ORACLE

Building a National Security Cloud

A Reference Model

March 2021, Version 1.0

Table of contents

Executive Summary

Defense, intelligence, interior, and border security agencies use information technology (IT) to enable operations and maximize effectiveness and efficiency. Like all modern enterprises, these agencies see cloud computing as an effective way to harness computing resources to meet mission needs. Yet, given the dire implications of the loss of confidentiality, integrity, or availability of IT resources within the national security community, any use of cloud resources must provide the same or higher levels of assurance as achieved in legacy computing environments. For this reason, many national security agencies around the world developed dedicated national security clouds that bring cloud computing resources onto separate and secure national security networks. This paper leverages past experience to provide guidance on how to develop a strategy, envision a common architecture, and work with cloud vendors to build a national security cloud.

Elements of a National Security Cloud

- **Fundamental Objectives:** Balance mission, security, modernization, and emerging technologies
  - ☐ What factors in the threat and competitive environment are driving cloud transformation?
  - ☐ How important is integrating commercial innovation to mission success?
  - ☐ What will be the critical trends and technologies for your enterprise over the next decade?
- **Interoperable Systems:** Define how cloud and on-premises systems will work as a coherent whole
  - ☐ What critical applications and systems exist in enterprise IT environments?
  - ☐ Which software and hardware vendors already exist in your environment?
  - ☐ What data is most critical to operations and which systems are storing it?
- **Commercial Partnerships:** Work with industry to deploy a multi-vendor environment
  - ☐ Where can commercial applications meet critical modernization needs?
  - ☐ How are vendors differentiated in the services that are most critical to the enterprise?
  - ☐ Which vendors have experience working with the enterprise and its processes?
- **Security, Policy, and Business Frameworks:** Transform operations to allow continuous change
  - ☐ Which organizations and offices are involved in administering and delivering IT?
  - ☐ Which private enterprises can serve as references for business process modernization?
  - ☐ Where are there IT management silos that can be merged to share resources?
- **Empowering Mission:** Push capability to end-users in remote locations
  - ☐ What operational units would benefit from access to cloud-based applications?
  - ☐ What operational environments can forward operators expect to encounter?
  - ☐ How will cloud-connected systems at the edge remain connected to central IT resources?

Introduction

"The Department of Defense (DoD) has entered the modern age of warfighting where the battlefield exists as much in the digital world as it does in the physical. Data and our ability to process data at the ready are differentiators to ensure mission success. Cloud is a fundamental component of the global infrastructure that will empower the warfighter with data and is critical to maintaining our military's technological advantage."

U.S. Department of Defense Cloud Strategy, December 2018

Even as the nature of the IT industry is evolving, digital technology is increasingly central to every part of society, from the corner grocery store to the supply chain logistics of global auto manufacturers. The national security enterprise is no different. As with the commercial sector, there is no single objective that has driven national security enterprises to adopt cloud computing. An extremely flexible technology, cloud computing can help to fulfil a variety of needs for institutional transformation. However, there are common themes behind why national security enterprises have deployed cloud technology.

Whether modernizing enterprise applications, building new mission critical systems, or shifting legacy applications to new virtual environments, cloud environments provide the ability to rapidly expand infrastructure to meet mission needs, improving reliability and reducing downtime. Building out cloud infrastructure has allowed national security organizations to jettison finicky hardware that is difficult to maintain and cut down on the number of data centers that the government must manage, secure, and maintain. With the U.S. Central Intelligence Agency's first cloud deployment, IT teams reduced the time to deploy a new, virtual server environment from months to minutes[1]. Furthermore, cloud enhances security, improves access to commercial innovation, enables continuous modernization, and eliminates the need for large capital investments in modernization, all with considerably less work by government employees.

Clearly articulating the full range of reasons and priorities for using cloud services has been crucial to helping the national security enterprise deliver a balanced solution. Even cloud vendors who deliver apparently similar solutions – such as compute infrastructure – are differentiated, each targeting different segments of the market by offering different capabilities. Close partnerships with multiple vendors who offer a varied yet balanced range of services, spanning applications to infrastructure, are also required. Furthermore, the construction of a national security cloud is just the beginning of the organization's cloud journey. After the environment is established, there will be a long process of moving data, migrating and translating systems into the cloud environment, and beginning development of new applications. The process is likely to touch every aspect of an organization, transforming operations as diverse as budgeting, workforce, and security certification. Finally, there will come the work of leveraging the new cloud infrastructure to harness emerging technologies and extend access to the tactical edge.

