

UNCLASSIFIED

CLEARED
For Open Publication

May 26, 2021

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Department of Defense
Outside the Continental United States (OCONUS)
Cloud Strategy



April 2021

Office of the DoD Chief Information Officer

Foreword

"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.

To succeed in the emerging security environment, our Department and Joint Force will have to out-think, out-maneuver, out-partner, and out-innovate revisionist powers, rogue regimes, terrorists, and other threat actors.

To support these missions, the Joint Force must gain and maintain information superiority..."

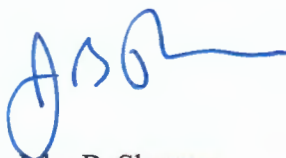
2018 National Defense Strategy

"Cloud devices employed by warfighters at the tactical edge... ..will ensure warfighters are retaining data, feeding it back into models, and fighting with the most recent algorithms. Doing this in a secure environment will be a force multiplier and directly support the primary goal of the cloud environment: information superiority."

2018 DoD Cloud Strategy

The Department of Defense (DoD) Outside the Continental United States (OCONUS) Cloud Strategy establishes the vision and goals for enabling a dominant all-domain advantage through cloud innovation at the tactical edge. It identifies areas requiring modernization to realize the potential of cloud computing in direct support of the warfighter, specifically: security, redundancy, reliability, and availability. It focuses on extending Continental United States (CONUS) cloud computing to the globally deployed elements of the Department to include the African, European, Indo-Pacific, Middle Eastern, and South American Theaters to the tactical edge. The outcomes of the strategy align with and further the priorities of the National Defense Strategy and DoD Digital Modernization Strategy.

DoD is committed to providing cloud computing to the warfighter at the tactical edge. These resources are fundamental to enabling a Joint Force capable of quickly and decisively mobilizing air, land, sea, space, and cyberspace capabilities in response to adversaries threatening United States (U.S.) and Allied National Security priorities and objectives.



John B. Sherman
Acting, Chief Information Officer of the
Department of Defense

Table of Contents

Foreword.....	ii
1. Operational Challenges at the Tactical Edge	1
2. DoD OCONUS Cloud Vision.....	1
3. Goals and Objectives	2
3.1. Goal #1: Provide Robust and Resilient Connectivity to the Tactical Edge	2
Objective 1: Modernize in Theater Communications Infrastructure.	3
Objective 2: Secure Cloud Connections Through OCONUS Cloud Access Points.	3
Objective 3: Leverage State-Of-The-Art Technologies to Connect D-DIL Environments.	3
Objective 4: Enable Access to Information From Multiple Devices and Data Sources.	3
3.2. Goal #2: Provide Computing Power that Enables Forces at the Tactical Edge	3
Objective 1: Deploy OCONUS Cloud Computing Under an Enterprise Construct.	4
Objective 2: Optimize Data Center Infrastructure for Resilient Access to Data and Services.	4
Objective 3: Provide Ability to Traverse Cloud Environments for Persistent Data Access.	4
Objective 4: Protect Data in the Cloud While Enabling Information Sharing.....	5
3.3. Goal #3: Deploy Talent at the Point of Need	5
Objective 1: Establish OCONUS Rotations for Technical Talent.	5
Objective 2: Institute Training for OCONUS Users to Maximize Use of Cloud Resources... ..	5
Objective 3: Deploy Research Talent to Better Address OCONUS Challenges.	5
4. OCONUS Unique Considerations	6
4.1. Host Nations.....	6
4.2. Real Estate, Space, and Power	6
4.3. D-DIL Environments	6
4.4. Data Sovereignty in the Mission Partner Environment (MPE).....	6
5. Next Steps	7

1. Operational Challenges at the Tactical Edge

The OCONUS environment presents unique challenges in meeting warfighter and mission owner requirements based on geographic location, mission set, partnerships, and operating conditions.

