CLOUD SERVICES SUPPLEMENTAL GUIDANCE

The DON is responsible for acquiring Information Technology (IT) services that meet its mission objectives and provide optimal solutions that are compliant with DoD cybersecurity requirements. The DON will:

1. Require system(s) registered in the DON variant of the DoD Information Technology Portfolio Repository (DITPR-DON) to identify any cloud service providers (CSPs) they are using and make CSP identification part of the DON Federal Information Security Management Act (FISMA) report.

2. Require that all applications are properly certified and formally approved by the appropriate Authorizing Official and that required entries are made in the DON Applications and Database Management System (DADMS).

3. Comply with DoD CIO annual IT budget guidance for cloud computing services and report all necessary information in the Select and Native Programming Data Input System- Information Technology (SNaP-IT).

4. Request connections to CSP environments for cloud security Impact Levels 4-6 through the DISA Connection Approval Office in accordance with specific commercial cloud procedures that will be published in the upcoming DoD Cloud Computing Security Requirements Guide (SRG) (reference (f)). In the interim, the DoD Information Networks (DODIN) Waiver Process should be used to obtain DoD connection approval.

5. Publish references to any processes and concepts of operation developed for DON cloud implementations. Technical components within the department are developing a managed service model to facilitate assessment, employment, and sustainment of authorized commercial cloud offerings by system and application owners. Details on the managed service provider (MSP) processes will be provided under separate cover.

Enclosure (1)