Pandora Cloud LLC
300 Colonial Center Parkway
STE 100N
Roswell, GA 30076
Info@PandoraCloud.net

Forging a digital culture: Unpacking cloud complexity to become more agile, interconnected, and digitally dominant.

CAPABILITY STATEMENT

Pandora Cloud is a computer and cloud consulting firm located across the U.S. We specialize in all things cloud, including consulting, vision, modernization, migration strategy, planning, execution, automation, agility, operations, and education. Pandora Cloud is a Woman Owned Small Business (WOSB) specializing in Cloud (AWS, Microsoft, Google, Oracle).

CONSULTING
Proof of Concept Creation, Pilot Deployment, Deploy and Operationalize on-premises cloud capabilities, Landing Zone Design, Deployment, and Operations, FedRAMP, CC-SRG, and ICD-503 cloud guidance, Comprehensive Technical, Cloud readiness auditing

SECURITY
Well-Architected Reviews, Penetration Testing, FedRAMP, CC-SRG, and ICD-503 cloud compliance audit, STIG Automation, RMF/IATT/ATO CSP Guidance, Patch Management and Security Automation, Business Continuity Plan and Backups, Disaster Recovery, Encryption, Identity and Access Management, Access Control, Data Retention and Protection, Incident Response, Infrastructure Security

MIGRATION
Application Migration, Cloud Readiness Assessment, Infrastructure, and Application refactoring for cloud deployment,

OPERATIONS
ITaaS, Service Catalog Creation and Deployment, Cloud Infrastructure and Application Monitoring, Dashboards, Notifications, Alerts, Centralized Logging, Ticketing System Implementation or Integration, Collaboration Tooling, Systems Management, and Patching, Cost Optimization

DEVSECOPS
DevSecOps Pipeline Design, Continuous Integration, Deployment, and Monitoring of Code Pipelines, Custom Automation, Static Code Scanning, Infrastructure as Code, CloudFormation, Terraform, AWS CDK, Custom Programming

AI / ML / ANALYTICS
Design and implement scalable, cost-optimized, reliable, and secure ML solutions, Data Engineering, Exploratory Data Analysis, Modeling, Machine Learning Implementation and Operations. Data Collection, Storage, and Management, Data Processing, Analysis and Visualization, and Data Security.

EDUCATION
Customer Focused Workshops, Custom Immersion Days, Boot Camps, Certification Preparation, Custom Training Classes

Company Information

EIN: 92-1281876
DUNS: 11-887-5521
CAGE Code: 9JSG7
GSA MAS: 47QTCA24D00D3
UNIQUE ENTITY ID: R36GQ3N4XT63
NAICS Codes:
518210 Data processing, Hosting, and Related Services
541512 Computer Systems Design
541511 Custom Computer Programming Services
541513 Computer Facilities Management Services
541519 Other Computer-Related Services
611420 Computer Training
Security Clearance:
Public Trust | TS with SCI Eligibility

Industry Certifications

- AWS Certified AI Practitioner
- AWS Solutions Architect Professional
- AWS DevOps Engineer Professional
- AWS Machine Learning Specialty
- AWS Advanced Networking – Specialty
- AWS Certified: SAP on AWS - Specialty
- AWS Security Specialty
- AWS Database Specialty
- AWS Solutions Architect Associate
- AWS SysOps Administrator Associate
- AWS Certified Developer Associate
- AWS Certified Cloud Practitioner
- AWS Certified Data Analytics Speciality
- Azure Fundamentals
- ICAgile Certified Professional - Enterprise Product Ownership
- Professional Scrum Master certification
- Project Management Professional certification
- Project Management Institute - Agile Certified Practitioner
- CompTIA Security+

Contact Us

Kim Howell – CEO
(314) 323-6745
Kim@PandoraCloud.net

Isi Lawson – CTO
(678) 448-6797
Isi@PandoraCloud.net

Experience

Customer Name: Amazon Web Services – U.S. Air Force
Customer POC: Jason Turse – tursej@amazon.com
Total Contract Value: $32,400
Period of Performance: 2024-09-13 – Present
Contract Number: CC OTH 00362854 2024 TR

Pandora Cloud was selected to provide comprehensive cloud architecture, discovery, and implementation services for a critical federal customer through AWS Professional Services. This initiative blended strategic planning with meticulous technical implementation, leveraging AWS-specific tools and compliance frameworks essential for government cloud operations. Key to this project was adherence to DoD, NIST, and FedRAMP standards, ensuring the cloud platform effectively supported the unique operational demands of federal agencies.