The goal of this paper is to help the national security enterprise effectively implement cloud technology. There are certain best practices that lead to better outcomes, based on our experience collaborating on cloud computing projects with national security customers. The sections below outline the critical steps that national security enterprises should take to maximize the value and return of their efforts.

[1] https://fcw.com/articles/2017/06/14/cia-cloud-aws.aspx. Accessed March 10, 2021

Elements of a National Security Cloud

- **Fundamental Objectives:** National security cloud can advance mission capabilities, improve security, accelerate modernization, and prepare for emerging technologies. Senior leaders should publish a ***national security cloud strategy*** that defines their vision and priorities for the national security cloud, including which of the outcomes mentioned above are most important.

  - ☐ What factors in the threat and competitive environment are driving cloud transformation?
  - ☐ How important is integrating commercial innovation to mission success?
  - ☐ What will be the critical trends and technologies for your enterprise over the next decade?

- **Interoperable Systems:** Data, applications, and workforce spread across cloud and on-premises environments need to work as a coherent whole. IT and technology leaders will need to establish a ***national security cloud architecture*** that defines the national security cloud that will be made available to the entire enterprise consistently and in a way that connects with existing systems.

  - ☐ What critical applications and systems exist in the enterprise IT environments?
  - ☐ Which software and hardware vendors already exist in your environment?
  - ☐ What data is most critical to operations and which systems are storing it?

- **Commercial Partnerships:** National security cloud should leverage the best services available in the commercial market. Acquisition leaders should consult with multiple vendors on high-level requirements, then look to integrate any vendor that offers differentiated capability into the national security cloud environment through multi-vendor contracting vehicles.

  - ☐ Where can commercial applications meet critical modernization needs?
  - ☐ How are vendors differentiated in the services that are most critical to the enterprise?
  - ☐ Which vendors have experience working with the enterprise and its processes?

- **Security, Policy and Business Frameworks:** Using cloud requires a framework designed for its continuous, automated nature. Leaders in a variety of business operations – in particular, those managing IT operations, budgeting and procurement, and security and compliance – should also adapt and update their operating policies to fully support cloud-based operations.

  - ☐ Which organizations and offices are involved in securing, administering, and delivering IT?
  - ☐ Which private enterprises can serve as references for business process modernization?
  - ☐ Where are there IT management silos that can be merged to share resources?

- **Empowering Mission:** In both the commercial and national security worlds, the value of cloud comes from pushing IT capability and decisions closer to end-users. Front-line leaders should evaluate how extending cloud access to front-line bases, units, and personnel operating cloud can assist the mission and increase operational effectiveness.

  - ☐ What operational units would benefit from access to cloud-based applications?
  - ☐ What operational environments can forward operators expect to encounter?
  - ☐ How will cloud-connected systems at the edge remain connected to central IT resources?

What is A National Security Cloud?

A *national security cloud* is a collection of cloud computing environments from multiple vendors dedicated to the use of the national security community of a country. The defining trait of a national security cloud is a collection of software services, underpinned by hardware and networking that operate according to procedures and policies to ensure availability at differing levels of security and connectivity. For example, national security organizations have unique security requirements, so national security clouds typically include both internet-connected and air-gapped regions. They may also operate systems at the *tactical edge* - such a forward base, a ship, or an aircraft – which are physically rugged and subject to intermittent connectivity.

National security cloud differs from commercial cloud in the engineering and operational experience required to deliver high security and work through intermittent connectivity or within air-gapped environments. Cloud computing succeeds based on the scaled delivery of IT software and hardware in globally consistent configurations. Operations are typically centralized in a few centers, which handle software troubleshooting and updates. Each region typically employs only a few people on-site to assist with hardware maintenance. As a result, working across gaps in connectivity – whether these gaps are required for security or created by operational realities – is challenging.

National security cloud requires special expertise to operate because it creates places where cloud operations cannot leverage existing scale. Introducing air gaps in an otherwise highly connected, scaled network make troubleshooting and updates more difficult. Security clearances limit the number of people who are able to update, troubleshoot, and fix systems. Navigating the complexities of government security accreditation processes requires special skills and experience. In the early days of cloud computing, this meant national security cloud environments were custom built and unable to fully take advantage of the scale and size of commercial markets. Despite these challenges, leading cloud service providers are increasingly delivering their commercial solutions in a national security cloud environment.

