United States Department of Agricultural

National Agricultural Statistics Service

Research and
Development Division
Washington, DC 20250

RDD Research Report
Number RDD-19-02

May 2019

Revisions to the NASS Confidentiality Pledge: Results of Cognitive Testing

Heather Ridolfo, PhD

EXECUTIVE SUMMARY

Federal statistical agencies currently collect data under the Confidential Information Protection and Statistical Efficiency Act (CIPSEA). Under the CIPSEA law, agencies are able to pledge to respondents that only sworn employees and agents will have access to identifiable information and that this information will be used for statistical purposes only. In 2015, the Cybersecurity Enhancement Act was passed. This new law gave the Department of Homeland Security (DHS), which serves as the clearing house for monitoring and evaluating cybersecurity threats within Federal agencies, the authority to monitor any information stored on or transited to or from civilian information systems for any lawful government purpose. As a result, statistical agencies, such as the National Agricultural Statistics Service (NASS), could no longer assure respondents that only their sworn employees and agents will have access to their identifiable information and that their information will be used for statistical purposes only.

In May 2016, the Office of Management and Budget (OMB) formed a working group to develop and test alternative pledge wording to inform survey respondents of this change. The workgroup consisted of representatives from ten statistical agencies, including NASS. Given differences in agency policies and survey populations (e.g., farmers, general population, prisoners, etc.), each agency developed its own pledge wording. The pledges were then evaluated using different methodologies. Findings from this research were then compiled and presented to OMB.

At NASS, two revised confidentiality pledges were developed. One revision explicitly named DHS as the agency that would be conducting the monitoring, and the other revision did not. In addition, NASS developed a statement to be added to the revised confidentiality pledges, which stated the actions NASS would take should a cybersecurity threat be detected. Respondents' comprehension of and reactions to the current CIPSEA pledge and these pledge revisions were evaluated using 30 cognitive interviews.

Respondents had a positive reaction to the current CIPSEA pledge and all respondents interpreted this pledge as conveying to them that their information would be kept confidential. Many respondents also observed that 1) their information would be identifiable only to NASS employees, 2) employees are required to take an oath and are subject to a jail term or fine if they disclose identifiable information, and 3) their information could be used for statistical purposes only.

In terms of the revised pledges, respondents generally had a negative reaction to the revised pledge that specifically identified DHS as the agency that would be conducting the cybersecurity monitoring. Respondents had little confidence in DHS to protect their data and felt that using a third party to conduct cybersecurity monitoring opened the data up to more potential security breaches. Respondents were also concerned that their data would no longer be confidential and perceived that DHS would be monitoring their data for purposes beyond cybersecurity (e.g. illegal behavior).

Respondents had a more positive reaction to the revised pledge that did not explicitly mention DHS. They felt it better explained why NASS was changing the way data are monitored and they liked that DHS was not named as the agency conducting the monitoring.

In both pledges, there was terminology and phrases that were difficult for respondents to comprehend. These terms included: “systems that transmit your data,” “cybersecurity monitoring,” “federal information systems,” “cybersecurity screening of transmitted data,” and “malicious activities.” Respondents often stated that the confidentiality pledges needed to be written using plain language. At times, these problematic terms caused respondents to misinterpret the intent of the message.

NASS also developed an additional statement, to be added to the end of the revised confidentiality pledges that informed respondents of the actions that NASS would take should a cybersecurity incident be detected. Respondents had a great deal of difficulty comprehending this sentence. Respondents also found this statement alarming as they interpreted it as indicating a cybersecurity breech will occur. This statement lowered respondents’ confidence in NASS’s ability to keep personal information confidential.

The results from this study indicate that, when revising the NASS confidentiality pledge, careful consideration needs to be taken to ensure transparency and clarity while balancing respondents’ expectations for confidentiality. The most important information respondents were looking for in the confidentiality pledge was that their data would be kept confidential. The revisions to the confidentiality pledge, particularly the mention of DHS and the additional statement, caused respondents to have less confidence in NASS’s ability to secure their data. These results and the results of research conducted in the other nine statistical agencies should be taken into consideration when revising the NASS confidentiality pledge.

RECOMMENDATIONS

1. Use plain language to convey that the information respondents provide on NASS surveys will be kept confidential and used for statistical purposes only. Direct respondents to a website that provides the full information on how we protect our survey data.

Example:

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: [insert web address].

2. Add a fifth statement to the NASS Confidentiality Pledge Page (https://www.nass.usda.gov/About_NASS/Confidentiality_Pledge/index.php) that conveys DHS's involvement.

Example:

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.

TABLE OF CONTENTS

Revisions to the NASS Confidentiality Pledge: Results of Cognitive Testing

Heather Ridolfo[1]

Abstract

Under the Confidential Information Protection and Statistical Efficiency Act (CIPSEA), the National Agricultural Statistics Service (NASS) pledges that only sworn employees and agents will have access to identifiable information and that this information will be used for statistical purposes only. However, the Cybersecurity Enhancement Act of 2015 conflicts with CIPSEA, since it requires the Department of Homeland Security to monitor any information stored on or transited to or from civilian information systems for any lawful government purpose. Given this change, NASS was required to revise the confidentiality pledge. Using 30 cognitive interviews, NASS evaluated respondents' comprehension of and reactions to two revised confidentiality pledges. Findings indicate the importance of balancing transparency, clarity and respondents' expectations for confidentiality.

Key words: Confidentiality, Cybersecurity, data security

1. INTRODUCTION

Data collected by the National Agricultural Statistics Service (NASS) are currently protected under the Confidential Information Protection and Statistical Efficiency Act (CIPSEA). Under CIPSEA provisions, data can be collected for statistical purposes only and public disclosure of data is strictly prohibited. All NASS employees are required to take a sworn oath assuring that they will maintain data confidentiality. Any employee who does not abide by these provisions is subject to fines and/or jail time.

The Cybersecurity Enhancement Act of 2015 (2015 Act) requires the installation of the Department of Homeland Security's (DHS) Einstein 3a on all Federal civilian information technology systems. Einstein 3a is a cybersecurity protection system that provides traffic monitoring and intrusion detection and prevention technology. The 2015 Act permits DHS to use survey data for any lawful purpose (statistical and non-statistical) and provides liability protection for any misuse of that information.

