KARTHIK CONSULTING
Beyond the expected

3120 Fairview Park Drive
Suite 800
Falls Church, VA 22042
www.karthikconsulting.com

AT A GLANCE

Ensuring TSA's Security Posture in the Cloud

Transportation Security
Administration

KEY SCOPE AREAS

- Review, assess, and test cybersecurity threats in TSA's portfolio of enterprise systems.
- Provide Security Control Audit (SCA) support.
- Develop TSA's Cloud Security Assessment Playbook
- Provide Cloud cybersecurity Subject Matter Expert (SME) Support as TSA migrates its systems to the cloud.
- Provide ISSO, GRC, and Penetration Testing support

KEY STATS

Supported assessment and security review of the following TSA systems:

- Candidate Cloud (Azure)
- Employee Cloud (AWS)
- Okta
- DocuSign
- Mobile Device Management (MDM)

KC CUSTOMER IN FOCUS.

The Transportation Security Administration (TSA) is responsible for screening the 2+ billion passengers that move through the nation's approximately 440 airports each day. TSA is also responsible for screening 100% of the cargo – 1.4 million checked items and 5.5 million carry-on items – that is transported on passenger airlines on a daily basis. In addition, TSA develops policy that helps to protect highways, railroads, buses, mass transit systems, ports, and pipelines. The TSA employs a workforce of 60,000 employees that carry out its mission across the nation.

SIGNIFICANCE OF REQUIREMENTS.

TSA made the decision to move its enterprise systems from data centers to the cloud. As one of the largest agencies within the Department of Homeland Security, its systems are broad in scope and many in number, involving tens of thousands of devices connected to different cloud systems, such as IaaS, PaaS, and SaaS, that are controlled by outside vendors. In addition, each cloud system came with multiple inherited security authorizations that added to the challenge. The agency wanted to ensure that as it moved its systems to the cloud, it could still adequately evaluate its security posture and architecture in the new paradigm. The agency required a process and methodology for security assessments and best practices. In addition, TSA needed assistance in auditing its many systems to determine whether they complied with the recommended processes and architecture.

DELIVERED RESULTS.

Working with the prime contractor, Karthik Consulting helped TSA develop a plan that centered around, investigating security threats, identifying vulnerabilities and analyzing risk, assisting with security audits, and providing support to the information security system officers (ISSOs). KC also validated the implementation of the recommendations.

Continued on next page

KEY AREAS OF KC IMPACT.

INVESTIGATE SECURITY TREATS AGAINST TSA TECHNOLOGIES PORTFOLIO

- Performed an ongoing review of industry/government best practices for system security, presented the recommendations for government approval, and implemented the approved recommended changes.
- Provided information security engineering support activities, which included providing subject matter expertise to the security requirements allocation and security architecture processes for the TSA portfolio of systems.
- Conducted security architecture/design reviews; developed whitepapers that address the security risks, design considerations, security requirements, use cases (assumptions, high level & detailed use cases), system/application specific requirements; and provides recommended mitigations/modifications.

> ***KC built the TSA Cloud Security Playbook for assessing security posture of cloud systems (IaaS, PaaS, SaaS)***

RISK ASSESSMENT OF TSA SECURITY VULNERABILITIES

- Identified system vulnerabilities and determined the security risks of existing and new technology to the TSA FISMA systems.
- Scheduled and performed exhaustive and authenticated scanning of all assets within the TSA FISMA system boundary.
- Coordinated with support contractors of the respective systems to track progress of patching and opened POA&Ms as necessary.
- Tracked all identified weaknesses found within the systems environment from identification through remediation and validation including Information Security Vulnerability Management (ISVM) Alerts & Bulletins and POA&Ms.
- Tracked the remediation progress for all POA&Ms provided by the government.
- Supported the review and triage of vulnerabilities prior to developing the POA&M, including POA&M triage, remediation, and planning a POA&M review meeting.

