



United States Department of Agriculture

Office of Inspector General





Security Review of National Agricultural Statistics Service's Lockup Procedures

Audit Report 26501-0001-12

What Were OIG's Objectives

We conducted an audit to perform a security assessment of the NASS lockup process and procedures to determine if physical, electronic, and other protection measures were properly implemented to assure sensitive market data were secured and released, according to established criteria.

What OIG Reviewed

NASS maintains specific procedures for gathering and securing commodity data, compiling them into agricultural reports, and preparing and releasing the reports in a secured area—known as lockup.

What OIG Recommends

OIG recommended that NASS develop, implement, and document periodic internal reviews for the entire lockup process, and submit the results to an independent evaluator for follow-up. NASS should also take action to mitigate IT vulnerabilities; implement controls to prevent data release delays; improve the physical security of lockup, IT equipment, and server rooms; and take steps to further secure sensitive data.

OIG audited the effectiveness of NASS' lockup procedures for securing market sensitive commodity data before their official release.

What OIG Found

The Office of Inspector General (OIG) found that the National Agricultural Statistics Service's (NASS) management needs to improve the security of its sensitive commodity market data and other information technology (IT) resources. We found that NASS did not adequately enforce critical procedures and physical security measures meant to protect the security of NASS information. Notably, although banned from lockup, OIG was able to bring a cell phone into lockup and witnessed a reporter using an iPad during lockup. NASS had also not taken mitigating actions to address outstanding IT vulnerabilities, thereby putting NASS' systems at risk. As a result, sensitive information could be compromised or leaked before its official release, which could adversely affect equitable trading in commodity markets. OIG notes that NASS experienced data release issues and has not yet remedied the underlying causes.

These issues occurred because NASS has not established a formal process for effectively monitoring lockup, nor a systematic process for documenting and following up on recommendations. Managers also did not review lockup procedures for gaps, adequately oversee contracted guards and equipment inventories, and were unaware of or did not have resources to meet Federal security requirements. NASS stated that it has taken action to address the majority of the issues found, and management decision has been reached for 14 of the 17 recommendations.



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



DATE: February 21, 2014

AUDIT
NUMBER: 26501-0001-12

TO: Cynthia Clark
Administrator
National Agricultural Statistics Service

ATTN: Lisa A. Baldus
Director, Financial Management Division
Agricultural Research Service

FROM: Gil H. Harden
Assistant Inspector General for Audit

SUBJECT: Security Review of National Agricultural Statistics Service's Lockup Procedures

This report presents the results of the subject audit. Your written response, dated January 16, 2014, is included in its entirety at the end of the report. Excerpts from your response and the Office of Inspector General's (OIG) position are incorporated in the relevant sections of the report. Based on your January 16, 2014, response and additional information received on January 22, 2014, we were able to accept management decision on Recommendations 3-8 and 10-17 in the report. To reach management decision on the remaining recommendations, please see the relevant OIG Position sections in the audit report.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days, describing the corrective actions taken or planned, and timeframes for implementing the recommendations for which management decisions have not been reached. Please note that the regulation requires management decision to be reached on all recommendations within 6 months from report issuance, and final action to be taken within 1 year of each management decision to prevent being listed in the Department's annual Agency Financial Report. For agencies other than the Office of the Chief Financial Officer (OCFO), please follow your internal agency procedures in forwarding final action correspondence to OCFO.

We appreciate the courtesies and cooperation extended to us by members of your staff during our audit fieldwork and subsequent discussions. This report contains publically available information and will be posted in its entirety to our website (<http://www.usda.gov/oig>) in the near future.

Table of Contents

Background and Objectives	1
Section 1: NASS Lockup Management.....	3
Finding 1: NASS Needs to Establish a Formal Review Process to Oversee Sensitive Data and IT Operations	3
Recommendation 1	7
Recommendation 2	7
Recommendation 3	8
Recommendation 4	8
Recommendation 5	8
Section 2: Lockup Security.....	9
Finding 2: NASS Needs to Improve Lockup Security.....	9
Recommendation 6	12
Recommendation 7	12
Recommendation 8	13
Recommendation 9	13
Recommendation 10.....	13
Recommendation 11.....	14
Recommendation 12.....	14
Finding 3: NASS Needs to Mitigate IT Security Weaknesses to Prevent Data Compromise and Work Disruption	15
Recommendation 13.....	17
Recommendation 14.....	17
Recommendation 15.....	18
Recommendation 16.....	18
Recommendation 17.....	19
Scope and Methodology.....	20
Abbreviations	21
Agency's Response	23

Background and Objectives

Background

The National Agricultural Statistics Service (NASS) is responsible for providing timely, accurate, and useful statistics regarding U.S. agriculture. The Agricultural Statistics Board (ASB)¹ is the subcomponent of NASS tasked with ensuring that the reports containing agricultural statistics are accurate, timely, and secure. NASS conducts hundreds of surveys each year and prepares production forecasts and final estimates for numerous commodities, including corn, wheat, cotton, soybeans, and oranges, as well as cattle and hog inventory estimates. Some of these are defined by Department Regulation as "speculative" because the estimates pertain to products traded on commodity markets.² ASB uses a special process and secure facility called "lockup" to prevent the early release of this information. The lockup facility is located inside the Department of Agriculture's (USDA) South Building in Washington, D.C.

Prior to lockup, NASS State statistical offices contact farmers and ranchers, using mail and phone calls, and record their information. NASS representatives are also dispatched to collect field data in-person from random locations. Once State officials aggregate their estimates, the data and comments for the speculative commodities are encrypted and transmitted to NASS headquarters. The encrypted data are saved onto removable media, only to be decrypted in lockup, where NASS prepares its estimates.

For non-national security programs and information systems, agencies must follow National Institute of Standards and Technology (NIST) standards and guidelines. NIST creates standards for information technology (IT) that ensure Federal systems meet the best practices of IT industry security, and produce a unified security framework. NIST standards state, for example, that facilities housing Federal IT systems' hardware must be protected from unauthorized entrants.

Lockup consists of a locked room guarded by an officer stationed outside the restricted area; attendees are not allowed to bring cellular devices inside. Opaque vinyl shades with steel reinforcement are drawn over windows and sealed to prevent unauthorized observation. All office telephones are disconnected, and computer systems are isolated from the "outside world" and secured. Lockup is also monitored to detect the presence of electronic transmissions. Journalists are allowed into lockup prior to the report release in order to develop articles about the report, which are released simultaneously with the report itself. Once permitted staff and the media have entered lockup, they are prohibited from leaving the area or contacting anyone outside until the report has been officially released.

The reports that NASS produces are extremely market sensitive and contain major principal economic indicators of the United States economy. For instance, NASS provides statistical data that are included in the World Agricultural Supply and Demand Estimates (WASDE) report. An

¹ ASB prepares and issues the official national and State forecasts and estimates relating to crop production, stocks of agricultural commodities, animals and animal products, agricultural wage rates, and other subjects.