WHAT IS A CLOUD?

An increasing number of adjectives are used to describe clouds such as "enterprise", "commercial", "public", and "government." This terminology masks a significant distinction between what *vendors* and *users* mean when they discuss "a cloud." This paper looks at "cloud" from the user's perspective, as described below.

A user-oriented "cloud" is the set of cloud services that a single organization uses to deliver functional capability. It includes services and applications from multiple vendors and operates as part of a larger IT fabric including on-premises data centers and edge devices. This is often discussed as an "enterprise" cloud and is the sense in which we used "national security cloud."

A vendor-oriented "cloud" is a region or set of regions built by a single vendor to address a particular set of customers. The two most commonly discussed are "commercial public" cloud – cloud regions accessible by anyone – and "government" cloud – cloud regions only available to government customers. This distinction is most useful for analyzing a market or defining requirements during procurement.

Fundamental Objectives

"The overwhelming advantages national security agencies will get from the capabilities provided by a secure cloud infrastructure, compared with traditional computing power allocated to specific agencies and functions within them, are clear. A high-technology fifth-generation military with the intelligence capabilities it will need (as proposed in the 2016 defence white paper) requires cloud infrastructure to work effectively. And Australian agency folk know enough about this from their exposure to US agencies with secure cloud infrastructure to get the point."

Michael Shoebridge, "Why Australia's national security agencies need the cloud", 30 Jul 2019

A national security cloud strategy should capture the vision of senior policy leadership and contain a description of the overall operational environment and vision for the project; a description of the desired outcomes; and a statement of the specific goals and imperatives for the project. Clearly articulating the full range of reasons and priorities for a national security cloud is crucial to ensuring adoption of a balanced solution. Even cloud vendors who deliver apparently similar solutions – such as compute infrastructure – take different technical approaches, each with differing strengths and weaknesses. Delivering on a strategy requires a balanced mix of multiple vendors offering varied services – including cloud applications and infrastructure. With a good strategy in place, the individual organizations, offices, and people who actually buy, use, and secure the cloud environment will have a clearer idea of what this mix of vendor services looks like. Beginning by defining the objectives in terms of the four categories identified below – **mission, modernization, security, and emerging technologies** - will help establish a clear picture of the relative priorities for the cloud environment.

Mission

As data and information technology is increasingly central to modern warfare and intelligence operations, national security organizations view their IT environments as critical to their success. Many national security enterprises conclude that serving their unique missions – which do not have parallels in the private sector – requires them to build specialized solutions. Cloud computing has allowed them to leverage the most modern hardware and software development tools and applications – along with continuing commercial innovation - to rapidly build, replicate, and scale workloads and data across multiple regions and classification domains.

Security

Network defenders face an increasing number of systems to protect, a growing number of capable threats, and an ever-changing technological landscape. Traditional techniques used to secure systems – such as use of classified intelligence, elite workforces, and air gapped networks – must be augmented to keep up with the scale of the threat. Cloud environments lets government piggyback on the expertise and experience of cloud vendors, who protect the systems of thousands of commercial customers, and leverage advanced security features and tools that cloud vendors build into their services.

Modernization

National security enterprises were early adopters of networking and computer systems. As a result, their IT environments are complicated tangles of custom-built and commercial applications, operating systems, and hardware of varying ages and currency. Cloud offers the chance to transform legacy applications, moving workflows into fully modern cloud applications, offering improved capability at reduced cost when compared to outdated, custom software. Specialized applications can migrate to cloud environments and harness newer versions of their underlying components, such as databases and identity management systems. Applications that are completely without commercial analogs can move to cloud infrastructure, where they can gradually transform into modern systems as old data centers and old hardware are retired. Furthermore, deploying modern cloud applications can help drive improvements to overall government business processes and financial activities that support IT operations.