SECURITY CONTROL AUDIT (SCA) SUPPORT

- Reviewed management practices and policies, baseline High Value Assets (HVAs), and identify ways to leverage continuous monitoring capabilities through the CDM program.
- Researched, assessed, and recommended tools and capabilities to the TSA IAD team.
- Supports HVA Assessments including RVA.
- Conducted Risk Management Framework (RMF) assessments for cloud and on-prem based enclaves and major applications throughout the TSA.
- Supported testing of all applicable security controls as defined in NIST SP800-53 for the specific system based on Confidential Availability and Integrity (CIA) with applicable overlays.
- Planed and/or performed security controls assessments for customer systems in accordance with cybersecurity standards.
- Assisted with identification and remediation of POA&Ms.
- Prepared and/or assisted in the preparation of reports and presentations required for communicating findings of the security control assessments.

Continued on next page

AT A GLANCE *(continued)*

SECURITY ENGINEERING

- Provided a holistic analysis of how an HVA's individual security components integrate and operate, including how data is protected during operations.
- Provided Information Systems Security Engineering (ISSE) support to help identify security vulnerabilities and minimize or contains risks associated with these vulnerabilities spanning the Systems Development Life Cycle (SDLC).
- Security Areas of Focus: Perimeter security, network security, endpoint security, application security, physical security, and data security.

TSA's SUPPORT TSA's INFORMATION SYSTEMS SECURITY OFFICERS (ISSOs)

- Provided resources support for the A-123 internal audit of FISMA High/HVA systems.
- Supported integrated external audits by attending kickoff meetings, compiling and submitting test artifacts, and participating in data center/infrastructure security processes and system walkthroughs.
- Supported the maintenance of the ATO for all of the TSA FISMA systems in our ISSO's portfolio through the A&A process.
- Maintained the Security Plan, Contingency Plan, Contingency Plan Test, and the Configuration Management Plan.
- Supported planned and unplanned security assessments by collecting and reviewing documentation, created new system/policy/procedure documents, reviewed and validated artifacts/evidence points.
- Assisted in triage of all TSA Security Operations Center (SOC) notifications, developed initial response processes, and communicatee notification(s) to the administrators, including, but not limited to: attending incident meetings, providing 24/7 support for incident management, reviewing security logs to ensure compliance, working to help identify, remediate, and/or research solutions to exceptions or false positives identified in the review of security logs and alerts, and managed the process for documenting those exceptions.

ABOUT US

Karthik Consulting was founded in 2008 to be a reliable and trusted advisor for our customers, providing independent, unbiased, and proven solutions that mitigate risk and help solve enterprise-wide IT challenges.

Our Cyber Security, Software Development and Program Management focus areas (and work methodology) ensure that we can deliver not just solutions, but architecture that scales and grows with the customer's needs over time. We are able to assist in projects ranging from short advisory engagements to assembling a full team to deliver a solution from concept through implementation and on-going management. KC has access to industry experts in various technologies and teaming partners to meet any of your IT challenges. The vision of KC is to bring the innovation, passion and agility of the commercial IT industry to meet the unique challenges of the federal government. We are a DOD Cleared Facility with a DCAA-approved accounting system.

CONTACT
Felix Martin, 571 435 7632
fmartin@karthikconsulting.com

CAGE: 56GH3
DUNS: 828199880
UEI: FGNNM7KNUPF6

PRIME CONTRACT VEHICLES:
GSA STARS III 8(a)
GSA MAS
GSA OASIS Pool 1 and 3
NIH CIO-SP3 8(a) & SB
Air Force SBEAS
Army RS3
Navy Seaport-NexGen
FAA eFAST

afaq ISO 20000-1 IT Service Management AFNOR CERTIFICATION
afaq ISO 27001 Information Security AFNOR CERTIFICATION

aws partner network
Select Consulting Partner
Public Sector Partner

ISO 9001:2015 CERTIFIED COMPANY
PRI Registrar PERFORMANCE REVIEW INSTITUTE

CMMIDEV/3℠