



## DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON  
WASHINGTON, D.C. 20301-6000

DEC 16 2013

CHIEF INFORMATION OFFICER

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
UNDER SECRETARIES OF DEFENSE  
DEPUTY CHIEF MANAGEMENT OFFICER  
COMMANDERS OF THE COMBATANT COMMANDS  
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION  
DIRECTOR, OPERATIONAL TEST AND EVALUATION  
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE  
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE  
ASSISTANT SECRETARIES OF DEFENSE  
ASSISTANTS TO THE SECRETARY OF DEFENSE  
DIRECTOR, ADMINISTRATION AND MANAGEMENT  
DIRECTOR, NET ASSESSMENT  
DIRECTORS OF THE DEFENSE AGENCIES  
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Supplemental Guidance for the Department of Defense's Acquisition and Secure Use of Commercial Cloud Services

- References: (a) DoD Chief Information Officer Memorandum, Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker, June 26, 2012  
(b) Defense Information Systems Network Global Information Grid Flag Panel Charter, April 2012

This memorandum provides supplemental guidance for the acquisition and secure use of commercial cloud services in the DoD. The DoD Chief Information Officer (CIO) established Defense Information Systems Agency (DISA) as the Enterprise Cloud Service Broker to consolidate enterprise demand to manage the acquisition and delivery of the Department's commercial cloud services, and to ensure a secure and efficient DoD cloud environment, reference (a). The broker will facilitate and optimize DoD's access and use of commercial cloud services that can meet our security and interoperability requirements.

On June 25, 2013, the Defense Information Systems Network (DISN) Global Information Grid (GIG) Flag Panel authorized DISA as the Enterprise Cloud Service Broker with the responsibility of issuing DoD provisional authorizations for Department-wide use of commercial cloud services for low-impact data and missions, in accordance with reference (b). The DISN GIG Flag Panel decided that use of commercial cloud services for moderate-risk data or missions, which include Controlled Unclassified Information, require DISN GIG Flag Panel approval, coordinated via the Broker. As such, the Broker developed a DISN GIG Flag Panel approval process for issuing DoD provisional authorizations for commercial cloud services, based on input and review of DISA's cyber security assessment by the Defense Information Assurance Security Accreditation Working Group.

**DoD Components must comply with DoD CIO and DISN GIG Flag Panel guidance and procedures that require the following:**

- **All requests for commercial cloud services proceed through the DoD Cloud Broker.**
- **Commercial cloud services have a DoD provisional authorization, or DISN GIG Flag Panel approval to proceed, prior to acquisition and use.**
- **Suspension of deployments of cloud services that do not have a DoD provisional authorization, or are not hosted within the Department's layered cyber defenses and layered cyber-attack detection, diagnosis, and reaction infrastructure.**

**In addition, DoD Components must address the issues identified in the DoD Cloud Computing Contracts Issue Matrix (attached), in the contracts/procurements for all for commercial cloud services. This includes ensuring that the Department has a direct contractual relationship with the vendor that has operation configuration and control of the data.**

**The DISA Designated Approving Authority has issued, and will continue to issue, DoD provisional authorizations leveraging the provisional authorizations granted by the Federal Risk & Authorization Management Program (FedRAMP) Joint Authorization Board. While the FedRAMP provisional authorizations include the accepted Federal minimum security baseline for low and moderate services, additional controls are needed to protect DoD data and information. As such, the DoD Cloud Broker defined a comprehensive cloud security model to establish security guidelines for hosting DoD data in cloud computing environments, over and above the FedRAMP baseline.**

**I am committed to achieving Information Technology (IT) efficiencies while ensuring our Department's cybersecurity posture and other IT requirements are met. As DoD Components leverage the availability of secure and less expensive commercial cloud services for the Department, they must do so through the DoD Cloud Broker.**

