Stealth Solutions, Inc.
Response
to
United States Coast Guard

For

Mariners Credentialing and Documentation Program (MCP)

Solicitation 70Z0G325QOIPL0001

Phase I – Factor 2: Technical Approach

April 14, 2025

Submitted electronically to:

Brenda E. Oberholzer
email: Brenda.e.oberholzer@uscg.mil
Cora B. Good
email: cora.b.good@uscg.mil
Brian J. Eichelberger
email: brian.j.eichelberger@uscg.mil

Submitted by:

Rahul Sundrani, President
46191 Westlake Dr. #112
Sterling, VA 20164

GSA Contract# 47QTCA22D0053

Factor 2: Technical Approach

The U.S. Coast Guard (USCG) demands a unified, robust, adaptable, and secure technology solution to support national security and economic prosperity driven by the multi-dimensional mariner community. NAVITA MCP implementation must address and overcome current challenges including lack of agility, lengthy and costly system changes, inefficient system integrations, poor customer experience, and limited modern capabilities. Its goals are automation-driven efficiency, real-time accuracy, enhanced user experience, and reduced costs.

The ***NAVITA MCP implementation*** is led by ***Stealth Solutions*** as the Small Business Prime Contractor, with strong tier one subcontractor support from ***ICF*** and ***VivSoft***—collectively known as ***Team Stealth***. This strategic partnership was purpose-built to meet and exceed the requirements of the ***USCG Mariner mission***, combining deep expertise in digital transformation, cloud solutions, Salesforce expertise, DoD Impact Level 4 (IL4/IL5) experience**,** and agile implementation to deliver a modernized mariner credentialing system.

Team Stealth brings a proven track record of delivering rapid, secure, scalable, and IL4/IL5-compliant solutions across both civilian and DoD agencies. ***Stealth Solutions***, a trusted Salesforce Consulting Partner, specializes in modernizing legacy on-premise systems by migrating them to secure, reliable, and scalable FedRAMP-certified cloud-hosted platforms designed to support thousands of users and high concurrency. ***ICF***, a Salesforce-verified partner, delivers the highest level of experience, quality, and expertise as a **Salesforce Summit Partner** and **Public Sector Expert** across the Salesforce ecosystem, including MuleSoft and Tableau. Recognized as an Agentforce-ready organization, ICF possesses the experts and resources to support any organization in implementing Salesforce AI innovations. With **110+ Salesforce-certified experts**, **400+ certifications**, and **100+ completed projects**, ICF offers robust implementation experience, skilled federal experts, and certified technology SMEs to deliver Salesforce solutions efficiently and effectively. ***VivSoft***, a small business IT systems integrator, excels in implementing open-source and emerging technologies, supporting high-impact programs across the **U.S. Air Force**, AETC, Cyber Warfare Mission Systems, and FDIC, with direct experience complying with **DOD IL4/5** requirements through its Platform One program. With certified expertise and deep experience in the Salesforce cloud platform, Team Stealth has successfully executed complex, FedRAMP High deployments, demonstrating its ability to meet and exceed contractual commitments. Prior experience includes rapid delivery of solutions for loan management, opportunity management, grants processing, and case management—closely mirroring the goals of the MCP BPA. Backed by a strong foundation in digital transformation, cloud enablement, and IL4/IL5 Agile implementation, Team Stealth is well-positioned to modernize the U.S. Coast Guard's mariner credentialing system. Figure 1: Transforming Mariner Credentialing with a Secure, Intelligent, and Scalable Solution—Powered by Salesforce and Implemented by Team Stealth-illustrates our end-to-end modernization approach, showcasing how our proven and collective capabilities to meet USCG's mission needs.

Team Stealth: DoD-Grade Cloud Modernization

Led by **Stealth Solutions** with **ICF** and **VivSoft**

- ✓ Secure **low-code/no-code** solutions in **DoD IL4/IL5 environments**
- ✓ Proven **ATO success** and **Agile delivery**
- ✓ **Legacy-to-cloud** migration expertise
- ✓ Scales to **125,000+ users** and **20,000 concurrent sessions**

Team Stealth recommends ***Salesforce*** as the optimal platform for MCP due to its ***low-code/no-code architecture***, enabling agile development, rapid configuration, and cost-effective updates. With unified capabilities in ***CRM, workflow automation, case management,*** and ***IL5 security***, Salesforce delivers unmatched scalability and performance—far exceeding traditional platforms. Leveraging proven success across DoD and civilian agencies, Team Stealth brings deep Salesforce expertise aligned with USCG's iterative development strategy, ensuring seamless integration of the ***Mariner Credential Program (MCP)*** and ***Vessel Documentation System (VDS)*** to support over 650,000 vessel documentation records annually without performance degradation. Salesforce is already in use at USCG—powering ***AUXData, Gangway, MISLE Enforcement,*** and ***MISLE Adjudication***—with multiple ***ATOs*** and integrations with ***FSMS, Direct Access,*** and ***gocoastguard.com***, offering a secure, scalable foundation. By building on this proven Salesforce ecosystem, Team Stealth ensures the MCP system is deployed reliably and at scale—delivering measurable improvements in mission impact, operational efficiency, and cost savings. Click/scroll to Figure 2: MCP Implementation on Salesforce: Accelerating Mission Impact, Efficiency, and Cost Savings to see how strategic priorities translate into real-world outcomes based on government benchmarks.

