White Paper

How Government Agencies Meet Security and Compliance Requirements with the Cloud

Sponsored by: Amazon Web Services

Shawn P. McCarthy  Adelaide O'Brien
September 2020

IDC OPINION

IDC believes that becoming cloud enabled is a foundational component for U.S. federal government agencies to achieve meaningful digital innovation and that cloud adoption strategies address short-term and long-term agency mission needs, technology readiness, and staff skills. As more agencies migrate applications and workloads to the cloud, including their most sensitive and heavily regulated data and workloads, a key consideration in their journey is the need to meet federal compliance and security mandates, including forethought that seeks to address any new legislation that may be passed. Managing security and compliance requirements, especially as laws and reporting requirements evolve, can become complex, tedious, and expensive.

By using the cloud, these agencies can take advantage of increased security, compliance, and resiliency for their most sensitive workloads. To realize these benefits, agency technology leaders must implement and manage cloud strategies using best practices, the right technologies, and a development environment that takes current and future compliance needs into consideration.

SITUATION OVERVIEW

There are many trends driving the need for secure cloud environments that meet the strictest requirements of various federal compliance regimes. As organizations move to the cloud, CIOs and IT departments are increasing overall demand for solutions that enable flexible business models, enhance customer experiences, and drive more efficient delivery of mission-critical services and information. Security and compliance are the cornerstone of this foundation.

Meeting security and compliance requirements when deploying cloud-based solutions is paramount for government and other highly regulated industries. Agencies are entrusted with many kinds of sensitive information that, if inappropriately accessed, could compromise national security, financial systems, energy production, and other critical infrastructures. The responsibility to secure this information introduces unique data protection challenges. Compliance with mandates including Federal Information Security Management Act (FISMA), International Traffic in Arms Regulations (ITAR), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), and other system and data protection frameworks is a key part of building and maintaining a highly secure cloud architecture.
Many agencies are adopting cloud-based initiatives to make data-driven decisions, enhance operations, and improve services, all within appropriate levels of security and protection of data. IDC Government Insights has observed the following IT modernization and digital transformation (DX) initiatives that support security and compliance:

- **Compliance with executive orders and legislation.** In addition to complying with security standards, policies, regulations, and other mandates, agencies must comply with executive legislation. The President’s Management Agenda encourages IT modernization to increase productivity and security by improving the customer experience that citizens and businesses can expect when interacting with federal services.

Legislation such as the Modernizing Government Technology (MGT) Act requires federal agencies to securely modernize IT systems and create more high-quality and time-sensitive services. Similarly, the Office of Management and Budget (OMB) has instructed agencies to adhere to the Cloud Smart policy, an interdisciplinary approach to federal IT modernization to maximize value from technology investments and enhance security.

The MGT Act promotes and supports agency efforts to invest in modern technology solutions that will improve service delivery to the public and "secure sensitive systems and data and save taxpayer dollars." Cloud Smart sets a broad governmentwide strategy designed to drive cloud adoption in federal agencies. Together, the MGT Act and Cloud Smart provide agencies with the information and recommendations they need for cloud success. These laws play a pivotal role in modernizing federal IT to improve accessibility, cybersecurity, and citizen-facing services while providing guidance for modern application procurement and upskilling the workforce to help foster cloud adoption and implementation.

In support of the MGT Act and Cloud Smart, cloud influence and guidance are also promoted in White House Memorandum M-18-12, which offers this advice for agency technology leaders moving to the cloud: "Successful projects will demonstrate a strong execution strategy, technical approach, and have a strong team with a demonstrated history of successful modernization efforts. Agencies should, to the extent practicable, consider the adoption of commercial technology solutions in their proposals and provide a strong technical approach and acquisition strategy to implement those solutions."

- **Moving workloads with Controlled Unclassified Information (CUI) to the cloud.** Controlled Unclassified Information is government-created or -owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and government-wide policies. CUI data is considered sensitive, but not classified, and can include information involving critical infrastructure, national defense, intelligence, legal, health records, statistical data, and personally identifiable information (PII). If lost, stolen, or destroyed, it could be considered a significant risk to national security.

Some cloud providers offer no-cost scripts and software templates that automate cloud controls, allowing customers to automatically stand up cloud environments in a matter of hours while adhering to specific standards. For example, templates are available to quickly and
automatically stand up environments aligned with NIST SP 800-53, which covers security and privacy controls for federal information systems and organizations, and NIST SP 800-171, which governs how to protect CUI within nonfederal information systems.