Every warfighting asset, including the warfighters themselves, is a potential producer and/or consumer of information. This information must be accessed, analyzed, and distributed to enable data-driven decisions at the speed of relevance. Operating effectively in theater requires persistent access to data sources and producers within a transient, dynamic, and often contested environment. The most significant challenge OCONUS users face is access and sharing information in Denied, Disconnected, Intermittent, or Limited (D-DIL) environments. This challenge is further complicated by the reliance on reach-back to CONUS to access data repositories, analytical technologies, and artificial intelligence/machine learning (AI/ML) advancements for the production of more precise, impactful information and thereby, advancing more informed decision making.

Hostile cyber actors will continue using technical and non-technical means to attempt to defeat the cloud's cybersecurity safeguards, access data and information, and interfere with or disable systems. An adversary's capabilities will evolve over time to become more lethal and elusive. It is essential that every DoD cloud employ world-class cybersecurity capabilities to continuously overmatch the threat.

Valuable data collected and stored locally in theater to support mobile mission sets are often disconnected from broader CONUS-based data repositories, impeding the ability of geographically separated forces to process and correlate perishable information. The joint battlespace requires innovative approaches to cloud resources to ensure data is available at the point of need.

At the tactical edge, use of cloud computing requires secure information sharing through human-to-human collaboration, human-to-machine teaming, and machine-to-machine data exchange while remaining, secure, redundant and available to the warfighter.

2. DoD OCONUS Cloud Vision

Enable dominant all-domain advantage through cloud innovation and resilience.

Cloud computing can help solve today's national defense challenges, but its true potential is to solve tomorrow's challenges. These challenges will require a Joint Force capable of quickly and decisively maneuvering and mobilizing air, land, sea, space, and cyber capabilities in response to adversaries threatening U.S. and Allied National Security priorities and objectives. Collaboration across these domains, increasingly enabled by high-tech, software-driven solutions, must occur at the global point of need, at the tactical edge, and at the fight. These collaborative efforts can't happen without a modern and resilient OCONUS infrastructure, of which cloud computing and zero trust principles are fundamental.

The DoD OCONUS Cloud Strategy establishes goals and objectives specifically focused on delivering cloud innovation forward to the tactical edge with the intent of achieving the following outcomes:

- ***An All-Domain Advantage:*** Modern warfare will require a force that can quickly utilize all appropriate assets in a decisive and concerted response. As such, operational strategies and plans will leverage information from strategic-level commands; sensors across air, land, sea, and space; cyber threat and vulnerability sources; and logistics and resource systems. Additionally, executing these strategies and plans will require cutting-edge analytics of critical information to ensure conditions remain appropriate and opportunities still exist. Cloud computing must enable this data aggregation by providing compute and store capacity with the global reach and innovative services to realize data potential through a data-centric design.
- ***Information Advantage for the Warfighter:*** The combination of access to a greater breadth of data and the growing use of wearable digital components, Internet of military things (IoMT), and unmanned systems (UMS) enable warfighters to transform cloud resources into an operational and tactical advantage. AI/ML must analyze and process large data files to inform the warfighter's decision. This will require computing capacity and innovative services at the tactical edge. Through mobile data centers and edge computing technologies, cloud computing must support these processing power requirements for our warfighters when and where needed.
- ***Continued Innovation of Capabilities:*** DoD's weapon systems and mission capabilities will be increasingly influenced by and dependent on software. Abilities such as rapidly implementing or tuning AI/ML algorithms, immediately responding to cyber threats, and deploying new software to fighter aircraft in flight will be critical. Accordingly, fighting and winning on the next battlefield will be dependent on the Department's proficiency in the rapid acquisition, integration, testing, and deployment of new software and cloud computing capabilities. Cloud computing, applying continuous delivery of services models (e.g., Development, Security, and Operations (DevSecOps), Continuous Integration/Continuous Delivery or Continuous Integration/Continuous Deployment (CI/CD)), and Infrastructure as Code (IaC)) must enable continued innovation of digitally-driven capabilities while in the fight.

3. Goals and Objectives

Delivering cloud innovation to the tactical edge requires modernization within all layers of the infrastructure. This modernization must meet the needs of a range of user-profiles in theater, from the warfighter operating outside the wire to the mission planner or I.T. administrator operating within an established base perimeter or U.S.-led humanitarian efforts. The following goals are specific for OCONUS modernization, taking into account the range of user-profiles and integration with enterprise cloud resources.