Architecture and Licensing Model

As depicted in Figure 3. Proposed MCP System Architecture, Team Stealth recommends ***Salesforce Public Sector Solutions (PSS)*** for the MCP System as it is tailored for government workflows and offers ***pre-built apps and low-code/no-code tools*** like Omnistudio, Action Plans, Document Tracking and Approvals, and Business Rules Engine to automate credentialing. The **PSS Licensing and Permit Management application** is particularly well-suited for MCP, as it streamlines the credentialing lifecycle from application submission through review, issuance, and renewals.

Team Stealth brings direct experience implementing PSS in licensing, registration, and workforce systems—including the **CHAMPS system** (Contractor Hiring and Management Processing System) for USAID, which closely mirrors mariner credentialing with role-based access, application verification, secure documentation, and workflow management. We have also delivered **secure, FedRAMP-ready cloud-native solutions** with credentialing-like functions across federal programs, including the Prosper Africa Tracker (PAT) for USAID, grants management systems for the U.S. Department of Veterans Affairs, DC Department of Health, and Inter-American Foundation, and the Home Energy Rebate Program for the Department of Energy, which went live in just three months. Each of these systems supports high-volume application intake, secure data handling, workflow automation, and self-service portals—demonstrating our ability to deliver scalable, compliant solutions aligned with MCP requirements.

Using ***Lightning App Builder and Flow Builder***, MCP system will automate business processes, reducing credential processing time while ensuring flexibility for future updates. The complete solution will comprise a ***Digital Experience Site***, the Salesforce mobile app, and internal applications. The entire application will be deployed on ***Government Cloud Plus*** and integrated with DISA BCAP, allowing MCP system to function as an extension of NIPRNet. Salesforce Government Cloud Plus, authorized at ***FedRAMP High (IL4/IL5)***, meets DOD security requirements, ensuring secure handling of CUI and mission-critical workloads. While Salesforce's

FedRAMP package covers infrastructure and platform-level controls, Team Stealth brings extensive expertise in implementing application-level security.

As part of Team Stealth's proposed solution approach, mariner users will initiate the credentialing process through a ***PSS License and Permit Experience Cloud Site***, creating accounts via **Login.gov**, a NIST 800-63-3 compliant identity proofing service. This portal enables registered mariners to submit applications, track progress, upload documents, and communicate with USCG staff, while both registered and unregistered users can submit inquiries. For a mockup of the portal, click/scroll to Figure 4. Mariner Portal: Streamlining the End-to-End Credentialing Process. ***Omnistudio*** will be used to configure a guided application process, leveraging out-of-the-box (OOTB) tools such as ***action plans*** to ensure that all steps are completed in a structured sequence with designated priorities, deadlines, and task owners. Additionally, ***document checklist items*** will be incorporated to streamline submission, review, and approval of key application components, including the physical exam report, drug test results, proof of training, and sea service. ***Action launcher*** will also be employed to facilitate quick follow-up if any application is missing required information. The system will allow mariners to withdraw their application at any stage of the process but will retain the canceled application for historical purposes. Mariners will be able to log their training using the OOTB ***Training Course objects***, while details related to at-sea and vessel-specific experience will be captured in ***custom objects***. By making use of the ***Business Rules Engine***, ***Decision Matrices***, and ***Expression Sets***, the MCP system will also be able to automatically calculate all fees due for an application. The Digital Experience site integrates seamlessly with USCG's internal application workflows, ensuring that submitted applications are automatically validated, routed, and approved. To facilitate proxy users acting on behalf of mariner users, we will build Apex solution and a data model to support it.

Other external users, including medical providers, vessel operators, and training providers will also be able to access the external portal to complete tasks such as validating mariner information, uploading documents, and submitting training courses for approval. ***Role-based access control*** (RBAC) will ensure that different user types see only data that is relevant to their business use.

Thinking toward the future, Team Stealth can leverage ***Agentforce*** in mariner portal to streamline the mariner credentialing process. By integrating AI-powered chatbots and automation, mariners can receive real-time assistance on application requirements, document submissions, and status updates without long wait times. Intelligent case routing ensures complex inquiries reach the right specialists, while self-service options reduce call volume by allowing mariners to check their application status and resolve common issues independently. AI-driven analytics help the USCG optimize processing times, enhance user experience, and improve overall service efficiency.

For internal users (i.e., USCG users), a ***custom Lightning app*** will be built to manage applications from initial submission to issuing credentials. Internal users will have a 360-degree view of the mariner's account, applications, evidentiary documents, and verifications. ***Flows***, including prebuilt PSS licensing and permitting flows, will be configured to review and adjudicate applications as well as handle appeals/reconsiderations. Furthermore, the internal app will allow USCG users to review and approve course training offerings, manage exam questions, and run analytics.