² Department Regulation 1042-042, *Agricultural Statistics Board* (May 29, 2009).

Economic Research Service economist found when the WASDE report is released, it is “followed by an immediate reaction reflected in the opening future prices for each commodity.”³

NASS has experienced incidents where its reports are not released in a synchronous manner with press articles.⁴ In 2011, three incidents involved the early release of press articles. Other times, NASS reports appeared on its official site later than the official release time, due to connectivity issues. NASS contracts with the National Information Technology Center (NITC) for servers that disseminate reports to the public. According to NASS, NITC re-configured the servers in 2012. NASS has since continued to experience connectivity issues.

When press articles were released earlier than the official release time in June 2011, NASS executive management staff requested the Office of the Chief Information Officer (OCIO)/Agriculture Security Operations Center (ASOC) to perform an in-depth, security-focused analysis and investigation of the occurrences.⁵ This audit provides additional support to the OCIO/ASOC review by examining how effective NASS’ lockup policies and procedures are at protecting the information from the time the estimates are received at NASS headquarters to the time the report is authorized to be released.

Objectives

We conducted an audit to perform a security assessment of the NASS lockup process and procedures to determine if physical, electronic, and other protection measures were properly implemented to assure sensitive market data were secured and released, according to established criteria.

³ *Quantifying the WASDE Announcement Effect*, Michael K. Adjemian, Oxford University Press, 2012.

⁴ The reports that experienced release issues were: *Quarterly Hogs and Pigs and Peanut Prices* – June 24, 2011; *Acreage, Grain Stocks and Rice Stocks* – June 30, 2011; *Dairy Product Prices, Grain Stocks, Rice Stocks and Small Grains Summary* – September 30, 2011.

⁵ Agriculture Security Operations Center- *Assessment and Findings of NASS Press Room Infrastructure* (August 11, 2011).

Section 1: NASS Lockup Management

Finding 1: NASS Needs to Establish a Formal Review Process to Oversee Sensitive Data and IT Operations

We found that NASS management is not taking adequate preventive measures to secure its sensitive commodity market data and other IT resources. Although Federal agencies are required to continually monitor the effectiveness of internal controls, NASS has records of only one documented review of lockup in 2011—which examined a limited portion of the data release process—and has not yet implemented all of the review’s recommendations. During our audit, we also found over 4,800 vulnerabilities on 899 devices across NASS’ network, including systems in lockup, which NASS was not taking action on.^{6,7} These issues occurred because NASS has not established a formal internal review process for lockup procedures, nor a systematic process for documenting and following up on review results. Also, no one person or group within the ASB is tasked with consistently following up on and addressing identified problems. Because they had performed no such reviews, NASS management incorrectly believed that the data in lockup were adequately secured. We found that existing lockup security procedures were not being followed—for instance, lockup entrants were able to easily carry cell phones inside (see Finding 2)—as well as gaps in procedures for critical areas, such as guard monitoring duties (see Finding 2) and security of IT equipment (see Finding 3). Data release delays have also taken place, which could adversely affect equitable trading in the commodity markets; the cause of the delays remains unresolved. The high number of vulnerabilities on NASS’ network devices puts all NASS systems at risk.

The Office of Management and Budget (OMB) requires agencies to continuously monitor the effectiveness of internal controls and conduct periodic reviews.⁸ Agencies should have a systematic process to address deficiencies in internal controls. OMB also requires agencies to prepare plans of action and milestones (POA&M) for identified IT security weaknesses,⁹ and NASS procedures¹⁰ require that high and medium vulnerabilities be mitigated within 2 weeks and low vulnerabilities within 30 days.¹¹ Further, OMB requires that statistical agencies ensure

⁶ Vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy. We scanned NASS’ system using a commercially available scanning tool.

⁷ The 4,858 vulnerabilities were made up of 35 critical, 1,805 high, and 3,018 medium vulnerabilities. A critical vulnerability is malicious in nature and will result in the compromise of the system if not acted upon immediately. A high vulnerability, if exploited, will result in the compromise of the entire system. A medium vulnerability, if exploited, will result in the partial compromise of a system; the attacker will gain access, but it will be limited.

⁸ OMB Circular No. A-123, *Management’s Responsibility for Internal Control* (December 21, 2004).

⁹ OMB Memorandum 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act* (August 23, 2004).

¹⁰ Security Policy Directive-01, *Vulnerability Assessment Scans* (May 5, 2011).

¹¹ A POA&M is a tool that identifies tasks needing to be accomplished to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. It details resources required to accomplish the elements of the plan, milestones in meeting the task, and scheduled completion dates for the milestones. The goal of a POA&M should be to reduce the risk of the weakness identified.

all users have equitable and timely access to data disseminated to the public.¹² A NASS document explaining statistical procedures states that anyone having early access to sensitive information would have an obvious advantage in trading on the commodities market, and equal, simultaneous public access to data for all is a hallmark of NASS reports.¹³

A Federal Reserve Bank of Kansas City study on agricultural commodity market volatility mentioned the delays as well, stating that anecdotal evidence suggests that individuals attempting to download reports precisely when they are released have faced significant delays.¹⁴ It suggests the effect this may have had on the markets, stating that, “Thus, higher volatility may have persisted... if some groups of traders, wishing to place a trade only after accessing WASDE, are unable to access the information at the same time as others with faster access.” This study also found a spike in price volatility “the instant the reports are released,” with the highest amounts of volatility occurring in the first 5 minutes. This brief period of high volatility can affect risk management strategies, creating an environment where a very short delay in accessing information has a large impact on traders.

In 2011, NASS experienced three incidents during which press articles were released before the authorized time. The NASS reports are supposed to be released simultaneously by media sources and on NASS’ official website. In each case, press articles written inside of lockup were released early. Normally, journalists write articles while in lockup and upload them into a queue, and NASS controls a switch that allows all articles to be released simultaneously at the official time. In the first instance, the press articles were not held back in a queue, but published as soon as they were uploaded. One article was sent as early as 14 minutes before the official data release time. The second time, anticipating that a similar problem could occur, NASS told reporters not to queue their articles until 2 minutes before release time. When the reporters uploaded articles into the queue, the switch again allowed the reports to be published early. A third early release, of 25 seconds, occurred in September because of human error when someone accidentally manually released the data. In each circumstance, a trader watching the NASS website—and not the media sources that prematurely released the articles—would not have had access to the commodity statistics as early as others.

To help remedy this issue, NASS requested that OCIO/ASOC review its data release process. This was a technology-related review of potential issues in the press room area in lockup. The August 2011 external review determined that an equipment malfunction was the cause of the incidents, specifically the switch that isolates NASS’ network during lockup. Since the switch was replaced after the OCIO/ASOC report, no other switch-related issues have been detected. Besides recommending replacement of the malfunctioning equipment, the report also called for other security enhancements to NASS’ system. The report contained six recommendations.

