



DEPARTMENT OF DEFENSE

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

CHIEF INFORMATION OFFICER

NOV 15 2017

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEF, NATIONAL GUARD BUREAU
COMMANDANT OF THE COAST GUARD
COMMANDERS OF THE COMBATANT COMMANDS
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTOR, STRATEGIC CAPABILITIES OFFICE
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Department of Defense Cybersecurity Activities Performed for Cloud Service Offerings

References: (a) DoDI 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations" Change 1, July 25, 2017
(b) DoD Cloud Computing Security Requirements Guide, March 6, 2017
(c) Memorandum of Agreement between the Department of Defense and The Department of Homeland Security Regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations, January 19, 2017.
(d) DoDI 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," June 6, 2012

This memorandum expands upon Reference (a) to address the engagement in Defensive Cyber Operations as DoD networks transition data, applications, capabilities and services to DoD and commercial cloud capabilities and services. Specifically addressed are activities that can be performed only by a DoD Cybersecurity Service Provider (CSSP) or a designated DoD organization in coordination with the DoD CSSP, and activities other qualified providers can perform on behalf of the mission owner and the Authorizing Official (AO). Mission owner terminology, is defined in Reference (b). For the purpose of this memorandum the term "Cloud Service Provider (CSP)" can mean the on-site hosting CSP, off-premise hosting CSP, or a third party CSP offering cloud security services such as a Cloud Access Security Broker (CASB)¹.

¹ Gartner IT Glossary: Cloud access security brokers (CASBs) are on-premises or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement.

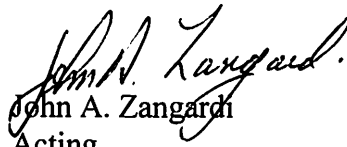
Throughout this memorandum, the term "DoD CSSP entity" will be used to describe a designated DoD organization in coordination with a CSSP.

This memorandum applies to Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the National Guard Bureau, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (referred to collectively as the "DoD Components"). In addition, this memorandum applies to the United States Coast Guard (USCG) in accordance with the direction in Paragraphs 4a, b, c, and d of Reference (c).

In accordance with the References (a) through (c), mission owners are required to register DoD networks, applications, data, and services that are migrating to DoD and/or commercial cloud capabilities and services. They are also required to identify the cloud service provider's alignment to an appropriate DoD CSSP in the DoD CIO System/Network Approval Process (SNAP) database. The mission owner is responsible for ensuring data migrated to a DoD or commercial cloud is at the appropriate security impact level In accordance with References (b) and (d).

Descriptions of those cybersecurity activities which must be performed specifically by a DoD CSSP or DoD CSSP entity, and those cybersecurity activities that could be performed on behalf of the mission owner by other service providers (e.g. CSP, DoD CSSP entity, CASB, milCloud, etc.) are provided at Attachment 1. A list of references is provided at Attachment 2. A list of abbreviations and acronyms is provide at Attachment 3.

The DoD CIO point of contact for this matter is, Dr. Mark Stanley, (703) 693-6685, mark.a.stanley38.civ@mail.mil.


John A. Zangardi
Acting

Attachments:
As stated