**My point of contact for DoD Cloud Computing is Mr. Robert Vietmeyer, 571- 372-4461, robert.w.vietmeyer.civ@mail.mil.**

**DoD Enterprise Cloud Service Broker questions or requests for support should be directed to the DISA Cross-Functional Solutions Center: Julie Mintz, 301-225-5753, julie.j.mintz.civ@mail.mil.**

  
Teresa M. Takai

## DoD Cloud Computing Contracts Issues Matrix

| # | Legal Rationale   | Description of Issue  | Applicable to:               |
|---|---|---|------------------------------|
| 1 | <p>Inspector General Act of 1978</p> <p>Federal Information Security Management Act of 2002 (FISMA)</p> <p>NIST 800-53</p>  | <p>PHYSICAL ACCESS</p> <p>The Agency needs to have physical access to a CSP data center to conduct inspections for FISMA, other audit purposes, or Inspector General investigations. These audits may be unannounced, so the Agency must ensure that its auditors have the access they need to complete their audits and investigations.</p>  | <p>All Commercial Clouds</p> |
| 2 | <p>HSPD -12</p>   | <p>PERSONNEL ACCESS</p> <p>In order to further protect DoD data, the Agency must require all CSP employees who have access to government data, architecture that supports government data, or any physical or logical devices/code be U.S. person per Executive Order 12333 and pass an appropriate background check as required by Homeland Security Presidential Directive -12.</p> | <p>All Commercial Clouds</p> |
| 3 | <p>Per the Freedom of Information Act (FOIA) case law unless there is a “consultant” relationship (see Department of Interior v Klamath) government information falls under the “release to one release to all” (see NARA v Favish) rule applies, which would prohibit the government from protecting information from the public if it was released to a contractor without an NDA. In addition 5 CFR 2635.703 prohibits Federal employees from releasing non-public information; a NDA is the equivalent for contractor personal.</p> | <p>NDA</p> <p>The Agency must require CSP employees with access to government data and other government confidential information to sign a non-disclosure agreement that would legally prevent a CSP employee from disclosing non-public government information.</p>  | <p>All Commercial Clouds</p> |

## DoD Cloud Computing Contracts Issues Matrix

|   |   |  |                                      |
|---|---|--|--------------------------------------|
| 4 | Asset availability procedures   | <p><b>ASSET AVAILABILITY</b></p> <p>The Agency should ensure that the service level agreement with the CSP contains provision for asset availability. The level of asset availability will be determined by the Agency's requirements.</p>   | All Commercial Clouds                |
| 5 | The banner language provides consent for government to view any content on the system without a warrant that would otherwise be required by the 4 <sup>th</sup> Amendment. See also, City of Ontario v. Quon. | <p><b>BANNER</b></p> <p>Banners or consent to monitor language allows Federal law enforcement the right to access and review government data including email created on a government system without a warrant or a subpoena. When a Government is only procuring hosting the banner will be a requirement of the government or contractor who developed the system, however, when the government procures software as a service, the Agency must require the CSP to display the Agency's approved banner language prior to allowing a user access to the system.</p> | All Commercial Clouds                |
| 6 | FAR 9.5 on Organizational Conflict of Interest prohibit a contractor from using information from its government work for other commercial needs.  | <p><b>ORGANIZATIONAL CONFLICT OF INTEREST</b></p> <p>When the government places non-public information on a commercial cloud, the Agency must ensure the CSP refrains from using government data for any purpose other than expressly stated in the requirements.</p>  | When CUI will be hosted in the cloud |
| 7 | FISMA states that the Agency is responsible for accepting the risk for an IT system.  | <p><b>CONTINUOUS MONITORING</b></p> <p>FedRAMP has mandated certain requirements for continuous monitoring in the "Continuous Mentoring Strategy Guide". These requirements require the CSP to produce certain reports and provide them to FedRAMP PMO and/or the FedRAMP 3PAO. The government client needs to request copies of these reports in its requirements (PWS/SOW), as the DoD Designated Authorizing Authority (DAA) is ultimately responsible for the protection of the data.</p>  | All Commercial Clouds                |