¹² OMB Federal Register, Part V, Statistical Policy Directive No. 4: *Release and Dissemination of Statistical Products Produced by Federal Statistical Agencies* (March 7, 2008).

¹³ National Agricultural Statistics Service. *About NASS*. ONLINE (December 2012).

http://www.nass.usda.gov/About_NASS/ASB_and_Lockup/Lockup_QA.pdf [July 2013].

¹⁴ *Quantifying the WASDE Announcement Effect*, Michael K. Adjemian, Oxford University Press, 2012.

NASS has taken action to address four of the recommendations, and two remain outstanding.¹⁵ While agencies have the flexibility to decide the best and most practical actions to address vulnerabilities, at a minimum, NASS should have developed OMB-required POA&Ms for all of the recommendations, as they dealt with IT security weaknesses. NASS did not create POA&Ms for any of the six recommendations. The POA&Ms would have detailed whether NASS accepted the recommendations, the reasoning behind its actions, and the eventual result—which is especially important for recommendations that an agency does not implement. NASS officials incorrectly believed that ASOC’s review did not require recommendations to be tracked by POA&Ms.

During our audit fieldwork, we found that data dissemination problems continued to occur in lockup, albeit under different circumstances. During the March 2013 lockup session, we observed a delay of 4 minutes in the release of a report to the public, due to connectivity issues. After additional discussions with NASS, we discovered that this has been and remains an ongoing issue; and some reports have not been uploaded timely to NASS’ website. We observed that data from news organizations were not delayed, allowing anyone who subscribes to their services to have access to the report information before others checking NASS’ website, resulting in inequality among users of NASS estimates. Since markets can have an immediate reaction to the reports, this reinforces the need for timely dissemination to all members of the public—not just those with news organization subscriptions.¹⁶

NASS contracts with the NITC for servers that disseminate reports to the public. According to NASS, NITC re-configured the servers in 2012, and NASS continues to experience connectivity issues. NASS stated that the delay occurred because NITC had changed the authentication requirements for NASS servers, which interrupted the connection and did not allow the report to be uploaded timely, thus, the report was unavailable to the public timely.

We found the agreement between NITC and NASS for server management was generic and lacked sufficient roles and responsibilities, as well as any formal recourse for addressing performance issues, such as penalties or other methods of enforcement. NASS is taking action by reviewing the agreement with NITC in order to determine how and what can be strengthened. However, given the length of time this issue has been occurring—almost a year—we believe that NASS should intensify its efforts to permanently solve the problem.

NASS did try to respond to the issue by creating a manual process for releasing the report that bypasses NITC servers, but the process involves opening an internet connection for one computer in lockup 5 minutes before the official release time. With an open internet connection prior to the official release, there is a risk that the report may be released early, or people inside the lockup may misuse the early internet connection. In the first live use of the manual process,

¹⁵ The two recommendations involved (1) installing a programmable switch that can facilitate data gathering, and (2) implementing best practices on the news agencies’ workstations and infrastructure. When we asked them why they had not acted on these issues, NASS officials stated they had not found a feasible way to maintain news agencies’ proprietary network independence while implementing the second recommendation. NASS officials also stated that they had installed two-layer manual switches to enhance security, but had not installed the programmable switch type that the recommendation asked for.

¹⁶ *Quantifying the WASDE Announcement Effect*, Michael K. Adjemian, Oxford University Press, 2012.

the report was available to the public on NASS' site 7 seconds after the official release time. We note that this is a temporary and manual solution, and there is still no guarantee that the reports will be released on time. This manual process creates an opportunity for the early release of reports.

We also identified other long-term challenges that NASS has yet to adequately remedy. Although NASS consistently performs monthly security scans of its network, it is not remediating the identified IT vulnerabilities in a timely manner. The scans we performed while conducting this audit found 4,858 critical, high, and medium vulnerabilities on 899 devices on NASS' network—which could result in the compromise of the system, if not acted upon immediately.

NASS scans of the lockup server indicated there were 3 high and 11 medium vulnerabilities that existed for at least 6 months. We note that NASS did not create any POA&Ms to resolve these vulnerabilities once they were detected—as required by NIST, the Department, and NASS procedures. Without creating a POA&M in the Cyber Security Assessment and Management (CSAM)¹⁷ system for each vulnerability, NASS was unable to track the progress of completion. When we spoke to NASS officials about this issue, they said they are establishing a group to address these vulnerabilities, and have since created one POA&M for all monthly scan results, in order to address critical, high, and medium vulnerabilities.

We believe that many of the issues identified in our field work—including our ability to send text messages from lockup (as described in Finding 2)—could have been discovered and addressed by a formal, systematic, periodic review process. Without a periodic review of implemented NASS lockup procedures, ASB cannot adequately perform its oversight duties and proactively mitigate weaknesses that could have a major impact on equitable trading during periods of high volatility just before and after release. NASS officials have stated they are currently forming a designated internal review group that would be able to take on such a project. We agree with NASS' action and encourage officials to assemble this group in a timely manner.

The current NASS report release methods do not allow all users equitable and timely access to public reports, which puts NASS' core mission at risk. NASS should make efforts to ensure that the findings of all reviews are properly tracked and implemented—and IT vulnerabilities are promptly mitigated. A formal internal review process that periodically tests the effectiveness of the lockup procedures, with independent oversight, would help NASS spot security weaknesses before they occur. The independent oversight should report to someone with the authority to execute changes identified during the internal reviews, such as the Under Secretary for Research,

¹⁷ CSAM is a comprehensive system developed by the Department of Justice, which can facilitate achieving Federal Information Security Management Act (FISMA) compliance. CSAM provides a vehicle for the Department, agencies, system owners, and security staff to: (1) manage system inventory, interfaces, and related system security threats and risks; (2) enter system security data into a single repository to ensure all system security factors are adequately addressed; (3) prepare annual system security documents, such as security plans, risk analyses, and internal security control assessments; and (4) generate custom and predefined system security status reports to effectively and efficiently monitor each agency's security posture and FISMA compliance. This includes agency-owned systems as well as those operated by contractors on the agency's behalf.

Education and Economics (REE). Also, NASS should take actions to address report release delays and mitigate known IT vulnerabilities.

Recommendation 1

Establish a group within NASS specifically responsible for internal reviews, and develop, implement, and document periodic, internal reviews of the entire lockup process. The review should involve documenting recommended actions to correct any identified issues. As part of the review, include the results of any audits, external reviews, or other types of internal reviews.

