



## Federal Law Enforcement Agency Moves Mission Critical Applications to Hybrid Cloud using 1901 Group's Cost Neutral Cloud Approach

With 7,500 employees in 280 offices across the U.S., this federal law enforcement Agency relies upon public facing applications, mission systems and large volumes of data, including sensitive law enforcement and evidentiary data to protect communities from violent crimes and acts of terrorism. Many of the Agency's activities are carried out in conjunction with task forces made up of federal, state and local law enforcement officers. In the event of an incident, law enforcement professionals from multiple organizations depend on rapid access to the federal Agency's applications and data to protect the public from violent crimes.

In response to the Office of Management and Budget's (OMB) Cloud First and Data Center Optimization Initiative, the Agency revised their architecture to replace their legacy data center with an innovative hybrid cloud architecture to meet its increasing mission needs and stringent security requirements. To improve operational performance while reducing costs, the Agency wanted to take advantage of cloud computing to turn capital expenses into operational expenses, reducing existing operations and maintenance (O&M) costs to create the funding to migrate their mission critical applications to the cloud.

The federal law enforcement agency turned to 1901 Group to support their journey to the cloud. This transformation is built upon 1901 Group's cost neutral cloud journey approach that immediately reduced the current O&M spending by 30%, enabling the agency to apply those savings to establish a hybrid cloud environment and migrate mission critical data and applications to the cloud. The first step was transitioning the infrastructure O&M contract to 1901 Group's FedRAMP authorized, network infrastructure as a service (NIaaS) offering that leverages process and technology automation and 24x7 managed services to improve performance and reduce costs. For step two, 1901 Group used their In3Sight™ FedRAMP authorized software as service (SaaS) platform to assess the Agency's mission systems,

applications and data to build a cloud migration plan. Upon approval of the migration plan, 1901 Group established a FISMA High, Private cloud storage as a service (STaaS) to provide disaster recovery as a service (DRaaS) with a recovery point objective and recovery time objective of less than one minute. 1901 Group then established the cloud infrastructure as a service (IaaS) and began the migration of cloud ready, live workloads to the cloud DR environment using cloud and data synchronization tools, which ensure no mission disruption. The last phase was the systematic refactoring of legacy applications to an open source solution and establishing a DevSecOps environment to support continuous integration/continuous development to improve the efficiency, security and O&M costs for refactored mission system and applications. The net result is a transformed environment that leverages hybrid cloud, adhering to all federal security mandates that significantly reduce costs over time through 1901 Group's cost neutral cloud journey.

### Customer Challenges



80% of IT budget is spent on O&M of legacy infrastructure making it difficult to fund transformation initiatives in a cost neutral approach



End of life hardware and diverse, non-standardized technology stacks coupled with increased customer demands for computer, storage and infrastructure services



Many of the legacy applications operate on legacy operating systems and applications not supported by cloud service providers



Maintain compliance with FISMA High requirements



Federal law enforcement chain of custody data requirements prevents the agency from leveraging the public cloud for data storage



## Cost Neutral Cloud Journey Concept of Operations



1901 Group's Cost Neutral Cloud Journey solution encompasses the following steps:

- 1 Move Management of the Current Infrastructure O&M to a FedRAMP Authorized Managed Service.** We leveraged 1901 Group's In3Sight™ integrated IT Service Management (ITSM) platform, ITIL based processes, and secure monitoring and management from a central 24x7 FedRAMP authorized Operations Center. We performed discovery and assessment activities on the existing environment, established DR target and Hybrid infrastructure, and built in FISMA High and federal law enforcement data security controls and compliance.
- 2 Focus on DR First and Start with Data.** To provide a logical path for migrating production workloads to the cloud, we conducted "full stack" application discovery to visualize data, infrastructure, and service dependencies, which was a critical step to developing a cloud migration roadmap. We used replication tools to move Agency data off their legacy storage device to a Private Cloud STaaS model where data storage is procured on a per-terabyte basis.
- 3 Establish Hybrid Cloud by Leveraging Commercial Data Center Services.** Our hybrid cloud solution includes Private cloud for storage to ensure data chain of custody; Public and Community cloud compute, backup and storage, and; commercial data center for hosting of applications that are not cloud ready. We automated the server request and provisioning process and managed the server uptime through established policies, Red Hat's Cloud Forms and elasticity engineering.
- 4 Migrate Cloud Ready Applications to DR Environment.** Where possible, used industry leading tools to automate the migration, and if not, manually deployed applications where needed. We connected cloud DR Applications to Private Storage data and established cloud instances in AWS GovCloud to support high data input/output based applications.
- 5 Refactor Applications that are Not Cloud Ready, then Migrate them to the Cloud.** We identified a business objective to provide application refactoring in an "as a service" model to reduce the dependency on expensive, commercial software by transitioning functionality from a legacy application to open source systems, potentially saving the Agency millions of dollars in licensing and maintenance costs.
- 6 Day-2 as a Managed Service:** After all applications are migrated to the cloud, we extend the data center Managed Services to the Hybrid cloud environment. We augment the integrated toolset with cloud specific tools for orchestration, automation, and governance and continue to leverage 24x7 FedRAMP authorized Operations Center to manage Cloud infrastructure.

