



**DEPARTMENT OF DEFENSE**

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

AUG 07 2019

CHIEF INFORMATION OFFICER

MEMORANDUM FOR CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF  
DEFENSE

SECRETARIES OF THE MILITARY DEPARTMENTS  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
UNDER SECRETARIES OF DEFENSE  
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  
DIRECTORS OF DEFENSE AGENCIES  
DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: Treatment of Personally Identifiable Information within Information Impact Level 2  
Commercial Cloud Services for the Department of Defense

- References:
- (a) DoD Cloud Computing Security Requirements Guide, V1.r3, March 16, 2017
  - (b) NIST SP 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," April 2010
  - (c) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology," July, 28, 2017 (revision)
  - (d) DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," August 1, 2017 (revision)
  - (e) DD Form 2930, "Privacy Impact Assessment (PIA)," June 2017
  - (f) CNSSI 1253, "Security Categorization and Control Selection for National Security Systems," Appendix F, Attachment 6
  - (g) NIST SP 800-60 Volume 1, "Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008 (revision)
  - (h) DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," July 25, 2017 (revision)

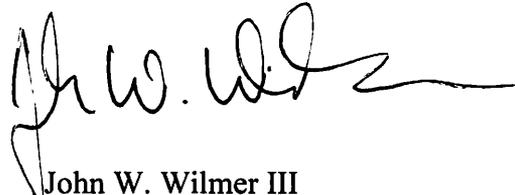
This memorandum establishes Cloud Security Information Impact Level 2, identified in Reference (a), as the minimum cybersecurity requirement for DoD applications/systems containing low confidentiality impact level Personally Identifiable Information (PII), as determined in accordance with Reference (b). Specifically, Information Impact Level 2 cloud services may be used to host low confidentiality impact level PII when no other risk factors exist that would require a higher impact level cloud service.

Reducing the minimum cloud requirement from Impact Level 4 to Impact Level 2 specifically for low confidentiality impact level PII is consistent with requirements outside of cloud environments and lowers barriers for cloud adoption for activities that require minimally low confidentiality impact level PII. DoD Components must continue to:

- Categorize information systems and implement appropriate cybersecurity controls in accordance with Reference (c).
- Assess and provide for the confidentiality impact level of the hosted PII in accordance with References (b), (d), and (e), as well as the confidentiality needs of all other hosted data.
- Complete and document Privacy Impact Assessments as described in Reference (e).

These determinations will take into account all relevant factors as presented in Section 3.2 of Reference (b). It is important to note that relevant factors should be considered together. One factor by itself might indicate a low impact level, but another factor might indicate a high impact level, and thus override the first factor. Even when a low confidentiality impact determination is made, the specific type of PII and type of cloud service used may require additional cybersecurity controls per Reference (f). The authorizing official is accountable to ensure that appropriate cyber assessments are performed per References (c) and (f), and that required cybersecurity support services are instituted in compliance with Reference (h). The authorizing official should use this memorandum and all applicable regulations as guidance for making a final determination.

My point of contact for this matter is Mr. Kevin Dulany at [kevin.m.dulany.civ@mail.mil](mailto:kevin.m.dulany.civ@mail.mil), (571) 372-4699.

A handwritten signature in black ink, appearing to read "John W. Wilmer III", with a long horizontal flourish extending to the right.

John W. Wilmer III  
Deputy Chief Information  
Officer for Cyber Security