Agency Response

In the agency response dated January 16, 2014, NASS agreed with this recommendation and stated it will establish a group responsible for developing, implementing, conducting and documenting, on an annual basis, internal reviews of the entire lockup process by October 1 of each year, and the results of this review will be shared with an independent evaluator and integrated with other evaluations.

OIG Position

While NASS agreed with the recommendation to establish a group responsible for conducting internal reviews, we are unable to reach management decision based on NASS' agency response. To reach management decision, NASS needs to provide a date by which it will establish this group.

Recommendation 2

Once started, submit the results of the internal review process to an independent evaluator not affiliated with lockup, who is selected by the NASS administrator. The evaluator will monitor, track, and report the results of corrective actions back to the Under Secretary for REE.

Agency Response

NASS agreed with this recommendation and stated it will employ an independent evaluator to monitor, track and report results of corrective actions of the entire lockup process. NASS further stated that the results of this independent evaluation will be shared with REE's Under Secretary bi-annually by October 1 of odd-numbered years.

OIG Position

We are unable to reach management decision based on NASS' response. To reach management decision, NASS needs to provide an estimated date for when the independent evaluator will be in place. Additionally, results from each review conducted should be reported to REE's Under Secretary.

Recommendation 3

Create POA&Ms to track any identified vulnerabilities or recommendations from internal and external reviews. Document the reasons for any unresolved recommendations or weaknesses.

Agency Response

NASS agreed with this recommendation and is currently conducting POA&Ms as part of its corrective action plan and has incorporated these into USDA's CSAM System.

OIG Position

OIG reviewed these POA&Ms and found that they have an estimated completion date of April 30, 2014. We accept NASS' management decision for this recommendation.

Recommendation 4

Immediately take action to prevent report release delays. As part of the process to eliminate the delays, create a long-term plan to prevent their reoccurrence that includes specific deadlines and then implement the solution.

Agency Response

NASS agreed with this recommendation and stated it is and has taken several actions to minimize report release delays and it will have a plan in place by March 15, 2014, and will incorporate continual analysis and assessment as part of the internal review process.

OIG Position

We accept NASS' management decision for this recommendation.

Recommendation 5

Create a service level agreement with NITC to include specific responsibilities and minimum performance standards.

Agency Response

NASS agreed with this recommendation and stated it will update its service level agreement with NITC to include specific responsibilities and minimum performance standards by October 1, 2014.

OIG Position

We accept NASS' management decision for this recommendation.

Section 2: Lockup Security

Finding 2: NASS Needs to Improve Lockup Security

NASS is not enforcing critical lockup procedures and physical security measures meant to protect the security of NASS information. Specifically, contrary to NASS procedures, OIG was able to bring a cell phone into the lockup area and witnessed a reporter in lockup using a wireless iPad, which may also have had cellular capabilities. Also, NASS did not ensure that its staff and contractors followed proper security measures, and had insufficiently documented procedures for some aspects of lockup security, such as guard duties. Finally, managers did not maintain proper key card access and confidentiality records for current, retired, and separated employees. This occurred because managers did not review the lockup and separated lockemployee procedures for gaps, and did not adequately monitor the contracted guards. Although cameras are in place at the entrance of lockup, lockup procedures only require the cameras to be checked periodically to ensure the system is operating. In addition, guards need additional training to effectively perform their lockup duties. As a result of these security weaknesses, sensitive market information could be compromised or leaked before the official release of data, which could adversely affect NASS' mission and equitable trading in the commodity markets.

NASS ASB Lockup Procedures require NASS to take specific security measures to ensure the integrity of lockup, which we found were not always followed. The particular issues are detailed below:

Prohibited Devices

NASS' procedures require it to (1) prevent wireless devices from entering lockup, (2) detect Wi-Fi and cellular transmissions within the confines of lockup spaces, and (3) require visitors to declare that they do not have any wireless devices when entering lockup. However, on two different occasions, OIG was able to bring a cell phone into lockup with minimal effort to conceal it (inside a pocket). We were able to use the phone to send two text messages, both of which went undetected by NASS. Though NASS uses software to detect wireless equipment within the area, the software, due to technological restrictions, is unable to accurately identify the location of a cellular signal. For instance, someone could be using a cellular phone on the floor just above lockup, and the software will still flag it. Therefore, NASS staff cannot be certain when and if any cellular activity is occurring in lockup, as the software continually detects signals. When we sent the text messages, a NASS employee was observing the software and did not detect our text message being sent. NASS officials were aware of the software's shortcomings, but said that there is no other software available to replace it. Without effective software in place, physical measures for preventing cellular devices from entering lockup take on an even greater importance.

Additionally, OIG observed a reporter in the press room using a wireless iPad, which may have had cellular capabilities. All who enter lockup are required to sign in and indicate that they are not currently in possession of a cell phone, laptop, or other wireless

device. We checked the lockup records and found that this reporter selected the “no” checkbox specifying that he did not have any such devices.

Also, while procedures state a NASS staff member is to be in the press room at all times monitoring the press members during lockup; we found that the person did little to monitor the press prior to the official release. Later, OIG notified NASS of what we had observed and NASS had to go back and look at security footage to verify our observation. NASS then suspended the news organization from entering lockup for a specified time period.

Guard Duties

NASS procedures state that the guards are assigned to observe the area outside of lockup and to control the movement of people and materials into the lockup area. They are also responsible for reminding all personnel to leave all wireless devices in a locker prior to entering lockup, checking passes of people who enter, and preventing anyone from leaving lockup before the release time. The guards are contracted Federal Protective Service (FPS) officers. NASS’ contract with FPS is a one-page document that details payment amounts and the location of lockup, and only states that guards will, “provide protective services for [fiscal year] FY 2013 NASS 'Crop Report' Lockups. Officers needed to admit authorized personnel to lockup area and prevent early release of official estimates.” It does not include details on the expectations for the guards’ services and formal ways to address any performance issues.

Due to the nature of the contract, NASS does not know who FPS will assign prior to lockup, or if the specific guard has worked a prior NASS lockup. While guards are provided with a set of written procedures, we found that they were not always followed and did not sufficiently cover all duties. Also, the guards were not provided adequate training on lockup procedures or monitored by NASS personnel to ensure they followed them.

When OIG auditors entered lockup using expired passes, the security guard allowed us access without collecting our passes. We then used these expired passes to enter a subsequent month’s lockup; this also went unnoticed by the guard. The guard also did not verify our names to our security badges. While NASS stated that this was a required procedure for guards, this action was not documented in the instructions given to the FPS officers. Instead, NASS said they gave instructions verbally. We also observed the guards occasionally have a shift change during lockups; when this occurs, NASS needs to have established procedures that can stand alone and clearly outline the guard’s duties, without any verbal instructions from NASS.