It is important for technology leaders to understand how sensitive and heavily regulated CUI data is classified and securely stored, processed, and transferred. Many secure cloud-based solutions offer a standardized and accelerated path to achieving compliance with government policies and regulations, including requirements found in the following:

- **Federal Risk and Authorization Management Program (FedRAMP),** which provides a standardized approach to security, system compliance assessment, and adherence to specific cloud security standards
- **International Traffic in Arms Regulations,** which seeks to check and enforce compliance with rules that restrict and control the export of defense and military-related technologies
- **The Department of Defense Security Requirements Guide (DoD SRG),** which provides a standardized assessment and authorization process for cloud service providers to deliver DoD provisional authorization so that systems are able to serve DoD customers
- **Export Administration Regulations (EAR),** which works toward compliance with export control laws that affect the manufacturing, sales, and distribution of technology
- **The Federal Bureau of Investigation’s (FBI) Criminal Justice Information Services (CJIS),** which provides tools and services to law enforcement, national security, and intelligence community partners
- **Cybersecurity Maturity Model Certification (CMMC),** which is a set of processes and best practices designed to reduce risk related to specific sets of cyberthreats (While the effort has had some early pains, it's likely to be part of the federal IT landscape going forward.)

Each of these policies and regulations introduces guidance on how a secure cloud should be set up to better safeguard sensitive information, including all categories of CUI. In any service provider relationship, including with cloud providers, security is a shared responsibility between the cloud service provider and the customer. With cloud, the cloud provider is responsible for the ongoing operations, management, and controls from the host operating system and virtualization layer down to the physical security of the datacenters. This model shifts many of the requirements for meeting and maintaining a secure environment off of the customer, reducing the operational burden and costs to meet security and compliance requirements, compared with scenarios where agencies are utilizing on-premises systems and datacenters. For CUI and other sensitive workloads, some cloud providers also offer isolated infrastructure that is only available to U.S. persons and managed by U.S. citizens. These cloud providers meet strict security requirements to support CUI and citizenship requirements from EAR and ITAR.

- **Adoption of flexible, commercial technology solutions.** Successful cloud providers also foster a community of consulting and technology partners that provide government-vetted technologies. Online marketplaces are available to help customers discover, purchase, migrate, and immediately start using software-as-a-service (SaaS) and platform-as-a-service (PaaS) solutions that are FedRAMP compliant. Many of these solutions are consumption based, meaning you only pay for what you use, and are engineered to be low friction so that agencies can be quickly and easily deployed at the project level or agencywide. This can help agencies achieve mission objectives in days versus months, through 100% cloud-hosted solutions that also meet stringent government security requirements.
Risks of Not Adopting Cloud

Legacy systems (i.e., outdated computing software and/or hardware that is still in use and typically owned, operated, and maintained within the government on-premises datacenter) have challenges ... These systems tend to carry higher risks of failure, a higher cost of ownership, and greater security vulnerabilities. In addition, they offer limited integration and orchestration between various systems and applications, limiting the speed and scale at which the IT organization can operate. These downsides end up affecting an agency's ability to innovate, modernize, and reduce technical debt over time. When a system remains on premises, the agency misses out on the benefits from the shared responsibility model and is usually responsible for everything/managing the entire technology stack, from infrastructure and application security upgrades and patch management to expanding system functionality and security controls (often with new coding) when a new law is passed. Also, when a legacy system goes down, it's the internal staff that ends up having to troubleshoot and fix the problem, absorbing time and redirecting focus from serving agency mission and citizens. Further:

- **Security and transformation.** Besides having to manually coordinate security upgrades and patch management, administrators must make sure their legacy IT solutions are compatible and integrated with enterprise access control systems and enterprise system monitoring tools. This is a tall order, and sometimes not a priority for CIOs. When security and other management challenges are not fully addressed by IT teams, agencies risk falling behind and postponing important upgrades. But, most importantly, they grow increasingly vulnerable to cyberattacks and fail to capitalize on cloud-enhancing security capabilities like secure APIs, agile governance, and ubiquitous encryption.