3.1. Goal #1: Provide Robust and Resilient Connectivity to the Tactical Edge

Warfighters at the tactical edge must inform and be informed by strategic-level planning. The need to receive the most current information by leaders OCONUS or to provide the latest information to leaders in CONUS is crucial in operational planning efforts and in achieving a decision-making advantage. The warfighter often operates in environments with limited bandwidth, sporadic connectivity, or no connection to the Internet due to OCONUS infrastructure and/or physical limitations. This goal requires the ability to quickly and securely receive and send

information at all classification levels from both well-connected regions and D-DIL environments. DoD requires OCONUS transport and network capabilities that allow for robust and resilient communications. The OCONUS infrastructure must be capable of forward deploying enough data to support a disconnected user or a user at the tactical edge, and once communications allow, seamlessly re-integrating those users and their data into the broader enterprise, while not revealing their location to adversary forces.

Objective 1: Modernize in Theater Communications Infrastructure.

As the number of connected devices and sensors grows exponentially, so does the need for increased communications connectivity. The communications infrastructure (e.g., data transport optical fiber, data relay towers, and ground stations) must support an increasingly complex data architecture to connect data consumers and producers to the digital services they require as well as to each other. This transport must be fast, secure, and resilient, aiming for reduced latency, redundancy, and minimal degradation to data quality.

Objective 2: Secure Cloud Connections Through OCONUS Cloud Access Points.

Boundary Cloud Access Points (BCAP) establish a protected boundary between the Defense Information Systems Network (DISN) and an approved commercial service provider. Voice Cloud Access Points (VCAP) interconnect current DoD Plain Old Telephone System/Public Switched Telephone Networks (POTS/PTSN) with VoIP/Cloud Phone systems contained within commercial service provider collaboration and office productivity tool suites. These cloud access points must be appropriately implemented and deployed OCONUS at all classification levels at commercial Points of Presence (PoP) to ensure secure connections between cloud providers and DoD networks while maintaining the high-speed delivery of data.

Objective 3: Leverage State-Of-The-Art Technologies to Connect D-DIL Environments.

Users at the tactical edge routinely operate with limited bandwidth, limited Size Weight and Power (SWaP), and with a need to minimize the likelihood of detection. Connectivity to remote locations requires additional communications capabilities, such as satellite or wireless communications provided by local telecommunications companies. New technologies for connecting data flows to the tactical edge, including capabilities like 5G, Software-Defined Wide Area Networking (SDWAN), and industry pursuits of satellite constellations for the Internet everywhere, are also underway, presenting new opportunities for connecting to the tactical edge. These technologies must be explored and integrated to provide warfighters with consistent and secure connectivity anywhere, anytime.

Objective 4: Enable Access to Information From Multiple Devices and Data Sources.

Operational conditions may not always permit the use of desktops/workstations to access data. Mobile devices, laptops, and other tactical communications equipment (e.g., transit cases, antennas) require interface with cloud resources to ingest or disseminate mission data.

3.2. Goal #2: Provide Computing Power that Enables Forces at the Tactical Edge

OCONUS users require on-demand access to mission-critical information, applications, and services at the tactical edge for command and control and information sharing with higher headquarters to establish a common operational picture of the battlefield. Additionally, as weapon systems and mission capabilities become more digitally dependent, updating software quickly, such as refining AI/ML algorithms, must be done locally to optimize the capability. Today,

available and evolving enterprise digital solutions are often CONUS-based. For OCONUS users, reaching back to CONUS-based solutions reduces mission effectiveness in theater (e.g., added latency, lack of resilient data transport and access). DoD requires innovative, secure, reliable, and redundant cloud computing at the tactical edge with reach back to CONUS to empower the Joint Force and achieve an operational advantage.

Objective 1: Deploy OCONUS Cloud Computing Under an Enterprise Construct.