The approach began with thorough requirements gathering through strategic workshops and stakeholder interviews, focused on defining organizational structure, account structure, operations, network configuration, security, governance, and compliance requirements. Our team engaged in detailed technical analyses, reviewing existing infrastructure and compliance demands to ensure the cloud architecture aligned with operational objectives. We also developed comprehensive documentation of customer decisions across technology, operations, and security areas, ensuring that the cloud platform we developed was tailored to the organization's unique requirements.

The architectural design process employed best practices and continuous refinement, creating scalable and secure designs. We developed an initial minimum-security baseline (MSB) based on compliance requirements and AWS best practices, along with referenceable playbooks and runbooks supported by sample code and architectural diagrams. This process involved detailed implementation planning to predict performance alongside continuous refinement and iteration to achieve an optimal design. This approach guaranteed cloud architecture tailored to the government's specific operational requirements.

To establish adherence to stringent DoD standards and guidelines for security and compliance, the approach encompassed implementing security measures such as DoD-compliant network connectivity for unclassified cloud services, secure DNS setup including name resolution for internet, on-premises, and cloud-hosted DNS zones, and network configuration with defined routes for internet, inter-account, and cloud to on-premises routing. Implementation included integration with the customer's existing identity provider solution for secure account access, ensuring comprehensive security across the environment.

The implementation strategy focused on automation and standardization, deploying detective and preventative guardrail rules for new accounts and resources aligned to customer specifications. This included comprehensive deployment of network infrastructure, security controls, event management mechanisms, monitoring systems, access controls, and data storage solutions. Our approach prioritized automated infrastructure deployments integrated with the customer's overall continuous integration/continuous deployment strategy.

Deliverables from this project included comprehensive documentation of the cloud governance framework, implementation of secure and scalable cloud architecture, and automated deployment processes. This body of work reflects Pandora Cloud's commitment to advancing cloud technologies in federal operations and sets a benchmark in creating efficient, secure, and collaborative cloud environments that significantly enhance mission readiness and success for federal agencies.

Customer Name: Taylor Protocols - Cloud Migration and Managed Services
Customer POC: Greg Taylor - greg.taylor@taylorprotocols.com
Total Contract Value: $11,943.24
Period of Performance: 08/2024 – Present
Contract Number: NA (Commercial)

Pandora Cloud was selected to provide comprehensive cloud architecture, migration, and ongoing managed services for Taylor

Protocols' development and production environments. This initiative blended strategic planning with meticulous technical implementation, leveraging AWS-specific tools and best practices to ensure a secure, scalable, and cost-optimized cloud platform supporting critical business applications.

The approach began with thorough requirements gathering and architectural design, focusing on creating a robust infrastructure for both development and production environments. Our team conducted detailed technical analyses of the existing infrastructure and application dependencies to ensure the cloud architecture would meet operational objectives. We developed comprehensive documentation and implementation plans for the migration of their Windows-based .NET application and associated databases, ensuring minimal disruption to business operations.

The architectural design process employed best practices and continuous refinement, creating scalable and secure designs across both environments. We implemented a comprehensive AWS architecture including Virtual Private Clouds (VPCs) with public and private subnets, Application Load Balancers for traffic distribution, EC2 instances for application servers and jump boxes, and Aurora MySQL database clusters. The design included sophisticated security controls through security groups, network access controls, and AWS Web Application Firewall (WAF) implementation.

To establish robust security and operational excellence, the implementation encompassed comprehensive monitoring and management capabilities. This included AWS CloudWatch for monitoring and alerting, defined maintenance windows for system updates, and established procedures for .NET Framework updates requiring explicit customer approval. The solution provided secure access through NAT Gateways for outbound internet access from private subnets, ensuring a strong security posture while maintaining necessary connectivity.