Salesforce categorizes users as either internal and external, and provisions licenses based on these categories. **Internal users are employees of U.S. Coast Guard who have a USCG email address. External users are external stakeholders that access Salesforce for an experience or service provided by the U.S. Coast Guard (e.g., mariners, training providers). External users do not have a USCG email address.** Team Stealth recommends the following licenses/products:

Recommended License Type	User Group	Est. Number of Licenses	Rationale/Benefit to the Government
Government Cloud Plus (GovCloud+)	Platform level	1	This is a dedicated, high-security environment within Salesforce's cloud infrastructure designed specifically for **U.S. federal** and supports **DoD IL5** requirements.
Public Sector Foundation – Advanced	Internal USCG users	600	This is the base PSS license for all internal users. Anyone who needs access to internal data (e.g., to review applications, to view analytics, to review and approve training courses) and/or with a uscg.mil email address will require this license.
Customer Community Plus for Public Sector - Login	External mariner users	~35,000 logins/month	Customer Community Plus for Public Sector is an Experience Cloud–based license that includes permissions for constituents to access Public Sector Solutions functionality. Also allows users to run reports on their own information. Login-based (pooled) licenses count one login per user per day, regardless of how many times they log in, avoiding the need for seated licenses.
Public Sector Application Forms	External mariner users	20,000	Experience Cloud—based license that includes permissions for constituents to access Public Sector Solutions for License, Permit, and Inspections Management. Licenses provide a quantity of 20,000 of user and permission set licenses needed for Application Mgmt.
Partner Community Login	External partner users (e.g., medical providers, marine employers)	~6,000 logins/month	External partner users who are part of an organization (e.g., a maritime academy) will use this license type to manage their information (e.g., course information/enrollments) within the mariner portal., Login-based (pooled) licenses count one login per user per day, regardless of how many times they log in, avoiding the need for seated licenses.
Salesforce Shield	Platform level	1	Salesforce Shield ensures data security, compliance, and auditability, aligning with DHS, DoD, and USCG cybersecurity mandates. Platform Encryption protects sensitive mariner data, meeting DISA IL5 security requirements. Event Monitoring tracks user activity for real-time threat detection, while Field Audit Trail logs credential modifications for compliance audits. Shield supports Zero Trust principles, ensuring secure, compliant, and resilient credentialing for USCG.
CRM Analytics (includes Tableau Core, Creator, and Data Mgmt.)	Platform level	1	CRM Analytics provides AI-driven insights into credentialing trends, risk assessments, and workflow bottlenecks. By analyzing historical data on credential issuance, processing times, and compliance violations, it will help USCG identify areas for improvement. Dashboards and automated reports enable real-time monitoring of backlogs, approvals, and security risks, ensuring system efficiency and resiliency to operational demands.
MuleSoft Anypoint Platform	Platform level	TBD	MuleSoft Anypoint Platform will be MCP system's integration backbone, enabling seamless connectivity between Salesforce, legacy systems, and external data sources. It supports real-time

			APIs, and batch data synchronization for migrating millions of credentialing records, and event-driven data flows to maintain credential status accuracy and compliance. Team Stealth recommends an API-first approach with reusable APIs to provide consistent, well-documented interfaces. Our team will assess integration needs, size APIs, and evaluate vCore capacity, while prioritizing scalability and interoperability, avoiding point-to-point integrations. We understand that USCG currently has MuleSoft licenses which are based on vCore capacity. Our team will identify specific MCP integration use cases and decompose them into granular APIs. We will size these APIs and work with USCG to determine the amount of vCore capacity needed and if an increase to their existing licenses is necessary.
Own for Salesforce	Platform level	N/A	To meet the backup requirements (i.e., full daily backups, rapid roll-back to prior state, prompt recovery, and off-premises storage), Team Stealth proposes procuring Own for Salesforce. Own is a FedRAMP-approved cloud solution that secures, archives, and recovers data using to ensure operational continuity, data integrity, insider threat mitigation, zero trust security, proactive monitoring, and data preservation with customizable retention policies for data archives. Additionally, Own for Salesforce can accelerate development by seeding sandboxes with data for safe environments to develop, test, and train users.
Appinium	Platform level	TBD	Appinium, is the only native third-party learning management system (LMS) on the App Exchange. We will use Appinium as the provider for the exam module solution.

Agile Program Management

Team Stealth utilizes an ***agile scrum*** methodology lead by a Certified ScrumMaster to approach all aspects of the SDLC. Team Stealth's approach begins by first providing client with an "agile primer" to ensure that everyone has a common understanding of the scrum framework. Team Stealth emphasizes an integrated agile approach that includes the participation of the scrum developers, the government product owner, and other essential stakeholders for all scrum ceremonies to include sprint planning, daily scrum, sprint review, sprint retrospective, and backlog refinement. By using agile practices, Team Stealth will be able to deliver iterative releases and act quickly on government feedback. Moreover, developing in sprints allows us to accommodate ad hoc tasks and urgent data requests as part of routine backlog refinement. During the unprecedented COVID-19 crisis, Team Stealth leveraged Agile processes to develop a minimum viable product in just six days for the U.S. Treasury. This rapid deployment facilitated the disbursement of critical CARES Act financial relief packages, providing essential support in a time of great need to help stabilize the economy. Additionally, Team Stealth's organizational change management approach for MCP ensures a smooth transition, equipping staff for adoption before go-live. Combining leadership support, clear communication, targeted training, and a train-the-trainer model, we enable USCG super users to scale knowledge transfer efficiently. Our change management lead drives internal marketing and engages "change champions" to normalize the transition.