The 2015 Act compromises current Federal confidentiality pledges as statistical agencies can no longer assure 1) data will only be accessed by employees of the statistical agencies, 2) data will be used for statistical purposes only, and 3) agents of the statistical agencies will be subject to fines and jail terms if data are intentionally disclosed to unauthorized persons and/or used for non-statistical purposes. Consequently, all Federal civilian statistical agencies need to develop new confidentiality pledges to inform respondents of this change in circumstances.

[1] Heather Ridolfo is an Agricultural Statistician with the National Agricultural Statistics Service, Research and Development Division, 1400 Independence Ave S.W., Washington, DC 20250. The author would like to thank Kerry McBride, Gary Keough, Mallory Dolan, Cheryl Turner, Wendy Vance, Kathy Ott, Tyler Wilson, and Rachel Sloan for their assistance on this research project.

Although, it is necessary to revise the confidentiality pledge in order to ensure transparency, the required revisions have the potential to negatively impact response rates. Consequently, the Office of Management and Budget (OMB) formed a working group in May 2016 to develop and test alternative pledge wording and provide recommendations back to OMB. Methodologists from ten statistical agencies participated in this workgroup. Agencies developed alternative pledges that were reflective of changes covered in the 2015 Act and their own agency policies. The revised pledges were tested across various populations using multiple methods. The results of this workgroup were presented in a report to OMB in August 2016 (Scope Confidentiality Pledge Revision Subcommittee Final Report). The following report will detail the methodology used at NASS and present results and recommendations from this research.

2. METHODS

2.1 Sample

NASS conducted 30 interviews with farm and ranch operators. Respondents were recruited using the NASS list frame and snowball sampling. In order to participate in this study, respondents' operations had to be considered a farm or ranch by NASS definition and therefore eligible for selection in NASS surveys or Census. By definition, an operation is considered a farm or ranch if it has any combination of sales, potential sales and government payments totaling at least $1,000. Respondents were selected from various regions of the country to ensure geographical differences in agriculture and attitudes were covered.

Table 1 summarizes the characteristics of the sample. The majority of respondents were older. Forty-seven percent of the sample were older than 65. Fifty percent of the farms in our sample operated less than 200 acres, and 40 percent of the sample had a total of sales below $150,000. The respondents in this sample were similar to the U.S. farm population in terms of age, total acres operated and value of sales (USDA, 2014).

Table 1. Demographic Summary of Sample (n=30)

	Number	Percent
Age		
35-44	5	17
45-64	10	33
65 and older	14	47
Unknown	1	3
Farm Type		
Livestock	13	43
Crops	17	57
Total Acres Operated		
<100	7	23
100-199	8	27
200-499	4	13
500-999	5	17
1000 or more	6	20
Value of Sales		
<20,000	8	27
20,000-49,000	0	0
50,000-149,000	4	13
150,000-499,000	6	20
500,000 or more	12	40

2.2 Data Collection

Twenty-nine interviews were conducted in person and one interview was conducted over the phone. All interviews were semi-structured and lasted one hour. The goal of the interviews was to assess respondents' comprehension of and reaction to the current and revised pledge language. During the cognitive interviews, different wording options were evaluated to determine which

option would be the most effective in ensuring confidentiality and have the least negative impact on willingness to respond to NASS surveys.

Respondents were presented with three versions of the confidentiality pledge: the current NASS confidentiality pledge, a pledge that explicitly mentioned DHS's involvement (Revised Pledge A) and a pledge that does not mention DHS (Revised Pledge B). Respondents were also presented with an additional statement after each revised pledge that indicated the actions NASS would take should a cybersecurity breach occur. Respondents all read the current NASS confidentiality pledge first. However, the order in which respondents were presented the revised pledges was randomized so that half of the respondents read Revised Pledge A first and half read Revised Pledge B first. All respondents were presented with the additional statement following the revised pledges. Respondents were probed concurrently to determine their comprehension of and reactions to the pledge wording and the additional statement. The pledges and additional statement can be found in Figure 1. Materials used during testing can be found in the appendices.

Interviews were conducted by headquarters and field staff who have been trained to conduct cognitive interviews. Interviews took place in nine states: New Hampshire, New York, Pennsylvania, Maryland, Virginia, Kentucky, Ohio, Colorado, and Washington. Interview data were analyzed using the constant comparative method of analysis (Strauss and Corbin 1990).

Figure 1. Confidentiality Pledges Used During Testing

Current NASS Confidentiality Pledge

The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, every employee and agent has taken an oath and is subject to a jail term, a fine, or both if he or she willfully discloses ANY identifiable information about you or your operation.

Revised Pledge A

The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, any person is subject to a jail term, a fine, or both if he or she willfully discloses ANY identifiable information about you or your operation. Your data are further protected by Department of Homeland Security employees and contractors through cybersecurity monitoring of the systems that transmit your data.

Revised Pledge B

The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and

other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, any person is subject to a jail term, a fine, or both if he or she willfully discloses ANY identifiable information about you or your operation. Per the Cybersecurity Enhancement Act of 2015, Federal information systems are protected from malicious activities through cybersecurity screening of transmitted data.

Additional Statement

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.

3. RESULTS

3.1 Current NASS Confidentiality Pledge

> The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, every employee and agent has taken an oath and is subject to a jail term, a fine, or both if he or she willfully discloses ANY identifiable information about you or your operation.

All but one respondent had a positive reaction to the current NASS confidentiality pledge. All respondents interpreted this pledge as stating that the information they provide on NASS surveys will be kept confidential. Many respondents also interpreted this pledge as stating that (1) identifiable information will not be disclosed to anyone other than NASS employees, (2) employees are subject to a jail term and/or fine if they disclose identifiable information, (3) their information can be used for statistical purposes only and (4) employees have taken an oath to ensure confidentiality.

There were some comprehension issues with this pledge. First, two respondents indicated that they were not familiar with "Title V, Subtitle A, Public Law 107-347." However, this did not prohibit them from understanding the other information provided in the pledge. Four respondents indicated they were not sure who could access their identifiable information. This ambiguity stemmed from the term "agents." Three respondents specifically asked for the term "agents" to be defined. One respondent presumed that this term was referring to contract employees of NASS and another respondent presumed that this was referring to FBI or CIA agents. Not knowing who could access his identifiable information caused one respondent to have a negative reaction to this pledge.

The majority of respondents understood that their information would be used to produce agricultural statistics and NASS reports. One respondent thought his information could be combined with other information the government collects (e.g., IRS data). Two respondents did not know how the information they provided on surveys was used.