The implementation strategy focused on cost optimization and operational efficiency, leveraging 3-year EC2 savings plans and 1-year reserved instances for Aurora MySQL to achieve significant cost savings. Our approach included automated infrastructure deployments, standardized patching procedures, and comprehensive support coverage including out-of-hours response for cloud provider outages. This ensured both development and production environments maintained high availability while optimizing operational costs.

Deliverables from this project included comprehensive infrastructure implementation, migration execution, ongoing managed services, and detailed documentation of operational procedures. This body of work reflects Pandora Cloud's commitment to delivering efficient, secure, and cost-effective cloud solutions that significantly enhance operational capabilities while ensuring robust security and compliance controls.

Customer Name: USSF SLD30 & SLD45 Nebula Cloud Platform Project
Customer POC: Capt. Andrew Holland - andrew.holland.4@spaceforce.mil
Total Contract Value: $472,577.60
PoP: 10/30/2023 – 10/30/2025
Contract Number: FA2521-23-F-0149
CPARS is available upon request

Pandora Cloud was entrusted with the design of a comprehensive architecture of a secure, scalable, and financially optimized cloud infrastructure for Space Launch Delta (SLD) 30 and SLD45. This design ultimately became known as Nebula. This initiative blended strategic planning with meticulous technical implementation, leveraging AWS-specific tools and compliance frameworks essential for government cloud operations. Key to this project was the adherence to critical DoD, NIST, and FedRAMP standards, ensuring the cloud platform effectively supported the unique operational demands of spaceport activities.

The approach began with thorough requirements gathering through strategic workshops and stakeholder interviews, followed by detailed technical analyses to align the cloud architecture with organizational goals. Our team engaged in detailed technical analyses, reviewing existing infrastructure and compliance demands to ensure the cloud architecture aligned with operational objectives. We also utilized surveys and cloud assessment tools to refine our understanding of specific needs further, ensuring that the cloud platform and landing zone we developed were tailored to the organization's unique requirements.

The architectural design process employs best practices and continuous refinement, creating scalable and secure designs. We leveraged architectural frameworks and tools to ensure the designs met current and future needs. This process involved detailed proof-of-concept modeling to predict performance alongside continuous refinement and iteration to achieve an optimal design. This approach guaranteed cloud architecture tailored to the government's specific operational requirements.

To establish adherence to stringent DoD standards and guidelines for security and compliance, the approach encompassed implementing security measures, such as encryption, fine-grained access controls, and continuous monitoring, in line with DoD's Security Requirements Guide (SRG) and Risk Management Framework (RMF). Compliance was integrated according to FedRAMP regulations, conducting thorough vulnerability assessments and security audits, collection of centralized logs, and being able to drill down into incidents to examine root causes.

In addressing network accessibility, we adopted the principles of Zero Trust architecture, enhancing network security through the Cloud Native Access Point (CNAP) to ensure robust data flow management across commercial and NIPR networks. Cloud Native Access Points (CNAP) were chosen over the traditional Boundary Cloud Access Points (bCAP), aligning with the Secure Cloud Computing Architecture (SCCA). This approach, coupled with Zero Trust principles, ensured network segmentation and security. Our network design managed data flows between various networks, using CNAP to bolster security measures in line with DoD's operational and security standards for cloud environments, adhering to the imperative of 'never trust, always verify.'

Our financial operations strategy was fundamental. Utilizing AWS tagging was core to providing precise cost tracking and chargeback, thus promoting financial transparency. This enabled all Nebula customers hosted on the platform to utilize detailed FinOps to manage and track cloud costs. This setup allowed for precise cost allocation and chargeback to launch partners, ensuring financial transparency and compliance.

Customer onboarding was designed to be seamless and thoughtful, establishing efficient processes for integrating new users into the Nebula platform. This involved establishing repeatable processes and patterns for assessing a customer's existing infrastructure and tailoring a migration architecture that aligns with Nebula's framework. Our approach was designed to simplify decision-making and ensure ease of integration for the customer.

