STRATEGIC PLAN TO ADVANCE CLOUD COMPUTING IN THE INTELLIGENCE COMMUNITY

JUNE 26, 2019

Table of Contents

From the IC CIO **1**

What We Need – Future State **2**

Purpose **2**

The Way Ahead **3**

Objectives

Cloud Reach 4

Cloud Application 5

Cloud Functions 6

Cloud Operations 7

Cloud Capabilities 8

Cloud Acquisition 9

Cloud Culture 10

Conclusion **11**

Appendices

Appendix A - Alignment to National-level Documents **12**

Appendix B - Evolution of the IC Cloud Enterprise **15**

Appendix C - Terminology **17**

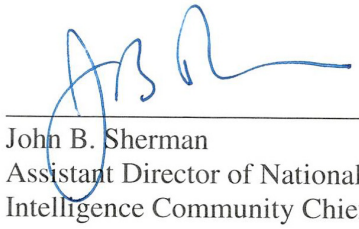
From the IC CIO

The IC faces global technology changes, now creating information at a scope and scale that challenge our ability to quickly deliver insightful and actionable intelligence. Our adversaries are moving out quickly in many areas such as cyber, artificial intelligence and machine learning, information and asymmetric warfare, not to mention other capabilities such as conventional arms and space. We must respond with equal urgency. We can and must win in an arena increasingly defined by technology, data, and cybersecurity. This requires even greater innovation and partnership between the government, industry, allies, and academia.

In this context, a group of IC element Deputies and CIOs met in November 2018 to discuss and outline strategic priorities for IC ITE. We identified a clear need for a strategic plan to address growing requirements for diversified cloud computing capabilities across the IC to help the IC remain agile and adaptive – all the way to the mission edge. The IC requires computing infrastructures that allow our collectors and analysts to tackle tough problems, using artificial intelligence and machine learning to make sense of our vast datasets. These capabilities must not only be secure; but, being federated in their composition, must interoperate seamlessly across security fabrics. Lastly, the IC needs to leverage industry's innovation and speed to stay ahead of evolving world threats.

Recognizing the above, Community CIOs asked key cloud and other experts from the IC to identify what we must do to establish a cloud environment that can adequately address our future needs. The enclosed strategic plan performs three key functions: 1) presents a Community perspective on needed capabilities; 2) charts a course with objectives and initiatives to achieve them and; 3) lays the foundation for subsequent implementation plans. This strategic plan aligns with IC-wide strategies and current acquisition plans. Success will come with follow through, so I will ask the IC CIO Council to prioritize these initiatives, assign owners to implementation, and then oversee progress.

I want to thank my fellow CIOs for their investment in the collaborative model that this strategic plan represents. This is not an IC CIO strategic plan, it is a Community plan. We must – and we will – get this right. And, I look forward to seeing this IC ITE future for the IC.



John B. Sherman
Assistant Director of National Intelligence and
Intelligence Community Chief Information Officer

INTRODUCTION

What We Need – Future State

The Intelligence Community (IC) requires an integrated, interoperable cloud ecosystem that promotes mission success through reliable, survivable, dynamic, and innovative information technology (IT) services with secure access to functions, capabilities, and data anywhere, anytime, and under all conditions. The IC will use Government and multiple commercial cloud capabilities that are interoperable and support workflows within and across multiple security fabrics. To maximize rapid reuse of these capabilities, IC elements will emphasize security trust through shared knowledge and transparency of security assessments and authorizations.

The IC's cloud capabilities will support a diverse set of users to include disconnected or edge operations. These capabilities will provide innovative and contemporary technologies such as artificial intelligence (AI), machine learning (ML), and high-performance computing to meet current and future needs. These capabilities will require unified security processes and acceptance that enable quick adoption and portability of applications, data, and code. The IC will leverage these capabilities in an approach that favors vendor flexibility, simplifies use and adoption of new and cloud-native technologies, and promotes necessary culture changes.

Purpose

The *Strategic Plan to Advance Cloud Computing in the Intelligence Community* lays out seven interrelated objectives and 38 initiatives the IC must achieve to realize the future state described above. More detailed than a strategy yet not as specific as an implementation plan, this strategic plan is designed to be used by executives and engineers alike to align IC elements' efforts; guide IT development and acquisition; modify or establish IC policy, guidance, and specifications; and provide a consensus-driven approach to advancing cloud computing in the IC.