In general, respondents had no concerns regarding how NASS handles the information they provide on surveys. Many respondents stated that they trusted NASS and/or USDA to keep their information confidential. Only one respondent had concerns regarding how NASS handles his information and, again, this stemmed from not knowing who is defined as an "agent."

Several respondents expressed having no concerns that their identifiable survey data would be stolen. Although these respondents were confident in NASS's ability to keep their information confidential, six respondents expressed having general concerns that their identifiable data could be released to other groups such as the EPA, DOL, FDC, environmental groups, animal rights groups, marketers, and seed companies. A couple of respondents also expressed concern that NASS data could be subpoenaed or data could be requested under the Freedom of Information Act.

3.2 Revised Pledge A

> The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, any person is subject to a jail term, a fine, or both if he or she willfully discloses ANY identifiable information about you or your operation. Your data are further protected by Department of Homeland Security employees and contractors through cybersecurity monitoring of the systems that transmit your data.

3.2.1 Interpretation of Revised Pledge A

Twenty of the 30 respondents interpreted the changes to this pledge as indicating that DHS would be monitoring NASS data to make sure it is not accessed by unauthorized individuals. Two respondents mentioned that this monitoring is done during the electronic transmission of data. Ten of the 30 respondents did not understand what "cybersecurity monitoring" meant and this led to multiple misinterpretations of DHS's role. Two of these respondents interpreted this to mean that DHS was ensuring NASS's data remain confidential but they did not understand how that was done. Other respondents had more concerning interpretations, which included (1) DHS will be monitoring NASS data for criminal behavior on the part of respondents, (2) DHS will be using the data to watch for criminal activity against agricultural producers, (3) DHS will be monitoring agricultural producers' personal computers and (4) DHS will be monitoring the data to ensure enumerators are entering valid data.

Respondents were also probed on their understanding of the phrase "systems that transmit your data." Specifically, respondents were asked how they interpreted the term "systems" in this phrase. The majority of respondents interpreted this as referring to electronic devices that store and transmit data including desktops, laptops, cell phones, servers, and routers. Others mentioned email, the internet, and the cloud. However, seven respondents did not know what was meant by this term.

When probed on their knowledge of DHS, respondents had varying degrees of knowledge of this agency. Two respondents were not familiar at all with DHS. Five respondents had heard of the agency but did not know their purpose. The remaining respondents indicated that DHS was responsible for preventing terrorist threats against our national security.

3.2.2 Reactions to Revised Pledge A

Twelve of the 30 respondents had a positive reaction to this pledge, 17 had a negative reaction, and one had no reaction. Respondents' reactions were not directly tied to whether or not respondents interpreted the revised pledge correctly.

When respondents had *positive* reactions to Revised Pledge A, they generally felt that it was good that there was an extra layer of monitoring and felt it made their data more secure. However, some of these respondents misunderstood the scope of DHS's monitoring. These respondents' misinterpretations were similar to the concerns raised by those who reacted negatively to this pledge but, for whatever reason, these interpretations were not a cause of concern to those who reacted positively to Revised Pledge A. These misinterpretations included (1) the data are no longer confidential and (2) DHS is reviewing the data for criminal behavior on the part of survey respondents (e.g., hiring of illegal immigrants, stockpiling ammonium nitrate, misreporting financial information).

Respondents had negative reactions to this pledge for various reasons. The most common reasons centered around the involvement of a third party in securing the data and, in particular, the involvement of DHS. Some respondent felt that the involvement of a third party made the survey data less secure as it provided more opportunities for security breaches. Respondents also did not like the mention of "contractors" in the pledge. This term made some respondents immediately think of Edward Snowden, a contractor working for the National Security Agency (NSA) who leaked classified information. The thought of contractors having access to their identifiable information made them feel less confident in the security of their data. Respondents also had a very strong negative reaction against the involvement of DHS in securing their survey data.

> They are telling me a bunch of [expletive deleted]. This is the worst damn statement of them all! Homeland Security is a useless blanket of catch-all positions and contractors. Come on! Who is it? We outsource so much stuff to contractors. You get what you get and we can still end up with a Snowden.

Respondents, who had negative reactions to this pledge, had little confidence in DHS's ability to secure their data and did not trust that DHS would be accessing their data for cybersecurity purposes only. Some respondents were concerned that DHS would be monitoring the survey data for criminal behavior on the part of survey respondents such as hiring of illegal immigrants, stockpiling ammonium nitrate, polluting water systems, and tainting food supplies. Some respondents also questioned why DHS needed to be involved and others commented that DHS has too much power and latitude.

Other questions raised regarding DHS included: (1) would DHS be able to monitor their home computers? (2) When in the data lifecycle would DHS's monitoring begin? (3) Would DHS be able to change answers to survey question and skew the statistics? and (4) Why did DHS need to be involved?

Beyond DHS, some respondents were concerned that the survey data could be shared with other Federal and State agencies (e.g., EPA). Furthermore, respondents also perceived that their data would no longer be confidential and that DHS and other groups could link their identity with their survey answers. Finally, this pledge raised respondents' awareness of potential data security breaches that they had not previously considered. Ultimately, two respondents indicated they would not respond to a NASS survey that had used Revised Pledge A.

3.3 Revised Pledge B

> The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, any person is subject to a jail term, a fine, or both if he or she willfully discloses ANY identifiable information about you or your operation. Per the Cybersecurity Enhancement Act of 2015, Federal information systems are protected from malicious activities through cybersecurity screening of transmitted data.

3.3.1 Interpretation of Revised Pledge B

Most respondents generally interpreted the changes to this pledge as indicating that their information would be protected from unauthorized access of the survey data or hacking. However, respondents understanding of how and why this protection was implemented varied. For example, a couple of respondents interpreted this as indicating that only data that are submitted in an online survey are protected. Some respondents interpreted this pledge as indicating that they were personally protected if NASS data are hacked. However, one respondent interpreted this as indicating that if NASS data were hacked, she has no recourse against NASS. One respondent thought this pledge was informing respondents that their data could be hacked. Several respondents mentioned that this pledge is telling them that there is a new act related to cybersecurity; however, they all indicated that they are not familiar with this act and what it entails. A couple of respondents indicated that they assumed this act was put in place to protect them.

Nine respondents did not understand the intent of Revised Pledge B. Two respondents interpreted the revised statement as indicating the survey data would be screened for criminal behavior on the part of respondents. One respondent interpreted this statement as indicating that loopholes that threaten confidentiality would be closed. Five respondents indicated they did not know what this new statement was conveying. Some understood that it had something to do with securing the data but they did not understand how this would be done.