- **Misalignment with compliance requirements.** Many legacy government IT systems are configured to meet the business deliverables of a past time period and an outdated set of laws no longer in effect. As compliance and regulatory requirements adapt to address IT advancements and an evolving threat landscape, or as agencywide requirements are adjusted, adherence to new compliance standards becomes a challenge. While cloud solutions do not inherently reduce the risk of missteps with custom-coded application, cloud-based workflows and integrations allow for some agility, and they are often highly flexible adhering to new compliance requirements.

While legacy systems and other on-premises systems can be reconfigured and reprogrammed, the amount of effort grows as the system ages. For older systems, staying current with compliance requirements can take up an increasingly large portion of IT staff time. Keeping compliance requirements and management efforts in sync across an organization becomes easier when there is a standard solution set hosted by a cloud provider. The cloud can save time by rapidly deploying compliant infrastructure and services, reduce complexity through automation and support services, and provide greater flexibility to scale and pivot as the agency's needs change.

- **Accumulating technical debt.** According to the GAO-19-471 report issued on June 11, 2019, OMB estimates that out of a $90 billion IT budget in FY19, about $72 billion (80%) is allocated for operations and maintenance of aging and legacy technologies. (One rule of thumb suggests that agencies should plan on spending 30% of the original system cost on annual maintenance.) All on-premises IT systems need maintenance to keep the system working the way that it was designed to, and often this is deferred, accumulating technical debt. In addition to forgoing maintenance, agencies may postpone patch management, addressing security...
issues, and updating access controls to the extent that systems are so old and antiquated that they effectively cannot be updated.

- **Ill prepared for the next emergency.** Challenges from the COVID-19 pandemic propagate the fact that DX is critical, as traditionally siloed government transactional systems not only limit access to information but also make it challenging for employees seeking data from numerous sources in obtaining a holistic view of citizen needs. COVID-19, and other emergency situations, demonstrates the pressing need for operational continuity and resiliency to quickly pivot to enabling a remote workforce. Legacy systems also significantly limit the ability to make service delivery transparent and often hamper delivery of critical information and services. Agencies that have started their digital transformation journey with cloud as the operational underlining of agency DX and agencies that have already migrated to the cloud are faring much better during the pandemic compared with agencies that have not started this journey. Cloud-based platforms have enabled employees to move from office work to telework literally overnight and enabled them to securely collaborate with their partners and serve citizens via highly resilient and secure access to data. Legacy systems would struggle to meet the resiliency and backup capabilities of the cloud, during a pandemic or any emergency, exacerbating cybersecurity vulnerabilities and risking technical workforces falling behind.

### Paying Off Technical Debt

The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) migrated its systems to a cloud architecture. Mason McDaniel, chief technology officer at ATF, provided insights about moving to cloud at the recent AWS Public Sector Summit in Washington, D.C. “We knew we wanted to move to the cloud from day one. There is no government datacenter that can compete with the security, scalability, and the efficiency of the cloud. We wanted to try to tackle a huge part of our infrastructure and pay off the technical debt that we’d accumulated over 10, 15, 20 years of not investing in our IT and get us up to a common modern technology baseline. The only way we could really do that at scale efficiently enough and quickly enough to make a difference was we flipped it … We migrated all the data (development, test, and production data) into AWS and got our full security approval to operate.”

### Expected Benefits of Cloud

Many of the risks of not adopting cloud that may come from remaining with on-premises solutions (as listed in the previous section) are heightened with the increased security, operational resiliency, flexibility, and steps toward DX that come with cloud-hosted systems.

In a recent survey, IDC asked government decision makers to select which benefits in the cloud evaluation process they expected to achieve from their organization’s cloud purchase, use, and strategy. The following are the top choices selected as shown in Figure 1.

- **Business agility and innovation.** Improving business agility, driving modernization through DX, and improving time to market are top benefits that U.S. federal agencies expect from public
cloud purchase and usage as seen in Figure 1. These top choices reflect the fact that the latest releases of platform services that enable innovation tend to reside on public cloud, and coupled with innovation accelerators like advanced analytics, machine learning, artificial intelligence (AI), and Internet of Things (IoT), agencies can drive innovation and transformation. And the near unlimited scalability of public cloud provides agencies the resources needed to quickly meet changing business needs with the reliability of a cloud provider’s network of servers and marketplace of innovative solutions.