This strategic plan aligns with and complements Federal Government, IC, and Department of Defense (DoD) guidance (detail provided in Appendix A). As articulated in the *National Security Strategy*, the *National Intelligence Strategy*, and supplementary guidance, we face diverse threats such as foreign state and non-state actors and domestic sources challenging us on land, air, sea, space, and cyberspace. This means technology, data, and cybersecurity demand continued innovation and investment to outpace our adversaries and protect our national security. To succeed, the IC must continue to transform and protect its information environment, pushing for better, more modern IT capabilities.

The IC faces daunting challenges from the scope of its missions, the pace of world and technological change, and the scale of available data and information. To meet these challenges, the IC needs greater mission and analytical agility and sophisticated sense-making abilities like AI, ML, and big data analytics. The Community also requires secure, flexible, and rapidly deployable IT capabilities with global reach that also protect privacy and civil liberties.

By achieving the goals and initiatives depicted in this plan, the IC will be able to:

- Extend cloud capabilities to locations in which mission leaders and Chief Information Officers (CIOs) need them
- Build interoperability across the ecosystem to access data and cloud capabilities
- Promote innovation and competition using the best capabilities available from multiple cloud vendors and from across the U.S. Government
- Provide cloud services across multiple fabrics and access to data where it resides
- Enable speed and flexibility through smart implementation of security decisions and procedures
- Broadly share information about cloud computing technologies across the Community
- Initiate a process to collect Community cloud requirements; guide cloud-related acquisition shaped by these requirements; and provide for IC element coordination on acquisition decisions having IC-wide impact
- Make lasting change to mission with cloud computing by fostering needed culture and knowledge

Assumptions

1. Strong governance is key to the success of this strategic plan.
2. This document does not address specifics of data content or data management (e.g., data tagging). Data in IC Information Environment (IC IE) clouds is addressed in the *Intelligence Community Information Environment Data Strategy*.
3. Success of evolving to a cloud ecosystem depends heavily on the *Identity, Credential, and Access Management Reference Architecture* and the *Data Reference Architecture*.
4. Initiatives cited in this document are unconstrained by resources and timelines. More work remains to prioritize, fund, and implement the initiatives of this strategic plan.
5. Collaboration with FVEY partners is integral to accomplishing IC missions. While not specifically cited in this strategic plan, the IC will evolve cloud capabilities to support FVEY collaborations as our allied IT infrastructure matures.

The Way Ahead

The IC is investing extensively to expand and deepen its cloud and high-performance compute capabilities. The *Strategic Plan to Advance Cloud Computing in the Intelligence Community* will influence the Community's shared investments over the next two to six years. Building upon lessons learned and successes of Epoch 1 of the Intelligence Community Information Technology Enterprise (IC ITE) (described in Appendix B), Epoch 2 focuses on establishing interoperability, security, and mobility for IC ITE services and cloud technologies in a federated environment.

Accordingly, IC element CIOs identified seven interrelated objectives addressed below to guide the design, development, and implementation of an IC cloud ecosystem. When implemented, this strategic plan will allow the IC to employ the latest technologies, methodologies, and policies, and evolve along with technological advances to promote our national security interests and the safety of Americans and our allies.

CLOUD REACH

From Core to Edge

Objective A:

Develop and implement a set of resilient, global cloud capabilities across multiple fabrics to enable core and edge users' critical missions across the IC.

Intent:

The IC must deliver actionable, timely, and agile intelligence that provides decision advantage and operational resiliency to partners ranging from national-level policy makers to those at remote or denied locations at the edge. Regardless of mission or location, each user must be able to access, process, and analyze needed information. This includes "forward deploying" cloud capabilities, functions, and data to users operating at the edge.

Initiatives:

A01: Mature data policies and governance to allow for secure, multiple location options at the edge, including commercial properties.

A02: Assess and modify, as needed, logistics and procurement processes to provide OPSEC mechanisms to deliver to edge locations.

A03: Define and engineer IT functions and capabilities needed to operate at the edge.