Respondents were probed on specific terms and phrases in the last sentence of Revised Pledge B. Respondents had varying interpretations of the phrase "Federal information systems." Some respondents understood this as referring to computer systems, databases and data collection systems. Others interpreted this as referring to all data the government collects on the American public. A couple of respondents thought this phrase included government statistics and reports. One respondent interpreted this as referring to government entities and agents. Four respondents indicated they could not comprehend the meaning of this phrase.

When probed on their understanding of the phrase "malicious activities," the vast majority of respondents interpreted this as referring to hacking into survey data and using the information for unauthorized purposes. Respondents generally perceived this would be done for identity theft purposes; however, one respondent perceived this would be done to change survey answers and skew agricultural statistics. Two respondents interpreted "malicious activities" as referring to criminal behavior and one respondent interpreted this phrase as meaning violent or inappropriate behavior. Two respondents indicated they did not know what this term meant.

Respondents were also probed on their understanding of "cybersecurity screening of transmitted data." Some respondents interpreted this phrase as indicating the survey data would be protected from hackers. Others were more specific in their interpretations. Some indicated that the survey data would be screened to ensure there were no viruses, malware, or hidden code. Others interpreted this phrase as indicating that the data that were transmitted electronically would be screened. About half of the respondents misinterpreted the intent of this phrase. One respondent interpreted this pledge as saying the survey data would be encoded before it was transmitted. Another respondent interpreted this phrase as indicating that the data would be screened to determine whether it contained sensitive information. One respondent interpreted this phrase as indicating that the survey data would be screened to determine whether respondents were providing valid responses. Two respondents indicated that the federal government would be reviewing their personal survey data and one respondent indicated the federal government would be looking for illegal activity. Four respondents indicated they did not understand this phrase.

Finally, respondents were probed on their understanding of the term "data." The majority of respondents understood this as referring to responses to survey questions. However, one respondent interpreted this as referring to information provided on a computer, and another respondent interpreted this as referring to NASS publications.

3.3.2 Reactions to Revised Pledge B

Nineteen of the 30 respondents had a positive reaction to this pledge, eight had a negative reaction, one had a mixed reaction, and two had no reaction.

When respondents had a positive reaction to Revised Pledge B, it was often because they interpreted this pledge as indicating that their survey data would be protected from hacking. One respondent indicated that he assumed NASS was already securing data in this way and was reassured by this pledge. Respondents who read this pledge last, often reacted positively to this pledge because it did not mention DHS.

Respondents, who misinterpreted the intent of this pledge, often had negative reactions toward it. For example, one respondent's negative reaction to this pledge was due to her misinterpreting this pledge as stating that if NASS data were hacked, she would have no recourse. Another respondent was concerned that his individual survey answers would be screened, and therefore had a negative reaction to this pledge. Finally, a couple of respondents felt that this pledge raised their awareness of potential data security breaches and made them think their data were less secure.

One respondent indicated he would not respond to a NASS survey after reading this pledge. Two respondents indicated they would be reluctant to disclose certain types of information: fertilizer and chemical use, workers who are illegal immigrants.

3.4 Additional Statement

> 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.

Respondents had a great deal of difficulty comprehending this sentence. About two-thirds of the respondents understood that this sentence was conveying that if NASS data were hacked, NASS would take steps to resolve the issue. However, respondents had varying interpretations of the steps NASS would take to resolve the issue. One-third of the respondents could not comprehend this sentence or entirely misinterpreted the intent.

As mentioned above, respondents had varying interpretations regarding the steps NASS would take to resolve a hacking incident. Some respondents interpreted this statement as conveying that their identifiable survey answers would be used to help identify the source of the intrusion. Other respondents believed that NASS would access their personal computers to find the source of the intrusion. One respondent believed that information from DHS would be used to identify the source of the intrusion. One respondent thought NASS would need to release his name and address to prove the data had been hacked.

Others interpreted this statement as conveying that the data could be hacked in the future and their information could be stolen. One respondent described this statement as a "cop out," stating that this sentence says "you were warned if NASS gets hacked." Another respondent stated, "It's almost like we're going to protect you but there's 'buts' at the end of it." Some interpreted this sentence as saying their information is no longer confidential and secure, and because of this, it was contradictory to information provided in the preceding sentences. One respondent stated,

> This is bad! Initially, the paragraph is saying that the data are not available to others, but now this line is saying the data will be used. This is contradictory. Worse than contradictory, this is saying the exact opposite of the rest of the paragraphs. This is very bad.

Others had completely different interpretations of this sentence. One respondent interpreted this sentence as conveying that the information provided in the survey data could be used to prosecute anybody for terrorist activities pertaining to agriculture. Another respondent

interpreted this statement as saying that the government would be checking on him to determine whether he provided valid responses to survey questions.

Respondents were also probed on the specific terminology and phrases in this statement. Respondents often mentioned that there were too many legal terms in this sentence, and it needed to be rewritten using plain language. One respondent stated, "This makes no sense to an ordinary person. It is legal mumbo jumbo."

Sixteen of the 30 respondents indicated that they did not know what "sources" this statement was referring to when it said, "Information from these sources may be used to help identify and mitigate the incident." Some asked if this referred to their identifiable survey data or the individuals accessing the survey data.

> This is vague, what are 'these sources'? Is that good or bad? Is this the source of the leak or the incident or the identification of the source of the leak? I can't tell if the sources are related to me or to the leak.

Five respondents were also not familiar with the term "mitigate." One respondent asked,

> And what do you mitigate? How do you mitigate a hacking? The rest of these paragraphs made a lot of sense. This, like, is way out there.

This respondent indicated that in agriculture the term mitigate is often used when one resource lessens the loss of another. For example, farmers can mitigate carbon emissions from coal power plants by using no-till practices. He kept coming back to this example and had difficulty applying this use of the term to data security breaches.

Two respondents did not understand what "pursuant to any required legal process" meant.

Finally, some respondents felt this sentence was unnecessary. They assumed that NASS would take steps to prosecute those responsible for security breaches. They found this sentence to be alarming in that it is indicating that a security breach may happen. One respondent indicated that this sentence is presenting the worst case scenario and if this was the last thing she read before beginning a survey she may think twice about responding. Finally, this sentence made respondents feel less confident that the data would be kept secure and their personal information would be kept confidential.