- **Improved customer experience.** Cloud can enable remote agents (as well as IT help desks), empower omni-channel contact center capabilities, and enhance customer experience with artificial intelligence-enabled contact centers. Most importantly, it can standardize IT and app platforms in a way that can help agencies directly address any misalignment they may have felt with older systems, such as being out of sync with current or evolving compliance and reporting requirements.

- **Improved security.** Improving cybersecurity is another top expected benefit from cloud. IDC has observed that agencies are embracing the fact that a fully deployed cloud solution with network segmentation, monitoring capabilities, advanced identity management features, and encryption enables more rapid prevention, detection, and response to threats as they emerge than do legacy systems. Cloud can also provide standardization and easier deployment of critical security patches. Even organizations with the most sensitive workloads are convinced that cloud enhances security while enabling faster innovation. And, according to Sean Roche, associate deputy director of Digital Innovation at CIA, at the 2018 AWS Public Sector Summit in Washington, D.C., "The cloud on its weakest day is more secure than client/server solutions."

---

“The cloud on its weakest day is more secure than client/server solutions.”

— Sean Roche, associate deputy director of Digital Innovation at CIA
FIGURE 1

Benefits Expected from Public Cloud Purchase, Usage, and Strategy

Q. While in the evaluation process, which of the following benefits did you expect to achieve from your organization’s cloud purchasing, usage, and strategy?

<table>
<thead>
<tr>
<th>Benefit</th>
<th>(% of respondents)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improve business agility</td>
<td>44</td>
</tr>
<tr>
<td>Improve time to market and/or expand into new market segments</td>
<td>41</td>
</tr>
<tr>
<td>Help drive innovation and/or digital transformation in the business</td>
<td>41</td>
</tr>
<tr>
<td>Improved customer experience (CX)</td>
<td>40</td>
</tr>
<tr>
<td>Improve IT security</td>
<td>39</td>
</tr>
<tr>
<td>Give business units (e.g., sales, marketing, corporate communications, customer support) more direct control over sourcing their own IT solutions</td>
<td>38</td>
</tr>
<tr>
<td>Reduce the total size of IT budget</td>
<td>35</td>
</tr>
<tr>
<td>Simplify and standardize IT infrastructure and applications platforms</td>
<td>34</td>
</tr>
<tr>
<td>Improve IT staff productivity and/or reduce size of staff</td>
<td>31</td>
</tr>
<tr>
<td>Get access to the newest functionality faster</td>
<td>20</td>
</tr>
</tbody>
</table>

n = 93


AWS PROFILE

AWS builds highly reliable, scalable, and low-cost infrastructure platforms in the cloud. It is one of the largest such providers in the world, with millions of customers including most government agencies in the United States and many around the globe. Its systems power hundreds of thousands of business and government customers around the world. At AWS, security is a top priority. AWS customers benefit from datacenter and network architecture built to meet the requirements of the most security-sensitive organizations.
AWS offers government customers infrastructure technologies, including compute, storage, and databases. AWS’ GovCloud (US) regions also host and offer emerging technologies, such as machine learning and artificial intelligence, data lakes and analytics, and support for Internet of Things.

With the AWS Cloud, agencies control where data is stored, who can access the data, and what resources an organization is consuming at any given moment. Fine-grain identity and access controls combined with continuous monitoring for near-real-time security information ensure that the right resources always have the right access to agency information. AWS also provides security automation and activity monitoring services to detect suspicious security events, such as configuration changes across an integrated system. AWS has the ability to significantly accelerate compliance (and associated compliance authorizations) by moving workloads into a purpose-built, compliant cloud environment. This can assist agencies in avoiding compliance "fatigue" with automation, visibility, and scale.

AWS offers dedicated infrastructure services to support government workloads across the full range of sensitive data classifications, including Unclassified, Sensitive, Secret, and Top Secret. By moving sensitive workloads to AWS, the U.S. government is better able to securely and compliantly deliver necessary information and data to mission stakeholders.

Two dedicated and isolated (both logically and physically) AWS GovCloud (US) regions are purpose built to meet with strict compliance requirements including FedRAMP High baseline, CJIS, ITAR, EAR, DoD SRG for Impact Levels 4 and 5, FIPS 140-2, IRS-1075, and other compliance regimes. These regions are exclusively operated by employees who are U.S. citizens on U.S. soil and are only accessible to U.S. entities and root account holders who pass a screening process and can enable government agencies to up-level their disaster recovery and continuity of operations capabilities.