Emerging Technologies

Technologies ranging from 5G to Artificial Intelligence to the Internet of Things are critical capabilities to deploy for warfighting and intelligence operations. National security communities understand their competitive edge depends on how quickly they can adapt these rapidly evolving commercial capabilities to their unique mission requirements. Modernization will prepare many existing applications to integrate with these emerging capabilities, but over the long-term, new IT systems will need to be deployed. Because most leading commercial companies in these fields are building their products in cloud environments, national security organizations can more readily keep up with the pace of commercial innovation by also deploying their versions of these technology in cloud environments.

Interoperable Systems

Defining a cloud interoperability framework will help govern the national security cloud and facilitate its integration with existing information technology. These frameworks can help achieve the strategic goals of the environment and guide specific contracting and purchasing requirements. Furthermore, they can help determine how the national security cloud will work in practice. No one path is right for all organizations, but every organization should deliberately consider and build a few common features into their enterprise cloud architectures.

A national security cloud reference architecture should be prepared by the senior national security IT officer, such as a department/ministry -level CIO. It should define how the national security cloud will relate to existing IT environments; how it will operate and be managed; and how it will be used by the organization. An effective framework begins by outlining objectives and approaches across four key areas – **connectivity, security, services, and management.**

Connectivity

Develop a plan that will help ensure connectivity to a consistent set of cloud services in all networks and operational environments. Cloud is appealing because it can deliver a suite of applications, platforms, and infrastructure to an entire organization across multiple sites. This makes it easier to interconnect data sets, replicate and move workloads, and re-prioritize scarce IT talent across different networks and organizations.

Security

Define a set of outcome-oriented goals for ensuring security. Because different cloud vendors approach security in different ways, a high-level architecture that sets security outcomes and goals – rather than granular requirements - will help deliver consistent outcomes across vendors without being overly specific. Furthermore, it leaves room for individual vendors to differentiate themselves by going beyond baseline requirements with new features, services, and capabilities that address the overall goals of the security architecture in innovative ways.

INTEGRATING WITH EXISTING TECHNOLOGY

In planning for and building a national security cloud, it is always necessary to map older existing IT deployments. A national security cloud exists as part of a larger environment that includes on-premises solutions. Some of these solutions will be more compatible with the cloud services of a particular vendor, so including that vendor in the national security cloud will accelerate cloud migration.

DATA ARCHITECTURES AND CLOUD ARCHITECTURES

One of the most frequently recurring goals of a national security cloud is to create an architecture that will facilitate and accelerate data sharing. And while having common cloud applications and technology can help with this goal, cloud architectures deal only with the applications, platforms, and infrastructure used to store, secure, manage, and manipulate data – not the data itself.

Organizations looking to improve sharing and use of their data need data architectures to deal with the structure, formatting, and accessibility of specific data sets. Data architectures apply across an entire IT environment – including both on-premises and cloud environments. They may inform a cloud computing initiative but should be approached separately.

Services

Define a specific set of essential solutions and capabilities that sit at the center of any move to cloud environments. The vast majority of cloud usage will come from just a few applications and services, yet the market for cloud technologies contains thousands of offerings. Identifying specific IT applications and capabilities that matter most, up front, will help filter this universe down to a reasonable set of solutions for technical evaluation and initial inclusion in the environment. The focus will help ensure solutions – such as pre-built cloud applications - are not overlooked in favor of tool-based approaches that take more work to operate and maintain – such as custom code built on cloud infrastructure.

Management

Create an approach for managing the cloud environment that leverages the experience, capability, and relationships of the entire enterprise. This may be entirely separate from existing, on-premises management approaches and may need to include incentives to encourage cloud adoption or migration. Keep any centralized management operation as small as possible by harnessing vendor security and operations teams. Minimize centralized policies while empowering program offices and project managers to pick the solution that works best for their particular need.

Combine the resources and relationships that exist across the entire enterprise. A national security cloud is rarely the first time *any* organization in the national security establishment has worked with cloud. Leveraging experience that already exists within an organization will allow the cloud deployment to scale rapidly.

OPEN TECHNOLOGY

The term "open" is often used in technology to designate something that is freely accessible. However, the terms associated with "open" have very different implications for implementations of technology in the cloud. Three terms come up particularly often – *open data, open standards,* and *open source.*

Open data is a *use case* for cloud services, where a government organization makes data widely accessible by the public or a specific community. It is facilitated by cloud but depends on how the user designs the system.

Open standard denotes compliance with a certain set of *technical specifications*. Systems that comply with an open standard can interconnect with other systems using that standard. In the cloud, this often means it is simpler to port code built to use an open standard from one environment to another.