3.5 Preferences

When asked which revision they preferred, half of the respondents preferred Revised Pledge B over Revised Pledge A. Respondents preferred Revised Pledge B over Revised Pledge A because (1) it did not mention DHS's or contractors' involvement, (2) it explained why the data are protected and (3) they felt their data were more secure because it was being protected versus monitored. This likely stems from the difference in language used in the two pledges ("protected" versus "monitoring"). Six out of 30 respondents preferred Revised Pledge A over Revised Pledge B because Revised Pledge A explained who would be conducting the cybersecurity monitoring and they felt it was easier to understand. Nine respondents had no preference.

Finally, some respondents assumed that if the data are hacked, they will be protected because NASS takes steps to make sure data are unidentifiable. Their understanding was that survey data are always unidentifiable but these pledges made them question when in the process their identities are removed from the data, and whether there is ever a point in the process when their data may be identifiable. In some cases, these revisions caused them to have more questions than answers. As one respondent stated, "I had concerns before. I have more concerns now."

3.6 Revision Goals

At the end of the interviews, respondents were told the following: *the Department of Homeland Security will be monitoring the electronic systems where survey data are transmitted and stored. They won't be looking at individual survey answers, instead monitoring the systems to look for viruses, malware and other threats.* Respondents were then asked if that was consistent or inconsistent with the revisions they were shown.

About half of the respondents thought the revised pledges were consistent with the above statement and about half thought they were inconsistent. A couple of respondents indicated that only Revised Pledge A was consistent with the above statement because it specifically identifies DHS as the organization conducting the cybersecurity monitoring. One respondent commented that both revisions were consistent with the above statement; however, the additional statement was not.

Respondents were also asked which of the revised pledges better conveyed the information provided in the statement above. About one-third of the respondents felt A did, one-third felt Revised Pledge B did and, one-third felt neither did.

Finally, respondents were asked to provide any additional suggestions on how NASS can improve the confidentiality pledge to convey the changes in data handling. Some respondents suggested combining Revised Pledges A and B. These respondents liked that Revised Pledge A told respondents who was conducting the cybersecurity screening and that Revised Pledge B explained why the cybersecurity screening was needed. A suggestion was: *Per the Cybersecurity Enhancement Act of 2015, DHS is responsible for monitoring the systems that transmit your data.* One respondent also stressed the importance of enumerators being able to explain these changes, as he only responds to in-person interviews.

Many respondents suggested that NASS use plain language in the pledges as opposed to legal terms. Several suggested that NASS use the language in the statement above (*The Department of Homeland Security will be monitoring the electronic systems where survey data are transmitted and stored. They won't be looking at individual survey answers, instead monitoring the systems to look for viruses, malware and other threats*). One respondent said, "I think what you just told me is 1,000 times easier to understand than what these statements say." Respondents also suggested that the pledges be kept as brief as possible if the desired outcome was for respondents to read them.

> Well, there's always the old debate – how much information? Too much information and if the paragraph becomes a whole page, I'm not going to read it. Try to give me as much information as briefly as possible.

Finally, a few respondents indicated that they just want to be assured that NASS will do everything in its power to secure the data. When asked what other suggestions he had for NASS, one respondent stated, "I want tight security and if information is taken, I will do this for you. But why say cybersecurity? Why use big words?"

4. CONCLUSION AND RECOMMENDATIONS

In conclusion, both of the revised pledges were difficult for respondents to comprehend. The revised pledges also solicited mixed reaction from respondents. However, more respondents had a negative reaction to Revised Pledge A, which explicitly mentioned DHS. These revisions and the additional sentence, which described actions NASS would take should a cybersecurity breach occurred, caused some respondents to have less confidence in NASS's ability to secure their information.

Respondents desired a pledge that used plain language and assured them that their data would be used for statistical purposes only and would be kept confidential. NASS must find a balance between meeting respondents' expectations and conveying the changes in how data are secured. The following recommendations are based on these findings:

1. Use plain language to convey that the information respondents provide on NASS surveys will be kept confidential and used for statistical purposes only. Direct respondents to a website that provides the full information on how NASS protects its survey data.

Example:

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: [insert web address].

2. Add a fifth statement to the NASS Confidentiality Pledge Page (https://www.nass.usda.gov/About_NASS/Confidentiality_Pledge/index.php) that conveys DHS's involvement.

Example:

> **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.

5. REFERENCES

Scope Confidentiality Pledge Revision Subcommittee Final Report. Submitted to Paul Bugg, Office of Management and Budget, August 12, 2016.

Strauss, Anselm C., and Juliet Corbin. 1990. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Newbury Park: Sage Publications.

USDA, NASS. 2014. 2012 Census of Agriculture United States Summary and State Data. Vol. 1, Geographic Area Series, Part 51. Report AC-12-A-51. Washington, DC.
Report to OMB

APPENDIX A: INTERVIEW PROTOCOL

NASS Confidentiality Pledge Cognitive Testing
Cognitive Interview Protocol
July 2016 (Due July 29, 2016)

I. Background

The purpose of this project is to assess respondent reactions to the NASS confidentiality pledge. The Cybersecurity Enhancement Act of 2015 requires the installation of the Department of Homeland Security's Einstein cybersecurity protection system on all Federal civilian information technology systems by mid-December 2016. As a result, NASS can no longer state that respondents' data will be seen only by a statistical agency's employees or its sworn agents in our confidentiality pledges. Consequently, we need to develop and test a revised confidentiality pledge that informs respondents of this change in circumstances. The primacy task is to determine respondents' reactions to changes to our confidentiality pledge.

Population and Sampling

Potential respondents to NASS surveys should be recruited for this study. Because this study will be evaluating the NASS confidentiality pledge, it is important that respondents have no affiliation with NASS/NASDA.

In total, 30 cognitive interviews will be completed per OMB approval. The majority of the interviews will be conducted by HQ staff with assistance from the RFOs.

RFO	States	Trained Cognitive Interviewers	Number of interviews requested
Eastern Mountain	KY	Mallory Dolan	2
Northeast	NH	Gary Keough	2
Mountain	CO	Kerry McBride	2
Northern Plains	NE	Ben Blomendahl	2
Great Lakes	OH	Cheryl Turner	2
Northwest	WA	Wendy Vance	2
	HQ	Heather Ridolfo	7
	HQ	Kathy Ott	3
	HQ	Jaki McCarthy	2
	HQ	Ken Pick	2
	HQ	Rachel Sloan	2

	HQ	Tyler Wilson	2

II. Cognitive Interview Procedures

Recruitment Plan

HQ and States and Regional Field Office staff should recruit any potential respondent to NASS surveys. Cognitive interview respondents should be informed that the intent of the cognitive interviews is to evaluate NASS's confidentiality statement and that their participation is voluntary. Recruiting, setting up interviews, and writing notes is expected to take 3-4 hours per interview.

