UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

# STATEMENT OF THE HONORABLE PHYLLIS K. FONG

## INSPECTOR GENERAL

Before the

Subcommittee on Department Operations,
Oversight, and Credit

Committee on Agriculture

U.S. House of Representatives

December 1, 2011

Good morning, Mr. Chairman, Ranking Member Fudge, and Members of the Subcommittee. I am joined by Gil Harden, the Assistant Inspector General for Audit and Karen Ellis, the Assistant Inspector General for Investigations. Thank you for the opportunity to update the Subcommittee on the Office of Inspector General's (OIG) work on preventing fraud in the Supplemental Nutrition Assistance Program (SNAP) and reviewing the Department's information technology (IT) programs for compliance with all applicable laws and regulations.

## **Database Analysis to Reduce SNAP Fraud**

As part of our ongoing efforts to help minimize fraud, waste, and abuse within SNAP, OIG is performing a series of audits analyzing 10 States' participant databases.[1] These databases store critical information which helps identify ineligible participants who are receiving benefits. Detecting and investigating program violations is one of the State agencies' primary responsibilities. State agencies are required to check their information against Federal and State databases to ensure, for example, that people using deceased individuals' social security numbers (SSN) do not receive benefits, or that their submitted income is the same as is listed in official records. If applicants do not meet eligibility requirements at the time of application or on a recurring 6 to 12 month basis, State agencies are required to disqualify them. Doing so ensures that taxpayer dollars go to those who are truly in need.

To monitor State agencies' progress in identifying and preventing improper payments, we checked several of these databases ourselves. We have completed work in two States—Kansas and Florida—and found a total of 3,572 recipients who were receiving potential improper payments:[2]

- *878 recipients were either deceased or using the SSNs of deceased individuals.*[3] State agencies did not investigate individuals using the SSNs of deceased persons due to a backlog stemming from increased participation in SNAP in recent years, as well as a system crash. Additionally, some recipients received benefits because State agencies only checked State death records, which do not identify deceased participants who died in

[1] The 10 States are Alabama, Florida, Kansas, Louisiana, Massachusetts, Mississippi, Missouri, New Jersey, New York, and Texas.
[2] Kansas: 883; Florida: 2,689.
[3] Kansas: 71; Florida: 807.

a different State, instead of checking against the required national Social Security Administration database.

- *160 active participants were previously disqualified from receiving SNAP benefits.*[4] One of the most basic ways to protect against SNAP fraud is to prevent intentional program violators from reenrolling, but FNS does not require States to check FNS' database of disqualified participants before admitting them into SNAP.[5] We found that because of this policy, in Florida alone, 160 participants who had previously been disqualified in other States were actively receiving SNAP benefits.

- *973 participants received dual benefits simultaneously from another State for 3 consecutive months.*[6] *Of these, 165 were enrolled in both States for 6 months or longer*[7]*—and 1 was a dual participant for a year and a half.*[8] This occurred because, at present, FNS does not have a nationwide database of participant data. Instead, the States, at their own discretion, utilize an optional, multi-State system, which results in significant gaps in coverage. For example, even though Florida utilizes this system, it did not know that 370 SNAP participants were simultaneously receiving benefits in Alabama because Alabama does not participate in the system, and thus the system does not contain Alabama's data.

- *1,555 individuals had invalid SSNs.*[9] The States did not always check their own databases for anomalies, which increased the risk of improper payments to individuals with invalid SSNs. Agencies attributed most of these errors to data entry errors or incorrect SSNs provided by participants. With potentially incorrect information, it is difficult for States to determine which participants may be intentionally manipulating the system.

[4] Florida: 160.
[5] FNS uses a database known as the Electronic Disqualified Recipient System (eDRS).
[6] Kansas: 90; Florida: 883.
[7] Kansas: 58; Florida: 107.
[8] Kansas: 1.
[9] Kansas: 720; Florida: 835.

- *6 individuals were receiving dual benefits under two separate accounts*.[10] State agencies determined that a rare IT system issue created dual records, but were unable to diagnose the cause.

Participants in Kansas receive on average $124.40 in benefits a month, while participants in Florida receive an average of $141.40 a month. We estimate that these 3,572 recipients could be receiving a total of $490,070 a month.[11]

Databases provide some of the most comprehensive and robust information for fraud detection. However, we found that because State agencies do not fully utilize them—even when they are required to do so—they may continue to issue SNAP payments to those who are not entitled to receive the benefit.

Taken within the context of SNAP as a whole, our findings to date do not represent large monetary sums, but they do show areas where FNS and the States could make progress in reducing potential improper payments. Moreover, as FNS strives to bring its rate of improper payments below 3 percent, it will need to make use of data analysis as a straightforward way of identifying payments that should not be made. OIG is in the process of completing similar data analysis audits in another eight States.

