oracle, and 100% of applications are AWS hosted.

Correlation/Cross-Walk to TAs and HRSA NPDB Program Requirements:

TA 1: Program and Project Management: We provide Agile Software Development support for O&M and modernization of user-centric (both for Border Agents and aliens tracked) mission-critical enterprise-level ICE Enforcement Systems. We provide oversight of the execution of Agile and DevSecOps-based requirements analysis, architecture modernization, code development, testing, configuration, deployment, administration, monitoring, and maintenance of each business segment of Enforcement Systems. We continuously manage fast-paced, data-driven projects for O&M and the modernization of the ERO application portfolio. Our work responds to the dynamic nature and growth in border crossing activities, implementing applications to support the full enforcement lifecycle for apprehension, detainment, and removal if applicable, and asylum case handling. We have 5 teams: Booking, Case, Data, LBM, and Special Projects (SWB). Each team has a Scrum Master assigned except SWB which has 2. Our teams manage unplannable corrective (e.g., break-fix) and preventive (e.g., zero-day patching) maintenance, and planned (timeboxed) enhancements. This allows a high degree of flexibility and responsiveness to changing priorities. We complete all on-demand work before completing the sprint and pull from the next highest priority item in the backlog according to the defined work-in-progress (WIP) limits. Each team has their own Jira backlog, and each backlog aligns the applications they support as Components and uses Nature of Work labeling to effectively manage and report on work types as well as priority classification. We groom stories for a second integrated backlog for the modernization project. Our team provides manual testing for multiple applications as part of continuous integration cycles. The output includes metric reports from multiple ICE-approved testing and reporting tools. Part of the definition of done for every Agile story, we only close a story after all functionality is met (per the acceptance criteria), all unit tests are written as passed, the code has been peer-reviewed, and a functional test has been written for every acceptance criterion. This mandatory step empowers the government and the development team to run regression testing at any point. This ensures that newly added functionality does not break existing functionality. Therefore, regression testing rarely finds defects and can be completed quickly and efficiently to ensure quality and on-time releases.

TA 3: DME Services: Like NPDB, we support a complex case management system for booking called Case Acceptance System (CAS) containing 22 applications. CAS is a mission critical system used to facilitate the jurisdictional transfers of individuals from CBP custody to ICE custody under the Enforce Alien Removal Module (EARM). The ICE ERO applications we took over upon transition-in used modern AWS cloud native features but were failure-prone due to essentially using a proprietary framework, having complex event message sequences in AWS, and not being amenable to rapid creation of new applications needed by ICE as the processing of cases at the southwest border was growing. The incumbent provided minimal assistance on transition-in. We continued O&M of the application portfolio. Our modernization has included rebuilding and expansion of the entire infrastructure pipelines for efficient and effective internal testing and UAT. As part of the rebuild and the new pipelines, we have also built containerized environments to enhance data security as well as building in “Blue/Green” containerized environments for both backend and frontend containers; this has never been successfully completed by any other contractor for ICE ERO. We also overcame minimal documentation about the environments (dev, test, production in AWS) and applications, which required extensive time and effort to accurately backward engineer and document the environments, CI/CD pipelines, and each application with meticulous details for all screens, data fields, types, elements, functions, and sequence/workflows. Almost all information that we display (and must protect) is PII or Personal Health Information (PHI) regarding processing, handling, and communication of aliens. The nature of the user interfaces enables agents and others to input, review and, when authorized, modify information at different points in time and ensure the information is consistently maintained in the EID database. As part of our discovery process to identify customer and user requirements and properly clarifying the correct business processes within ICE, we employ sequence, data flow, and business process workflow diagrams as part of our requirements analysis for the UI/UX. We design user-friendly, intuitive, customer-centric web applications using a human-centered design approach. We apply DHS and ICE standards and guidance for the UI design to be 508 compliant. Prior to production updates to any UI, applications go through review with the ICE DHS Quality Assurance (QA) group as a final confirmation of compliance, including Section 508 compliance. We assure that the event-driven applications in AWS commit transactions before providing an agent with an acknowledgement (which was not guaranteed in the implementation we transitioned into)

Our Business Systems Analysts and Developers create and maintain all artifacts associated with the graphical user interface (GUI) and UX. The primary tools and artifacts we use include:

• Style Guide: Ensures consistency and provides guidance to develop visual components in the system, including navigational elements, color schemes, and layout

• Wireframes: Visual depiction (or Hypertext Markup Language [HTML] mockup) of UI within the system tied to Jira stories with corresponding business rules, range of user actions, and the responsive scenarios

• Usability Assessment: Assessment of system usability from user testing, analysis of performance monitoring logs, review of previous assessments, and comparison of best design practices including application of the U.S. Digital Services Playbook (who with GSA 18F collaborated to create the USWDS), with an overall set of recommendations to improve UI/UX.