Open source denotes *free software* with available source code that can be modified by various participants and often distributed without cost. Some cloud services sell open source managed services, where the user is still not charged for the underlying software license but is billed for any compute, storage, and network services consumed. Many open source companies continue to adjust to cloud business models, particularly since some cloud service providers use open source software developed by others as the core of their paid service offerings.

Commercial Partnerships

Building a modern national security cloud requires selecting the right partners. The cloud applications, platform, and infrastructure markets contain thousands of companies – ranging from massive hyperscale providers of cloud-based enterprise applications and infrastructure to small start-ups offering highly specialized applications and infrastructure capabilities. The situation is further complicated by the presence of specialized contractors and consultants, who build customized virtual environments using third-party or open source technology, and integrators, who re-package and resell services from other companies. All describe their services and offerings in different ways.

Understanding the cloud market helps in identifying and selecting the right partners to build the cloud environment. Media and analyst reports are useful for research, but they take a broad view that often emphasizes raw market share over technical quality. Vendors can help provide technical information, but few will expose and explore all the trade-offs involved in using their solutions. Internal IT staff and developers can help identify requirements, but they may not fully understand or embrace enterprise business and strategic interests of the enterprise.

Ultimately, senior executives and mission owners need to own the project, with support from cloud champions at every level of the organization. The most difficult task will be to cut through the technical terminology and market jargon. Procurements should be conducted based on strategy and architecture, using high-level requirements and partnerships with multiple commercial vendors. It is best to begin with consultations with both cloud service vendors and users before moving to requests for information and, finally, procurement. Procurements are best phased, building in complexity towards a fully realized, multi-vendor cloud environment. As the total procurement amount achieves larger scale, government can often incentivize vendors to build regions at their own expense by offering to support security accreditation. The following section breaks down the cloud market by three key axis – **accessibility, IT layer, and business model** - using market terminology to help structure this process.

Accessibility

Cloud computing pools and shares resources for many users in a single environment. Cloud services are also offered in different regions, with access to each granted based on the type of user or service offered. The following categories are arranged in order of increasing complexity:

- **Public clouds** are standard, commercially available offerings, built by a company to service most of their customers. Because they are open to use by nearly any customer, they are best for non-sensitive data, such as open data sets or facility websites. They are readily accessible, and useful for initial pilots and experimentation.
- **Community clouds** are isolated cloud environments built to service a specific set of customers – such as government agencies or the military – and may be required to demonstrate compliance with specific security certifications. Depending on the size of the customer set, they may be built "at risk" by a cloud vendor who sees potential for growth, or with cost split between the customer and the vendor through a commitment for minimum annual or periodic spend. Costs for community clouds are typically comparable to public clouds, though some vendors make these regions the last to receive price cuts and new services as a result of their more limited market

SOVEREIGNTY AND THE CLOUD

Deploying cloud means working with vendors from around the world. Yet many governments – and national security enterprises in particular - are reluctant to work with foreign companies. Fear that a vendor could be influenced by outside pressure to compromise cloud software, networks, data, and operations is understandable, but it is a risk that can be managed.

It is possible to work only with domestic companies – and, for certain, extremely sensitive applications, this may make sense. But limiting competition to domestic vendors is not possible in most cases and will certainly limit access to the most modern commercial capabilities. A better solution is to focus on the level of control over a cloud service required to reduce risk, then make purchase decisions accordingly.

Aspects to consider include logical control of updates and virtual environments, operational control of networks, physical control of hardware, and access control for personnel. Vendors offer cloud technology and business model options that offer varying levels of control over all these areas. Finally, many companies offer versions of major platforms that work the same whether deployed in the cloud or on-premises.

and more stringent security certification requirements. They are useful once a government has decided to commit to scaled cloud migration and operation.

- **Dedicated clouds** or private clouds are built for a single, specific customer to meet their unique specifications. Historically, these have been custom-built private clouds, where the customer bore the full cost of building and operating the environment, and have been the most difficult, complicated instantiation of cloud services. However, cloud vendors increasingly offer variants of their commercial services built and operated to customer specifications, sold at commercial rates, similar to community cloud offerings.