By leveraging Nebula for operational launch data, we've initiated the development of a centralized repository accessible across the range. This repository will streamline how range operations and launch partners access and utilize data, fostering enhanced collaboration for mission success. The centralized location of holistic datasets allows for deeper insights and more informed decision-making, significantly benefiting each partner. This step towards centralized data management increases operational efficiency and shared success in mission-critical activities.

Deliverables from this project included comprehensive documentation of the cloud governance framework, implementation of secure and scalable cloud architecture, and regular validation reports against AWS best practices. This body of work reflects Pandora Cloud's commitment to advancing cloud technologies in federal space operations and sets a benchmark in creating efficient, secure, and collaborative cloud environments that significantly enhance mission readiness and success for SLD30 and SLD45.

Customer Name: USSF SLD30 & SLD45 Cloud Center of Excellence
Customer POC: Capt. Andrew Holland - andrew.holland.4@spaceforce.mil
Total Contract Value: $472,577.60
PoP: 10/30/2023 – 10/30/2025
Contract Number: FA2521-23-F-0149
CPARS is available upon request

The project involves providing an enterprise-level solution focusing on cloud governance, brokerage services, Cloud Center of Excellence (CCoE) enhancement, and consulting for Space Launch Delta (SLD) 30 and SLD45. The aim is to streamline cloud governance, efficiently manage service brokerage, and develop a more robust Cloud Community Office of Excellence Practice.

Key objectives include designing and implementing solutions for cloud governance and brokerage services, enhancing the CCoE Practice through industry best practices and collaborative learning, assessing feasibility for cloud application migrations, and offering consulting services to align with AWS best practices.

The approach encompasses systems engineering, where gaps and opportunities in the existing architecture will be identified, and a robust cloud governance framework developed. Systems integration will focus on unifying SLD30 and SLD45's existing systems into a cohesive cloud ecosystem, ensuring interoperability and data consistency. Additionally, cybersecurity is a major component, involving comprehensive assessments to safeguard cloud environments and ensuring compliance with industry standards.

A feasibility assessment will evaluate the suitability of applications for cloud migration, modernization, and performance optimization. The consulting and validation phase involves ongoing services to ensure adherence to AWS best practices, with regular reviews and audits for compliance with security and performance benchmarks.

Deliverables include cloud governance framework documentation, implementation of a service brokerage platform, enhancement plans for the Cloud Community Office of Excellence Practice, feasibility reports, and regular validation reports against AWS best practices. The team comprises qualified personnel specializing in AWS, cloud systems architecture, legacy systems integration, cloud cybersecurity, cloud migration, and operations, and consulting.

This Body of Work represents a comprehensive strategy to achieve these objectives, integrating systems engineering, systems integration, cybersecurity, feasibility assessment, and continuous validation against AWS best practices. This collaboration aims to support the emerging needs of SLD30 and SLD45 in their cloud-centric initiatives.

Customer Name: Guidehouse/U.S. Census Bureau (USCB)
Customer POC: Justin Marchand - jmarchand@guidehouse.com
Total Contract Value: $41,250.00
Period of Performance: 05/2024 – Present
Contract Number: HHSN316201200111W/1333LB24F00000059 (Prime Contract)
Purchase Order: PO0500340

Pandora Cloud is delivering cloud modernization expertise for the U.S. Census Bureau through Guidehouse, focusing on automation and Infrastructure as Code (IaC) implementation in AWS. This initiative demonstrates our ability to transform traditional infrastructure management into modern, automated cloud operations.

Our technical delivery centers on developing comprehensive Infrastructure as Code solutions using AWS CloudFormation and other AWS-native tools, enabling the Census Bureau to automate their infrastructure deployments and management. We are implementing automated pipelines for infrastructure deployment, ensuring consistent and repeatable environments while reducing manual intervention and potential human error.

The modernization effort includes developing reusable code modules for common infrastructure patterns, establishing version control practices for infrastructure code, and implementing automated testing frameworks for infrastructure deployments. Our work creates a foundation for continuous infrastructure deployment and management, allowing the Census Bureau to adopt modern DevOps practices in their cloud operations.