At the end of each sprint, Team Stealth will hold ***sprint reviews*** to demonstrate completed work to stakeholders, gather feedback, and ensure alignment with expectations. These reviews enhance

transparency, engagement, and responsiveness by allowing quick incorporation of stakeholder input into future sprints. Additionally, the team will conduct ***sprint retrospectives*** with the government product owner and key stakeholders to reflect on performance and identify improvements. This structured discussion helps recognize successes, address challenges, and refine processes for future sprints. Both sprint reviews and retrospectives are essential for promoting continuous improvement, enhancing collaboration, and ensuring efficient workflows. By maintaining an iterative feedback loop, the team can adapt quickly, improve product quality, and drive project success.

Team Stealth approaches ***user story development*** with framework of standardized questions presented in a visual collaboration environment. The questions *(What is the desired outcome? Who is this for? What value will this create? How much effort will this take? What problem are we trying to solve?)* are phrased in such a way to invite open discussion. The use of Lucidchart, as depicted in Figure 5. Team Stealth's Standardized User Story Refinement Board, in this activity allows all participants to contribute ideas freely and then work together to synthesize a shared vision for the user story and its acceptance criteria. All user stories are added to the ***product backlog***, which is prioritized by the business product owner. The MVCR backlog would comprise a prioritized subset of stories from the complete product backlog for the initial release. The scrum team and product owner collaborate during sprint planning to choose a sprint goal and select the stories required to meet that goal. Team Stealth uses a story point estimation guide developed over years of experience and across numerous projects to assign baseline points to common Salesforce development tasks. By using this guide, we can accurately quantify the effort required for each user story, enabling effective capacity management and reliable sprint delivery. This approach drives quick delivery by making it easier to prioritize, plan, and deliver MVPs that maximize business value. It has also resonated strongly with government product owners at agencies like ***USAID, DC DOH***, and the ***VA***.

The ***quality assurance (QA) team*** is fully integrated with the development team from day one and a test plan is drafted before development begins. Q***uality control practices*** are enforced by our DevSecOps framework using the following tools ***Apex Test Framework, Checkmarx*****,** and ***Tricentis NeoLoad*** to automate testing, security compliance, and performance validation; and ***ANDI, Wave, JAWS, Axe DevTools*****,** and ***NVDA*** to ensure compliance with Section 508. The testing scope encompasses both functional and non-functional ***test events***, covering unit, system, regression, end-to-end, acceptance, usability, accessibility, compatibility, security, and recovery tests. Testing begins with the first sprint and continues throughout the lifecycle of the project.

Usability testing with real mariners ensures the system is intuitive and meets practical needs. By interacting with prototypes, they provide feedback to identify and fix issues early, leading to a user-friendly final product. A more intuitive system simplifies the transition, reducing training and change management efforts. Similarly, we will test key internal workflows with USCG staff to optimize the system for all users. This comprehensive approach enhances user satisfaction, improves adoption, and ensures efficient, effective implementation. Effectively managing ***technical debt*** is key to a project's long-term sustainability. Each sprint, we will identify, size, and assess technical debt items, prioritizing them alongside new features in the sprint backlog. By dedicating part of each sprint to addressing technical debt, we can systematically reduce it, preventing accumulation and maintaining a clean, scalable codebase. This proactive approach

improves code quality, enhances development efficiency, and ensures adaptability to evolving requirements and technologies. Regularly managing technical debt fosters a more resilient and sustainable project.

Security

Team Stealth brings extensive cybersecurity expertise from working across DoD environments at **IL2, IL4, and IL5**, which directly informs our **security-first approach** for the MCP system. At Platform One (P1), we've supported over 90 applications annually, providing end-to-end support for Certificate to Field (CtF), Authority to Operate (ATO), and Continuous ATO (cATO). Our team collaborates with the Cyber Accreditation Team (CAT) and Mission DevOps (MDO) to conduct vulnerability assessments, penetration testing, and implement quality gates within CI/CD pipelines—aligned with Zero Trust and DevSecOps principles.

We secure every layer of the stack, applying controls aligned with NIST 800-53 Rev. 5, and tailored guidance from 800-190 (containers), 800-204 (microservices), and 800-207 (Zero Trust). Our DevSecOps model uses policy-as-code and compliance-as-code to ensure continuous alignment with DoD's SRG and CMMC. We employ tools like Twistlock, Kubernetes auditors, SBOM tracking, and CVE scanning via NVD to maintain security hygiene. Real-time monitoring, alerting, and incident response are supported through Splunk-based SIEM/SOAR platforms.

For MCP, we propose delivery on Salesforce Government Cloud Plus—a FedRAMP High-authorized, IL4/IL5-compliant platform. This enables USCG to inherit the majority of NIST 800-53 controls, while Team Stealth implements the remaining application-specific configurations using Salesforce-native security features. These include Salesforce Shield for encryption, audit trails, and event monitoring; CAC/PIV for internal authentication; and Login.gov for external users—all integrated with MFA and least-privilege access control. Data is encrypted in transit and at rest (AES-256). APIs are secured with TLS 1.2+, mutual authentication, client certificates, and optional PGP encryption, with all access events logged and fed into Splunk for centralized visibility and response.