## DoD Cloud Computing Contracts Issues Matrix

|    |   |  |   |
|----|---|--|---|
| 8  | <p>Memorandum M-07-16, May 22, 2007, for safeguarding against and responding to breaches of PII; FISMA; requirements for agency incident response plans and reporting to the Federal information security incident center established by the Act, i.e., United States-Computer Emergency Readiness Team (US-CERT), within the Department of Homeland Security. See 44 U.S.C. 3544(b)(7), 3546.</p> <p>Applicable law and policy includes section 208 of the E-Government Act of 2002 (E-GOV Act), and Office of Management and Budget (OMB) Memorandum M-03-22.</p> | <p><b>DATA BREACH/PIA</b></p> <p>As with any IT system there is always a risk of a data breach. As such, the Agency must require the CSP to provide a plan for handling such a breach which includes the requirement to notify the Agency of a breach within 60 minutes (US Cert Requirement). In addition, the Agency is required to conduct a Privacy Impact Assessment (PIA) on all its IT systems. The purpose of the PIA is to analyze how information in identifiable form is handled: to ensure that its handling conforms to applicable legal, regulatory, and policy requirements for privacy; to determine the risks and effects of collecting, maintaining, and disseminating such information in an electronic information system; and to examine and evaluate protections and alternative processes for handling such information to mitigate potential privacy risks. To assist the Agency in developing the PIA, the CSP must be required to provide the Agency with any required data about the CSP environment.</p> | <p>When CUI will be hosted in the cloud</p> |
| 9  | <p>Inspector General Act of 1978</p> <p>FISMA</p>   | <p><b>FACILITY INSPECTIONS</b></p> <p>FISMA and DoD policy require that facilities hosting DoD data meet certain security standards. Routine inspections ensure that facilities are in compliance with these standards. Usually these inspections are conducted by the government; however, in the case of a CSP the government may agree to allow a third party to conduct an inspection based on the government's criteria.</p>  | <p>All Commercial Clouds</p>                |
| 10 | <p>FISMA</p>  | <p><b>COMPLIANCE</b></p> <p>It is important to remind CSP's that when hosting government data they must comply with the FISMA and subsequent Agency policies.</p>  | <p>All Commercial Clouds</p>                |

## DoD Cloud Computing Contracts Issues Matrix

|    |  |   |                       |
|----|--|---|-----------------------|
| 11 | Common law theory of privity of contract. The government needs to be in contract with the host of the data.  | <p><b>USE OF SUBCONTRACTORS</b></p> <p>When subcontracting, the Agency should ensure the prime retains operational configuration and control of DoD data. This is particularly important in the event of a data breach.</p>   | All Commercial Clouds |
| 12 | Sovereign Immunity clause of the Constitution Article III Section II. The government has not granted immunity to be sued for actions by third parties. See also the Federal Torts Claim Act. | <p><b>INDEMNIFICATION</b></p> <p>Indemnification by the CSP protects the government when third parties sue the government for a tort when the CSP, not the government was liable. Indemnification also allows the government to recoup any costs related to a third party law suit.</p>   | All Commercial Clouds |
| 13 | Liability insurance requirement.   | <p><b>INSURANCE</b></p> <p>The Agency must require a CSP to have the necessary insurance to pay for any costs stemming from a breach of DoD data or to replace any damages to the DoD system.</p>   | All Commercial Clouds |
| 14 | Sovereign Immunity under the Article III Section II of the Constitution. US Government data is sovereign and is not subject to other jurisdictions.  | <p><b>JURISDICTION</b></p> <p>DoD data can only be released by an authorized official or by a court order from a US Federal Court. If a CSP places DoD data in a foreign jurisdiction its servers would be subject to the laws of that jurisdiction and risks DoD data being seized by a foreign government.</p>  | All Commercial Clouds |
| 15 | Inspector General Act of 1978<br><br>FISMA<br><br>Law Enforcement Authorities  | <p><b>LAW ENFORCEMENT</b></p> <p>As mentioned above, all users to DoD systems have consented through the banner language to monitoring of their use of a DoD system and use of that data for law enforcement purposes. As such, Federal law enforcement officials do not need a warrant or a subpoena to access government data on a government system.</p> | All Commercial Clouds |
| 16 | This clause just discusses maintenance responsibilities.   | <p><b>MAINTANCE</b></p>   | All Commercial        |

