INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

December 7, 2021

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Audit of DoD Actions Taken to Implement Cybersecurity Protections Over Remote Access Software in the Coronavirus Disease–2019 Telework Environment (Project No. D2022-D000CR-0043.000)

We plan to begin the subject audit in December 2021. We are conducting the subject audit at the request of the House Committee on Oversight and Reform. The objective of this audit is to determine the actions taken by the DoD to configure remote access software used to facilitate telework during the coronavirus disease–2019 (COVID-19) pandemic to protect DoD networks and systems from potential malicious activity. We will also determine the extent to which the DoD implemented security controls to protect remote connections to its networks. We may revise the objective as the audit proceeds, and we will consider suggestions from management for additional or revised objectives.

We will perform the audit at the Offices of the DoD Chief Information Officer, Joint Force Headquarters–DoD Information Network, and Defense Information Systems Agency. We will determine additional Components to assess within the Military Departments and Defense agencies from those that acquired, used, and maintained remote access software during the COVID-19 pandemic. In addition, attached is our request for data related to remote access software.

Please provide us with a point of contact for the audit within **5 days** of the date of this memorandum. The point of contact should be a Government employee—a GS-15, pay band equivalent, or the military equivalent. Send the contact's name, title, grade/pay band, phone number, and e-mail address to audcso@dodig.mil.

You can obtain information about the Department of Defense Office of Inspector General from DoD Directive 5106.01, "Inspector General of the Department of Defense (IG DoD)," April 20, 2012, as amended; DoD Instruction 7600.02, "Audit Policies," October 16, 2014, as amended; and DoD Instruction 7050.03, "Office of the Inspector General of the Department of Defense Access to Records and Information," March 22, 2013. Our website is www.dodig.mil.

If you have any questions, please contact [redacted] or [redacted]

Carol N Gorman
Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

Attachment:
As stated

DISTRIBUTION:

UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING
UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT
UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER OF THE DEPARTMENT OF DEFENSE
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, JOINT STAFF
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES
AUDITOR GENERAL, DEPARTMENT OF THE NAVY
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

Attachment

We request that you use the accompanying spreadsheet to provide the following requested information to audcso@dodig.mil by December 21, 2021.

1. Please list all remote access software used by your Military Service or agency. Using the attached spreadsheet, please identify[1]:
   - the name and a brief description of your remote access software;
   - the date the remote access software was given the authority to operate;
   - the remote access method used for this software (such as Virtual Desktop or Virtual Private Network);
   - whether the remote access software was purchased or reconfigured to support maximized telework as a result of the COVID-19 pandemic; or was the use of the remote access software in place prior to the COVID-19 pandemic;
   - the point of contact (name, position title, e-mail address, and phone number) for the organization responsible for the configuration management of the remote access software; [2] and
   - the number of users authorized to telework that uses the remote access software.

2. Please provide any risk assessments or similar analysis that identifies the risks associated with the use of remote access software. Please include any risk acceptance documentation for the remote access software listed above in item Number 1 (if applicable).

[1] For the purposes of this audit, remote access software is defined as an application provided by the operating system or a third-party vendor that connects an authorized user to an organization's internal network of nonpublic information through an external network, such as the Internet.

[2] This includes any memorandums of agreement or understanding with other Military Services or agencies that may control all or part of the configurations of the remote access software.