A04: Prioritize the delivery and availability of services on all fabrics to expeditiously deliver those most needed.

A05: Regularly collect and report on cloud requirements (e.g., CONUS and OCONUS on/off-premises) for services with secure access to functions, capabilities, and data anywhere at anytime to meet current and future needs.

A06: Collect performance metrics to determine performance issues throughout the IC cloud environment and engineer improvements.

A07: Create rapidly deployable cloud services to better respond to worldwide national security events.

CLOUD APPLICATION

Innovative and Agile

Objective B:

Adopt best practices and modular design methods that reduce barriers to entry and accelerate collaboration to allow users the flexibility to rapidly leverage commercial innovation across the cloud ecosystem.

Intent:

IC collectors, analysts, and developers must keep pace with evolving threat landscapes and respond rapidly and flexibly to mission requirements. To meet this challenge, the IC must incorporate, leverage, and operationalize the latest developments in cloud, AI, and ML technologies by partnering with DoD and other Federal Government agencies, industry, academia, and allies.

Initiatives:

B01: Conduct business process re-engineering to streamline and automate IT governance and enable use of new capabilities.

B02: Leverage industry, academia, and other areas to foster collaborative innovation and solve Community problems through cloud capabilities.

B03: Develop secure, no cost/low cost training, guidance, approved templates, tools, and test environments that enable users to learn cloud capabilities through self-service experimentation.

B04: Create suggestion and reward programs to elicit innovative solutions.

CLOUD FUNCTIONS

Interoperable and Seamless

Objective C:

Implement compatible architectures, standards, and common frameworks within the cloud ecosystem to enable seamless system functionality, capabilities, mission success, and promotion of interoperability regardless of technology platform.

Intent:

The IC must collaborate and share information internally and with our external partners. This requires cloud capabilities, system interoperability, and seamless IT interfaces. The need is acute given the explosion in volume and velocity of data and the projected threat landscapes.

Initiatives:

C01: Identify services, policies, standards, and application programming interfaces across the cloud ecosystem to establish seamless operations between systems, agencies, departments, and allies.

C02: Collaborate with technical SMEs, DoD, industry, academia, and vendors and provide workforce incentives to establish, implement, and improve architectures, standards, and frameworks that support interoperability.

C03: Establish integrated testing policies and processes to assess interoperability for IC capabilities in development.

C04: Deprecate closed systems and migrate data/capabilities onto compatible platforms to foster interoperability.

C05: Capture and publish proven design patterns to reduce cost of delivering services and increase speed to delivery.

CLOUD OPERATIONS

Secure and Trusted

Objective D:

Identify, automate, and implement common (inheritable) security controls to enable rapid re-use of best solutions, accelerate available capabilities for mission, and foster shared insights across the IC.

Intent:

The IC must secure and protect its systems and data. The IC's dynamic IT environment provides unique cybersecurity challenges and opportunities in managing its risk posture.

Initiatives:

D01: Mature cybersecurity guidance and processes that incentivize the use of good security practices and automation to streamline assessment and authorization (A&A) across the IC.

D02: Elevate security and risk management concerns, coordinate future work plans, and share information security knowledge and best practices to promote trust and transparency across the IC.

D03: Implement software assurance mechanisms into the development environment and employ joint penetration testing when executing security compliance testing activities in the test environment to reduce the threat landscape and risks earlier in the software development delivery process.

D04: Facilitate A&A by reducing unique security implementations, sharing essential elements of information from Bodies of Evidence, and emphasizing the use of tools and automation to overcome barriers to applications and code portability among IC elements.

D05: Maintain separate security stacks for the elements' enterprise computing environment and the IC cloud environment to prevent introducing an element's risks into the commonly shared cloud.

CLOUD CAPABILITIES

Portable, Mobile, Multi-fabric

Objective: E

Develop common technical standards and enable usage of data regardless of location, service, or technology platform to promote workload portability within and across multiple fabrics, and achieve delivery of the right data to the right people at the right time in the right form.

Intent:

The IC must discover, access, process, and analyze information and foster enterprise-wide information sharing and collaboration. Central to this is a fully featured cloud environment that enables portability of services, analytics, applications, and data across multiple IC IE fabrics, platforms, and geographic locations.