NASS procedures require that, upon entering lockup, all persons sign in. However, we found not all persons did so. The sign-in sheet was on a podium just inside of lockup, but was easily missed by visitors because no one provided direction to sign in or verified that everyone had signed in. If an accurate record is not kept, NASS will not have a record of

all individuals present in the event of an emergency, or be able to hold those individuals accountable in the event of a security breach.

Confidentiality Forms

NASS procedures require all employees who enter lockup to sign confidentiality agreement forms (ADM-004) on an annual basis. We reviewed the NASS employees who signed into two lockup sessions in March 2013 and found that out of the 41 employees, only 3 had current forms signed within the past year. This occurred because supervisors are not maintaining and reviewing employee records to ensure that the form is signed annually by applicable employees.

Key Card Access

NIST requires organizations to disable and remove accounts for terminated or transferred users.¹⁸ We found that NASS does not have an accurate database of current key card holders for the lockup area. Specifically, we found 4 individuals on the lockup access list that NASS was not able to identify as current NASS employees or other authorized persons, and 38 separated employees remained on the list. This occurred because NASS officials did not have a documented process for removing a terminated employee from the card reader access system, and were not performing reconciliations between current employee lists and the list of key card holders. NASS recently implemented a new internal process to administer badges, and officials stated that they did not have the time or resources to deactivate badges from separated employees.

NASS has a separation checklist used to document that the USDA photo identification (ID) card and lockup pass have been collected and destroyed before the employee leaves NASS. However, we found that this form is not being used regularly. We non-statistically sampled five separated employees and found that NASS could only provide two separation checklists of the five requested. A NASS employee who maintains the key card access database stated that there were no controls in place to ensure separated employees were consistently removed from the database. As a result, unauthorized and terminated employees could still gain access to restricted areas.

Disaster Recovery

NIST requires agencies to develop and test a contingency plan for an information system disruption. Although NASS has a disaster recovery plan and emergency procedures in place, we were not able to discern all steps for emergency procedures within lockup and had to speak with NASS officials to clarify. Therefore, we are concerned that even with this plan, NASS employees would be unaware of specific emergency procedures in the event of a disaster.

¹⁸ NIST SP800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations* (August 2009).

NASS needs to strengthen its physical security measures, and timely and accurately update its employee files and key card access database. As NASS works to establish its new internal monitoring group, officials should take the opportunity to strengthen procedures for: physical security, lockup entry, tracking and monitoring employee lockup access, and disaster planning. These actions, when done in conjunction with the formal internal reviews recommended in Finding 1, will serve to reduce the possibility of serious information breaches.

Recommendation 6

Immediately implement additional short-term procedures to prevent wireless and cellular devices within lockup. Also, research and implement a permanent solution to prevent cellular activity within lockup.

Agency Response

NASS agreed with this recommendation and stated it has purchased, and with each lockup is now using, an electronic screening device that all lockup entrants must pass through to prevent wireless and cellular devices within lockup. The response further stated that NASS submitted a waiver request to the National Telecommunications & Information Administration in September 2013 to allow cellular blocking within the lockup area. This request was denied. NASS stated it will continue to investigate mitigation strategies for limiting cellular access and that this review will be incorporated into the annual review process. Additional correspondence received from NASS on January 22, 2014 stated that the electronic screening device was implemented on November 8, 2013. This device will screen for cellular and wireless devices.

OIG Position

We accept NASS' management decision for this recommendation.

Recommendation 7

Revise the current FPS contract to include detailed guard responsibilities, in accordance with NASS procedures, as well as recourse if performance is not adequate.

Agency Response

NASS agreed with this recommendation and stated that by June 1, 2014, it will revise the current FPS contract to include detailed guard responsibilities, in accordance with NASS procedures, as well as recourse if performance is not adequate.

OIG Position

We accept NASS' management decision on this recommendation.

Recommendation 8

As a part of NASS' new internal review group, include duties for monitoring the work of guards to the group's responsibilities.

Agency Response

NASS stated it had instituted a procedure to co-locate a NASS employee with FPS personnel to ensure duties are carried out in accordance with contractual agreements, and further stated that it will continue to enhance these procedures and monitor FPS personnel when a new contract is signed. Additional correspondence received from NASS on January 22, 2014, stated that it started co-locating NASS staff with FPS officers as of June 28, 2013.

OIG Position

We accept NASS' management decision on this recommendation.

Recommendation 9

As part of a formal, periodic review process for lockup, validate that confidentiality forms are signed annually by employees and contractors involved in lockup.

Agency Response

NASS stated that it will implement a process to ensure NASS employees and contractors update and sign confidentiality forms. This process will coincide with the annual performance review process.

OIG Position

We are unable to reach management decision based on NASS' response. In order to reach management decision on this recommendation, NASS needs to validate confidentiality forms for all NASS employees and contractors involved in lockup and provide a date when validations will begin.

Recommendation 10

Develop procedures to remove terminated or retired employees from the key card access database, and maintain accurate documentation of separation checklists.

Agency Response

NASS agreed with this recommendation and stated it has developed procedures and will continue to conduct monthly audits to assure that terminated or retired employees are removed from the key card access database and that accurate documentation of separation checklists is

maintained. According to additional information received from NASS on January 22, 2014, NASS implemented new procedures on December 13, 2013.

OIG Position

We accept NASS' management decision for this recommendation.

Recommendation 11

Revise lockup procedures to include more specific guidance on the steps to take in the event of a disaster during lockup, and the locations that staff, press, and visitors will be moved to. Train NASS and media staff on disaster recovery procedures.

Agency Response

NASS agreed with this recommendation and stated it will revise lockup procedures by October 1, 2014, to include more specific guidance on the steps to take in the event of a disaster during lockup, and the locations to which staff, press, and visitors will be moved, and will train its own staff and media representatives on disaster recovery procedures.

OIG Position

We accept NASS' management decision on this recommendation.

Recommendation 12

Strengthen the FPS guards' role to increase the level of lockup security, including requiring that the guards maintain a sign-in sheet that records the time of entry into lockup. Also, add a step to the guards' procedures requiring them to verify that information on lockup entrants' ID cards and passes match.

Agency Response

NASS agreed with this recommendation and stated that FPS guards have a revised protocol to check bags and identities. NASS has taken action to ensure that FPS guards have and follow updated and clear security procedures in regards to identity checks and documentation. The response further stated that by June 1, 2014, NASS will update the statement of work for the FPS guards to increase the level of lockup security, in line with the recommendations.

OIG Position

We accept NASS' management decision for this recommendation.

