**United States Department of Agriculture**

Office of the Secretary

Office of the Chief Information Officer

1400 Independence Avenue S.W.

Washington, DC 20250

**TO:** Gary Washington
Chief Information Officer
Office of the Chief Information Officer

**FROM:** Ja'Nelle DeVore
Chief Information Security Officer
Office of the Chief Information Officer

**DATE:** March 16, 2023

**SUBJECT:** Risk Determination of ChatGPT

**Purpose:** To determine if ChatGPT is approved for use in the United States Department of Agriculture (USDA) enterprise network infrastructure.

**Background:** On January 26, 2023, the National Institute of Standards and Technology (NIST) released the Artificial Intelligence (AI) Risk Management Framework (RMF) (AI RMF 1.0) in response to the National Artificial Intelligence Initiative Act of 2020 (P.L. 116-283).

The goal of the AI RMF is to offer a resource to organizations designing, developing, deploying, or using artificial intelligence (AI) systems to help manage the many risks of AI and promote trustworthy and responsible development and use of AI systems. However, this guidance does not apply to the federal government use of the open-source technology ChatGPT, or any of the application programming interfaces (APIs) created by the third-party entity OpenAI, that have not been fully evaluated for cybersecurity risks to determine alignment with the NIST AI RMF 1.0.

**Risk Determination:** ChatGPT is an open-source AI chatbot technology that has become increasingly popular with its powerful conversational capabilities. It understands posed questions by creating automated responses, while furthering the conversation with additional feedback. ChatGPT also offers malicious actors assistance with advanced computer programming capabilities such as writing scripts to perform tasks and compiling full-length sophisticated writeups based on input requested by the user.

ChatGPT displays multiple concerning indicators and vulnerabilities that will pose a risk if used in the USDA enterprise network infrastructure. The National Vulnerability Database (NVD) listed one documented vulnerability with WordPress that involves the ChatGPT technology ( CVE-2023-0405) which describes a missing authorization check that allows users the ability to access data or perform actions that should be prohibited. This can lead to a wide range of problems, including information exposures, denial of service, and arbitrary code execution.

The ChatGPT technology has insufficient safeguards and (E used as a tool to develop phishing schemes, compromise business emails, write and share malware code, and redirect people to malicious websites. While OpenAI alleges having safeguards in place to mitigate these risks, use cases demonstrate that malicious users can get around those safeguards by posing questions or requests differently to obtain the same results. Use of ChatGPT poses a risk of security breaches or incidents associated with data entered the tool by users, to include controlled unclassified information (CUI), proprietary government data, regulated Food and Agriculture (FA) sector data, and personal confidential data.

Lastly, use of ChatGPT responses may render misleading and incorrect response information, as the tool responses are not validated nor regulated by the federal government.

The assessed risk impact is **HIGH**.

**Recommendation:** Effective with the date of this memorandum, the recommendation is to prohibit the use of ChatGPT on all USDA networks and replace with secure approved products.

**Decision By the CIO:**

**Approve** ☑ **Disapprove** ☐ **Discuss** ☐