What to Bring

Interviewers should bring the following items to the cognitive interviews:

- A copy of the interview guide (1 or 2 – see instructions below)
- The Current NASS Confidentiality Pledge Showcard
- The Revised Statement A Showcard
- The Revised Statement B Showcard
- The Additional Text Showcard

Interviews

We will be testing three versions of the NASS confidentiality statement: the current NASS confidentiality statement and two revised versions (Statement A and Statement B). We would like to alternate the order in which respondents read and react to the revised confidentiality statements. Therefore, you have been provided two interview guides. **Please use Interview Guide 1 for your first interview and Interview Guide 2 for your second interview.** In addition to the interview guides, interviewers have been provided copies of the confidentiality statements.

During the interviews, hand the respondent the current NASS confidentiality pledge and ask the respondent to review it. When finished, administer the probes for the current pledge. Repeat these steps for the remaining two pledges. After respondents have been probed on all three pledges, administer the Additional Text showcard and ask related probe questions. Finally, administer the revision goal probes. Detailed instructions are provided in the interview guide.

III. Deliverables expected back from cognitive interviewers

Detailed notes for each interview should be typed into the interview guide and saved as a Word document. Notes should be labeled using the PID and/or POID. **All PII must be removed from the notes before emailing.** PII includes things like operator name, operation name, and address. All time should be recorded under Project Code 531.

IV. Contact Information

Any questions or concerns about the overall task should be directed to Heather Ridolfo (HQ/RDD) at (202)-690-3228 or heather.ridolfo@nass.usda.gov

APPENDIX B: INTERVIEW GUIDE 1

Interview Guide 1

(Revised Statement A Presented First)

State:	
POID:	
PID:	
Type of Operation (commodities, size, partnership, etc.)	
Date:	
Starting Time:	
Ending Time:	
Interviewer Name:	

Introduction

Thank you for taking the time to meet with me today. My name is ( ). I work for the National Agricultural Statistics Service. Let me explain a bit about what we'll be doing today. NASS conducts hundreds of surveys every year and prepares reports on virtually every aspect of U.S. agriculture. In order to earn, and keep, the trust of our respondents we work hard to keep all the information they give us safe and protected. We are actually required by law to protect the data.

Recent changes to the laws require us to make some changes in the way we explain how we keep data protected to our respondents. To ensure that the changes we make are clear and easy to understand to respondents, we are talking to you and many others to get your feedback to the wording.

We are looking for your honest feedback and reactions. There aren't any right or wrong answers here, your opinions and thoughts are what matters today. We want to know what you would think if you heard the language before responding to NASS surveys. With your 'respondent hat' on, I'll be giving you the new language and then asking you a series of questions to get your feedback on it. Do you have any questions before we begin?

Current NASS Confidentiality Statement

(Hand respondent a copy of the Current NASS Confidentiality Statement) *Here is the way we currently explain how we protect data. Take a moment to read this over and let me know when you are done.*

Current Confidentiality Statement for interviewer reference:
The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, every employee and agent has taken an oath and is subject to a jail term, a fine, or both if he or she willfully discloses ANY identifiable information about you or your operation.

1. *Can you tell me what this means in your own words?*

2. *What is your general reaction to this statement?*

3. *If you heard or read this statement before a survey, would it influence your decision to participate or not? Please explain.*

4. *Do you have any concerns with how your (operation's / personal) information would be treated after hearing/reading this? If so, what are they?*

5. *I want to ask you some questions about what the language covers and doesn't cover. Please make your best guess, even if you're not sure of the answer. If you gave NASS data and were assured confidentiality using this language, who would be able to see your information?*

    a. *What would they be able to do with your information?*

    b. *I'm going to read a list of groups, tell me if they'd be able to see the information you provided*
        1. *National Agricultural Statistics Service (NASS)*
        2. *United States Department of Agriculture (USDA)*
        3. *Internal Review Service (IRS)*
        4. *Department of Homeland Security (DHS)*
        5. *All federal government agencies*
        6. *Congress*

6. *Besides who can access your information, the language also talks about what can be done with it. Specifically it says it can only be used for "Statistical purposes." What do you think that means?*

7. *I'm going to read a list of activities, tell me if you think they'd be allowed under this language?*
    1. *It could be combined with other survey answers to create summary statistics*
    2. *It could be published exactly as you provided it*
    3. *It could be given to other statistical agencies*
    4. *It could be given to the IRS*
    5. *It could be given to other federal government agencies*
    6. *It could be given to private companies*

8. *What else could be done under this language?*

Revised Statement A

As I mentioned, there have been changes to the laws related to the protection of NASS survey data. This next statement reflects those changes. I would you like you review this statement and let me know when you are finished. (Take back current statement and hand respondent a copy of Statement A)

Revised Statement A for interviewer reference:
The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, any person is subject to a jail term, a fine, or both if he or she willfully discloses ANY identifiable information about you or your operation. **Your data are further protected by Department of Homeland Security employees and contractors through cybersecurity monitoring of the systems that transmit your data.**

1. *The main difference between this and the previous statement is the addition of the last sentence - Your data are further protected by Department of Homeland Security employees and contractors through cybersecurity monitoring of the systems that transmit your data. – What does that statement mean to you?*

2. *What is your general reaction to it?*

3. *If you read this language before a survey, would it influence your decision to participate or not?*

4. *NASS collects a variety of information from its farmers and ranchers including things like agricultural inputs and yield, chemical use, farm labor and wages, income and expenditures, etc. Would receiving this statement before a survey, impact your willingness to disclose any types of information? If so, what types?*

5. *Do you have any concerns with how your personal information would be treated after reading this? If so, what are your concerns?*

6. *The new addition mentions the Department of Homeland Security. Are you familiar with that agency?* If yes: *what do you know about them?*

