

# PDSD TIMES

Issue 15▲ Fall 2006▲

## Financial 'Fall' Cleaning

### Your Credit Report and Associated Rights under FCRA

One of the leading issues in background investigations is financial indebtedness. The Adjudicative Guidelines state the inability to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control, lack of judgment, or an unwillingness to abide by rules and regulations, all of which can raise questions about an individual's reliability, trustworthiness and ability to protect classified information.

It is recommended that employees review their credit reports annually to ensure there are no reporting errors, especially prior to your background investigation. A credit report includes information on where you live, how you pay your bills, and whether you've been sued, filed for bankruptcy, or hold tax liens.

The Fair Credit Reporting Act (FCRA) requires each of the nationwide consumer reporting companies – Equifax, Experian, and TransUnion – to provide you with a free copy of your credit report, at your request, once every 12 months. To order, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), or call 1-877-322-8228.

Keeping accurate financial records on debt payoffs, repayment agreements, and written disputes will help mitigate any issues that arise in your investigation.



### THIS ISSUE'S REMINDERS

#### 1. Bulletin 06-07

Released 9/26/06, this bulletin provides the updated OPM Investigations Reimbursable Billing Rates for FY07. View at <http://www.usda.gov/da/pdsd/bulletins.htm>.

#### 2. Bulletin 06-08

Released 9/26/06, this bulletin provides an overview of the new reinvestigation products for TS positions. View at <http://www.usda.gov/da/pdsd/bulletins.htm>.

#### 3. Training Available

PDSD will hold forms review and e-QIP training on 12/19/06 in the South Building. If you are involved in reviewing security questionnaires and/or e-QIP taskings, please contact Vet Thorpe to sign up (16 slots) at 202/720-4390.



**Personnel & Document  
Security Division (PDSD)  
USDA/DA/OPPM/PDSD**

### IN THIS ISSUE

Imaged OPM Investigations  
Contracting Concerns  
Staff Updates  
Information Security News

**Page 3**  
e-QIP  
Updates

**Page 5 & 6**  
HSPD-12  
Newsflashes!

**Page 7**  
Reciprocal  
Recognition of  
Security  
Clearances

1400 Independence Ave., SW  
RM S-310  
Washington, DC 20250  
(202) 720-7373  
(202) 720-1689 FAX

<http://www.usda.gov/da/pdsd/>

## Modernization Update:

### Receiving Imaged Investigation Reports from the Office of Personnel Management

The Personnel and Document Security Division (PDSD) has volunteered to pilot test a direct connection program with the Office of Personnel Management (OPM), which will allow USDA to electronically receive imaged results of background investigations.

Receiving imaged investigative reports will reduce time lags between the closing date of the investigation and the date of adjudication. PDSD expects to enter into a Memorandum of Understanding with OPM within the first quarter of fiscal year 2007 and begin enhancements to the modernized SETS database to facilitate the receipt of imaged results by the end of FY 2007.



**Ideas, Comments, or Suggestions for future newsletter articles? Do you want to be added to the distribution list?**

Contact Carrie Moore at [carrie.moore@usda.gov](mailto:carrie.moore@usda.gov).



## In the News: Information Security

**Congressional Research Service (CRS)  
Report to Congress  
Protection of Security-Related Information  
Dated September 27, 2006  
<http://www.fas.org/sgp/crs/secrecy/RL33670.pdf>**

This report describes the current state of the law with regard to the protection of security related information. Topics are evaluated such as Freedom of Information Act exceptions, Protected Critical Infrastructure Information (PCII), and Department of Transportation's Sensitive Security Information.

**Congressional Research Service (CRS)  
Report to Congress  
Protection of National Security Information  
Dated June 30, 2006  
<http://www.fas.org/sgp/crs/secrecy/RL33502.pdf>**

This report provides a synopsis of existing laws and statutes and their penalties for not protection of sensitive and classified information.

## PDSD Staff Changes

**Please join us in welcoming our new additions!**

Susan Gulbranson, Chief of the Personnel Security Branch, has been selected to fill the position of Chief of the Personnel and Document Security Division previously held by Marty Brumback. Susan spent 14 years with the Defense Security Service in a variety of field and headquarters positions before joining USDA in the summer of 2003.

The PDSD welcomed a new team member in August 2006 when Kim Elosser joined the Personnel Security Branch as a Personnel Security Assistant. Kim brings personnel and information security experience from her prior positions within defense contractor facilities and she is the primary point of contact for questions concerning the processing of national security and public trust personnel security forms. Kim can be reached on (202) 205-7934 or by emailing [persecadmin@usda.gov](mailto:persecadmin@usda.gov).



# e-QIP Updates

## e-QIP System Access

Many e-QIP applicants have been experiencing some problems accessing e-QIP 2.0. We would like to remind the agency POC's to provide the applicants with instructions and the e-QIP brochure that explains the process step by step.

e-QIP has been tested with and supports the following browsers: Microsoft Internet Explorer 6.0 and later, Mozilla Firefox 1.0 and later, and Netscape 7.0 and later.

