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

CHIEF INFORMATION OFFICER

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Temporary Authorization to Use Impact Level (IL) 2 Cloud Environment for Certain Basic Controlled Unclassified Information (CUI)

(The COVID-19 pandemic and resulting high demand for remote work have stressed beyond capacity the Department's technical capabilities in support of remote workers. To enable the vital work of the Department to continue during this time of exigent circumstance, the DoD CIO is standing up the Commercial Virtual Remote (CVR) work environment. CVR is a new, quick-response cloud computing environment, established in the Microsoft Impact Level 2 (IL2) Government Community Cloud (GCC), to create additional capacity and support effective collaboration. CVR is only intended for the duration of the exigent circumstances related to the COVID-19 pandemic. When DoD has returned to a normal operational status, CVR will be decommissioned and its data erased at the direction of the DoD CIO and USCYBERCOM Commander.

Given DoD's operational needs during this national crisis, I am temporarily waiving with caveats, as described herein, the DoD Cloud Security Requirements Guide (SRG) requirement that limits the processing of CUI data to an IL 4 or higher level cloud environment. This waiver applies to all categories of CUI, except as noted below and applies to the CVR environment only. The following CUI data categories must still abide by the DoD Cloud Computing SRG requirement related to IL 4 processing, and are not permitted in the CVR environment: 1) CUI under the control and direction of the Department of Defense (Controlled Technical Information, Critical Infrastructure Security Information, Naval Nuclear Propulsion Information and Unclassified Controlled Nuclear Information – Defense); 2) all data types under the Law Enforcement CUI grouping; and 3) all data types under Privacy data, with the exception of low confidentiality impact personally identifiable information (PII) as described in Reference A. Due to the temporary nature of the environment, users are responsible for ensuring that data entered into the CVR environment meets retention, or other requirements, associated with that data type. Further, users should assume the environment will not meet those requirements on their behalf.

This waiver is subject to the following conditions: The CVR environment must meet and maintain the security requirements for Basic CUI DoD Instruction 5200.48; the CVR environment must also comply with security requirements contained in Appendix A; Users connecting to the environment must comply with the Telework Dos and Don'ts published by DISA at: https://cyber.mil/covid19/.

The CVR environment is not permitted to synchronize or migrate data with an IL 4 or higher environment.

Component CIOs are responsible for ensuring their organization users are aware of the limitations and requirements of the environment.
This waiver will expire within 6 months, or upon decommissioning of the CVR environment.
The point of contact for this matter is Mr. McKay Tolboe at email: mckay.r.tolboe.civ@mail.mil, (571) 372-4648.

WILMER.JOHN.W.III.1267975430
Digitally signed by WILMER.JOHN.W.III.1267975430
Date: 2020.03.26 09:28:57 -04'00'

John W. Wilmer
DoD Senior Information Security Officer

REFERENCES:

(a) Treatment of Personally Identifiable Information within Information Impact Level 2 Commercial Cloud Service for the Department of Defense, Deputy Chief Information Officer for Cybersecurity Memo, 07 August 2019.