## DoD Cloud Computing Contracts Issues Matrix

|    |   |   |                                      |
|----|---|---|--------------------------------------|
|    |   | Agencies should require CSPs to conduct regular maintenance including patches on its environment to prevent intrusions.   | Clouds                               |
| 17 | Sovereign Immunity under the Article III Section II of the Constitution. US Government data is sovereign and is not subject to other jurisdictions. | <p>NOTIFICATION</p> <p>Similar to jurisdiction, CSP data centers are subject to state and local law enforcement officials, and state and local subpoenas. The Agency must ensure the CSP notifies the Agency of a warrant or a subpoena so that the Department of Justice can protect Agency data from release.</p>   | All Commercial Clouds                |
| 18 | <p>Federal Records Act</p> <p>Freedom of Information Act</p> <p>Federal Rules of Civil Procedure</p>  | <p>RECORDS</p> <p>The Agency is required to maintain and produce records per the Federal Records Act, the Freedom of Information Act, and the Federal Rules of Civil Procedure. Records are kept based on the Agency's disposition schedule. The government should work with the CSP to ensure that all government records and CSP records about government data are kept in accordance with Agency record's schedules.</p> | All Commercial Clouds                |
| 19 | CNSS 1001   | <p>SPILLIAGE</p> <p>Occasionally, classified information spills over to an unclassified system. When this happens, the agency must ensure the CSP follows the procedures in CNSS 1001.</p>  | All Commercial Clouds                |
| 20 | HSPD 23 and NSPD 54, NDAA 2011 Section 806, DoDI 5200   | <p>SUPPLY CHAIN</p> <p>The Agency must ensure CSPs exercise due diligence to use genuine hardware and software products that are free of malware.</p>   | When CUI will be hosted in the cloud |
| 21 |   | <p>TERMS OF SERVICE</p> <p>Many commercial services have Terms of Service Agreements that contain clauses that the government cannot accept. Below are some examples:</p>   | All Commercial Clouds                |

# DoD Cloud Computing Contracts Issues Matrix

|  |                                      |  |
|--|--------------------------------------|--|
| <p>Freedom of Information Act</p>  | <p><b><u>CONFIDENTIALITY</u></b></p> | <p>This is a clause where the government agrees not to release confidential information. However, the government is subject to the Freedom of Information Act and must follow its procedures to release or protect commercial information.</p>   |
| <p>Article I Section 8 of the US Constitution. Congress has to appropriate money.</p>  | <p><b><u>INDEMNIFICATION</u></b></p> | <p>Many terms of service agreement contain an open ended indemnification clause where the government will indemnify the CSP against third party claims. This type of clause violates the Anti-Deficiency Act because the government is committing to funds that have yet to be appropriated. This clause needs to be re-worked to reference other applicable laws.</p> |
| <p>Sovereign Immunity under the Article III Section II of the Constitution. US Government data is sovereign and is not subject to other jurisdictions.</p> | <p><b><u>GOVERNING LAW</u></b></p>   | <p>Many terms of service agreements have the governing law for the agreement to be a specific state and have a venue for any disputes to be in that state's courts. As the Federal government is not subject to state law, it can only be sued in Federal court.</p>   |
| <p>5 C.F.R. 2635.702, the Federal Acquisition Regulation (FAR) (48 C.F.R. §3.101-1), Executive Order 12731</p>   | <p><b><u>ENDORSEMENT</u></b></p>     | <p>Many terms of service agreements also have a clause where the CSP may quote / cite the government's use of its product as an endorsement or testimonial. The government does not endorse commercial products or services.</p>   |