We are establishing standardized approaches to AWS resource provisioning and management, incorporating security best practices and compliance requirements into our Infrastructure as Code templates. This includes automated implementation of security controls, networking configurations, and monitoring solutions, ensuring consistent application of security and operational standards across the cloud environment.

Through this engagement, we demonstrate Pandora Cloud's expertise in federal cloud modernization, particularly in transforming

manual processes into automated, code-driven solutions that enhance operational efficiency and reliability while maintaining strict security and compliance requirements.

Customer Name: Canoja Technologies - Managed Cloud and Development Services
Customer POC: Richard Campbell, CEO - rcampbell@canojatech.com
Total Contract Value: $100,000
Period of Performance: 01/2024 – Present
Contract Number: NA (Commercial)

Pandora Cloud was selected to deliver comprehensive managed information technology, cloud, and development services for Canoja Technologies. This initiative demonstrates our ability to provide end-to-end technology solutions, combining cloud operations, development services, and IT management into a cohesive managed services offering that ensures operational efficiency, security, and scalability.

The approach began with establishing robust IT management services, including comprehensive account lifecycle management, implementation of enterprise applications, and network infrastructure optimization. Our team provided extensive technical support services, including 24/7 monitoring and incident response capabilities, ensuring continuous operation of critical business systems. This was complemented by sophisticated security measures including cybersecurity assessments, threat mitigation strategies, and implementation of comprehensive security controls.

The cloud management component employed industry best practices and continuous refinement, implementing Well-Architected Framework reviews and landing zone configurations. We established sophisticated cloud operations including resource optimization, backup and disaster recovery strategies, and comprehensive monitoring solutions. The architecture included serverless solutions, database management, and containerization services, creating a scalable and efficient cloud environment. To support development operations, we implemented comprehensive development services including custom software development, pipeline deployment and management, and sophisticated data integration solutions. This included establishing CI/CD pipelines, implementing ETL processes, and providing data analytics capabilities. The development approach encompassed both cloud-native application development and legacy system modernization, ensuring a modern and efficient technology stack.

The implementation strategy focused on operational excellence through automated workflows, standardized procedures, and comprehensive support coverage. Our approach included regular Well-Architected reviews, cost optimization analysis, and continuous improvement of operational procedures. This ensured the environment maintained high availability while optimizing operational costs and maintaining security compliance.

Deliverables from this project included comprehensive IT infrastructure management, cloud operations support, development services, and detailed documentation of operational procedures. This body of work reflects Pandora Cloud's commitment to delivering efficient, secure, and comprehensive technology solutions that significantly enhance operational capabilities while ensuring robust security and compliance controls.

Amazon Web Services
Defense Innovation Unit (DIU) - Hybrid Space Architecture
Customer POC: Pete Bahmani – pbahmani@amazon.com
Total Contract Value: $52,000.00
PoP: 09/01/2023 – 09/30/2024
Contract Number: CC OTH 00215746 2024 TR
CPARS is available upon request

The DIU’s project to develop the Hybrid Space Architecture is now heavily focused on leveraging cloud capabilities to enhance communication in space. This initiative aims to design and deploy a sophisticated network topology using cloud technologies,

ensuring resilient and uninterrupted access to communication resources for space customers. The use of cloud technologies is key in overcoming traditional limitations and preventing denial of service in space communications.

The heart of the project is the integration of cloud computing with existing space and ground-based communication networks. This integration is designed to provide a more flexible, scalable, and robust communication system. By adopting cloud technologies, the architecture can leverage virtualization, distributed computing, and advanced data management techniques to enhance the efficiency and resilience of space communications.

The deliverables for this project now include a comprehensive cloud-based design for the Hybrid Space Architecture, implementation strategies for deploying the cloud network, and operational protocols. The project also aims to set cloud-specific guidelines and standards for space communication networks.