We implement microservices to enable more modular updates, simplified maintenance of the code base, better scalability, and faster integrations. We use DevSecOps for faster deployments without taking the system down for many production updates. We perform integration with other DHS systems by consuming events and using their APIs, and by generating events for other systems to use along with developing APIs for external users. In the event processing architecture, we store data in PostgreSQL DB and DynamoDB, then transform it to feed into the main Oracle DB (for other systems’ use). Our modernization enhances the benefits of Event-First Architecture by rapidly adapting ERO applications to changing requirements and regulations.

Regarding quality, we develop, conduct, integrate and manage all testing needed to ensure production-ready development through our lean Agile test methodology by applying whole-team testing; continuous testing; combining Test-Driven Development (TDD) with in-sprint Behavior Driven Development (BDD) testing to identify system-level defects from a business flow level; Acceptance Test Driven Development (ATDD) to ensure that software behavior, at story and feature levels, meets customer/user expectation; creating reusable version-controlled test automation scripts and test environment provisioning scripts using infrastructure as Code (IaC); and cross-system testing including upstream and downstream systems, testing middle tier (asynchronous) services, business processes, business rules, and business flows. As part of the definition of done, stories cannot be closed until all functionality is met as described in the acceptance criteria, all unit tests are written as passed, code has been peer reviewed, and an automated functional test has been written for every acceptance criterion. This mandatory step empowers the government and development team by enabling them to run automated regression testing at any point ensuring newly added functionality does not break existing functionality, meaning manual regression testing rarely finds defects and can be completed quicky and efficiently to ensure quality and on time releases.

TA 4: O&M Services: We provide support for more than 40 named applications (modernizations in progress/planned) including Tier 2/3 Helpdesk support, oversight of the execution of Agile and DevSecOps-based requirements analysis, architecture modernization, code development, testing, configuration and change management, deployment, administration, monitoring, and maintenance of each business segment of Enforcement Systems. We apply DevSecOps for faster deployments without taking the system down for any production updates. This is done through our teams having achieved Agile Maturity approval for Team Managed Deployments (TMD). Frequent releases allow us to deliver reliable and predictable increments of business value to the customer throughout the development lifecycle, leveraging state-of-the-art CI/CD DevSecOps automation to establish a harmonic cadence to synchronize release schedules with business schedule and planning cycles. Release of maintenance code will normally occur at sprint completion (except for break-fixes); the release will be in the form of a fully tested and deployable release (even if there is no plan to deploy to production). We manage and support ICE ERO’s highly complex central database that interfaces directly or indirectly with 35 components at ICE, USCIS, CBP, DOJ, NPPD, DoS, SSA, DOD, and other law enforcement organizations. We provide database management and interface artifacts including Data Model (an entity relationship model of the databases and views including color coding to depict functional categorization, grouping by application, tables and column names, primary key/foreign key relationships, data types, and size limitations); Data Asset Catalog (inventory of services, interfaces, source/destination, functionality, business contacts, triggers and associated business rules, indexes, and stored procedures); Data Management Plan (our plan to continually improve the use and management of data assets including assessments of evolving technology trends and their potential benefit in implementation [e.g., PostgreSQL DB, Dynamo DB, data quality, search and storage, and alternative database technologies]); Oracle and PostgresSQL Database (major and maintenance releases); DB support for developing database queries, batch jobs, and stored procedures with Procedural Language/Structured Query Language (PL/SQL) and Not Only SQL (NoSQL), Data Marts, Database Services and integration; Database Security Scans (authenticated/unauthenticated) to identify potential database security vulnerabilities such as SQL injection, excessive user and group privileges, unpatched databases, default/missing passwords and other database related vulnerabilities/issues; Tier 2/3 support, patching, account creation/database access, and data fixes. Between 5/2022 – 3/31/2024, we maintained staffing levels at 98.56%, completed several numerous software migrations and upgrades, completed approximately 39,000 Jira tickets and 53,000 story points, completed 412 releases, and supported a total of 44 outages (partial or full/ planned & unplanned), as well as all O&M and Tier 2/3 support activities.

TA 5: Forms and Correspondence Systems for Users: We are replacing a paper-based system within the NTA MicroApp, which will transform services for ICE agents who must currently print, sign, fax (for wet signatures) or mail paper forms. Our new web-based application that we developed applies biometric information including fingerprinting and photographic identification via facial recognition drawn from interfaced systems (e.g., EAGLE) to replace a paper-based process with a fully digital workflow. We account for transitional techniques (e.g., legacy records consolidation) as we update the central database and repository – where many forms processed previously were never digitized. We are digitizing and transitioning hundreds of paper forms to a storage repository. This includes transitioning the workflow of how to pull and save database data, with a printing option for forms. We implement stories, automating key steps in the credible fear and asylum referral lifecycle that save officers time by reducing case handling durations and improving data quality and subject outcomes. This reduces rejection rates and automates and simplifies rejecting bond cancellations. This process occurs frequently and requires offline email communication/coordination. We are transforming reporting/collection processes for program operation metrics. We consolidated sources across the program to design live, near-real-time presentations for ICE leadership to display all program metrics and time-based trends in a web-based dashboard for a single view of program health.

