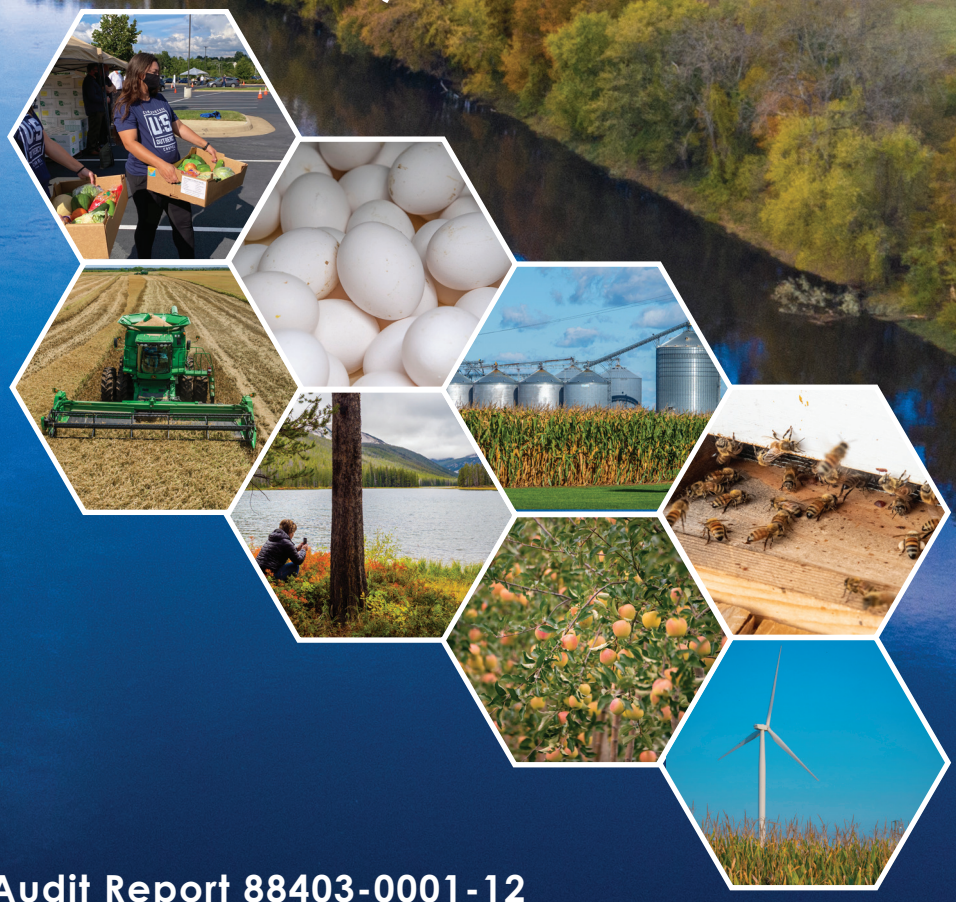
USDA
United States Department of Agriculture

Independent Service Auditor's Report on the Office of the Chief Information Officer's Description of Its Data Center Hosting and Security Systems and the Suitability of the Design and Operating Effectiveness of Its Controls for the Period October 1, 2020 to June 30, 2021



Audit Report 88403-0001-12

September 2021

OFFICE OF INSPECTOR GENERAL

IMPORTANT NOTICE

This audit report contains sensitive information that has been redacted for public release, due to privacy concerns.

USDA OFFICE OF INSPECTOR GENERAL
United States Department of Agriculture

DATE: September 29, 2021

AUDIT NUMBER: 88403-0001-12

TO: Gary S. Washington
Chief Information Officer
Office of Chief Information Officer

ATTN: Megen Davis
Director, Strategic Planning, E-government and Audits

FROM: Gil H. Harden
Assistant Inspector General for Audit

SUBJECT: Independent Service Auditor's Report on the Office of the Chief Information Officer's Description of Its Data Center Hosting and Security Systems and the Suitability of the Design and Operating Effectiveness of Its Controls for the Period October 1, 2020 to June 30, 2021

This report presents the results of the System and Organization Controls 1 Type 2 examination conducted in accordance with Statement on Standards for Attestation Engagements No. 18 for the United States Department of Agriculture (USDA) Office of the Chief Information Officer's (OCIO's) description of its data center hosting and security systems used to process user entities' transactions throughout the period October 1, 2020 to June 30, 2021. The report contains an unmodified opinion on the description and controls that were suitably designed to provide reasonable assurance that the control objectives would be achieved.

Davis Farr LLP, an independent certified public accounting firm, conducted the audit. In connection with the contract, we reviewed Davis Farr's report and related documentation and inquired of its representatives. Our review, as differentiated from an audit in accordance with Government Auditing Standards (issued by the Comptroller General of the United States), was not intended to enable us to express, and we do not express, opinions on the USDA OCIO's description of its data center hosting and security systems used to process user entities' transactions throughout the period October 1, 2020 to June 30, 2021. Davis Farr LLP is responsible for the attached auditor's report, dated September 16, 2021, and the conclusions expressed in the report. However, our review disclosed no instances where Davis Farr LLP did not comply, in all material respects, with Government Auditing Standards, issued by the Comptroller General of the United States, and relevant attestation standards established by the American Institute of Certified Public Accountants.

It is the opinion of Davis Farr LLP, in all material respects, based on the criteria described in OCIO's assertion that:

A. The description fairly presents the OCIO's data center hosting and security systems for processing user entities' transactions that were designed and implemented throughout the period October 1, 2020 to June 30, 2021.

B. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2020 to June 30, 2021, and subservice organizations and user entities applied the complementary controls assumed in the design of OCIO's controls throughout the period October 1, 2020 to June 30, 2021.

C. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2020 to June 30, 2021, if complementary subservice organization and user entities controls assumed in the design of OCIO's controls operated effectively throughout the period October 1, 2020 to June 30, 2021.

We appreciate the courtesies and cooperation extended to us by members of your staff during our audit fieldwork and subsequent discussions. The redacted version of this report will be made publicly available at http://www.usda.gov/oig in the near future.

UNITED STATES DEPARTMENT OF AGRICULTURE
Office of the Chief Information Officer

Independent Service Auditor's Report on the Office of the Chief Information Officer's
Description of its Application Hosting and Security Systems
and on the Suitability of the Design and Operating Effectiveness of its Controls

For the period October 1, 2020 through June 30, 2021

Table of Contents

DavisFarr
CERTIFIED PUBLIC ACCOUNTANTS

Davis Farr LLP
18201 Von Karman Avenue | Suite 1100 | Irvine, CA 92612
Main: 949.474.2020 | Fax: 949.263.5520

INDEPENDENT SERVICE AUDITOR'S REPORT

Chief Information Officer, Office of the Chief Information Officer
Inspector General, United States Department of Agriculture

Scope

We have examined the United States Department of Agriculture (USDA) Office of the Chief Information Officer's (OCIO's) description of its application hosting and security systems entitled "OCIO's Description of Its Application Hosting and Security Systems" for processing user entities' transactions throughout the period October 1, 2020 to June 30, 2021 (description) and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Assertion of the Management of the Office of the Chief Information Officer" (assertion). The controls and control objectives included in the description are those that management of the OCIO believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Application Hosting and Security Systems that are not likely to be relevant to user entities' internal control over financial reporting.

The OCIO uses the General Services Administration (GSA), a subservice organization, for the care, maintenance and access to the building that houses the data center. The description includes only the control objectives and related controls of the OCIO and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by the OCIO can be achieved only if complementary subservice organization controls assumed in the design of OCIO's controls are suitably designed and operating effectively, along with the related controls at the subservice organization. Our examination did not extend to controls of the subservice organization and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of OCIO's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section II, OCIO has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. OCIO is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten

the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and applicable *Government Auditing Standards*, issued by the Comptroller General of the United States (U.S. Government Accountability Office). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2020 to June 30, 2021. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves—

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.

- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.

- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.

- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing user entities' transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section IV of this report.

Opinion

In our opinion, in all material respects, based on the criteria described in OCIO's assertion—

a. the description fairly presents the Application Hosting and Security Systems that were designed and implemented throughout the period October 1, 2020 to June 30, 2021.

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2020 to June 30, 2021 and subservice organizations and user entities applied the complementary controls assumed in the design of OCIO's controls throughout the period October 1, 2020 to June 30, 2021.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2020 to June 30, 2021 if complementary subservice organization and user entity controls assumed in the design of OCIO's controls operated effectively throughout the period October 1, 2020 to June 30, 2021.

Other Matters

As noted in management's description, the following OCIO controls did not operate during the period October 1, 2020 through June 30, 2021 because the circumstances that warrant the operation of the controls did not occur during the period. Our opinion is not modified with respect to this matter.

- There were no security incidents required to be reported to the Site Incident Response Coordinator (SIRC). Therefore, we did not test the operating effectiveness of a portion of Control Objective 1, "Controls provide reasonable assurance that access to programs, data, and computer resources relevant to user entities' internal control over financial reporting is restricted to authorized users, processes, and devices," solely as it relates to security incidents required to be reported to the SIRC.

- There were no requests to grant permanent access to the data center. Therefore, we did not test the operating effectiveness of a portion of Control Objective 2, "Controls provide reasonable assurance that physical access to computer and other resources relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate personnel in order to safeguard assets and information security. Physical access limits the access to rooms, data center, and physical IT assets. This control also keeps tracks of who is coming and going in restricted areas. Finally, these controls provide reasonable assurance that physical access to computer and other resources relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate personnel. The Enterprise Data Center is designed to document, test and authorize the DISC Data Center facilities," solely as it relates to granting permanent access to the data center.

- There were no security incidents that resulted in a finding required to be reported to the Information System Security Manager and Security Administrator. Therefore, we did not test the operating effectiveness of a portion of Control Objective 3, "Controls provide reasonable assurance that network infrastructure is configured as authorized to support the effective functioning of application controls to result in valid, complete, accurate, and timely processing and reporting of transactions and balances relevant to user entities' financial reporting; protect data relevant to user entities' financial reporting from unauthorized changes; and support user entities' internal control over financial reporting. Controls also provide the communication path and services between users, processes, applications, services and external networks/the internet," solely as it relates to security incidents that resulted in a finding required to be reported to the Information System Security Manager and Security Administrator.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of the OCIO, user entities of OCIO's Application Hosting and Security Systems during some or all of the period October 1, 2020 to June 30, 2021, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Irvine, California
September 16, 2021

The subsequent sections of the report Section II—Assertion of the Management of the Office of the Chief Information Officer (pages 5–7); Section III—OCIO's Description of its Application Hosting and Security Systems (pages 8–28); and Section IV—Tests of Controls and Results (pages 29–63) are not being publicly released due to the sensitive security content.

Learn more about USDA OIG
Visit our website: **www.usda.gov/oig/index.htm**
Follow us on Twitter: @OIGUSDA

How to Report Suspected Wrongdoing in USDA Programs

Fraud, Waste, and Abuse
File complaint online: **www.usda.gov/oig/hotline.htm**

Monday–Friday, 9:00 a.m.– 3:00 p.m. ET
In Washington, DC 202-690-1622
Outside DC 800-424-9121
TDD (Call Collect) 202-690-1202

Bribes or Gratuities
202-720-7257 (24 hours)