These features help address technology leadership concerns that sensitive, heavily regulated data is classified, processed, stored, and secured per federal guidelines. That makes for a set of skills and solutions that also enable program managers and mission owners to leverage cloud-based capabilities. This set of government-focused solutions includes core service areas such as compute, storage, database, networking, and security as well as numerous native AWS services that are authorized to run FedRAMP High, DoD Impact Level 5, and ITAR workloads. The goal is to help address potential issues related to latency, capacity, and also ongoing security, resiliency, flexibility, and scalability.

Security and compliance are primary considerations for many organizations as they begin their cloud journey. However, agencies can face obstacles and challenges using commercially available solutions that may not have the required security certifications due to complexity, time, and cost to achieve an Authority to Operate (ATO). To accelerate the authorization journey for technology partners seeking an ATO for FedRAMP, DFARS, CJIS, and many other compliance programs, AWS offers ATO on AWS. ATO on AWS is a partner-driven process that includes training, tools, prebuilt AWS CloudFormation templates, control implementation details, and prebuilt artifacts. Software solution providers are able to access direct engagement and guidance from AWS compliance specialists and consulting and technology partners that are a part of the AWS Security Automation and Orchestration (SAO) initiative. As of August 2020, AWS has helped more than 100 partners achieve FedRAMP ATO. And 53 technology solution providers have 56 products built on AWS GovCloud (US) to achieve/maintain their FedRAMP ATO (at the Moderate and High baseline). Agencies are able to find nearly 1,800 solutions available in the AWS Marketplace for AWS GovCloud (US). Agencies can develop strategic partnerships with systems integrators that have successful past experiences bringing cloud-hosted
systems into government networks. By leveraging the extensive partner expertise and the tools available on ATO for AWS, solution partners can expedite compliance security certifications such as FedRAMP and provide sought-after solutions securely on AWS GovCloud (US).

As of August 2020, AWS has 79 services, and 92 services authorized for FedRAMP High and Moderate, respectively, with new services continuously under audit for ATO by the FedRAMP PMO. Similarly, it has 79 services available in AWS GovCloud (US) that are authorized to support DoD SRG IL4 and IL5 workloads. This broad portfolio of compliant, native SaaS solutions enables agencies to quickly determine if the solution has the required security compliance and select the best fit for mission. Further:

- **One agencywide application migration success story from the Navy.** Historically, in the U.S. Navy, on-premises systems were dispersed across various bases or programs. That could complicate efforts to collect, process, and quickly analyze mission-critical data. The Navy worked with AWS and SAP National Security Services to migrate the services' large SAP enterprise resource planning (ERP) system to AWS GovCloud (US). The new system, which includes CUI, displays details on inventory and the movement of tens of billions of dollars in parts and services into a single, widely available solution set. It supports over 72,000 users and 6 U.S. Navy commands while helping staffers make up-to-date and informed decisions related to logistics, financial reporting, and budgets. It can also be set up to display maintenance and repair logs. The Navy also procured high-end in-line databases and other brand-name solutions to help internal customers securely move applications and workloads to the cloud. The full migration was completed ahead of schedule and under budget.

- **Another DX success story that helped improve citizen engagement is the U.S. Census.** The 2020 Census is the first time the Census Bureau has allowed people to participate in the decennial count online, making it a remarkable DX success story. To help make this happen, the Census Bureau worked with AWS to host its 2020census.gov website on AWS GovCloud (US). This allows the Census Bureau to host sensitive data while enabling better citizen engagement and secure data collection, meeting U.S. government security and compliance requirements. The system collected 9PBs of data before the middle of 2020. The site has over 4,000 Amazon Elastic Compute Cloud (Amazon EC2) instances allowing the system to scale as needed, as it meets the demands of millions of citizen participants, in a secure and accurate way. Ultimately, this supported better citizen engagement and data collection.

To avoid purchasing expensive hardware and software, the Centers for Disease Control and Prevention (CDC) turned to AWS for its low-cost pay-per-use model, high availability, and security and compliance practices. This helped CDC create a national repository of syndromic surveillance data that includes all the protections needed to protect privacy including independent security testing at the FISMA Moderate Level.

