



United States Department of Agriculture  
Office of Inspector General  
Washington, D.C. 20250



DATE: August 11, 2016

AUDIT  
NUMBER: 50501-0012-12(1)

SUBJECT: Summary of OIG Report on USDA's Covered Systems—Interim Report

In December 2015, President Obama signed the Cybersecurity Act of 2015 (the Act) into law. Section 406 of the Act—Federal Computer Security—requires that by August 14, 2016, Inspectors General of “covered agencies” submit a report to Congress that includes information collected from their agencies regarding Federal computer systems. The Act defines “Covered agencies” as agencies that operate “covered systems,” which are further defined as (1) national security systems, or (2) Federal computer systems that provide access to personally identifiable information (PII).

In order to comply with the mandate in the Act, Department of Agriculture (USDA) Office of Inspector General (OIG) issued a data call asking the questions stipulated in the Act. The data call was sent to USDA's Office of Chief Information Officer (OCIO), who forwarded the questionnaire to all USDA agencies' Chief Information Officers and Information Systems Security Program Managers to populate and return to OIG. We collected and reconciled the responses received from the entities with USDA's official inventory. We then followed up on any identified differences and updated the response results with the correct data, or we had the entities correct the official inventory, as needed.

USDA does not have any national security systems. While we did collect and reconcile the data, we did not test or validate the information, nor verify the statements made. We are not making any conclusions or recommendations at this time. Select information will be incorporated into the 2016 Federal Information Security Modernization Act (FISMA) audit engagement and related report.

We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

**Due to the sensitive nature of the Departmental computer system information contained in this interim report, it will not be publicly released.**