The deployment of OCONUS cloud computing must be managed as an enterprise to ensure more efficient technology approvals. This is particularly relevant for security accreditation and parity of cloud services between the enterprise and OCONUS. Doing so provides more efficient use of cloud resources based on mission needs across the region and greater efficiencies in fielding proven cloud capabilities. Data needs to be processed close to its source and staged as close to the warfighter as possible to enable data-driven decisions. The warfighter requires the ability to apply analytical tools or to rapidly stand up temporary Task Force collaboration environments regardless of geographic location. OCONUS users must have access to deployable cloud computing, high-performance computing, and edge computing capabilities as they become available. This includes innovative cloud services that enable agile software development, robust collaboration, and powerful analytics such as AI/ML. Individually approving and implementing these capabilities at the point of need results in duplicative efforts and sub-optimal use of capacity. Management on an enterprise-level will also require the facilitation of data flows between domains of varying levels of classification while ensuring appropriate accreditation policies and procedures are maintained. This will be both an information assurance and an information security effort at the enterprise level to ensure that the warfighter maintains the advantage at the tactical edge.

Objective 2: Optimize Data Center Infrastructure for Resilient Access to Data and Services.

DoD recognizes that not all systems can reside in a cloud environment. There is a continued need for data center infrastructure, which must be optimized in alignment with cloud resources to account for reliability and availability (e.g., continued operations, data replication). Distributed mobile cloud data centers and their integration with DoD data centers must allow for a distributed cloud model for broader availability of cloud capabilities, including automated failover of stored data in times of crisis and operational disruptions (e.g., cyber-attacks, infrastructure degradations, or outages). DoD's data center infrastructure must appropriately integrate with cloud resources to allow for a seamless and resilient OCONUS user experience.

Objective 3: Provide Ability to Traverse Cloud Environments for Persistent Data Access.

A warfighter carrying out a mission requires persistent access to information hosted by various cloud providers, in different environments, and at multiple classification levels. This information ecosystem must include data to and from various tactical devices and mission partner environments that enable information sharing with coalition partners. Mission owner and warfighter access to information must not be tethered to a specific cloud solution or data center. They must be available regardless of geographical location or coalition partnership. This requires the automated synchronization of data across the cloud environment to include ruggedized tactical devices when available.

Objective 4: Protect Data in the Cloud While Enabling Information Sharing.

OCONUS mission success relies heavily on the Department's relationships with mission partners. The ability to share information in a protected environment with non-DoD users is critical. OCONUS cybersecurity solutions must incorporate zero trust principles to ensure protections closer to the data and include robust identity, credential, and access management (ICAM) to drive out anonymity and enable the secure sharing of information. Zero trust solutions must control user activity within emerging cloud-enabled cyber terrain. In coordination with the Cyber National Mission Force, they must also facilitate the deterrence, disruption, or the defeat of hostile red actors in cyberspace. DoD data hosting environments and services require the same cybersecurity protections and defenses when operating in and traversing OCONUS cloud-hosted environments when they are operating CONUS.

Additionally, an OCONUS Cloud Defensive Cyber Operations Concept of Operations (DCO CONOPS) must be developed before technology acquisition and implementation to guide these activities. While requirements may vary from theater to theater, cybersecurity measures must be implemented to support the warfighter's confidentiality, integrity, and availability of mission data. The measures should be tested against realistic cyber threat representations on a recurring basis to ensure effectiveness.

3.3. Goal #3: Deploy Talent at the Point of Need

Effective OCONUS cloud capabilities require an understanding of the OCONUS mission environment. In addition, they require an influx of personnel with novel aptitudes, expertise, and credentials. DoD must begin to deploy and grow OCONUS talent (Military, Civilians, and Contractors) to maximize the use of new technologies and inform the research and development of future capabilities.

Objective 1: Establish OCONUS Rotations for Technical Talent.

Cloud computing, and the solutions it enables, require new skillsets at the tactical edge. New knowledge areas not typically seen may include software development and AI/ML. DoD must seek and rotate technical talent OCONUS to maximize the benefits of technology to drive a greater competitive advantage. Rotations also provide direct mission experience for improved development of OCONUS solutions.