Finding 3: NASS Needs to Mitigate IT Security Weaknesses to Prevent Data Compromise and Work Disruption

We found that NASS had several unresolved IT security weaknesses: NASS officials (1) were unaware of physical security issues in IT facilities, (2) used live data in a system that had lost its authorization,¹⁹ and (3) used sensitive data on a system that was not categorized at a “high-impact” level of security. NASS was unaware of some issues because it had not conducted a physical controls review of the lockup server room. NASS officials said they were unaware of the potential risk in using live data in a system that had not completed the assessment and authorization process. Each of these problems, if exploited by outside attackers or unscrupulous persons, could impact NASS’ operations and create a risk of compromised statistical data, and compromise the lockup itself. For instance, due to inadequate physical security of an electrical closet, the entire lockup area is at risk for losing power, which could affect report releases.

NIST guidelines and Departmental regulations require agencies to implement specific security measures to ensure the integrity of physical infrastructure and systems. The issues we found are described in detail below:

Physical IT Security

NIST requires that organizations maintain visitor access records and enforce physical access restrictions to the facility where an information system resides.²⁰ OIG visited the server room within lockup where the switches and the ASB server are located. We entered the server room on multiple occasions and were never asked to sign in upon entering the room, and did not see any sign-in sheet available.²¹ In the event that the server equipment was tampered with or changed, NASS would have no record of individuals that could be responsible. When we spoke to them about this, NASS officials were unaware of the visitor's log requirement. After we brought up the issue, NASS implemented a mandatory server room visitor log.

NIST SP 800-53 and the Department also require organizations to develop and maintain an inventory of their information systems.²² We found that NASS does not have an accurate inventory listing of its server room equipment. NASS provided us a list of what it believed was all the equipment in the server room. While all of the equipment listed was present, we identified eight additional devices in the server room that were not included on NASS’ inventory. This occurred due to a lack of management oversight; NASS staff said they simply forgot to include the other devices in their inventory.

¹⁹ The Estimation and Publication (EP) system was authorized to operate until NASS made major changes to the system, at which point NASS did not report the major changes to the Department, nor did it test the proper controls. This resulted in the loss of authorization for the system to operate.

²⁰ NIST SP800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations* (August 2009).

²¹ Anyone not authorized to be in the server room needs to sign the log and document their reason for being in the server room.

²² DM 3545-002 *USDA Information Systems Security Program* (March 31, 2006) & DM 3565-001 *Annual Security Plans for Information Technology (IT) Systems* (February 17, 2005).

Without an accurate inventory, NASS is unaware of all the equipment connected to its network, and therefore cannot monitor, maintain, and secure all equipment, or replace it in the event of a disaster.

We also identified an unlocked, unsecured electrical closet that provides power to the lockup area and server room. The electrical panel containing circuit switches was clearly labeled in detail, and contained the main power switch for the entire lockup area. NIST requires that power equipment and cabling for the information system be protected from damage and destruction. The Department is responsible for the electrical closet and ensuring it is locked. OIG spoke with the USDA building electrical engineer and confirmed that the closet did contain the power for the lockup area and should not be accessible. This occurred because NASS officials were unaware of the closet, its location, and the security implications of leaving it unlocked. As a result, the lockup area is at risk of power failure and disruption, which could result in a delay when releasing the report. The Department has since locked the closet.

Estimation and Publication (EP) System

Departmental Regulation 3140-001 states that USDA's goal is to identify, protect, and secure critical and sensitive USDA systems and data.²³ As a component of EP, NASS has developed a new system that collects and secures statistical information; however, “live” encrypted speculative data were used to test the new system. Therefore, the speculative data—which need to be kept confidential until their official release—were stored on a system that NASS had not yet received an authorization to operate. The authorization process involves testing controls and ensuring a system is secure; considering the high number of vulnerabilities we found on NASS' authorized systems, we are concerned about sensitive speculative data present on an unauthorized system. We found 732 vulnerabilities when we scanned the network that contained the EP system. NASS officials said they were unaware of the potential risk in using live data in the test system.

Federal law requires organizations to categorize their information systems as low-impact, moderate-impact, or high-impact, based on the security objectives of confidentiality, integrity, and availability.²⁴ We found that NASS categorized the EP system, which holds highly sensitive data, as moderate. A moderate system is not required to have all the security controls tested that would be required for a system categorized as high. Therefore, NASS is not testing the security controls for a system with market sensitive data at the highest level.

The EP system holds sensitive information from States that, when aggregated, would be considered speculative—and therefore should be kept confidential and on a system with high integrity, as per the NIST criteria for categorization. For instance, if unscrupulous

²³ USDA Departmental Regulation (DR) 3140-001, *USDA Information Systems Security Policy* (May 15, 1996).

²⁴ Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004).

persons were able to access a crop estimate from a speculative State prior to the official release, they would have information that might give them an unfair advantage in the commodity market.

NASS explained that the EP system connects with NASS' General Support System (GSS).²⁵ If the EP system was categorized as a high impact system at all times, the controls for the GSS—and therefore NASS' entire network—would need to be tested at the “high” level as well, which would be more costly. Still, we believe that such an action is warranted, as sensitive data reside on EP at other times besides during lockup. For example, States periodically input sensitive crop information into EP. Therefore, NASS, in cooperation with the OCIO, needs to determine and implement the proper categorization of EP. OCIO is responsible for validating that proper categorization documentation and justification is accurate in CSAM.

We acknowledge that NASS has taken actions to address some of these IT issues, and believe that it needs to do more to strengthen its IT security. Without the proper NIST physical and environmental controls in place, NASS is increasing the risk of compromising statistical data and lockup itself. In addition, NASS must ensure that sensitive information resides only on authorized systems with the proper security categorization, and that equipment and power sources are adequately secured.

Recommendation 13

As part of the internal review process in Recommendation 2, include a checklist for reviewers to examine how NASS complies with NIST's Special Publication 800-53's physical and environmental controls.

Agency Response

NASS agreed with this recommendation and stated that as a part of the internal review process in Recommendation 2, NASS will, by October 1, 2014, include a checklist for reviewers to examine how NASS complies with the physical and environmental controls in NIST's Special Publication 800-53.

OIG Position

We accept NASS' management decision for this recommendation.

Recommendation 14

Develop and implement procedures to verify that electrical equipment and server rooms are locked at all times.

²⁵ A GSS is a collection of interconnected information resources supporting general IT services. A GSS normally includes hardware, software, information, data, applications, communications, facilities, and people, and provides support for a variety of users and common applications.

Agency Response

In its response dated, January 16, 2014, NASS agreed with this recommendation and stated that it has developed, is executing, and will continue to execute a pre-lockup checklist, which includes verifying that electrical equipment and server rooms are locked at all times. In subsequent correspondence, dated January 22, 2014, NASS stated that this checklist was completed and implemented January 1, 2014.

OIG Position

We accept NASS' management decision for this recommendation.

Recommendation 15

Conduct and maintain a comprehensive inventory of all equipment located within the lockup server room.

Agency Response

NASS agreed with this recommendation and stated that it now maintains a comprehensive inventory of all equipment in the lockup server room. This inventory list will be checked against equipment in the room as part of the pre- lockup checklist. According to additional information received from NASS on January 22, 2014, NASS implemented the new pre-lockup checklist on January 1, 2014.

