Recent Success Story from DOJ's Move to the Cloud
April 2020

Spurred by the advent of the commercial cloud, the Internet of Things, and near ubiquitous broadband connection, consumer demand for fast, reliable, and secure information technology (IT) has increased exponentially. This has raised the bar for IT providers and largely outpaces governments' ability to deliver. To prevent falling behind the innovation curve, the Department of Justice (DOJ) continuously monitors the technology landscape for new methods to advance its mission of enforcing the law and defending United States interests. One method that has proven successful for many in the DOJ enterprise is the transition to a cloud-optimized IT environment.

In 2020, approximately one third of DOJ's IT systems are cloud-based, up from less than a handful five years ago. While a technology gap persists between those Components that have transformed their environments and those that have not, the DOJ Office of the Chief Information Officer (OCIO) strives to bridge this gap by delivering world-class, mission-enhancing IT to all Components, Offices, Boards and Divisions. Last year, OCIO did just that by supporting one of its Components as it successfully transitioned to a hybrid public-private cloud model.

In 2019 the Office of the Inspector General (OIG) was relocating its offices, and it needed to determine the best approach for migrating its local on-premises infrastructure. Through assessment and analysis, OIG learned of the benefits of cloud computing and decided to transition many of its existing systems from on-premises infrastructure to a cloud service provider in anticipation that migration to a cloud environment would provide OIG with better scalability, flexibility, availability, and economies of scale.

Collaborating with OCIO's Cloud Management Team (CMT), which performed a comprehensive cloud readiness assessment of the OIG environment, OIG first determined the feasibility of migration. OIG defined core business requirements to govern the strategic direction of any infrastructure transition and based its technical decisions and migration plans on the rule that any transition to the cloud:

1. Must maintain or enhance the level of integration, and it must leverage infrastructure and connectivity to OIG's other systems and external dependencies, such as other DOJ Components.

2. Must increase operational efficiency for the system, for example, by simplifying monitoring or backup processes.
3. Should reduce operational cost, such as using scalable architectures to dynamically allocate resources only when needed.

Ultimately, a hybrid public-private approach proved to be the best solution for OIG, where systems ineligible for migration would be located at a government-owned, government-operated (GOGO) DOJ Core Enterprise Facility (CEF), and cloud-ready, updateable systems would move to the new commercial cloud environment, which would also provide backup services given its more reliable data recovery capability.

The OCIO team successfully engaged with OIG to plan the migration strategy and together the teams determined that working through the DOJ's enterprise-level task order was the best procurement option. This was serviced by the U.S. Department of Interior's (DOI) Foundation Cloud Hosting Services (FCHS) Indefinite Delivery Indefinite Quantity (IDIQ) contract, which also offers FedRAMP compliant IaaS solutions. OIG also determined that streamlining its procurement processes could yield opportunities for improved performance, automation, and other efficiencies to reduce the total cost of ownership.

Following procurement, OIG successfully migrated its eligible test, production, and backup systems to the cloud environment, and, in less than a year from the start of its planning, OIG completed the project in July 2019.

OIG leveraged a handful of practices that ultimately served as keys to success, including:

1. IT Security staff within the OIG were engaged early and often to support and assist the acceleration of requirement implementation related to the ATO process.
2. The OIG-OCIO team shared a clear understanding of network requirements, such as the data routing, netflows, and attentiveness to security requirements, including those associated with the Justice Cloud-Optimized Trusted Internet Connection (TIC) Service (JCOTS).
3. The OIG-OCIO team applied and shared best practices, and they incorporated guidance from early adopters as well as from OMB's Cloud Smart Strategy.

Cloud migration is not simply an infrastructure refresh, but rather a fundamental shift in how technology is managed and consumed. The approach adopted by OIG has instilled new focus on the continued development of complementary operational and procedural changes and demonstrates how solutions can be tailored to meet the unique needs and challenges of an organization and prepare them to overcome IT challenges swiftly and successfully in support of the mission.