IT Layers

Cloud makes compute a service, with the vendor taking responsibility for managing, maintaining, and updating part of the IT environment. How much responsibility falls on the service provider, as opposed to the user of the service, is another key way to divide the market.

- **Applications:** Commonly called *Software-as-a-Service (SaaS)*, a cloud application is fully managed by the service provider, while the user retains control over, and responsibility for, managing the data stored in that application.
- **Infrastructure:** Commonly called *Infrastructure-as-a-Service (IaaS)* and *Platform-as-a-Service (PaaS)*, cloud infrastructure often provides a virtualized version of the basic hardware used to run systems as well as the tools that can be used to build complete applications.

CONSIDERING DATA

Data is commonly the sole responsibility of the users, but service provider policies and fees around data movement critically impact who has practical control of user data. Vendors can further be divided between those who embrace open architectures, with low or no data movement fees and interoperability provided through open standards, and those who embrace proprietary architectures, with higher data movement fees and interoperability hampered by custom standards and formats.

Business Models

The cloud market has existed for over twenty years, giving rise to companies with a wide array of business models. The market can be divided based on how they deliver cloud services. The following are arranged by ease of contracting and implementation:

- **Commercial**: Commercial cloud service providers focus on *technology* and *engineering*, building and operating scaled cloud services that they sell to many other customers without modification. Most of the vendor's workforce will focus on researching, developing, and building new technology
- **Resold**: Reselling businesses and systems integrators focus on *management* and *integration* of one or more solutions and services built by other commercial firms. Most of their workforce will focus in sales, procurement, and relationship building between firms.
- **Custom:** Firms focusing on a hybrid model of *contracting* and *consulting*, building bespoke cloud data centers, applications, and environments for use by a single customer. Most of their workforce will focus on working directly with customers and managing projects.

Security, Policy, and Business Frameworks

Cloud transformation is not simply a matter of changing technology – it also requires and drives transformation of the processes, procedures, and organizations that support technology and form the bureaucratic glue holding any enterprise together. The cloud migration and transformation process in the private sector has been extensively evaluated, and many comparable large and small private sector organizations have taken this journey. These organizations, which include many enterprises perceived as "low tech" and specializing in sectors other than technology and software, can be harnessed for learning.

Beyond the experiences of these pathfinders, government – and national security organizations in particular – may face unique challenges in three key areas: **IT Operations, Budget & Procurement, and Security & Compliance**.

IT Operations

Cloud migration is as much about facilitating organizational and cultural change as it is about deploying new technology. The workforce will take time to understand and adapt to the new environment, a process that may seem slow from the outside. Key lessons include:

- **Focus on simplifying migration:** Designing tools to help teams learn to use the cloud, such as reference architectures, breaks down barriers to migrating workloads to the cloud. By focusing on making the process of cloud migration easier, more of the workloads that migrate to the cloud will be prepared in advance for their new operational environment.
- **Be cautious with cloud mandates:** Many organizations have created aggressive cloud migration mandates, only to find that some systems cost more and perform worse in a cloud environment. A 2019 study found that 80% of surveyed organizations were planning to "repatriate" workloads to on-premises environment.[2] A measured approach will avoid moving workloads multiple times and unwind policy mandates that have been built into budgeting and management processes.
- **Ask vendors to cross-connect:** The commercial market is increasingly benefiting from service providers who cross-connect their cloud environments, making it simpler to run systems that leverage the strengths of multiple providers.[3] Making this type of interconnect a part of the national security cloud architecture will reduce workload on IT staff.

Budget & Procurement

Cloud up-ends traditional paradigms of IT investment, shifting most expenses from one-time purchases to ongoing, monthly expenses. Adapting budgeting and procurement mechanisms to this new paradigm make it easier for everyone involved in government procurement – from program managers to senior leaders and legislators – to understand and benefit from cloud services. Key lessons include:

- **Make cloud an operational expense:** Reforming budget and contractual procedures to treat cloud services as an operating expense will significantly simplify relationships with vendors and align with the best practices identified by the private sector.
- **Partner with industry:** Service providers and commercial firms have extensive experience using cloud technology. Soliciting their advice and feedback on the future of the technology, as well as specific system requirements, through strategic consultations and by issuing Requests for Information (RFIs) early in the process of project definition helps tap that expertise.
- **Build an environment with continuous competition:** Use procurements that place multiple vendors on open-ended contract vehicles, leaving each program office free to choose the cloud services that work best for their

[2] https://www.crn.com/news/running-your-business/idc-increased-services-pullback-from-public-clouds-huge-it-disrupters

[3] https://www.esg-global.com/blog/microsoft-azure-and-oracle-are-done-being-bullied

needs through individual task order competitions. This encourages vendors to compete continuously, delivering the best price, capability, and performance without complicated contractual provisions or oversight.