One of the browsers listed above must be used to ensure that all e-QIP system screens display and function properly. If you have any questions about e-QIP requirements, please contact Vet Thorpe at 202/720-4390 or [arviet.thorpe@usda.gov](mailto:arviet.thorpe@usda.gov).



## e-QIP Printing Problems

We have experienced some printing problems with Adobe 6.0 and IE. A bug in Adobe causes the browser to crash when attempting to open a .pdf within the browser window. The easiest way to work around this is to point at the DISPLAY link and RIGHT click to 'SAVE the Target File' to your PC. Simply open the saved file and you should have no problems. If you have any questions, please contact Vet Thorpe at 202/720-4390 or [arviet.thorpe@usda.gov](mailto:arviet.thorpe@usda.gov).

## e-QIP SF85 Implementation

PDSO has completed our final phase of e-QIP implementation which entailed training and setting up USDA Human Resources offices to use the electronic Standard Form (SF) 85, "Questionnaire for Non-Sensitive Positions." As of October 13, 2006, seven USDA agencies/staff offices are enabled to use the SF85 in e-QIP. These include the Office of Inspector General (OIG), Office of the Chief Information Officer (OCIO), Office of Executive Resources (OES), Food Safety & Inspection Service (FSIS), National Finance Center (NFC), Agricultural Research Service (ARS), and Food and Nutrition Service (FNS).

# Federal Contracting

## Contracting Concerns

### SECURITY REQUIREMENTS IN CONTRACTING

Iraqi military authorities in Baghdad reported on Oct 8th, 2006 that several hundred people were sickened by suspected *intentional poisoning of the food supply* at a base populated with the Iraqi 4<sup>th</sup> Division of National Police. Some of the policemen began bleeding from the ears and nose after the meal, which led authorities to believe the poisoning was intentional. An Australian contractor responsible for the food subcontracted the food preparation to another Iraqi company. The food was prepared at another location and brought to the kitchen.

This event illustrates the importance of security requirements in USDA's contracting program. Do USDA agencies monitor what sensitive work is being contracted and are we sufficiently tracking the subcontracts? If your agency is using contractors to perform work that involves national classified information, a DD Form 254 (Contract Security Classification Specification) must be part of the contract package. The DD 254 informs the contractor of the level of information they will be required to access, the level of security clearance the contractors will need, and how they will process, store, transmit, and destroy the classified information when the contract is complete. If the contractor then subcontracts the work, they are obligated, under the National Industrial Security Program, to pass those requirements on to the subcontract. The form can be found at:

[http://www.classmgmt.com/about\\_NCMS/DD0254.doc](http://www.classmgmt.com/about_NCMS/DD0254.doc)

Contracts requiring work that is unclassified but sensitive should also be evaluated to ensure that contractors have undergone an appropriate level of background investigation to perform the required duties.

### PROTECTION OF UNCLASSIFIED BUT SENSITIVE INFORMATION

USDA agencies must be aware of information they are publicly releasing and how the information can be compiled to create highly sensitive or classified information. Such knowledge and awareness is critical to the process of Operations Security or OPSEC. The OPSEC evaluation process is determined by indicators, which are defined as friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information. When these indicators are known, agencies can take appropriate measures to eliminate any vulnerabilities regarding exploitation of or threat to their information.

Information sharing with the public is contrary to protecting information, yet both are critical to the USDA mission. The onset of electronic bulletin boards, blogs, digital cameras, email, and websites have created an open door for employees to share information and provide our adversaries access to collect pieces of information that can supply a path for a terrorist. This problem has become so large that on August 6<sup>th</sup>, 2006, the Secretary of Defense published a mandate to all of DOD that no information can be placed on websites that are readily accessible to the public, unless it has been reviewed for security concerns and by trained OPSEC personnel.

USDA must take extra precautions to protect industry information, trade secrets, investigations, relationships with our partners, and future developments, such as food security, crop protection, and animal safety. If you would like to know more about the security requirements in contracting and the protection of unclassified but sensitive information, please call the Information Security Staff at 202-720-7373.

# HSPD-12

## newsflash

### NEW USDA EMPLOYEE/CONTRACTOR IDENTIFICATION CARD COMING SOON!

In the wake of 9/11, President George W. Bush issued Homeland Security Presidential Directive 12, commonly referred to as **HSPD-12**, in response to the increasing need to ensure we know, with certainty, who is accessing our Federal buildings and computer systems. This directive called for establishment of a common identification standard for all Federal employees and contractors.

The most visible result of this directive is a **new common identification card** for the Federal government. The replacement of current identification badges will be rolled out in phases. Initial production of the new ID card begins in late October 2006 in Washington DC, Atlanta, New York, and Seattle, where a shared service provider under contract to GSA will produce the cards. A large-scale roll out begins in January 2007. It will take approximately 2 years for the new ID card to reach everyone in USDA.

***USDA is naming its card the “Lincpass,” in honor of President Abraham Lincoln, founder of the Department of Agriculture.***

The new identification card contains robust security features, is tightly controlled, is resistant to fraudulent reproduction, will be recognized across the government, and requires a stringent process for issuance. Rigorous federal standards have been developed to describe what the card looks like, what personal information it contains, and how it will be used.