Initiatives:

E01: Mature IC guidance and processes for establishing a secure method for moving data and code across domains and fabrics to ensure portability.

E02: Apply common security and privacy protections to data to enable rapid access by authorized users while preventing unauthorized disclosures.

E03: Leverage cloud capabilities to automate and augment data lifecycle activities across environments based on common standards to enable timely use by authorized people and machines.

E04: Move processing and analytic capabilities in alignment with data repositories to assure data availability anytime, anywhere.

CLOUD ACQUISITION

Fast and Flexible

Objective F:

Streamline the IC procurement processes, develop procurement mechanisms, and implement consumption-based funding and acquisition models to keep pace with the rapidly changing technologies, leverage cloud flexibility, and ensure delivery of new capabilities at the speed of mission.

Intent:

The IC's cloud capabilities must evolve along with rapidly developing commercial IT innovations. To achieve this, the IC must develop and implement an acquisition and procurement environment, consistent with law that can obtain cost-effective, enterprise-level cloud solutions and services with a speed and flexibility that matches the agility offered by industry. This will require training acquisition and procurement staffs and the user workforce. It will also necessitate modifying or developing procurement policies, procedures, and mechanisms.

Initiatives:

F01: Identify common services that can be shared/consolidated to improve cost efficiency.

F02: For acquiring cloud computing services, publish or revise guidance on the use of specific appropriation types (e.g., O&M, RDT&E, PROC) with information that helps minimize impacts from spending limits, availability periods, and narrow definitions of use to enhance IC-wide operational flexibility and consistency.

F03: Develop new or improved policies, processes, and practices to rapidly acquire cloud capabilities and provision cloud services (e.g., IC-wide service catalog).

F04: Establish policies and processes to frequently perform price reasonableness checks of cloud service providers' costs for a given capability.

F05: Train acquisition and user workforce to understand pricing models.

F06: Leverage the IC Procurement Policy Council (ICPPC) to publish license and contracts guidance for more IC-wide consistency for IC clouds.

F07: Have cloud service providers, whenever possible, assume O&M costs with the understanding that these expenses could be recouped through service pricing to streamline budgeting.

CLOUD CULTURE

Changing and Needed

Objective G:

Invest in Community training, development opportunities, and marketing strategies to provide the necessary knowledge and shared understanding that fosters a culture shift toward cloud technologies.

Intent:

The IC must develop new skill sets, enhance personnel understanding and acceptance, and accelerate adoption to fully realize the benefits offered by cloud computing capabilities. To support these shifts, the IC must promote cloud literacy and cultural change in how the IC workforce collects, finds, accesses, uses, protects, and stores data in a cloud-enabled environment. This change will require robust support from senior IC leadership.

Initiatives:

G01: Develop a marketing plan to educate users and provide cloud-pertinent information.

G02: Develop a tailored cloud adoption plan to provide mission with options for cloud development and migration.

G03: Provide cloud training/material to teach technical and non-technical personnel on building cloud instantiations and deploying basic capabilities through self-service.

G04: Implement directives with senior leadership buy-in and senior leadership champions as well as incentivize influential developers to drive both top-down and bottom-up culture change throughout the IC.

G05: Routinely collect and disseminate examples of successfully executed missions in the cloud and lessons learned to build mission, partner, and user confidence in this environment.

G06: Promote culture change that emphasizes market-based cloud solutions and minimizes custom-built approaches to accelerate adoption and lower development times.

CONCLUSION

Information is exploding in volume and velocity and challenging our ability to expeditiously collect, analyze, and draw conclusions from disparate data sets. Additional manpower will not close the resulting gap; we must leverage leading edge technology. The future IC cloud environment presented herein will effectively function as a force multiplier to enhance our effectiveness and address mission challenges.

Modernizing our cloud computing will provide innovative capabilities to missions and users where and when needed. These capabilities will also expand flexibility and improve our ability to leverage data. Moreover, using multiple commercial cloud vendors can promote greater innovation and rapid deployment of new capabilities.

The *Strategic Plan to Advance Cloud Computing in the Intelligence Community* will allow the IC to operate effectively, leveraging technology as well as commercial innovation to better meet evolving mission needs. After implementing this plan, each IC element and the Community as a whole will be closer to unlocking the power of data by managing it as a Community asset and thus providing advantage to the Nation's decision makers.