OIG Position

We accept NASS' management decision for this recommendation.

Recommendation 16

When testing a system, only use test data or data that have already been released.

Agency Response

NASS agreed with this recommendation and stated it only uses test data or data that have already been released when testing a system. NASS provided additional correspondence and information obtained on January 22, 2014, indicating that it formally requested this through its Change Control Board on January 21, 2014.

OIG Position

We accept NASS' management decision for this recommendation.

Recommendation 17

In cooperation with the Department, determine and implement the appropriate security categorization and system boundaries of the GSS and the EP System.

Agency Response

NASS agreed with this recommendation and stated by October 1, 2014, in cooperation with the Department, NASS will review the IT systems boundaries and make adjustments where necessary as part of the assessment and accreditation process.

OIG Position

We accept NASS' management decision for this recommendation.

Scope and Methodology

Our audit analyzed current NASS lockup procedures, covering the process of aggregating and securing commodity data, and compiling them into agricultural reports that are prepared and released using NASS' lockup process. We focused on determining if data used to create the reports are secured throughout the lockup process.

We conducted our audit fieldwork from February 2013 to August 2013. We visited NASS headquarters in Washington, D.C.

To determine the security of NASS data, we performed the following steps:

- Interviewed NASS staff.
- Tested NASS' physical control environment prior to, during, and following lockup.
- Conducted scans of NASS' network to identify vulnerabilities.
- Analyzed past issues with data security during lockup, noted any ongoing issues, and determined corrective actions taken.
- Reviewed the ASB system controls to determine if they are suitably designed, and if they conform to the minimum security requirements mandated by NIST SP 800-53 r3, *Recommended Security Controls for Federal Information Systems and Organizations*.
- Participated in and tested controls during three lockup sessions to determine if they operated with sufficient effectiveness to provide reasonable assurance of data security.
- Followed up on a review of NASS conducted by OCIO/ASOC and reviewed the recommendations to determine if they had been implemented.
- Obtained and reviewed current policies for lockup and verified whether they are sufficient to secure sensitive data related to agricultural reports issued by NASS.
- Reviewed various Departmental Regulations and manuals related to IT security and Governmentwide publications, such as NIST Special Publications, OMB Circulars, and the Government Accountability Office Federal Information Systems Controls Audit Manual, as guidelines for this review.

We used a commercially available scanning tool to evaluate IT security. 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Abbreviations

ASB	Agricultural Statistics Board
ASOC	Agriculture Security Operations Center
CSAM	Cyber Security Assessment and Management
EP	Estimation and Publication
FPS	Federal Protective Service
GSS	General Support System
ID	Identification
IT	Information Technology
NASS	National Agricultural Statistics Service
NIST	National Institute of Standards and Technology
NITC	National Information Technology Center
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestone
REE	Research, Education and Economics
USDA	Department of Agriculture
WASDE	World Agricultural Supply and Demand Estimates

**USDA'S
NATIONAL AGRICULTURAL
STATISTICS SERVICE'S
RESPONSE TO AUDIT REPORT**

United States Department of Agriculture
National Agricultural Statistics Service
Office of the Administrator

January 16, 2014

TO: Gil H. Harden
Assistant Inspector General for Audit

FROM: Cynthia Clark /s/ **Cynthia Clark**
Administrator
National Agricultural Statistics Service

SUBJECT: Security Review of the National Agricultural Statistics Service Lockup
Procedures, Audit 26501-0001-12

Thank you for the opportunity to comment on your final draft report. NASS appreciates your thorough and thoughtful report and takes your review and recommendations seriously. We are committed to implementing each of the recommendations and to the continuous improvement of our systems and procedures. Our responses identify these commitments and highlight actions we have already taken that were not mentioned in the report.

As background, in 2011 NASS originally asked the Agriculture Security Operations Center (ASOC) and the Office of the Chief Information Officer to conduct an audit of the Lockup press room following incidents during which news stories were inadvertently released out of Lockup before NASS released the official data. NASS sought to identify vulnerabilities and ways to improve its Lockup security systems and processes.

Following the ASOC review in 2011, NASS addressed recommendations in the report including:

- Installing new redundant switches in the press room to control network connectivity;
- Segregating the press room communication equipment into two cabinets – one containing government equipment and the other containing news agency equipment;
- Adding cameras outside of all Lockup doors (they are monitored by the USDA command center); and
- Installing lockers outside of Lockup to hold personal items prohibited in Lockup.

The Office of the Inspector General (OIG) conducted a subsequent audit of the broader Lockup process during 2013. This report documents the OIG's audit findings. NASS implemented many of the recommendations found in this report during the audit period and since its completion. While the OIG report does mention some actions NASS has already taken, we have completed actions on many more recommendations that are not documented in the report. During the exit conference, the auditors agreed noting that they could not include actions that they did not observe during their visits or that occurred between their last visit and the report preparation.

The OIG's recommendations to improve Lockup procedures and the security of the press room fall into three primary categories: Lockup Management, Lockup Security, and IT Security. NASS is responding with actions it has taken in each of these areas.

Room 5041A-South Building · 1400 Independence Avenue, SW · Washington, D.C. 20250-2001
(202) 720-2707 · (202) 720-9013 FAX · www.nass.usda.gov

LOCKUP MANAGEMENT – Recommendations 1-5

The initial recommendations in this section are the foundation of OIG's final recommendations to assure long-term review and improvement of NASS Lockup management. NASS is establishing an oversight group responsible for ongoing review of Lockup security procedures and practices, including establishing a more comprehensive set of standard operating procedures (SOPs) and consistently using plans of actions and milestones (POA&Ms). Each October, an annual report will be provided to an external evaluator. Until the oversight group is established, personnel in charge of Lockup elements have established standard operating procedures and have taken actions to implement recommendations in their areas of responsibility.

In the area of Lockup management the report mentions IT vulnerabilities. NASS took immediate and significant actions regarding the finding of 4,800 network vulnerabilities. In our first action, about 3,900 vulnerabilities were either resolved or added to a POA&M. We have implemented a stricter vulnerability mitigation process to avoid future vulnerabilities. This will be reviewed by both internal and external review groups.

After the early release that occurred in 2011, NASS has taken multiple steps to prevent both early release and report release delays. NASS is actively monitoring results and will incorporate continual analysis and assessment as part of the internal review process. This will include revising our agreement with the National Information Technology Center (NITC) to include specific responsibilities and minimum performance standards.

