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

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: DoD Use of Contractor-Owned Collaboration Tools

References: (a) Authorized Telework Capabilities and Guidance, 13 April 2020
(b) 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.
(c) COVID-19 Response: Remote Work Capability, 19 March 2020.
(d) Temporary Authorization to Use Impact Level (IL) 2 Cloud Environment for Certain Basic Controlled Unclassified Information (CUI), 30 March 2020.
(e) Commercial Virtual Remote Environment June 15, 2021 Extension, 18 September 2020.
(f) Extension of Temporary Authorization to Use Impact Level (IL) 2 Cloud Environment for Certain Basic Controlled Unclassified Information (CUI), 23 September 2020.
(g) DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended.

DOD CIO has published a number of memos clarifying policy and providing guidance on collaboration and remote telework capabilities in response to the COVID 19 pandemic (see references). DOD CIO has received questions from within the Department and from industry partners regarding the scope of this guidance. Specifically whether the memos published prevented DOD personnel for participating in collaboration sessions with industry partners on contractor owned and operated systems where controlled unclassified information (CUI) is discussed. To clarify, the memos referenced above apply to DOD systems and do not apply to contractor owned or operated systems.

DoD personnel may participate in contractor-hosted collaboration sessions involving CUI, provided the Contractor is in compliance with 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting). Specifically, contractors, by providing the collaboration session, are asserting that the collaboration tools used meet the security requirements for handling the appropriate level of CUI for that collaboration session.

DOD personnel should continue to comply with the DOD Information Security Program and implement Operational Security best practices in these sessions. The point of contact for this matter is Mr. McKay Tolboe at mckay.r.tolboe.civ@mail.mil, (571) 372-4640.

HAKUN.MARK.GERARD.1036745564
Digitally signed by HAKUN.MARK.GERARD.1036745564
Date: 2020.09.29 13:35:29 -04'00'

Mark G. Hakun
Deputy Senior Information Security Officer

DISTRIBUTION:
CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF OF THE NATIONAL GUARD BUREAU
GENERAL COUNSEL OF THE DEPARTMENT OF DEFNSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES 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