Our cybersecurity framework—shaped by both DoD and civilian agency experience—is proactive, repeatable, and proven. Notably, we led the Department of Transportation's Digital Transformation Center (DTC) in achieving a platform-level ATO at FISMA Moderate by leveraging Salesforce FedRAMP inheritance and implementing a governance framework that enabled rapid ATOs at the program level. We bring this same approach to MCP—ensuring it is secure by design, compliant from day one, and resilient against evolving cyber threats, delivering long-term mission assurance and operational confidence to USCG.

Scalability

The Salesforce platform is purpose-built for **enterprise-scale operations**, supporting high concurrency, large data volumes, and mission-critical workflows. Its **multi-tenant architecture** leverages distributed caching, asynchronous processing, and event-driven design to handle surge demand. Team Stealth has successfully delivered solutions supporting over **125,000 users** and **20,000 concurrent sessions**, demonstrating our ability to meet the performance needs of the **MCP system**.

Deployed within **DISA IL4/IL5-compliant environments**, Salesforce **Hyperforce** provides elastic compute capacity while maintaining data isolation and compliance. This allows the MCP system to scale dynamically during peak credentialing cycles without compromising security or availability. To support scalable integrations, Team Stealth employs the **MuleSoft Anypoint Platform**, avoiding point-to-point connections by implementing **governed, reusable APIs**. Using **MuleSoft API Manager**, we enforce thresholds for payload size, transaction volume, and concurrency—preventing downstream bottlenecks and enabling independent scaling of services.

Salesforce supports a **99.9% uptime SLA** through **multi-zone redundancy**, **active-active failover**, and continuous monitoring within IL4/IL5-certified U.S. data centers. It consistently achieves **MTBF > 4,450 hours**, **MTTR ≤ 12.5 hours**, and **SRO > 0.85**—exceeding federal performance standards.

To ensure optimal performance, Team Stealth will use **Salesforce Performance Profiler**, **Optimizer**, **JMeter**, and **Neoload** to simulate load, stress-test APIs, and validate Lightning component responsiveness. This ensures the MCP system remains responsive, reliable, and compliant at scale.

Supportability

Team Stealth will work with the USCG in-house support desk to implement a tiered support model using tools such as ServiceNow. **Tier 1** handles routine issues (e.g., password resets) via SOPs; **Tier 2** manages more complex requests. Issues escalated to **Tier 3** are handled by Team Stealth's support team—developers, admins, testers, and functional leads—who perform root cause analysis, replicate issues in test environments, and classify them as defects, enhancements, or features for the agile backlog. **Tier 4** covers external dependencies such as vendor-related issues.

We apply the same development rigor to production issues as to new features. If issues aren't reproducible, we collaborate with Tier 1/2 for additional context and live troubleshooting. All defects are tracked in a USCG-approved system, prioritized with the product owner, and scheduled into sprints. After go-live, we monitor system performance and provide monthly operational reports, including ticket metrics. To reduce Tier 1 load, we'll deploy **Salesforce Knowledge** for self-help content and optionally integrate **Salesforce Agentforce** to deliver AI-powered assistance, automate routine questions, and improve user experience.

Labor Mix

The proposed MCP system MVCR implementation will be completed within 12 months, consisting of 2 months for discovery, 8 months for development, and 4 months for ATO approval and rollout—executed in parallel with development activities. As shown in Figure 6. Team Stealth Structure, the team is organized for seamless execution with leadership, core Salesforce expertise, and integration/migration specialists. Strong governance ensures strategic oversight, architectural direction, and security compliance. To accelerate delivery, the ***Salesforce Core Team*** focuses on business process automation through Salesforce configuration and customization, while the ***Integration and Data Migration Team*** ensures system interoperability and legacy data transition. Operating as separate sprint teams allows parallel development, increasing efficiency and focus. With DoD IL2 to IL5 experience and extensive Salesforce implementation, Team Stealth delivers

a secure, scalable, and compliant MCP system deployment. See the table below for proposed labor categories and associated hours for each:

Labor Category & Responsibilities	Hours
Project Manager (Key Personnel): Oversees all aspects of the project—including scope, budget, quality, resources, and risk management—while guiding deliverables and managing team and stakeholder expectations. Maintains schedules, work plans, and tracking tools; handles change requests to control scope; provides regular performance updates to leadership; and ensures accurate financial reporting and cost control.	1,920
Scrum Master (Key Personnel): Facilitates all Scrum ceremonies; coaches the team and stakeholders on Agile principles; removes impediments; supports sprint goal setting, backlog refinement, and continuous improvement. Partners with the Product Owner on MVP and backlog prioritization. Leverages Agile and collaboration tools (e.g., Jira, Mural) for tracking, planning, and reporting.	1,920
ISSO: Advises the system owner on security matters; oversees ATO documentation and access controls; conducts continuous monitoring (e.g., audits, assessments, incident response); and manages CSAM records.	960
Senior BA / Functional Lead: Leads requirements elicitation, process modeling, and user story development; supports testing; mentors analysts; and ensures quality and alignment of deliverables.	1,920
Business Analyst: Conducts requirements elicitation, documents business processes, develops user stories, supports testing, and ensures deliverables meet project needs and standards.	5,760
Salesforce Admin/Release Manager: Manages Salesforce environments and user access; oversees pull requests, branch merges, and version control; plans and executes release cycles, including scheduling, deployment coordination, and post-release validation; tracks platform updates and produces release notes	1,920
Data Architect / MuleSoft Integration Architect: Designs and implements integrations using MuleSoft; architects data flows between Salesforce and external systems; oversees data migration and integrity; defines API standards, security protocols, and governance; and develops data models and dictionaries.	960
Data Migration / Integration Developer: Executes data extraction, transformation, and loading (ETL); defines mapping rules; ensures data accuracy and consistency; automates migration and integration processes; develops and maintains integration scripts and APIs; conducts testing and troubleshooting; and provides documentation and post-migration support.	960
Salesforce Technical Architect: Designs scalable Salesforce solutions aligned with business needs and best practices; guides development teams and enforces technical standards; implements security and access controls; translates business requirements into technical designs; and prepares architecture documentation.	1,920
Salesforce Developers: Designs, develops, tests, and deploys custom Salesforce solutions using Apex, Lightning, Visualforce, APIs, and web technologies; translates business requirements into scalable, functional applications; optimizes performance; builds OmniStudio components (FlexCards, OmniScripts, Integration Procedures, Data Mappers, Expression Sets, Decision Matrices, Industry Consoles); and performs declarative configuration of apps, objects, flows, reports, dashboards, and Experience Cloud pages.	5,760
QA Engineers: Defines testing strategies, creates test plans and cases, and conducts functional, regression, and performance testing; identifies and tracks defects; collaborates with teams to ensure quality, performance, and security compliance.	3,840