**AWS CHALLENGES AND OPPORTUNITIES**

Most government agencies know that AWS GovCloud (US) regions are designed to host sensitive data and regulated workloads and address the most stringent U.S. government security and compliance requirements. And in addition to providing AWS GovCloud (US) to government customers, the focus of this white paper, AWS GovCloud (US) is also available to other vetted industries such as nongovernmental organizations (NGOs) and commercial companies in industries such as aerospace, defense, financial services, energy, and healthcare. From CUI, PII, sensitive patient medical records, and financial data to law enforcement data, AWS can help customers address compliance at every
stage of their cloud journey. IDC recommends that AWS consider more aggressive outreach to these government-regulated industries, often ecosystem partners of U.S. federal agencies, to educate key decision makers on AWS’ security and compliance capabilities. AWS should consider specific thought leadership collateral of how each of these different market segments have accomplished mission outcomes while protecting Controlled Unclassified Information.

AWS also needs to remind agencies that hosting solutions in an AWS GovCloud (US) region is always an option. Agencies sometimes fall into routines where they mostly buy off the same contract or work with specific vendors. But AWS has governmentwide contracts that can be tapped into – by both civilian and defense agencies (even if those agencies are mainly authorized to buy from specific contracts). Outreach to procurement officials and legal compliance teams for contracts may be necessary to clarify all of the options that are available.

ESSENTIAL GUIDANCE FOR PUBLIC SECTOR DECISION MAKERS

IDC believes that becoming cloud enabled is a foundation for digital transformation to meet agency mission needs. IDC recommends that agency initiatives include a cloud strategy and road map the agency needs to take now and in the coming years and an assessment of its mission needs, technology readiness, and staff skills.

IDC also recommends that agencies adopt a change management approach to address employee morale and organizational health as well the steps required to digitally transform and implement cloud. Successful cloud deployment is all about leadership and involves every function and level in the organization. Many agencies are hierarchical, and following the leader is a norm; however, to successfully deploy cloud, leadership must have a shift in cultural/organizational mindsets, establish the goal of leading the agency into a cloud modern age, and create and communicate the vision to the entire organization. Leaders should also champion success and articulate the benefits cloud will bring about to the organization, employees, and constituents.

Transition plans should include the level of effort required to move workloads to cloud, the readiness of staff, and the capability and security certifications of vendors as well as uses and deployments of 3rd Platform technologies of Big Data, mobility, and social business apps and innovative technologies such as AI, machine learning, and IoT. Agencies must understand the sensitivity of the data that will be used with cloud service providers to ensure that the vendor selected will be able to provide the right level of security.

Data protection and privacy by design are the core of many risk-based management decisions. Protecting data and privacy is foundational for agencies to ensure ethical actions and accountable social responsibility, as well as laying strong building blocks of trust. Understand the scope of the security requirements your agency must follow. What regulations apply? What information that you collect, store, process, and transmit is subject to these security requirements? and What workloads and data stores subject to regulation are you considering moving to cloud?

Due to the migration challenges exacerbated by accumulating technical debt, IDC Government Insights advises that agencies not wait for end of life of their legacy systems to replace on-premises systems with cloud. In addition to exorbitant maintenance costs, agencies that accumulate technical debt are unable to deploy innovative technologies such as Big Data, AI, machine Learning, and IoT.
DoD customers can decrease the system authorization burden they face by working directly with DISA to focus on speed and compliance related to their cloud migration.

Some agencies have more success at starting their cloud migration by moving smaller, easier workloads and then working toward larger systems. Lifting and shifting is easier than working through the challenges of enterprise-level workflow analysis and system reengineering. As agencies migrate with a greater pace and scale, overall modernization efforts will become more transformative with long-term impact on citizens and technology capabilities. It's also worth seeking out other agencies that have tackled similar use cases and moved similar workloads to the cloud to identify what opportunities and challenges they faced during journey to the cloud.

Remember, compliance is a journey, not a destination — and requires continuous monitoring, auditing, reporting, and upgrades to stay abreast of latest requirements. Cloud providers become key providers in helping agencies meet these challenges. When engaging with cloud providers, agencies should build out detailed compliance plans that summarize how their organization will work with a cloud provider to satisfy requirements imposed by security regulations. Solutions such as AWS GovCloud (US) have substantial security and compliance capabilities built, tested, and conformant with many federal requirements already. Select a cloud provider that has comprehensive security services and features and can improve your ability to meet core security and compliance requirements, such as data locality, protection, and confidentiality and CUI, as required.
About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data – Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2020 IDC. Reproduction without written permission is completely forbidden.