7. *With this new language, what will the Department of Homeland Security be doing?*

a. *What will they have access to?*

b. *Will they be able to see your individual answers to NASS survey questions?*

8. *What does "cybersecurity monitoring" mean to you?*

9. *What do you think "the systems that transmit your data" are?*

Proposed Statement B

(Take back Statement A and hand respondent a copy of Statement B) *We are also considering this revision of our confidentiality statement. You will notice that the only difference in wordings between this statement and the previous statement is the last sentence. Take a minute to review this statement and let me know when you are done.*

Revised Statement B for interviewer reference:
The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, any person is subject to a jail term, a fine, or both if he or she willfully discloses ANY identifiable information about you or your operation. **Per the Cybersecurity Enhancement Act of 2015, Federal information systems are protected from malicious activities through cybersecurity screening of transmitted data.**

1. *Let's look at that last sentence - Per the Cybersecurity Enhancement Act of 2015, Federal information systems are protected from malicious activities through cybersecurity screening of transmitted data. - What does that statement mean to you?*

2. *Do you think it means the same thing as the first revised version I showed you, or is it different?*

    a. *How is it the same/different?*

3. *What is your general reaction to this new language?*

4. *If you read this new language on a survey asking for information about your operation would it impact your decision to respond?*

5. *NASS collects a variety of information from its farmers and ranchers including things like agricultural inputs and yield, chemical use, farm labor and wages, income and expenditures, etc. Would receiving this statement before a survey, impact your willingness to disclose any types of information? If so, what types?*

6. *When this statement says "Federal information systems" what does this mean to you?*

7. *When this statement says "protected from malicious activities" what does "malicious activities" mean to you?*

8. *What does "cybersecurity screening of transmitted data" mean to you?*

9. *When this says "transmitted data," what kinds of information do you think is included as "data"?*

10. *With this language, who do you think could see your information?*

11. *Based on this language, who could conduct the cybersecurity screening of transmitted data?*

    a. *NASS*

    b. *USDA*

    c. *The Department of Homeland Security*

    d. *The IRS*

    e. *Anyone else?*

12. *Will those who conduct the cybersecurity screening be able to see your individual answers to NASS survey questions?*

13. *Do you have any concerns with how your personal/operation's information would be treated after reading this statement? If so, What are you concerns?*

14. *Would you be more or less likely to respond if you received one version or the other?* (show both)

15. *Which version do you think best conveys that your information would be kept confidential?*

Additional Change

In addition to the revisions we have discussed, NASS is also considering adding an additional sentence to the end of either revised statements. (Hand the respondent Additional Change showcard). *Take a minute to read this over and let me know when you are done.*

Additional change for interviewer reference:
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.

1. *What do you think this statement means?* If respondent has difficulty comprehending this statement, probe to see which parts of the statement are confusing.

2. *What is your general reaction to it?*

3. *When this statement says "a cybersecurity incident" what do you think this means?*

4. *When this says "information from these sources may be used to help identify and mitigate the incident" what type of information do you think will be used?*

5. *When this says "mitigate the incident" what do you think this means?*

6. *Do you have any concerns after reading this additional statement? If so, what are they?*

Revision Goals

1. *What we're trying to communicate is that the Department of Homeland Security will be monitoring the electronic systems where survey data is transmitted and stored. They won't be looking at individual survey answers, instead monitoring the systems to look for viruses, mal-wear and other threats. Is that consistent or inconsistent with the revisions I showed you? (show all versions)*

2. *Do you think that one version does a better job at communicating that than the other?*

3. *Do you have any suggestions on how we might better communicate that?*

4. *We're almost done, thanks for your feedback so far. In general, do you have any concerns about how the government treats the data you provide for surveys?*

5. *Do you have any suggestions or other feedback?*

APPENDIX C: INTERVIEW GUIDE 2

Interview Guide 2

(Revised Statement B Presented First)

State:	
POID:	
PID:	
Type of Operation (commodities, size, partnership, etc.)	
Date:	
Starting Time:	
Ending Time:	
Interviewer Name:	

Introduction

Thank you for taking the time to meet with me today. My name is ( ). I work for the National Agricultural Statistics Service. Let me explain a bit about what we'll be doing today. NASS conducts hundreds of surveys every year and prepares reports on virtually every aspect of U.S. agriculture. In order to earn, and keep, the trust of our respondents we work hard to keep all the information they give us safe and protected. We are actually required by law to protect the data.

Recent changes to the laws require us to make some changes in the way we explain how we keep data protected to our respondents. To ensure that the changes we make are clear and easy to understand to respondents, we are talking to you and many others to get your feedback to the wording.

We are looking for your honest feedback and reactions. There aren't any right or wrong answers here, your opinions and thoughts are what matters today. We want to know what you would think if you heard the language before responding to NASS surveys. With your 'respondent hat' on, I'll be giving you the new language and then asking you a series of questions to get your feedback on it. Do you have any questions before we begin?

Current NASS Confidentiality Statement

(Hand respondent a copy of the Current NASS Confidentiality Statement) *Here is the way we currently explain how we protect data. Take a moment to read this over and let me know when you are done.*

Current Confidentiality Statement, for your own reference:
The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, every employee and agent has taken an oath and is subject to a jail term, a fine, or both if he or she willfully discloses ANY identifiable information about you or your operation.

1. *Can you tell me what this means in your own words?*

2. *What is your general reaction to this statement?*

3. *If you heard or read this statement before a survey, would it influence your decision to participate or not? Please explain.*

4. *Do you have any concerns with how your (operation's / personal) information would be treated after hearing/reading this? If so, what are they?*

5. *I want to ask you some questions about what the language covers and doesn't cover. Please make your best guess, even if you're not sure of the answer. If you gave NASS data and were assured confidentiality using this language, who would be able to see your information?*

    a. *What would they be able to do with your information?*

    b. *I'm going to read a list of groups, tell me if they'd be able to see the information you provided*
        i. *National Agricultural Statistics Service (NASS)*
        ii. *United States Department of Agriculture (USDA)*
        iii. *Internal Review Service (IRS)*
        iv. *Department of Homeland Security (DHS)*
        v. *All federal government agencies*
        vi. *Congress*

6. *Besides who can access your information, the language also talks about what can be done with it. Specifically it says it can only be used for "Statistical purposes." What do you think that means?*

7. *I'm going to read a list of activities, tell me if you think they'd be allowed under this language?*
    i. *It could be combined with other survey answers to create summary statistics*
    ii. *It could be published exactly as you provided it*
    iii. *It could be given to other statistical agencies*
    iv. *It could be given to the IRS*
    v. *It could be given to other federal government agencies*
    vi. *It could be given to private companies*