In our reports, we have recommended that FNS require the Florida and Kansas agencies to ensure they use a national database to perform death matches and SSN verifications, and that they perform checks to make sure information is entered correctly. We also recommended the State agencies review the individuals we identified and recover improper payments, as appropriate. Generally, FNS agreed. To prevent interstate dual participation, the agency is in the process of implementing regional databases. FNS also encourages States to check for interstate dual participation by using the optional national database, but notes that some States feel the information in this database is not timely. FNS has not yet provided timelines to

[10] Kansas 2: Florida: 4.
[11] $109,845 in Kansas; $380,225 in Florida.

implement checks for dual enrollment, which we require to reach agreement on management's decision for corrective action.[12]

Additionally, we have found that FNS needs to take measures to ensure that other information used in fraud detection efforts is accurate and reliable.  In one audit, we found that the files used to back up FNS' Anti-Fraud Locator Electronic Benefit Transfer (EBT) Retail Transaction system, which stores the data from EBT transactions, were incomplete and disorganized, which could hinder fraud detection efforts.  As a result of our audit, FNS has agreed to strengthen system controls, including system redesigns and upgrades by June 2012.[13]

## OIG Investigations of the Illegal Trade in SNAP Benefits

Just as there are individuals willing to misrepresent themselves to receive benefits, so there are individuals and retailers who illegally exchange food benefits for cash or other commodities. For example, by giving a recipient $50 in cash for $100 in benefits, an unscrupulous retailer can make a significant profit; recipients, of course, are then able to spend the cash however they like. In some cases, recipients have exchanged benefits for drugs, weapons, and other contraband. Not only does this illegal exchange interfere with FNS' ability to efficiently use its resources to feed hungry families, but it undermines the goal of providing nutritional and wholesome food to those in need.

In FY 2011, OIG devoted about 46 percent of its investigative resources to SNAP-related criminal investigations.  In that year, our investigations resulted in 179 convictions and monetary results totaling $26.5 million.  In recent months, OIG has concluded a number of SNAP investigations, including the following:

- A judge recently ordered a Brooklyn store owner to serve 2 years in jail and pay $1.4 million in restitution for defrauding SNAP.  From September 2007 to September 2009, OIG agents exchanged a total of $2,664 in SNAP benefits for $1,875 in cash in a series of transactions demonstrating that the owner was in the habit of trafficking

[12] Audit Report 27002-0002-13, "Analysis of Florida's SNAP Eligibility Data" (November 29, 2011) and Audit Report 27002-0001-13, "Analysis of Kansas' SNAP Eligibility Data" (November 23, 2011).
[13] Audit Report 27002-0001-DA, "Analysis of Supplemental Nutrition Assistance Program ALERT Database" (November 22, 2011).

in SNAP benefits. Subsequent investigation and analysis of financial data demonstrated that the store's fraudulent SNAP transactions amounted to approximately $1.4 million. In 2009, the store owner and her son were charged with conspiracy to commit SNAP trafficking. The store owner pled guilty and was sentenced to 24 months' imprisonment and ordered with her son to pay restitution of approximately $1.4 million and forfeiture in the amount of $105,524. The owner's son fled, but he was apprehended in Florida in July 2010. He pled guilty in December 2010, and in June 2011, was sentenced to 15 months' imprisonment.

- After being deported from the United States for food stamp fraud in the 1990s, one criminal illegally re-entered the country in 2000 and resumed EBT fraud. With the assistance of an accountant, this individual opened several stores using other individuals' names. The false owners of these stores signed their names on FNS documents to obtain authorization to accept SNAP benefits, but the subject, his wife, and his brother actually operated these stores. Subsequently, an OIG investigation resulted in the subject and his brother being charged with fraud. In June 2011, the owner was sentenced to 57 months of incarceration, 3 years of probation, and restitution of $1.7 million, and will again be subject to deportation. His brother was sentenced in May 2011 to 21 months of incarceration, 12 months' probation, and restitution totaling $362,764. Court actions are pending against the store owner's wife.

- In Cincinnati, a 2-year joint criminal investigation led by OIG disclosed that the owner, manager, and employees of two SNAP-authorized retailers exchanged SNAP benefits for firearms, cash, stolen tobacco products, narcotics, and drug paraphernalia. In April 2011, two store employees, who were brothers, were sentenced to 51 months' incarceration followed by 3 years' supervised release, and were ordered to pay fines. Their mother was sentenced in May 2011 to time served, 6 months' home confinement, and 3 years' supervised release after agents found EBT cards in her purse while searching for evidence involving her sons' illegal SNAP trafficking. Their father was sentenced to probation in September 2011 after he pled guilty to SNAP fraud and receipt of stolen property. One of the store owners and a manager are scheduled to be tried criminally later this year for illegal use of SNAP benefits.

OIG continues to work with FNS to develop new ways of detecting and investigating retailers at high risk of committing such fraud. In particular, we are engaged in ongoing discussions with FNS to identify ways to leverage resources with State and local partners so that they may better address fraud involving both retailers and recipients.