Security & Compliance

Organizations with national security clouds must rethink how they manage security and compliance for this environment. Cloud operates with economies of scale; therefore, approaches that focus on pooling resources across organizations and harnessing the continuous, automated nature of the cloud deliver better results. Key lessons include:

- **Harness existing certifications:** Most cloud providers invest significant resources in obtaining key cloud certifications, such as the UK GCloud-11, U.S. FedRAMP, and German C5 certifications. Harnessing these existing compliance frameworks by using community clouds certified to these standards will enhance security, speed deployment, and help manage costs.
- **Combine security and compliance resources across organizations:** National security organizations often like to separate their IT environments, yet cloud works by scaling data centers, hardware, and software. Identifying policies, processes, and technical solutions to enable combining resources across the national security community will avoid forcing providers to go through repeated certifications and audits, while also providing more resources to improve and scale security and compliance efforts.
- **Develop continuous, automated processes:** Cloud technology can deliver continuous, automated streams of information to security operations centers, providing better visibility into operational security than the periodic audits that many certification and compliance processes use today. Update certification and compliance procedures to take advantage of this visibility.

Empowering Mission

The data in national security information systems ultimately needs to reach a distributed and mobile workforce operating at the "tactical edge." This environment is defined by little-to-no connectivity, constant mobility, and harsh environments. Forward deployed equipment needs to operate in in varying thermal and environmental conditions while surviving harsh physical treatment. This is a radical departure for modern cloud computing, which relies on massive data centers with efficient power and cooling to achieve scale and constant connection and finely tuned networks to achieve optimum performance.

Cloud infrastructure service providers increasingly offer a tactical edge cloud environment as part of their commercial offerings. Jump-started by the requirements of industries like oil and gas - which need to collect, process, and transmit sensor data from remote locations – the national security tactical edge is a distinct product category for many vendors. These devices offer a number of cloud infrastructure services in ruggedized and portable forms. Service providers continue to upgrade the hardware associated with these devices, as well as the range of commercial cloud applications and services available on them.

Cloud at the tactical edge is best done in the second phase of a national security cloud initiative. Once core cloud environments are set-up, the organization can tackle more complicated tasks of extending application and data access out to the tactical edge. An effective project will address on the needs of remote elements across three key categories: **connectivity, portability, and ruggedization**.

Connectivity

Define how and how frequently tactical edge nodes will be able to connect back to the core of the national security cloud. Cloud providers increasingly include services for 5G and satellite connections as part of their standard environments. Cloud can also provide the backbone for running high bandwidth 5G networks, helping tactical edge nodes bring and extend their own network.

Portability

Define requirements for how edge nodes need to be transported and whether installations will be permanent or temporary. Tactical edge nodes can vary in size and functionality, ranging from units that can be carried by a single person to devices that can operate aboard a ship or in non-traditional locations. Similarly, define if the tactical edge node is a simple turnkey system or if it needs to work as part of a larger forward data center, temporarily assembled at an operational site.

Ruggedization

Understand and describe the potential operating environment. The tactical edge is a broad category, covering just about any operating environment that is *not* a permanent, temperature-controlled data center. Understand the range of location challenges, including temperature, power availability, shock, environmental contamination, and other operational constraints that make up indented tactical edge environments so requirements can be defined accordingly.

Conclusion

The national security community has learned much about cloud computing in the last decade. But cloud computing is by no means a perfected or static technology. Today, the commercial market spans a new selection of second-generation cloud service vendors, converged cloud offerings, and dozens of new tools and capabilities. These capabilities are rapidly making their way into national security applications. Following the best practices outlined here will help ensure any technology that is deployed meets the needs of the national security mission. Beginning with deliberate direction, high-level goals, and engagement with expert users and service providers will help achieve effective outcomes. Partnerships and continued education will aid creation of a national security cloud, providing a modern set of services that lay a foundation for continued mission success.