APPENDIX A
Alignment to National-Level Documents

The *Strategic Plan to Advance Cloud Computing in the Intelligence Community* supports the following: EO 13800, *Strengthening Cybersecurity of Federal Networks and Critical Infrastructure*; the *National Security Strategy*; the *National Intelligence Strategy*; the *Federal Cloud Computing Strategy, from Cloud First to Cloud Smart*; the *Consolidated Intelligence Guidance FY 2021 – 2025; IC 2025 Strategic Priorities*; IC Directive (ICD) 121, *Managing the IC Information Environment*; the *AIM Initiative*, *A Strategy for Augmenting Intelligence Using Machines*; the *IC IE Data Strategy*; the *IC Cybersecurity Implementation Plan*; the *National Defense Strategy*; and the *DoD Cloud Strategy*.

Executive Order 13800, *Strengthening Cybersecurity of Federal Networks and Critical Infrastructure:*

- Effective risk management entails more than protecting IT and data currently in place. This EO also requires planning so that maintenance, improvements, and modernization occur in a coordinated way and with appropriate regularity
- Agency heads shall show preference in their procurement for shared IT services, to the extent permitted by law, to include email, cloud, and cybersecurity services
- The United States seeks to support the growth and sustainment of a workforce skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace
- The Secretary of Defense, in coordination with the Secretary of Commerce, the Secretary of Homeland Security, and the Director of National Intelligence, shall assess the scope and sufficiency of U.S. efforts to ensure the U.S. maintains or increases its advantage in national security-related cyber capabilities

National Security Strategy states that the Federal Government will:

- Use the latest commercial capabilities, shared services, and best practices to modernize our IT
- Improve collaboration with and leverage technical expertise of industry, academia, and R&D sectors
- Establish strategic partnerships with U.S. companies to help align resources in the aforementioned sectors to priority applications supporting national security
- Recruit technical talent by finding ways to create career paths to facilitate the flow of scientists, engineers, and technologists into and out of public service

National Defense Strategy states that:

- The reemergence of long-term strategic competition, rapid dispersion of technologies, and new concepts of warfare and competition that span the entire spectrum of conflict require a Joint Force structured to match this reality
- The security environment is also affected by rapid technological advancements and the changing character of war… New technologies include advanced computing, “big data” analytics, artificial

intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology – the very technologies that ensure we will be able to fight and win the wars of the future

- The DoD will reform for greater performance and affordability:
  - Deliver performance at the speed of relevance
  - Organize for innovation
  - Drive budget discipline and affordability to achieve solvency
  - Streamline rapid, iterative approaches from development to fielding
  - Harness and protect the National Security Innovation Base

Federal Cloud Computing Strategy, From Cloud First to Cloud Smart. The Cloud Smart strategy helps agencies adopt solutions that streamline transformation and embrace modern capabilities. The document states that:

- Three areas require serious consideration and investment: security, procurement, and workforce. Deeply linked, they require an integrated, interdisciplinary approach for a cohesive cloud strategy
- Agencies should transition to security at the data layer instead of the network and physical infrastructure layers, and continuously monitor data to detect malicious activity
- A two-track approach is needed to increase standardization across Government of cloud usage and mitigate risks associated with siloed efforts at executive agencies: 1) determine contractual terms and conditions and; 2) clarify roles and responsibilities, establish clear performance metrics, and implement remediation plans for non-compliance
- Cloud strategies should enable leaders to develop and empower the IT and cybersecurity workforce with skills to achieve cloud migration goals and support the latest technology that will improve critical services. Agencies should also review IT portfolios to determine modernization plans for existing tools
- Federal agencies must ensure current and future workforces are prepared to support Federal cloud environments by consulting with Chief Human Capital Officers to:
  - Analyze skill gaps and remove barriers to expeditiously hire talent
  - Develop and deploy training and education programs
  - Communicate with the workforce about adopting cloud solutions

National Intelligence Strategy states that:

- **NIS Mission Objective 1: Strategic Intelligence** – The IC must master strategic intelligence issues through research, knowledge development, collaboration with experts within the IC and those in academia and industry, and the use of advanced analytics and tradecraft
- **NIS Mission Objective 2: Anticipatory Intelligence** – The IC will improve its ability to foresee, forecast, and alert regarding potential issues of concern and provide the best possible opportunities for action to our national security customers

- **NIS Mission Objective 3: Current Operations Intelligence** – The IC will prioritize its efforts and mitigate risk, operate in denied areas, balance forward presence with robust reach-back, and provide operational resiliency to more fully integrate intelligence with operations
- **NIS Mission Objective 4: Cyber Threat Intelligence** – The IC must continue to grow its intelligence capabilities to meet these evolving cyber threats as part of a comprehensive cyber posture, positioning the Nation for strategic and tactical response
- **NIS Enterprise Objective 1: Integrated Mission Management** – The IC must strike a balance between unity of effort and specialization, using the best of each to meet mission objectives
- **NIS Enterprise Objective 2: Integrated Business Management** – The IC will promote and identify best business practices and functions to optimize solutions and increase collaboration to create a culture of continuous learning, innovation, and partnerships across the Community
- **NIS Enterprise Objective 3: People** — The IC will make long-term strategic investments in the workforce to promote agility and mobility throughout employees' careers
- **NIS Enterprise Objective 4: Innovation** – The IC must drive new levels of innovation by proactively developing and rapidly incorporating breakthrough and incremental technologies, ideas, and constructs
- **NIS Enterprise Objective 5: Information Sharing and Safeguarding** – The IC will take a cutting-edge approach to appropriately access information regardless of where it resides. The IC must continue to adopt modern data management practices to make IC data discoverable, accessible, and usable through secure, modernized systems and standards
- **NIS Enterprise Objective 6: Partnerships** – The IC will optimize existing partnerships and forge new relationships to enhance intelligence and inform decisions

APPENDIX B
Evolution of the IC Cloud Enterprise

Today's IC cloud environment is building on the concepts of the IC Information Technology Enterprise (IC ITE) starting in 2012 when the IC began to evaluate more efficient, consistent, and reliable means to provide compute, storage, and network infrastructure. The Director of National Intelligence designated CIA and NSA as IC Cloud Service Providers, with CIA managing Commercial Cloud Services (C2S) and NSA managing the IC-GovCloud.

C2S was made available in July 2014 as a Community environment that provides cloud functionality on the Top Secret fabric. Over the past five years, the IC worked diligently to develop ways to secure even the most sensitive data in these environments. As C2S matured, the IC provided instances of C2S on the Secret and Unclassified fabrics beginning in 2017. C2S has consistently demonstrated an ability to stay current with technologies while staying ahead of the Government's usage demand.

IC-GovCloud, a government-designed and built cloud to handle large volumes of data, constitutes the IC's big data analytic environment. IC-GovCloud has transformed the IC's ability to analyze massive amounts of data and provide services at a critically needed scale at the speed of mission and is one of the Community's most powerful data analytic and high-performance analytic platforms.

During the past five years, the IC enjoyed many successes with cloud-based technologies, especially with these services. Both efforts initially offered comparable service models but with different approaches based on the needs of the implementing IC elements and their respective risk concerns. Using both cloud platforms enables the IC to keep pace with the latest cloud technology offerings. Collectively, they laid an important foundation for the Community's ongoing IT modernization.

IC CIO has collaboratively matured IC ITE from its early successes and is postured for Epoch 2 to ensure the Community maintains momentum gained since 2012 to deliver even greater mission impact for the next decade. Epoch 2 is characterized by the following:

1) Emphasize cybersecurity as a Community priority. Employ a more holistic and active approach to reducing enterprise IT security risks. Lead both IT transformation and protection of the IC IE to enable enhanced mission success.
2) Develop reference architecture (RA) frameworks to provide standards for common services such as Desktop (Collaboration RA providing capabilities such as universal email and chat), Data RA, and security (Identity, Credential and Access Management RA). In this fashion, IC elements can deploy solutions that fit their unique mission needs provided they comply with the appropriate RA. A main driver for the shift to Epoch 2 was to maintain single-source solutions where applicable, but allow for federated approaches to ensure mission needs are met while maximizing interoperability.
3) Mature the services on the Top Secret fabric and build to multiple fabrics. The IC's partners in the DoD, U.S. law enforcement, and international governments rely heavily on the Secret fabric.