TA 7: Security Services: We ensure systems remain secure and maintain security posture throughout the lifecycle of the IT systems/applications recertification and reaccreditation/reauthorization. The reauthorization process may involve testing/assessment of all or some of the DHS 4300A policies/requirements and NIST 800-53 controls (including vulnerability scans). We develop, maintain, and provide all support necessary to complete testing/assessment, including annual ICE failover testing. We certify the IT systems/applications supported are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC) and US Government Configuration Baseline (USGCB). We ensure standard installation, operation, maintenance, updates, and/or patching of software do not alter configuration settings from the approved FDCC/USGCB configuration and remain compliant with policies and guidelines. We follow OMB memorandum 07-18 and use Security Content Automation Protocol (SCAP) validated tools with FDCC/USGCB scanner capability to certify products operate correctly with FDCC/USGCB configurations and do not alter FDCC/USGCB settings.

TA 8: Transition: We transitioned support services in 60 days following award. We performed sourcing, hiring, clearing, and staffing of more than 100 staff, maintaining a pipeline of three staff for risk mitigation of staff attrition.

TA 9: Other Contract Requirements: Harmonia satisfies contract requirements to work with the ICE Office of Information Governance and Privacy and the Office of the Chief Information Officer to ensure that privacy documentation is kept on schedule, answers to questions in any privacy documents are thorough and complete, all records management requirements are met, and questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion. Harmonia complies with FAR 52.224-1 Privacy Act Notification (APR 1984), 52.224-2 Privacy Act (APR 1984), FAR 52.224-3 Privacy Training (JAN 2017), and privacy-related Homeland Security Acquisition Regulations (HSAR). We follow ICE’s System Lifecycle Management (SLM) process and comply with all deliverables subject to a tailoring plan for each major system release, and with the ICE SLM Handbook, ICE Agile/DevOps Playbook, and the ICE Web Standards and Guidelines among other guides. In addition, we follow requirements from elevation to the DHS Systems Engineering Life Cycle (SELC) as identified by ICE.

TA 10: Baseline Security Requirements: We are responsible for ensuring ICE ERO systems maintain privacy of PII data under our Privacy Lead, and providing DHS support for the PTA, PIA, SORN, and other supporting documentation to support privacy compliance. Our work uses ICE's most crucial database, the EID, which is also a DHS-shared repository, and we maintain a person-centric data view in Alien Files that uses the fingerprint identification number (FIN) to accurately link records to people. We integrate with multiple biometric exchanges: Integrated Automated Fingerprint Identification System, Automated Biometric Identification System, National Crime Information Center, and National Law Enforcement Telecommunications System. We perform security control design and annual assessment, assessing the DHS 4300A Sensitive Systems policies and requirements, and NIST 800-53 controls (e.g., vulnerability scans).

Hosting and Architecting Application(s) In AWS (Or A Comparable Cloud) Cloud: We provide Agile DME and O&M support of 25 user-centric, mission-critical enterprise ICE Enforcement Systems running more than 40 applications operated within AWS GovCloud East and West. Most applications are FISMA High and contain PII concerning migrants.

Experience With Data Analytics and BI Tools: The ICE ERO system collects information continuously starting with biometrics from the alien booking process via the EagleBRS, and correlates information in the application portfolio we support. We support data analytics and reporting for assignments to detention centers, court events and hearings, logistics and transportation events, health records, food and meals served, and communications. The continuous data ingestion on aliens who violate laws leads to information that must be reconciled and visualized according to an information architecture that we support via various reporting methods. Data includes case management, booking, notices (e.g., NTA), bond management, logistics, and detention information.

Application Development Using Java and The Agile Processes Used to Successfully Adapt to Changing Needs Across Multiple Value Streams: We run a total of 5 Agile DevSecOps teams (made up of 13 FTEs per team) supporting Java, Oracle, AWS architecture, and other technologies which are primarily assigned to addressing O&M issues, followed by delivering multiple value streams related to the multiple business units in ICE according to changing priorities at the Southwest Border and developing various applications within ICE’s AWS environment. We support the value stream originating from Solution Integration, Booking, Case Management, Logistics Management & Bonds Management, and Data Management. For example, we supported reaching production for two high priority applications, the Notice to Appear and the Credible Threat applications. Two of our DevSecOps teams concurrently support value streams from Special R&D enforcement and technical projects.

Use Of Open-Source Software and Technologies: The portfolio is architected using open-source technologies and cloud-native services such as Kafka (event streaming), ApacheMQ, AWS Lambda (serverless event-driven computing), Kinesis, Event Bridge, S3 Event Lake, DynamoDB, PostgreSQL, and API Gateways (on-demand scalability with highly secure PII data capture, storage, reconciliation, and reporting). In development, we use AngularJS, Java, and Spring Framework (in legacy code we are modernizing). We use Ansible, Chef, Docker, Jenkins, OpenShift, SonarCube, Terraform, and Vault to build, run, and scale applications using CI/CD.

DHS ICE Enforcement Systems O&M Support

Most recent CPARS provided below.