APPENDIX A FIGURES

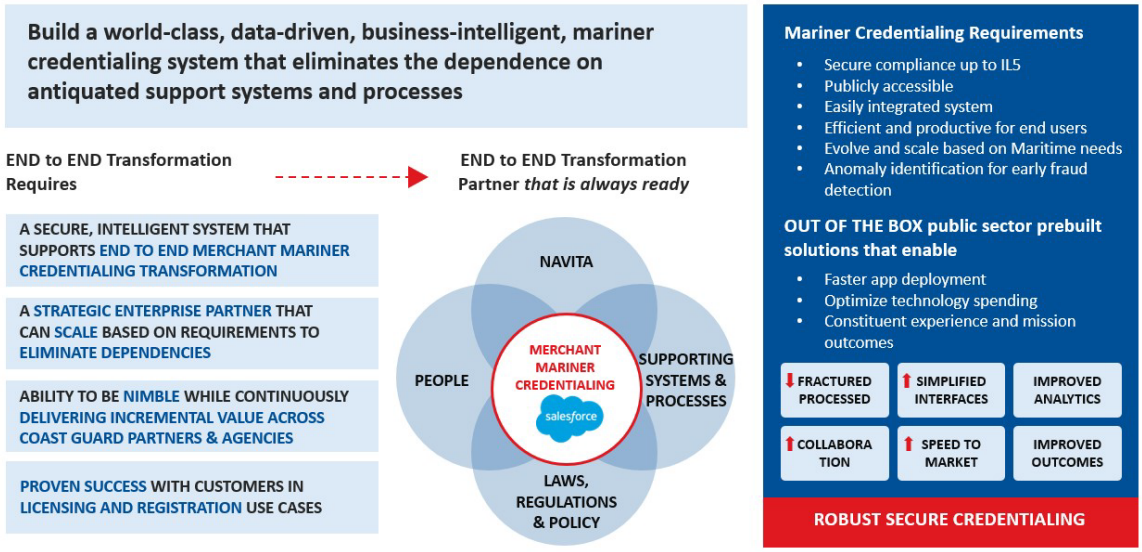

Figure 1. Transforming Mariner Credentialing with a Secure, Intelligent, and Scalable Solution—Powered by Salesforce and Implemented by Team Stealth

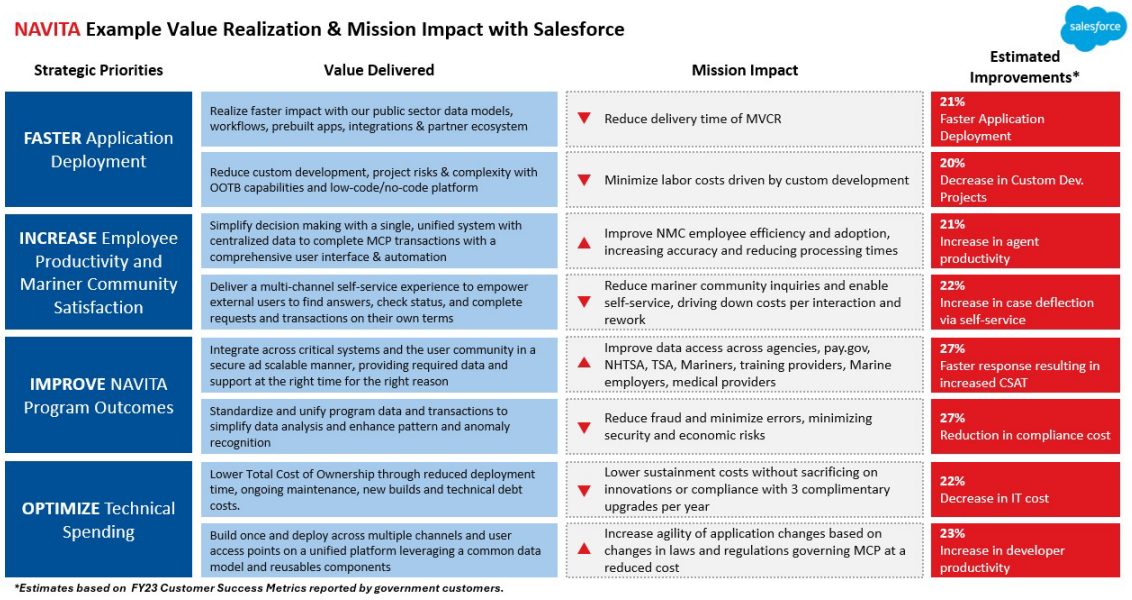

Figure 2. MCP Implementation on Salesforce: Accelerating Mission Impact, Efficiency, and Cost Savings