In conclusion, the DIU's Hybrid Space Architecture project, with its focus on cloud technologies, represents an innovative approach to solving the challenges of space communication. It aims to build a resilient, adaptable, and secure cloud-based network topology, enhancing the capabilities and security of space operations. This cloud-centric initiative is crucial for advancing strategic interests in space communication and technology.

Cloud Architecture
Space Launch Delta 45 (SLD45)
FY 2022 – 2023

We have worked with SLD45 as a part of their Range of the Future effort to modernize technical applications and infrastructure into commercial cloud providers. Demand for launch has doubled year over year and the current capabilities of Launch do not scale to meet the needs of the government and commercial customers.

During this effort, we have created and executed a customer-requested "Cloud Boot Camp" to educate range leadership, operators, and staff about how to accomplish their mission using commercial cloud solutions. This boot camp was a five-part series to educate USSF Launch (SLD45 and their California counterpart, SLD30, collectively called Launch) about Commercial Cloud Capabilities. Each session was comprised of 8-15 presentations over the course of one to two days as well as hands-on labs. This effort educated approximately 140 customers and continues to change the cultural attitude towards digital transformation.

We have assisted the SLD45 leadership in the creation of a Cloud Center of Excellence (CCoE) to enable a faster pace of cloud adoption and adherence to best practices, and to utilize the commercial cloud to take advantage of IT delivery, agility, efficiency, and innovation.

We have designed the cloud architecture that SLD45 will execute to create a Landing Zone within the commercial cloud to provide a compliant and secure enclave for the creation, migration, and deployment of range applications. This landing zone meets the stringent requirements of the DoD SRG, NIST 800-53, CNSSI-1253, and additional requirements related to using commercial cloud at Impact Level 4.

We have additionally provided architecture and engineering services to SLD45 in several areas including the design and deployment of an on-premises commercial cloud computing capability called Outpost, which brings cloud-native services to the local data center. This locality allows for latency-sensitive applications to take advantage of cloud services by expanding their data analytics capabilities. This effort enables the modernization and significant expansion of the Range and Security Force's security sensor coverage, processing, and operations.

We are engaged with the Range's application incubator, Forge, and application development organization, SupraCoders, as technical advisors. This has led to the creation of a repeatable deployment solution, Service Catalog, that ensures developer agility within secure governance frameworks. This capability increases the speed of development, security, and standardization of range applications.

SLD45 continues to seek our advice regarding technical questions about digital transformation, cloud services, and pricing to help drive business strategy.

Cloud Architecture
Space Launch Delta 30 (SLD30)
FY 2022 – 2023

Worked with Space Launch Delta 30 (SLD30) to modernize infrastructure at the Eastern and Western Ranges and to create efficiencies in the conduct of operations related to their range safety system (SAS/SAS-S). The primary systems used by the range are a set of High-Performance Computing (HPC) clusters used to predict material fallout after an anomaly that requires the destruction of the launch vehicle. These clusters are fixed in size and take input from analysts and output modeling of debris fields for different materials. Efforts included a detailed understanding of the existing HPC system design, long-term customer requirements, and scale and elasticity of the HPC clusters to accommodate future safety mission needs.

We have worked with SLD30 to understand their on-premises architecture and what it takes prior to launch to run their Monte Carlo modeling simulations for debris and toxin tracking, and potential effects on populated areas, and to help explain the probability and impact of risk and uncertainty in the modeled predictions. This effort allows SLD30 to support multiple or parallel launches while maintaining an appropriate risk profile for each.

We have designed the cloud architecture that SLD30 will execute to create a Classified Landing Zone within the commercial cloud Secret capability to provide a compliant and secure enclave for the creation, migration, and deployment of range safety applications. This landing zone meets the stringent requirements of the DoD SRG, ICD-503, NIST 800-53, CNSSI-1253, CNSSP-11, and additional requirements related to using commercial cloud at the Secret classification requirements of Impact Level 6.

We are also working with commercial partners of SLD30 to modernize the ARCTOS range safety software that runs on top of the cloud infrastructure to incorporate schedule coordination on the cluster nodes and to utilize tagging for easier cost tracking back to each individual launch.

We continue to advise SLD30 and have recently discussed the possibility of utilizing cloud-based digital twins for some of the launch simulation efforts used in the training of Launch operators.

