

DEPARTMENT OF AGRICULTURE**National Agricultural Statistics Service****Confidentiality Pledge Revision Notice**

AGENCY: National Agricultural Statistics Service, USDA.

ACTION: Notice of Revision of Confidentiality Pledge under the Title V of the E-Government Act, Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA) and Title 7, Chapter 55, Section 2276 (Confidentiality of Information).

SUMMARY: Under 44 U.S.C. 3506(e), and 44 U.S.C. 3501, the National Agricultural Statistics Service (NASS) is announcing a revision to the confidentiality pledge it provides to its respondents under CIPSEA and Title 7, Chapter 55, Section 2276. The revision is required by the passage and implementation of provisions of the Federal Cybersecurity Enhancement Act of 2015 (H.R. 2029, Division N, Title II, Subtitle B, Sec. 223), which permit and require the Secretary of Homeland Security to provide Federal civilian agencies' information technology systems with cybersecurity protection for their Internet traffic. More details on this announcement are presented in the SUPPLEMENTARY INFORMATION section below.

DATES: This revision becomes effective upon publication of this notice in the **Federal Register**. In a parallel **Federal Register** notice, NASS is seeking public comment on this confidentiality pledge revision.

ADDRESSES: Questions about this notice may be submitted by any of the following methods:

- E-mail: ombofficer@nass.usda.gov. Include the title “Confidentiality Pledge Revision Notice” in the subject line of the message.
- Efax: (855) 838-6382.
- Mail or Hand Delivery/Courier: David Hancock, NASS Clearance Officer, U.S. Department of Agriculture, Room 5336 South Building, 1400 Independence Avenue SW, Washington, D.C. 20250-2024.

FOR FURTHER INFORMATION CONTACT: R. Renee Picanso, Associate Administrator, National Agricultural Statistics Service, U.S. Department of Agriculture, (202) 720-4333, or email HQOA@nass.usda.gov. Because of delays in the receipt of regular mail related to security screening, respondents are encouraged to use phone or electronic communications.

SUPPLEMENTARY INFORMATION:

Under CIPSEA; Title 7, Chapter 55, Section 2276; and similar statistical confidentiality protection statutes, many federal statistical agencies, including NASS, make statutory pledges that the information respondents provide will be seen only by statistical agency personnel or their sworn agents, and will be used only for statistical purposes. CIPSEA and Title 7, Chapter 55, Section 2276 protect such statistical information from administrative, law enforcement,

taxation, regulatory, or any other non-statistical use and immunize the information submitted to statistical agencies from legal process. Moreover, many of these statutes carry criminal penalties of a Class E felony (fines up to \$250,000, or up to five years in prison, or both) for conviction of a knowing and willful unauthorized disclosure of covered information.

As part of the Consolidated Appropriations Act for Fiscal Year 2016 signed on December 17, 2015, the Congress included the Federal Cybersecurity Enhancement Act of 2015 (H.R. 2029, Division N, Title II, Subtitle B, Sec. 223). This Act, among other provisions, permits and requires the Secretary of Homeland Security to provide federal civilian agencies' information technology systems with cybersecurity protection for their Internet traffic. The technology currently used to provide this protection against cyber malware is known as "Einstein 3A". It electronically searches Internet traffic in and out of federal civilian agencies in real time for malware signatures.

When such a signature is found, the Internet packets that contain the malware signature are shunted aside for further inspection by Department of Homeland Security (DHS) personnel. Because it is possible that such packets entering or leaving a statistical agency's information technology system may contain confidential statistical data, statistical agencies can no longer promise their respondents that their responses will be seen only by statistical agency personnel or their sworn agents. However, they can promise, in accordance with provisions of the Federal Cybersecurity Enhancement Act of 2015, that such monitoring can

be used only to protect information and information systems from cybersecurity risks, thereby, in effect, providing stronger protection to the integrity of the respondents' submissions.

Consequently, with the passage of the Federal Cybersecurity Enhancement Act of 2015, the federal statistical community has an opportunity to welcome the further protection of its confidential data offered by DHS' Einstein 3A cybersecurity protection program. The DHS cybersecurity program's objective is to protect federal civilian information systems from malicious malware attacks. The federal statistical system's objective is to ensure that the DHS Secretary performs those essential duties in a manner that honors the Government's statutory promises to the public to protect their confidential data. Given that the Department of Homeland Security is not a federal statistical agency, both DHS and the federal statistical agencies have been engaged in finding a way to balance both objectives and achieve these mutually reinforcing objectives.