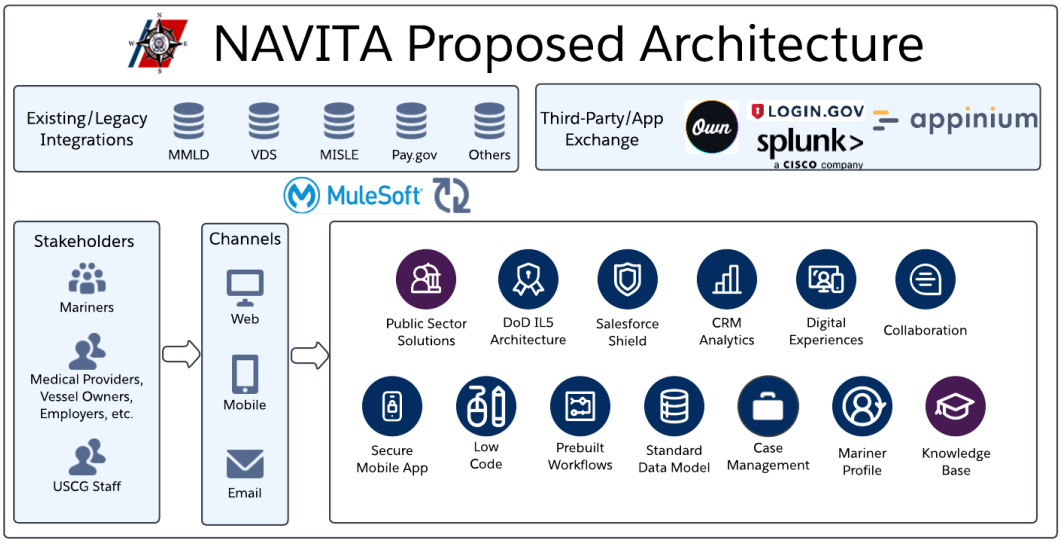

Figure 3. Proposed MCP System Architecture

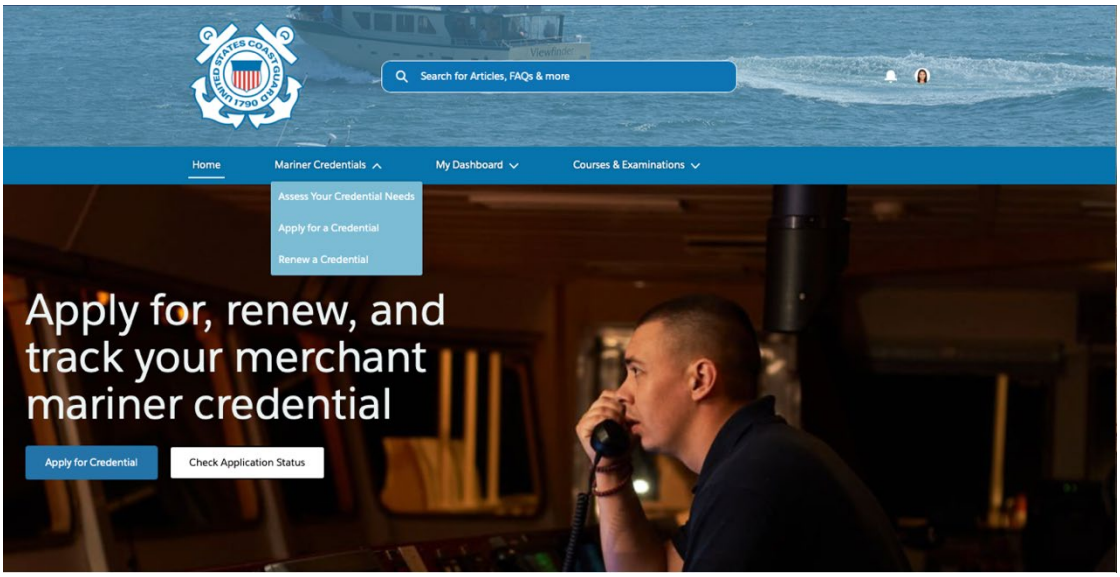

Figure 4. Mariner Portal: Streamlining the End-to-End Credentialing Process