8. *What else could be done under this language?*

Revised Statement B

As I mentioned, there have been changes to the laws related to the protection of NASS survey data. This next statement reflects those changes. I would you like you review this statement and let me know when you are finished. (Take back the current statement and hand respondent a copy of Statement B)

Revised Statement B for Interviewer reference:
The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, any person is subject to a jail term, a fine, or both if he or she willfully discloses ANY identifiable information about you or your operation. **Per the Cybersecurity Enhancement Act of 2015, Federal information systems are protected from malicious activities through cybersecurity screening of transmitted data.**

1. *The main difference between this and the previous statement is the addition of the last sentence - Per the Cybersecurity Enhancement Act of 2015, Federal information systems are protected from malicious activities through cybersecurity screening of transmitted data – What does that statement mean to you?*

2. *What is your general reaction to it?*

3. *If you read this new language on a survey asking for information about your operation would it impact your decision to respond?*

4. *NASS collects a variety of information from its farmers and ranchers including things like agricultural inputs and yield, chemical use, farm labor and wages, income and expenditures, etc. Would receiving this statement before a survey, impact your willingness to disclose any types of information? If so, what types?*

5. *When this statements says "Federal information systems" what does this mean to you?*

6. *When this statement says "protected from malicious activities" what does "malicious activities" mean to you?*

7. *What does "cybersecurity screening of transmitted data" mean to you?*

8. *When this says "transmitted data," what kinds of information do you think is included as "data"?*

9. *With this language, who do you think could see your information?*

10. *Based on this language, who could conduct the cybersecurity screening of transmitted data?*

    a. *NASS*

    b. *USDA*

    c. *The Department of Homeland Security*

    d. *The IRS*

    e. *Anyone else?*

11. *Will those who conduct the cybersecurity screening be able to see your individual answers to NASS survey questions?*

12. *Do you have any concerns with how your personal/operation's information would be treated after reading this?*

Proposed Statement A

As I mentioned, there have been changes to the laws related to the protection of NASS survey data. This next statement reflects those changes. I would you like you review this statement and let me know when you are finished. (Take back Statement B and hand respondent a copy of Statement A)

Revised Statement A for interviewer reference:
The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, any person is subject to a jail term, a fine, or both if he or she willfully discloses ANY identifiable information about you or your operation. **Your data are further protected by Department of Homeland Security employees and contractors through cybersecurity monitoring of the systems that transmit your data.**

1. *What does that statement mean to you?*

2. *Do you think it means the same thing as the first revised version I showed you, or is it different?*

    a. *How is it the same/different?*

3. *What is your general reaction?*

4. *If you read this new language before a survey, would it influence your decision to participate or not?*

5. *NASS collects a variety of information from its farmers and ranchers including things like agricultural inputs and yield, chemical use, farm labor and wages, income and expenditures, etc. Would receiving this statement before a survey, impact your willingness to disclose any types of information? If so, what types?*

6. *Do you have any concerns with ow your personal information would be treated after receiving this information?*

7. *The new addition mentions the Department of Homeland Security. Are you familiar with that agency? If yes: what do you know about them?*

8. *With this new language, what will the Department of Homeland Security be doing?*

   a. *What will they have access to?*

   b. *Will they be able to see your individual answers to NASS survey questions?*

9. *What does "cybersecurity monitoring" mean to you?*

10. *What do you think "the systems that transmit your data" are?*

11. *Would you be more or less likely to respond if you received one version or the other? (show both)*

12. *Which version do you think best conveys that your information would be kept confidential?*

Additional Change

In addition to the revisions we have discussed, NASS is also considering adding an additional sentence to the end of either revised statements. (Hand the respondent Additional Change showcard). *Take a minute to read this over and let me know when you are done.*

Additional change for interviewer reference:

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.

1. *What do you think this statement means? If respondent has difficulty comprehending this statement, probe to see which parts of the statement are confusing.*

2. *What is your general reaction to it?*

3. *When this statement says "a cybersecurity incident" what do you think this means?*

4. *When this says "information from these sources may be used to help identify and mitigate the incident" what type of information do you think will be used?*

5. *When this says "mitigate the incident" what do you think this means?*

6. *Do you have any concerns after reading this additional statement? If so, what are they?*

Revision Goals

1. *What we're trying to communicate is that the Department of Homeland Security will be monitoring the electronic systems where survey data is transmitted and stored. They won't be looking at individual survey answers, instead monitoring the systems to look for viruses, mal-wear and other threats. Is that consistent or inconsistent with the revisions I showed you? (show all versions)*

2. *Do you think that one version does a better job at communicating that than the other?*

3. *Do you have any suggestions on how we might better communicate that?*

4. *We're almost done, thanks for your feedback so far. In general, do you have any concerns about how the government treats the data you provide for surveys?*

5. *Do you have any suggestions or other feedback?*

APPENDIX D: SHOWCARD 1 (CURRENT NASS CONFIDENTIALITY PLEDGE)

Current NASS Confidentiality Pledge

The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, every employee and agent has taken an oath and is subject to a jail term, a fine, or both if he or she willfully discloses ANY identifiable information about you or your operation.

APPENDIX E: SHOWCARD 2 (REVISED PLEDGE A)

The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, any person is subject to a jail term, a fine, or both if he or she willfully discloses ANY identifiable information about you or your operation. Your data are further protected by Department of Homeland Security employees and contractors through cybersecurity monitoring of the systems that transmit your data.

APPENDIX F: SHOWCARD 3 (REVISED PLEDGE B)

The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, any person is subject to a jail term, a fine, or both if he or she willfully discloses ANY identifiable information about you or your operation. Per the Cybersecurity Enhancement Act of 2015, Federal information systems are protected from malicious activities through cybersecurity screening of transmitted data.

APPENDIX G: SHOWCARD 4 (ADDITIONAL STATEMENT)

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.

Example of addition in Statement A:

The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, any person is subject to a jail term, a fine, or both if he or she willfully discloses ANY identifiable information about you or your operation. Your data are further protected by Department of Homeland Security employees and contractors through cybersecurity monitoring of the systems that transmit your data. 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.

Example of addition in Statement B:

The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, any person is subject to a jail term, a fine, or both if he or she willfully discloses ANY identifiable information about you or your operation. Per the Cybersecurity Enhancement Act of 2015, Federal information systems are protected from malicious activities through cybersecurity screening of transmitted data. 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.