Objective 2: Institute Training for OCONUS Users to Maximize Use of Cloud Resources.

Tomorrow's warfighter must be equipped with the technical skillsets to operate and maintain software-driven mission capabilities at the tactical edge. DoD must train OCONUS users to effectively employ cloud services for faster aggregation and analysis of data, delivery of software, and response to cybersecurity threats. Therefore, robust warfighter training must include cloud computing to fully realize technical advantage, information superiority, and global Joint Force military advantage.

Objective 3: Deploy Research Talent to Better Address OCONUS Challenges.

DoD must continue to improve warfighting and mission capabilities, staying ahead of adversaries investing heavily in new technologies. As such, research and development efforts must be informed by OCONUS challenges to ensure warfighting relevance. Deploying research teams

OCONUS provides the on-the-ground experience needed to develop mission solutions that make a difference.

4. OCONUS Unique Considerations

OCONUS infrastructure modernization efforts have unique considerations not required when implementing infrastructure in CONUS.

4.1. Host Nations

Any DoD data center established in a host nation must be negotiated and agreed upon by both the U.S. Government and the host nation. Current cloud and data control laws allow the host nation to have full-scale access to cloud computing and data centers hosted on a country's soil, such as the European Union's General Data Protection Regulation (GDPR). In contrast, DoD requires full control and access to cloud computing and data centers. Given the challenges with meeting host nation data control requirements, cloud service providers must make a significant investment to support OCONUS locations.

4.2. Real Estate, Space, and Power

OCONUS space and power is limited. This limitation impacts the number of viable U.S.-controlled military locations for typical data center cloud infrastructure. Successful implementation of a tactical edge cloud will require the adoption of new and alternative commercial solutions that provide the necessary computational power at lower SWaP. Bringing cloud computing to the tactical edge will require resources, including resources such as space, power, and bandwidth provided by OCONUS base, camp, post, and stations to ensure reliable and secure connectivity and access at the point of need.

4.3. Denied, Disconnected, Intermittent, or Limited (D-DIL) Environments

The warfighter, service support, and U.S. led humanitarian efforts often operate in environments with limited bandwidth, sporadic connectivity, or no connection to the Internet due to poor OCONUS infrastructure and/or physical limitations. The OCONUS infrastructure must be capable of forward deploying enough data to support a disconnected user or a user at the tactical edge and, once communications allow, seamlessly re-integrating those users and their data into the broader enterprise while not broadcasting their location to adversary forces. Future edge devices connecting to the tactical cloud should be designed and operated with the goal of preserving operational effectiveness through different degrees of connectivity to the tactical cloud, including auto-synchronization with cloud capabilities, once re-connected.

4.4. Data Sovereignty in the Mission Partner Environment (MPE)

The requirement to integrate fully with the host nation and MPE is paramount to mission success. Successful operations within the MPE are dependent on ensuring the correct information gets to the authorized personnel at the speed of relevance to enable data-driven decision-making. This requires coordination with U.S./DoD Records and Security Officers to ensure that the U.S. maintains control and sovereignty over U.S. data collected, generated, or shared in the OCONUS environment. Special considerations must be taken into account for the host nation's data localization laws, which may require cloud service provider compliance to support DoD OCONUS.

5. Next Steps

DoD must take action to execute this strategy to ensure cloud capabilities are delivered to the warfighter. The Department will convene the DoD Components responsible for the planning, funding, and execution activities that will ***enable a dominant all-domain advantage through cloud innovation and resilience***. DoD CIO and the Joint Chiefs of Staff (J6) will co-lead the development of an enterprise OCONUS cloud architecture that will integrate the components of this strategy and inform OCONUS investments and technical implementation decisions. Based on the architecture and strategy, DoD CIO and the J6 will co-lead the development of an implementation plan to ensure coordinated execution of OCONUS modernization activities, including measurements of each objective's effectiveness and prioritization of each goal and objective to ensure the warfighter's needs are met at the tactical edge. Effective implementation is critical to maintaining the DoD's technical advantage and delivering information superiority.