Green Threads Capabilities and Past Performance

Green Threads LLC (Green Threads) has expertise in Identity Credential and Access Management (ICAM), Federal Identity Credential and Access Management (FICAM), cloud migration and cyber security in the federal IT marketplace. Our team has implemented secure, trusted ICAM/FICAM requirements with significant commercial, regulatory, and health-related missions for our customers including the Veterans Affairs (VA) Identity and Access Management (IAM) program; United States Patent and Trademark Office (USPTO); United States Postal Service (USPS), National Archive and Records Agency (NARA) Insider Threat program; and for the Department of Defense's Joint Artificial Intelligence Center (JAIC). We deliver ICAM/FICAM, Cloud, security, and operations solutions based on industry standards, and open architecture. Our team has a strong understanding of the agile development methodologies for a software factory based on DevSecOps processes and Continuous Integration and Continuous Delivery (CI/CD) for systems integrations and customization where required.

As part of our work for VA IAM Program, our team provides a comprehensive range of DevSecOps and closely related services, including maintenance and sustainment for enterprise-level ICAM solutions that integrates with external Credential Service Provides and Organizational Personal Identification Verification (PIV) for Homeland Security Presidential Directive 12 (HSPD-12) compliance. VA's IAM supports 950+ systems, over thousand applications, and more than 45 Million identities (including Non Person Entities (NPE)), also supporting identity management and identity proofing using external services. Our support to the IAM Program provides high availability and reliability to over 450,000 active internal users and the more than 18M active external users and systems, securing access, authentication, and authorization for critical VA resources, including Veteran's Healthcare systems and records. The IAM program provides Single SignOn (SSO) functionality for internal and external users for VA's resources. The program is comprised of ten enterprise applications with 99.99% availability requirements and is deployed in a FedRAMP-accredited Microsoft Azure GovCloud (MAG). The solution integrates with multiple identity provides to support the veteran's authentication credentials, including but not limited to the **DSLogon**, ID,me, and Login.gov. The solution is in compliance with the current government mandates like HSPD 12, for multi factor authentication leveraging **DoD CAC**, US Access issued PIV, and other PKI based and non-PKI based authentication options. The team works with the mobile groups and health services to integrate services for MFA compliance for mobile devices and has implemented derived credentialing to process PKI/PIV based authentication. Our Identity Services has established workflows that allows traits/identity synchronization with multiple Identity Stores including but not limited to: external CSPs, internal Active Directory, PIV Services, and Veteran Health Identity Card (VHIC) services. For the VHIC project team has delivered and currently manages over million cards for the veterans and their care givers. The team has deployed coarse-grained and fine-grained access controls leveraging Roles Based Access Controls (RBAC) leveraging XML and SAML and Attributes Based Access Controls (ABAC) leveraging XACML. The team has also implemented NIST 800-63-3, M-19-17 and M-22-09 guidelines and mandates.

As part of the cloud first initiative for VA our team executed the migration of a mission-critical and highly complex legacy system of systems at the VA to Microsoft's Azure Government (MAG) cloud. The system integrates with over 1,000 Department of Veteran Affairs (VA) partner applications and supports over 50 million identities. The system consists of 10 major sub-systems deployed on over 1,000 Virtual Machine (VM) instances. Green Threads' cloud-related services included capability assessment, solution preparation, cloud migration planning and implementation, integration, application development, and cloud operations and maintenance. Green Threads' development and operations personnel collaborated to apply DevOps principles and tools for automated processes (e.g., Ansible scripts and marketplace images) to shorten the schedule for this project. A particular emphasis for the VA effort was the issue of components related to monitoring and compliance to achieve three-year ATO based on National Institute of Standards and Technology (NIST) Risk Management Framework (RMF). These components were

essential to maintain operational awareness and enable rapid problem resolution to help the team stay on schedule. This migration effort was completed successfully and became the VA's "poster-child" for the benefits of cloud migration. Further, the project was delivered on time and budget, with zero unscheduled down time; this was achieved within 9 months of initiation, which was ambitious and unprecedented by VA standards. The requirements for the VA's enterprise cloud initiative were to leverage inherent cloud infrastructure, fabric, and services to increase system durability and availability for the enterprise services and reduce the cost of ownership to the government. The Green Threads team was instrumental in helping the VA achieve these objectives from inception to deployment by providing senior resources and subject matter expertise to include project management, architecture, systems engineering, and application development.

Green Threads has delivered a strategic Continuous Monitoring (ConMon) and diagnostic solution for the Department of Defense's (DoD) JAIC. JAIC's architecture was comprised of a multi-cloud platform which included Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform, and on-premises data centers. This was a very complex environment designed for a container-based architecture that allowed the DoD Mission Initiatives to develop products based on Artificial Intelligence (AI) and Machine Learning that can be deployed anywhere once developed. We delivered a strategy that identified the policies, processes, and architecture to enable rapid achievement of an ATO. A key component to this strategy was the design and development of a ConMon solution for the cloud infrastructure as a service, platform as a service, and software factory that was designed for continuous integration/continuous delivery (CI/CD). The team also provided the design and policies to create a single pane of glass view providing real-time visibility into the security posture of the individual mission's initiatives and a comprehensive security score card used to assist with security compliance.

At the United States Patent and Trademark Office, the team supported the architecture and deployment of the original Oracle IDM suite, with SailPoint, Broadcom PAM, Splunk and IBM QRadar capabilities. Our team conducted the analysis and proof of concept for the government to migrate from Oracle IDM Stack to Okta Identity Service. With successful evaluation, the government has executed the procurement of Okta Identity Services. Our team has created the new deployment architecture to enable phased migration of existing partners and users to the "to be" production system that lays down the foundation for zero trust architecture (ZTA). The architecture leverages Okta Access Gateway and Layer7 API Gateways to support existing legacy requirements while enabling SAML and OIDC patterns. Multi Factor Authentications (MFA) supported are PIV, PKI, OTP, SMS, FIDO, RSA, YubiKey and others. The team has migrated over 70 systems and 600k users to the new architecture, the system now supports over 1 million users. The team continues to provide support to address migrations efforts from NIST 800-53 version 4 to version 5 and help meet compliance for M-19-17 and M-22-09 guidelines and mandates. To address non-phishable MFA requirements from M-22-09 the team has created an YubiKey based implementation for external users and integrated PIV based authentication for internal users. As part of the Enterprise Architecture program our team has also provided support for systems ATO processes including System Security Plan development and Assessment as well as supporting agency sponsored FedRAMP for Software as a Service Providers. Our team has worked with the NOC and SOC teams to create monitoring and alerts for proactive threat management and ensure all telemetry data are available for forensic analysis during incident management activities.