Accordingly, DHS and federal statistical agencies (including NASS), in cooperation with their parent departments, have developed a Memorandum of Agreement for the installation of Einstein 3A cybersecurity protection technology to monitor their Internet traffic and have incorporated an associated Addendum on Highly Sensitive Agency Information that provides additional protection and enhanced security handling of confidential statistical data.

However, CIPSEA; Title 7, Chapter 55, Section 2276; and similar statistical confidentiality pledges promise that respondents' data will be seen only by

statistical agency personnel or their sworn agents. Since it is possible that DHS personnel could see some portion of those confidential data in the course of examining the suspicious Internet packets identified by the Einstein 3A technology, statistical agencies need to revise their confidentiality pledges to reflect this process change.

Therefore, NASS is providing this notice to alert the public to this confidentiality pledge revision in an efficient and coordinated fashion. Below is the revised confidentiality pledge as it will appear on NASS survey questionnaires, as well as the revision to NASS's confidentiality webpage. A list of the NASS OMB numbers and information collection titles that will be affected by this revision is also included below.

The revised confidentiality pledge to appear on NASS questionnaires is below:

The information you provide will be used for statistical purposes only. Your responses will be kept confidential and any person who willfully discloses ANY identifiable information about you or your operation is subject to a jail term, a fine, or both.

This survey is conducted in accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws. For more information on how we protect your information please visit:

https://www.nass.usda.gov/About_NASS/Confidentiality_Pledge/index.php

For voluntary surveys the statement, "Response to this survey is **voluntary**." will follow this pledge. For mandatory surveys the statement, "Response to this survey is **mandatory**." will follow.

The NASS confidentiality pledge webpage

(https://www.nass.usda.gov/About_NASS/Confidentiality_Pledge/index.php) will

be revised to include a fifth item explaining that DHS will monitor the transmission of data for cybersecurity threats. Item 5 is below:

5. Data are protected from cybersecurity threats

Per the Cybersecurity Enhancement Act of 2015, your data are further protected by the Department of Homeland Security (DHS) through cybersecurity monitoring of the systems that transmit your data. DHS will be monitoring these systems to look for viruses, malware and other threats. In the event of a cybersecurity incident, and pursuant to any required legal process, information from these sources may be used to help identify and mitigate the incident.

Affected information collections:

<u>OMB No.</u>	<u>Expiration Date</u>	<u>Information Collection Title</u>
0535-0001	04/30/2019	Cold Storage
0535-0002	10/31/2018	Field Crops Production
0535-0003	07/31/2019	Agricultural Prices
0535-0004	01/31/2019	Egg, Chicken, and Turkey Surveys
0535-0005	11/30/2017	Livestock Slaughter
0535-0007	01/31/2019	Stocks Reports
0535-0020	07/31/2018	Milk and Milk Products
0535-0037	08/31/2019	Vegetable Surveys
0535-0039	10/31/2019	Fruit, Nuts, and Specialty Crops
0535-0088	07/31/2018	Field Crops Objective Yield
0535-0093	11/30/2018	Floriculture Survey
0535-0109	03/31/2018	Agricultural Labor
0535-0140	01/31/2019	List Sampling Frame Survey
0535-0150	06/30/2017	Aquaculture
0535-0153	12/31/2018	Honey Survey
0535-0212	11/30/2018	Mink Survey
0535-0213	06/30/2017	Agricultural Surveys Program
0535-0218	07/31/2018	Agricultural Resource Management and Chemical Use Surveys (ARMS)
0535-0220	03/31/2017	Cotton Ginnings
0535-0226	10/31/2019	Census of Agriculture
0535-0243	08/31/2018	Census of Agriculture Content Test
0535-0244	11/30/2019	Nursery Production Survey and Nursery and Floriculture Chemical Use Survey
0535-0245	09/30/2017	CEAP - NRI Conservation Tillage and Nutrient Management Survey
0535-0248	04/30/2019	Generic Clearance of Survey Improvement Projects
0535-0249	12/31/2017	Organic Production Survey
0535-0251	05/30/2019	Residue and Biomass Field Survey
0535-0254	07/31/2017	Current Agricultural Industrial Reports (CAIR)
0535-0255	04/30/2018	Colony Loss
0535-0256	06/30/2018	Feral Swine Survey

0535-0257	10/31/2018	Organic Certifier Census
0535-0258	11/30/2018	Cost of Pollination Survey
0535-0259	03/31/2019	Local Foods Survey

Signed at Washington, D.C., November 30, 2016

Hubert Hamer,
Administrator