



PRESS RELEASE

June 8, 2023

FOR IMMEDIATE RELEASE

Inspector General Robert P. Storch announced today that the Department of Defense Office of Inspector General (DoD OIG) released a report on the "Audit of DoD Actions Taken to Protect DoD Information When Using Collaboration Tools During the Coronavirus Disease-2019 Pandemic." The report highlights concerns regarding the deployment and protection of collaboration tools used by the DoD to facilitate telework during the coronavirus disease-2019 (COVID-19) pandemic.

The report released today identified that DoD Components did not complete required cybersecurity steps outlined in a DoD Instruction before deploying collaboration tools on Component networks and did not ensure that all critical configuration settings or cybersecurity controls were implemented to reduce the risk of exposing DoD networks and systems to potential malicious activity.

IG Storch stated, "The COVID-19 pandemic resulted in a significant increase in teleworking in the DoD, which increased opportunities for malicious cyber actors to orchestrate attacks on DoD networks and systems. While this audit focused on the expanded use of collaboration tools during the pandemic, these same risks will continue to exist in a post-pandemic environment. The use of unauthorized collaboration tools introduces potential weaknesses that malicious cyber actors could exploit to gain unauthorized access to a network. If DoD Components do not consistently configure collaboration tools in accordance with cybersecurity requirements, the confidentiality, integrity, and availability of information shared using these tools may be at risk."

The OIG found that, as the DoD workforce continues to use collaboration tools to facilitate telework and remote work, DoD Components should implement basic configuration settings required to protect DoD networks and systems from potential malicious activity.

To address these issues, the DoD OIG recommended, among other things related to configuring collaboration tools, that the DoD Chief Information Officer direct DoD Components' Authorizing Officials to identify collaboration tools in use, verify whether cyber security processes were completed before deployment, and if not, complete the required cybersecurity process. The DoD agreed with the recommendations.