Statement by
Jonathan Alboum
USDA Chief Information Officer
Before the Committee on Oversight and Government Reform
Subcommittee on Information Technology
U.S. House of Representatives
November 16, 2016

Chairman Hurd, Ranking Member Kelly and Members of the Subcommittee, thank you for your diligent work on Cyber Security and the IT Scorecard. I appreciate having this opportunity to share USDA's efforts to strengthen its cybersecurity posture over the last few years.

The Department of Agriculture touches the lives of all Americans. Protecting USDA customer, partner, and employee data is a top priority for Secretary Vilsack and me. Together, we work across USDA to ensure we have the right tools and culture to meet new threats as they emerge.

In terms of cybersecurity tools, I'm pleased to tell the committee that USDA has successfully completed our initial implementation of Einstein 3A. USDA employs a risk-based approach to cybersecurity, prioritizing resources where they will have the most significant impact. Einstein is key to this approach. Over the coming weeks we will continue to work with DHS to bring additional Einstein capabilities online. We fully expect to meet all of the December deadlines.

I'm also proud to share that USDA is one of the leading agencies participating in the DHS Continuous Diagnostics and Mitigation program, also known as CDM. I've made this a priority for the Department. We are currently implementing the capabilities of Phase 1, which give us increased insight into what is on our network. This improved visibility helps us prioritize future modernization initiatives and protect the information of the people we serve.

Einstein and CDM, combined with our Security Operations Center (SOC), position USDA to proactively detect, prevent, and mitigate cyberattacks. The USDA SOC is starting to use "Big Data" technologies to analyze trends and anomalies by correlating security data from multiple sources. We have partnered with Defense Advanced Research Projects Agency (DARPA) to pilot many of these tools. As pilots

like these demonstrate positive results, USDA will explore the potential for Department-wide rollout.

Further, my team routinely conducts penetration testing assessments to identify security vulnerabilities in our systems. The findings are used to develop plans that remediate risks and improve system security. USDA also created a list of High Value Assets and has worked with DHS to perform additional penetration testing assessments of these systems over the past year.

Effective cybersecurity is as much about education and culture as it is about having the right tools in place. Secretary Vilsack strongly supports my office in ensuring that USDA's senior executives and employees understand their daily role in preserving the Department's reputation as a trusted government partner.

In the past year, USDA created a scorecard to build awareness of the Department's cyber security posture. Every two weeks, component agency heads are provided with a status of key cybersecurity hygiene factors for their organizations. This increased insight gives USDA officials the information they need to balance programmatic requirements with continuous improvements in cybersecurity. For example, this approach supported our drive to increase the usage of Personal Identity Verification (PIV) cards across the Department. Over the past 16 months, we increased our usage rate from 15% to over 92% for non-privileged users and from 6% to over 96% for privileged users.

USDA employees face an increasing number of malicious emails and social engineering cyberattacks, like phishing. Through an anti-phishing campaign in 2016, we recognized that additional safeguards, like email subject line warning messages, were needed to render phishing attacks less effective. As a result of these activities, USDA achieved a greater than 50% reduction in the click rate of simulated phishing attempts which further reduces Departmental vulnerabilities to such cyberattacks.

Further, my team and I fully support the push for additional measures to improve information sharing across Government to enhance cybersecurity readiness and response. In May 2016, USDA became the first Department to develop and successfully test new procedures required by the Federal Cybersecurity Enhancement Act for notifying Congress within 7 days of a Major Incident.

As threats continue to proliferate and to adapt to existing defenses, USDA, like all Government agencies, will need appropriate resources to employ emerging technologies and new approaches to mitigate these risks. For instance, the Department's FY 2017 Budget included a requested increase of $10 million to enhance USDA's cyber security capabilities. It is critically important that we discuss these issues and related impacts. So, again, I want to thank you for holding this hearing to shed light on this important topic. I am grateful for the opportunity to share information about our progress in strengthening USDA's cybersecurity program. We are committed to an open and continuous dialogue with Congress about new opportunities to improve our defenses, and I look forward to your questions.