Our responses to the five recommendations relating to NASS Lock-up management are:

- 1.** NASS will establish a group responsible for developing, implementing, conducting and documenting internal reviews of the entire Lockup process annually by October 1 of each year. The results of this review will be shared with an independent evaluator and integrated with other evaluations.
- 2.** NASS will employ an independent evaluator as recommended to monitor, track and report results of corrective actions of the entire Lockup process. Results of this independent evaluation will be shared with the REE Undersecretary bi-annually by October 1 of odd numbered years.
- 3.** NASS is currently conducting POA&Ms as part of its corrective action plan and has incorporated these into the USDA Cyber Security Assessment and Management (CSAM) System.
- 4.** NASS is and has taken several actions to minimize report release delays. NASS will have a plan in place by March 15, 2014, and will incorporate continual analysis and assessment as part of the internal review process.
- 5.** NASS will update its service level agreement with NITC to include specific responsibilities and minimum performance standards by October 1, 2014.

LOCKUP SECURITY – Recommendations 6-12

In the past two years, NASS has focused on multiple efforts to prevent wireless and cellular devices within Lockup. We have sought a permanent solution to actively prevent cellular activity within Lockup. In September 2013, we submitted a waiver request to the National Telecommunications & Information Administration (NTIA) to allow cellular blocking within the Lockup area. The NTIA denied this request. NASS will continue to investigate mitigation strategies for limiting cellular access. This will be incorporated into the annual review process.

We installed lockers to hold personal items that are prohibited in Lockup. We recently revised security procedures to enter Lockup. We have installed and are using electronic security detectors through which everyone entering Lockup must pass as one line of defense against electronic devices such as mobile phones. Federal Protective Service (FPS) guards have a revised protocol to check bags and identity. NASS has taken action to ensure that FPS guards have and follow updated and clear security procedures in regards to identity checks and documentation.

NASS is conducting monthly audits and developing procedures to remove terminated or retired employees from the key card access database and to maintain accurate documentation of separation checklists. NASS has reviewed records to ensure that all current employees and contractors have current confidentiality forms on file, and we will continue a periodic review. We are documenting a process to ensure employees sign confidentiality forms upon hiring and at their annual performance reviews.

We are also actively observing the security processes at the Lockup entrance and monitoring the activities of reporters in the Lockup press room. Reporters have been instructed again on procedures allowed in the room and penalties of prohibited actions.

Our responses to the seven recommendations relating to NASS Lockup security are:

6. NASS has purchased, and with each Lockup is now using, an electronic screening device that all Lockup entrants must pass through to prevent wireless and cellular devices within Lockup. This device will screen for cellular and wireless devices. NASS submitted a waiver request to the National Telecommunications & Information Administration in September 2013 to allow cellular blocking within the Lockup area. This request was denied. NASS will continue to investigate mitigation strategies for limiting cellular access. This review will be incorporated into the annual review process.

7. By June 1, 2014, we will revise the current FPS contract, to include detailed guard responsibilities, in accordance with NASS procedures, as well as recourse if performance is not adequate.

8. NASS has already instituted a procedure to co-locate a NASS employee with FPS personnel to ensure duties are carried out in accordance with contractual agreements. NASS will continue to enhance these procedures and monitor FPS personnel when a new contract is signed.

9. NASS will implement a process to ensure NASS employees and contractors update and sign confidentiality forms. This process will coincide with the annual performance review process.

10. NASS has developed procedures and will continue to conduct monthly audits to assure that terminated or retired employees are removed from the key card access database and that we maintain accurate documentation of separation checklists.

11. By October 1, 2014, NASS will revise Lockup procedures to include more specific guidance on the steps to take in the event of a disaster during Lockup, and the locations to which staff, press, and visitors will be moved. NASS will train its own staff and media representatives on disaster recovery procedures.

12. By June 1, 2014, NASS will update the statement of work for the FPS guards to increase the level of Lockup security, in line with the recommendations.

IT SECURITY- Recommendations 13-17

In the past two years, NASS has implemented many improvements to the server room security, access, inventory and pre-Lockup checklist. Clocks were installed in the server room in 2013 to assist with timely report dissemination. Our practices will be included in a checklist for the internal reviewers to examine how NASS complies with the physical and environmental controls in the National Institute of Standards and Technology (NIST) Special Publication 800-53.

NASS has developed and is using pre-Lockup checklist procedures to verify that electrical equipment and server rooms are locked at all times. We are also conducting and maintaining a comprehensive inventory of all equipment in the Lockup server room. This inventory list is checked against equipment in the room as part of the pre-Lockup checklist.

Since the OIG identified that NASS was using pre-release data to test its Estimation and Publication systems, NASS has successfully completed re-accreditation of the NASS Estimation and Publication Major Application. It achieved authority to operate (ATO) on September 6, 2013.

Our responses to the five recommendations relating to IT security are:

13. As part of the internal review process in Recommendation 2, NASS will by October 1, 2014, include a checklist for reviewers to examine how NASS complies with the physical and environmental controls in the National Institute of Standards and Technology (NIST) Special Publication 800-53.

14. NASS has developed, is executing, and will continue to execute a pre-Lockup checklist to include verifying that electrical equipment and server rooms are locked at all times.

Gil H. Harden
Assistant Inspector General for Audit

15. NASS now maintains a comprehensive inventory of all equipment in the Lockup server room. This inventory list will be checked against equipment in the room as part of the pre-Lockup checklist.

16. NASS only uses test data or data that have already been released when testing a system.

17. By October 1, 2014, and in cooperation with the Department, NASS will review the IT systems boundaries and make adjustments where necessary as part of the assessment and accreditation process.

Thank you once again for the opportunity to provide these comments.

To learn more about OIG, visit our website at
www.usda.gov/oig/index.htm

How To Report Suspected Wrongdoing in USDA Programs

Fraud, Waste and Abuse

e-mail: USDA.HOTLINE@oig.usda.gov

phone: 800-424-9121

fax: 202-690-2474

Bribes or Gratuities

202-720-7257 (24 hours a day)



The U.S. Department of Agriculture (USDA) prohibits discrimination in all of its programs and activities on the basis of race, color, national origin, age, disability, and where applicable, sex (including gender identity and expression), marital status, familial status, parental status, religion, sexual orientation, political beliefs, genetic information, reprisal, or because all or part of an individual's income is derived from any public assistance program. (Not all prohibited bases apply to all programs.) Persons with disabilities who require alternative means for communication of program information (Braille, large print, audiotape, etc.) should contact USDA's TARGET Center at (202) 720-2600 (voice and TDD).

To file a complaint of discrimination, write to USDA, Assistant Secretary for Civil Rights, Office of the Assistant Secretary for Civil Rights, 1400 Independence Avenue, S.W., Stop 9410, Washington, DC 20250-9410, or call toll-free at (866) 632-9992 (English) or (800) 877-8339 (TDD) or (866) 377-8642 (English Federal-relay) or (800) 845-6136 (Spanish Federal relay). USDA is an equal opportunity provider and employer.