Cloud Architecture
Space Dynamics Laboratory (SDL)
FY 2022 – 2023

We organized and led Space Dynamics Laboratory's Well-Architected Framework Review (WAFR) to help them better utilize, optimize, and standardize cloud implementations as part of their mission to provide multi-domain mission solutions with expertise in satellites, sensors and instruments, ground systems, and data processing, and advanced autonomous systems. The objective of a WAFR is to educate SDL to build secure, high-performing, resilient, and efficient infrastructure for a variety of applications and workloads. We focus SDL on building workloads based on the six pillars of the Well-Architected Framework: Operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability. This provides SDL with a consistent approach for partners to evaluate architectures and implement scalable designs.

We have additionally led several engagements and customer strategy sessions around architecting solutions for Ransomware, Disaster Recovery and Resilience, Enterprise Data Strategy, Quantum Computing, Machine Learning, and HPC compute loads.

SDL recognizes our technical expertise and frequently asks us questions about cloud service and capabilities, relying on our answers to make business and technical decisions.

Cloud Architecture

Aerospace Corporation
FY 2022 – 2023

The Missile Track Custody Demonstration (MTCD) is a prototyping effort to determine possible future satellite constellations supporting SSC's Missile Warning and Missile Tracking mission. We continue to work with this Space Systems Command (SSC) project to take digital engineering to the next level. We have provided them with the necessary control information to get them into the Secret Classified cloud region to start taking advantage of the scaling, agility, resiliency, and durability of the cloud to run their Cameo software and other digital engineering tools in prototyping effort to determine possible future satellite constellations supporting SSC's Missile Warning and Missile Tracking mission. This digital engineering, modeling, and simulation is being done to validate requirements for missile raid containment while building flight demonstration units that will validate performance and feed data back into the digital model to understand current missile threats: what they look like, how they fly, and how they emit heat. By helping MTCD receive IATT and providing them with reusable Infrastructure as Code (IaC) they have been able to rapidly start deploying environments in which they can begin simulating what their sensors would see, how well they can track position and velocity, contain them at a certain accuracy and how to tell the radars on the ground where to search for an inbound missile in order to launch an intercept.

The significance of the architecture we have created, and effort is the change in DoD policy to allow mission partners to establish connectivity with commercial cloud providers without the need to utilize existing classified DoD networks such as SIPRNet. This architecture has challenged the classified network accreditation boundaries with DCSA, USAF CloudOne, and the Space Authorizing Official related to the execution of an IATT and later an ATO that would allow for a service delivery partner network (accredited classified enclave specific to MTCD) to be connected to the commercial cloud provider via a CNSPP11 protected commercial circuit and then passed through the CloudOne Virtual Datacenter Security Stack (VDSS) before entering the partner owned cloud environment hosting the Digital Engineering Environment (DEE) capabilities. This routing of the CNSSP11 connection through the CloudOne VDSS is a custom-built design pattern that once accepted by CloudOne and DCSA would allow access to the classified commercial cloud using the USAF CloudOne capability for future customers.

We have designed the cloud architecture that Aerospace will execute to create a Classified Landing Zone within the commercial cloud Secret capability to provide a compliant and secure enclave for the creation, migration, and deployment of range safety applications. This landing zone meets the stringent requirements of the DoD SRG, ICD-503, NIST 800-53, CNSSI-1253, CNSSP-11, and additional requirements related to using commercial cloud at the Secret classification requirements of Impact Level 6. This architecture shows the network integration of key stakeholder organizations, such as Aerospace's Anvil Lab in addition to the two contractors working on the MTCD program: Boeing/Millennium Space and Raytheon. It has been used in numerous Government briefings to help build confidence and answer security-related questions and was vital in ensuring Aerospace's journey in getting their IATT.

Aerospace continues to engage us to strategize on the best ways to solve mission problems related to MTCD and other ongoing efforts such as Just-in-time Ground Station data processing and analytics, development of digital twins, and modernization of the satellite-based NOAA weather data feeds towards real-time data distribution.