To maximize collaboration and mission effectiveness, the IC is committed to moving capabilities and information to the Secret and Unclassified fabrics, as appropriate.

4) Continue to expand and improve the partnership with DoD and the defense intelligence enterprise, and enhance collaboration and partnerships in coalition environments.

APPENDIX C
Terminology

Capability: The ability to achieve a desired effect under specified performance standards and conditions through combinations of ways and means activities and resources to perform a set of activities.[1]

Cloud: The practice of pooling physical servers and using them to provide services that can be rapidly provisioned with minimal effort and time, often over the Internet. The term is applied to a variety of different technologies (often without clarifying modifiers); for the purpose of this document, cloud refers to physical computing and storage resources pooled to provide virtual computing, storage, or higher-level services.

Cloud Computing: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[2]

Cloud Interoperability: Allows seamless exchange and use of data and services among various cloud infrastructure offerings so they may operate effectively together.

Commercial Cloud: Computing, storage, and network resources and services that a commercial provider maintains, operates, and manages and that are made available to multiple customers (as opposed to cloud resources and services owned and operated by an organization for its own benefit, for example). Depending on the contract, the commercial cloud service provider may be performing in commercial facilities or on-premises in Government facilities.

Edge computing: Real-time cloud services and data processing at the tactical edge of the network near the source of data ingestion. Brings compute capabilities to where the mission occurs in the field; data does not have to be transmitted to a data center for processing. Serves as the decentralized extension of the enterprise networks, cellular networks, data center networks or the cloud.

Fabric: An information environment that supports data at a particular classification/security level, comprised of multiple agencies supporting a variety of authorities with multiple operational capabilities that can include infrastructure and systems (e.g., Secret fabric represents and spans the entirety of USG interconnected and isolated activities to include State, Local, Tribal (SLT), USG partners [U.S. and Non-U.S. based]).[3]

---

[1]DoDAF 2.0, Department of Defense Architecture Framework, Version 2.02, DoD Chief Information Officer, http://dodcio.defense.gov/dodaf20.aspx

[2]National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing*, September 2011

[3]Office of the Director of National Intelligence, *Intelligence Community Enterprise Architecture (IC EA): Multi-Fabric Reference Architecture*, v1.0, 18 Oct 2016

Intelligence Community Information Environment (IC IE): The individuals, organizations, and information technology capabilities that collect, process, or share Sensitive Compartmented Information or that, regardless of classification, are operated by the IC and are wholly or majority funded by the National Intelligence Program. The IC IE is an interconnected, shared risk environment where risk accepted by one IC element is effectively accepted by all.[4]

Interoperability: Ability of a system or a product to work with other systems or products without special effort on the part of the customer. Interoperability is made possible by the implementation of standards.[5]

Migration: The act of moving an application and data from one infrastructure or platform to another infrastructure or platform. Typically, this will require intermediate work to refactor the code to suit the new platform.

Modernization: The act of rebuilding existing software or hardware using modern methodologies and technologies. As an example, an outdated COBOL-based financial billing system might be modernized and developed as a modular, containerized micro-service backend architecture and single page application front end. Alternatively, this could mean replacing a physical server limited in processor speed, memory, and storage space with a more modern machine that uses modern processor architectures and networking protocols.

Security Stack: A stack of equipment or software that performs firewall functions, intrusion detection and prevention, enterprise management, virtual routing and forwarding, and provides a host of network security capabilities to defend and operate the network and respond to threats.

Workforce

- **Acquisition and User Workforce:** Encompasses those individuals who acquire, procure, order, develop, implement, or manage the IC-wide enterprise cloud capabilities.
- **IC Workforce:** The above plus all end users to include analysts, targeteers, collection managers, etc.

[4]Intelligence Community Directive 121, *Managing the Intelligence Community Information Environment*, 18 January 2017

[5]International Committee for Information Technology Standards, Standards Information: Glossary, http://www.incits.org/standards-information/glossary, accessed 30 April 2019


OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA


UNITED STATES INTELLIGENCE COMMUNITY