With its secure hybrid cloud solution, the agency has established a FISMA High hybrid cloud environment and an architecture for federal agencies that have stringent data requirements to improve performance, reducing IT budgets while improving operational efficiencies and security. The agency is proof that it is possible for one of the largest federal law enforcement agencies to maintain data control and governance while dramatically lowering costs using the cloud.



## Company Highlights



**Established in 2009** as an innovative Managed Service Provider delivering IT in an “as a service” model for federal and commercial customers.



**Experience, expertise, and best practices** securely migrating mission critical applications from on premise data centers to private and public cloud.



**FedRAMP authorized In<sup>3</sup>Sight™ SaaS and IaaS service platform** used to monitor, manage, and optimize enterprise IT environments.

## Services



### Cloud Services

- ▶ Migration Readiness Assessment & Planning
- ▶ Public, Private, and hybrid cloud solutions
- ▶ Fixed Price Application Migration
- ▶ Cloud Design & Engineering
- ▶ Application Re-factoring, Re-hosting, & Re-Platforming
- ▶ DevSecOps
- ▶ Elasticity Engineering
- ▶ Cloud Monitoring & Management



### Infrastructure Services

- ▶ Network Engineering & Mgmt
- ▶ Server Engineering & Mgmt
- ▶ 24 x 7 Network Operations Center
- ▶ Help Desk and Call Center
- ▶ Desktop Support
- ▶ Unified Communications
- ▶ Storage Engineering & Mgmt
- ▶ End-User Support



### Application Services

- ▶ System Administration
- ▶ Agile Development
- ▶ DevOps Platform
- ▶ Database Support
- ▶ Data Analytics and Business Intelligence
- ▶ Architecture and IT Modernization
- ▶ Open Source Development
- ▶ Automated Testing



### Security Services

- ▶ NIST, FISMA Cyber Security Compliance
- ▶ Continuous Monitoring
- ▶ 24 x 7 Security Operations Center
- ▶ Vulnerability & Patch Mgmt
- ▶ Security Log Collection/Analysis
- ▶ Intrusion Detection and Prevention
- ▶ Anti-X Security Control
- ▶ Disaster Recovery and COOP
- ▶ Security Information and Event Mgmt (SIEM)

# Additional Information

## Contract Vehicles / Blanket Purchase Agreement



**Alliant Small Business**  
GS-06F-0630Z



**GSA Schedule 70,**  
SIN 132-40: Cloud Services  
SIN 132-51: IT Professional Services  
SIN 132-52: Electronic Commerce and  
Subscription Services  
GS-35F-0617W

## Partnerships, Certifications, and Authorizations



**CMMIDEV / 3<sup>SM</sup>**  
Exp. 2021-12-04 / Appraisal # 1750



**CMMISVC / 3<sup>SM</sup>**  
Exp. 2021-12-04 / Appraisal # 1750



**FedRAMP**



- ▶ **Amazon Web Services (AWS)** – AWS Partner Network (APN) Consulting Partner
- ▶ **Equinix** – Gold Partner
- ▶ **Microsoft Azure** – Public Sector Channel Partner
- ▶ **NetApp** – Gold & CloudFirst Partner
- ▶ **ServiceNow™** – Managed Server Provider and Sales Partner

## Pertinent Codes:

NAICS  
Codes

518210  
541219

541511  
541512

541513  
541519

541712  
541720

DUNS

962637521

CAGE  
Code

60ZA4

TAX ID

26-4737123