## Improving USDA's IT Systems

OIG continues to provide oversight to ensure that the Department efficiently and effectively utilizes the funds it was provided to update its IT infrastructure. In FY 2010, the Office of the Chief Information Officer's (OCIO) baseline budget was increased from $17 million to $61 million for security improvements within the Department. Anticipating a total of $64 million in FY 2011, USDA pursued a total of 14 projects that year, including network monitoring and establishing a 24/7 security operations center. However, in April 2011, the passage of a final continuing resolution resulted in a decrease in overall appropriations available for the remainder of FY 2011. OCIO received a total of $40 million for FY 2011—$23 million more than in FY 2009, but $24 million less than what it anticipated. OIG is in the process of determining how OCIO used the additional funding it received, and if the additional funding resulted in improved security. We can state, based on our work to date, that the 14 projects initiated with this additional funding appear to have been significantly curtailed or delayed. In one example, with a decreased budget, USDA halted work by contractors to implement a $3.6 million software package. With the project not yet operational, and without access to the administrator account, the Department effectively found itself unable to use the software tool.

Apart from this ongoing audit, OIG routinely monitors the state of IT security at USDA. Each year, we conduct our mandated review of the Department's compliance with the Federal Information Security Management Act (FISMA). Bringing USDA's IT infrastructure into full compliance with all applicable laws and regulations is a formidable challenge, as the Department includes 33 agencies, most with their own IT infrastructure, and operates a total of 257 discrete IT systems. In FY 2011, USDA spent a total of $2.5 billion on IT-related expenses to maintain, upgrade, operate, or replace these systems.

The Department requires this infrastructure to process and manage the vast amounts of information needed to deliver benefits and services to the American public. However, overseeing such a diverse array of technology presents problems for any organization, and USDA is no exception. Since 2009, OIG has made 43 recommendations, including 10 from FY 2011, intended to help the Department remedy longstanding deficiencies in its IT security. Though the Department has closed only 6 of these 43 recommendations, it continues to work on resolutions for the remaining open recommendations.

As part of our FY 2011 FISMA review, OIG noted that OCIO has tended to attempt too many IT projects at the same time, which has resulted in USDA not meeting its project milestones. Given OCIO's tendency to disperse its efforts over a wide field—and thereby dilute their effect—we have recommended that OCIO prioritize its work on a few projects, and focus on completing those projects. To some extent, OCIO has responded. For example, in response to issues we reported previously, the Department installed a cyber security incident detection toolkit this year—this system should help USDA detect and respond to intrusions in its data systems. With appropriate resources, the Department can analyze up to 150 alerts to potential cyber attacks per week. OCIO, however, faced a decrease in its budget for this project, and was forced to reduce the personnel it relied on to perform this work. Now, it analyzes about 15 alerts weekly.[14]

OIG also has issued a number of recent reports dealing with IT problems in the Department, several of them dealing with contractors. Federal IT projects have historically involved contractors, but USDA has not always adequately overseen the contracts it relies on to fulfill its IT requirements. For instance, our audit of USDA's Domain Name System (DNS) revealed that OCIO needs to improve how it oversees the contractors who operate this critical system, which routes internet traffic through the network.[15] Like any other distributed computing system, USDA's system is susceptible to platform-, software-, and network-level vulnerabilities. OIG reviewed the Department's management and security controls to protect the integrity, validity, and availability of the information that travels across USDA's network. We found that OCIO has not always been diligent in ensuring that the management and security over DNS was

[14] Audit Report 50501-0002-12, "U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2011 Federal Information Security Management Act" (November 15, 2011).

[15] DNS is a data communication mechanism that translates Internet Protocol addresses into easy-to-understand website names, allowing users to navigate using a website name such as www.ocio.usda.gov rather than a series of numbers such as 192.168.200.100.

adequate. Ultimately, these types of problems leave the Department open to cyber attacks and the potential destruction or theft of valuable and private data.[16]

USDA, like other Federal agencies and private companies, is also facing challenges concerning integrating new technologies in a way that furthers the Department's mission while also meeting the most rigorous IT security requirements. The Department's employees are increasingly reliant on smart phones or other wireless handheld devices, but these powerful devices bring with them new security problems related to their portability. OIG reviewed 277 of USDA's approximately 10,000 wireless handheld devices, and found that all of these 277 devices were not adequately secured, as defined by guidance issued by the National Institute of Standards and Technology. For example, we found wireless handheld devices that were not password-protected, had no anti-virus software installed, and were not configured to encrypt removable media. We also found that all 22 of the Department's Blackberry servers were not secured in accordance with Departmental guidance, which allowed users to disable their passwords or bypass the Department's internet content filters. Ultimately, these problems occurred because OCIO took a decentralized approach to deploying these devices (allowing individual agencies to select and deploy smart phones) without providing clear guidance and oversight on how to configure and secure them, which resulted in inconsistencies.[17] OCIO accepted our recommendations.

## Conclusion

This concludes our written statement. I want to again thank the Chair and the Subcommittee for the opportunity to testify today. We welcome any questions you may have.

[16] Audit Report 50501-0001-12, "Fast Report – Critical Domain Name Systems (DNS) Servers" (April 15, 2011).
[17] Audit Report 50501-0001-IT, "USDA's Management and Security Over Wireless Handheld Devices" (August 15, 2011).