Initially, the card will be used for visual identification. In the near future, you will be able to use the cards electronically to gain access to federal buildings and computer systems.

For more information visit <http://lincpass.usda.gov>. From there, you will need to **login** with your **eAuthentication Level Two** login and password to access the full details regarding implementation of HSPD-12 at USDA.



# HSPD-12

## newsflash

### WHAT DO ALL OF THESE HSPD-12 TERMS MEAN?

In the wake of 9/11 and in response to the increasing need to ensure that we identify, with certainty, who is working for our government and accessing our Federal buildings and computer systems, President George W. Bush issued Homeland Security Presidential Directive 12, commonly referred to as **HSPD-12**. This directive called for establishment of a common identification standard for all Federal employees and contractors.

Below you will find a list of terms and definitions to help increase your understanding of HSPD-12 terms.

**PIV:** Personal Identity Verification. PIV is a process developed by the National Institute for Standards and Technology (NIST). PIV outlines a standard procedure that all Federal Departments and Agencies must follow to confirm the identities of its employees and contractors before issuance of a credential (identification badge). The PIV process was divided into two parts (PIV I and PIV II) to help all Federal agencies meet the deadlines for compliance.

**PIV I:** Personal Identity Verification Phase I standardized the processes used by Federal Departments and Agencies in issuing existing ID badges to its employees and contractors, but allowed for issuance of existing credentials using existing methods. The process requires sponsorship of an applicant, separation of duties for those sponsoring from those issuing the ID cards, and a standardized list of acceptable documents an applicant can provide as proof of identity. Applicants must also undergo or already possess a successfully adjudicated minimal background investigation. Departments and Agencies began using this new process to issue ID badges on October 27, 2005.

**PIV II:** PIV II takes PIV I a step further and requires issuance of a common identification card, using the process developed in PIV I. PIV II requires a significant technology infrastructure to support issuance of the new cards. The standards for the system were also developed by NIST. Departments and Agencies are required to have their own HSPD-12 systems operating, or to sign up with a HSPD-12 Shared Service provider, by October 27, 2006.

**FIPS 201:** Federal Information Processing Standards #201-1, entitled “Personal Identity Verification of Federal Employees and Contractors.” This document contains the detailed standards for the PIV process, the system, and the specifications for the resultant identification card. Read it at [www.hspd12.usda.gov](http://www.hspd12.usda.gov)

**GSA SSS:** General Services Administration (GSA) Shared Service Solution (SSS). Departments and Federal Agencies have the option to either develop the required HSPD-12 system solely for their own use, or to join one central system that can be shared by multiple agencies. GSA has developed a comprehensive Solution to serve the needs of small and large agencies, in which USDA has chosen to participate. Choosing this option allows agencies to consolidate the system’s technological components and reduce operating, implementation, and management costs.

**PIV Card:** The generic name for a common identification card that is produced by the HSPD-12 system. Departments and Agencies have the option to further brand the PIV card to make it more relevant and recognizable to employees and contractors. USDA has branded its PIV card the “LincPass.” A well-known example of PIV card branding is the Department of Defense’s “Common Access Card”, known as the CAC throughout the military.

**LincPass:** USDA branded its PIV card the “LincPass”. The unique spelling of LincPass is in honor of President Abraham Lincoln, founder of the Department of Agriculture. The card “links” your personal identity to the card and to your ability to access Federal buildings and computer systems with the card. The LincPass meets all FIPS 201 standards, is produced by GSA’s Shared Service Solution, will include USDA’s name and logo, and is used for access by USDA employees and contractors.

For more detailed information visit <http://lincpass.usda.gov>. You will need to **login** with your **eAuthentication Level Two** User ID and password to access the full details regarding implementation of HSPD-12 at USDA. To confirm eAuthentication access level and account information, visit <http://www.eauth.egov.usda.gov>.



## Security Education Training and Awareness (SETA)

For the month of September, the Defense Security Service Security Awareness Spotlight focused on **the Classified Non-disclosure Agreement** (SF-312).

You can view the video at <http://www.dss.mil/bnews/200>



## RECIPROCAL RECOGNITION OF SECURITY CLEARANCES

On July 17, 2006, the Deputy Director for Management for the Office of Management and Budget released a revision to the December 12, 2005 memo entitled, *Reciprocal Recognition of Existing Personnel Security Clearances*. You can view this memo at <http://www.archives.gov/isoo/pdf/update-omb-reciprocity-memo.pdf>.

### Reinvestigation Taskings for FY07

Recently, each agency Mission Area was mailed a packet to begin tasking those employees who are due or overdue for a reinvestigation. Agencies are reminded that those individuals identified as being more than 2 years past due for a periodic reinvestigation have until January 1<sup>st</sup> to submit new investigation requests. PDSB will cancel clearances that are no longer valid, e.g. out-of-date investigations.

### Contact Directory Changes

Please send all staff updates (Mission Area Personnel Officer and Agency Points-of-Contact) to Shemeka Lee at [shemekac.lee@usda.gov](mailto:shemekac.lee@usda.gov) to ensure you are included in PDSB distributions.