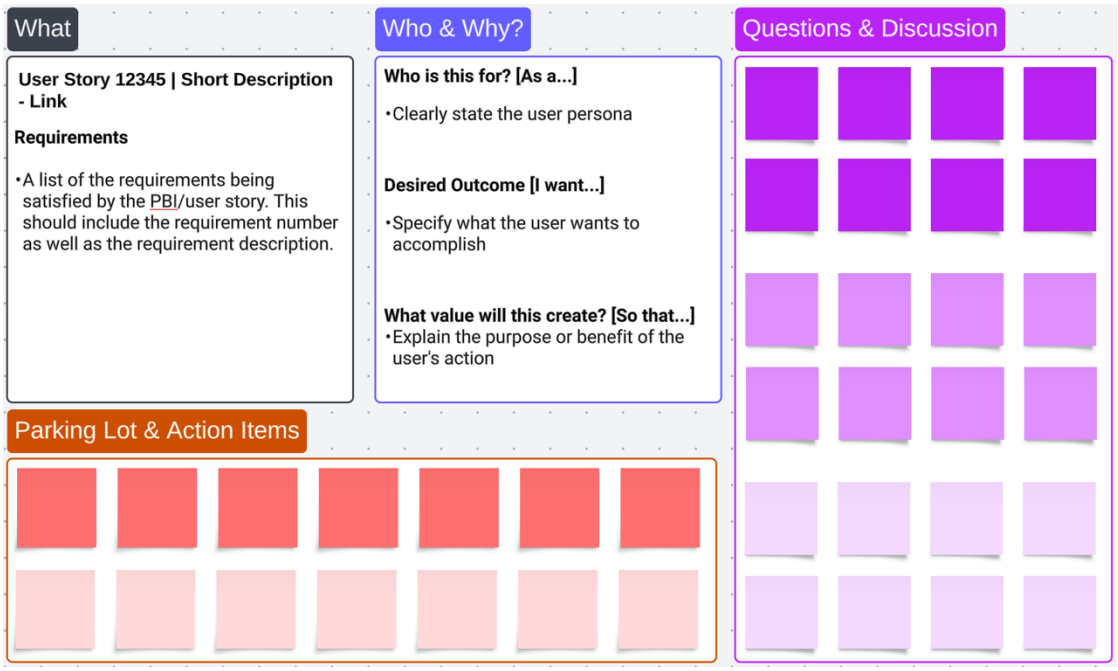

Figure 5. Team Stealth's Standardized User Story Refinement Board

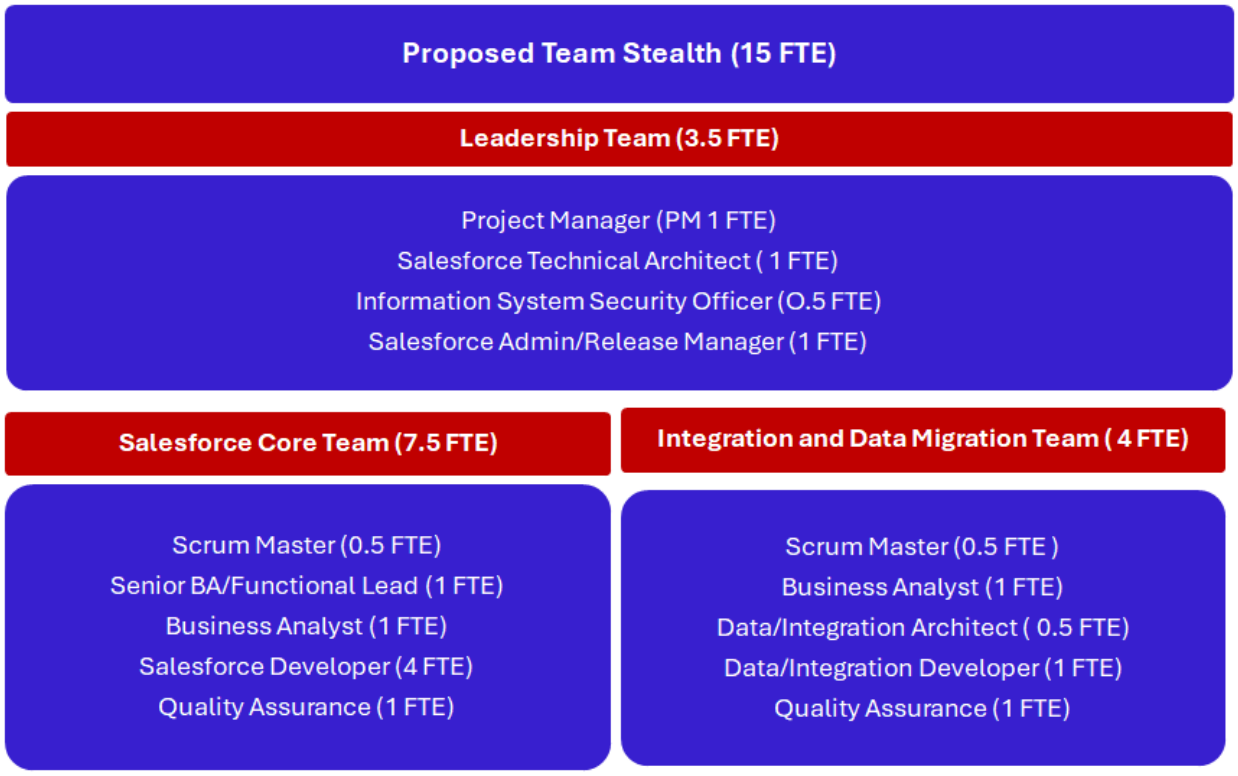

Figure 6. Team Stealth Structure