

# *pdsd*newsLETTER

Spring 2011

*what you'll find in this issue >*

## **SPRING CLEANING DONE RIGHT**

Handle with care. We'll show you how.

## **PDS&D BULLETIN #11-03**

Redating forms? STOP! We'll explain why.

## **IT'S TAX TIME**

Government employees, listen up.

## **FINANCIAL RESPONSIBILITY**

Foreclosures and your credit report.

## **RECIPROCITY & CVS**

"Please call" reminders.

## **IT IS OUR PLEASURE TO WELCOME...**

Our new PDS&D Chief!

## **RANDOM TIDBITS**

e-QIP Attachments; e-Verify Self Check; AD-1188 & SCI

## **SMARTPHONE THREATS**



## SPRINGTime.CoURsEs

SF86 2010

<http://www.opm.gov/investigate/events/form86event.aspx>

April 12

April 13

April 14

FREE

Web-based e-QIP Training from OPM  
<http://www.opm.gov/investigate/training/eqip/index.aspx>

# FINANCIAL RESPONSIBILITY. Focus on Foreclosures.

**L**enders filed a record 3.8 million foreclosures in 2010, up 2% from 2009 and an increase of 23% from 2008 according to Realty Trac. This year could be worse, with an expected 4 million foreclosures being filed. Millions of foreclosures will undoubtedly affect some USDA employees who are undergoing a Public Trust or National Security Investigation. A critical component of any background investigation is a check of the individuals Credit Bureau Report (CBR). Once the foreclosure process is initiated by the lender, the foreclosure is reported to the credit reporting bureaus and they update the individuals CBR to reflect "foreclosure initiated."

Personnel Security Specialists with the USDA Personnel Security Branch (PSB) will contact the subject of investigation to obtain additional information in these instances to determine 1) what the circumstances were that led to the foreclosure, 2) what steps are being taken to resolve the issue, and 3) has there been a pattern of financial irresponsibility. Any requests for information generated by the PSB regarding delinquent mortgages should be answered with very specific information showing the subject's actions and intentions taken to satisfy the debt.

Options for individuals facing foreclosure can opt for a Short Sale (an agreement with a lender to sell a home at a lower price of the mortgage balance, resulting in the bank accepting less than what is owed) or a loan modification (may receive a lower mortgage interest rate, a longer period to pay back a loan, or possibly some loan forgiveness). Another option available is a deed-in-lieu of foreclosure (when the home is given back to the lender, one takes their losses and thereby prevents the foreclosure). The deed-in-lieu of foreclosure is a faster solution than a short sale in that it is more likely to be accepted by the lender. The downside of the deed-in-lieu of foreclosure is if the lender sells the home for a price that doesn't pay off the original loan amount; the lender can get a deficiency judgment for the difference and try to collect it from you. About 1/3 of the states prohibit or limit banks from suing borrowers for a deficiency judgment for walking away from their mortgages. Those states are also known as nonrecourse states.

Having problems with a mortgage? Visit the Federal Trade Commission at <http://www.ftc.gov/bcp/edu/pubs/consumer/homes/rea04.shtm> or the new site for strapped homeowners launched by the Obama administration at <http://www.makinghomeaffordable.gov/>.

Everyone is encouraged to monitor their credit report and dispute any errors. Employees can obtain a free credit report [www.annualcreditreport.com](http://www.annualcreditreport.com). Reports can be requested once every 12 months from each of the nationwide consumer credit reporting companies: Equifax, Experian and TransUnion.

# Spring clean. *With Care.*

## **BEFORE YOU TOSS THOSE PAPERS, LISTEN UP!**

Now is a great time to do a little office cleanup. Get organized, finish some lingering filing, and purge inactive files. Before you toss, consider what is on those documents.

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

In accordance with the Employee Responsibilities and Conduct Department Regulation, 4070-735-001, every employee who has access to personally identifiable information (PII) of other employees, contractors, or the general public through the course of his or her employment at USDA is required to safeguard and protect such information from unauthorized disclosure.

PII is –any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Personnel records must be stored in metal filing cabinets which are locked when the records are not in use, or in a secured room.

Disposal and destruction of personnel records shall be in accordance with the General Record Schedule issued by the General Services Administration. Personnel Security Folders (PSF) at USDA are maintained for up to five years following the last day of employment. For more information, see PDSB Bulletin #09-05 at [http://www.dm.usda.gov/ohsec/pdsd/bulletin\\_history09.htm](http://www.dm.usda.gov/ohsec/pdsd/bulletin_history09.htm).

Shred sensitive information to ensure the data or record is unreadable and unrecoverable. Sensitive information and/or documentation containing PII must never be placed in the trash or in a recycling bin.

# It's Tax Time.

## **TAX PAYERS HAVE UNTIL APRIL 18<sup>th</sup> TO FILE THEIR TAX RETURNS.**

Executive Order 12674, as amended by Executive Order 12731, titled "The Fourteen Principles of Ethical Conduct for Federal Employees" requires that "Employees shall satisfy in good faith their obligations as citizens, including all financial obligations, especially those - such as Federal, State, or local taxes - that are imposed by law."

USDA is committed to ensuring that its employees continue to uphold the high standards of conduct expected of public servants.

Rates of delinquency for USDA employees are well below the average rate for all federal employees and have continued to decline. In an effort to further reduce the delinquency rate, we are reminding employees of their obligation to comply with federal tax laws.

Assistance in filing returns or in resolving any balance owed is available from the IRS at 1-800-829-1040. Forms, publications and additional information are also available on the IRS website at [www.irs.gov](http://www.irs.gov).

HR 4735 was introduced in March 2011 that would make an individual who has a seriously delinquent tax debt ineligible for appointment, or to continue serving as a federal employee.

<http://www.govtrack.us/congress/billtext.xpd?bill=11-4735>





# PDSD Team Building Day





## NEW PDSD CHIEF!

We are pleased to welcome Augustin “Augie” Larraga as the new Chief of PDSD as of April 11<sup>th</sup>! Augie joins us from the Washington Headquarters Services FSD/BRAC with approximately 25 years of security experience to include:

Serving as the Chief Security Officer for the FBI Denver Field Office.

Serving as the Director of Security, Army Space Command, Peterson Air Force Base, Colorado.

Serving as Security Manager, NORAD/USNORTHCOM, Peterson Air Force Base, Colorado.

Navy Officer, United States Navy, 24 years of service.

Augie replaces former Acting Chief of PDSD, John Loveless, who has moved on to Customs and Border Protection (CBP) with DHS.

# PDSD Bulletin 11-03: FIPC 391

On April 4, 2011, PDSD released its latest bulletin, #11-03, regarding the discontinuation of using FIPC 391’s on Public Trust and National Security requests at USDA. The FIPC 391, *Certification of Amended Investigation Form*, has been used by the Submitting Office Number (SON) to amend certain areas of the hard-copy questionnaires with the applicant’s intent and approval if the applicant was unable to personally make the necessary changes. It has also been used for date changes on the signature pages of the Electronic Questionnaires for Investigations Processing (e-QIP) forms; however, OPM tracks the initiation timeframe starting from the date the subject certifies their form in e-QIP (see the date/time shown on the CER Signature Form page). Therefore, using the FIPC 391 for the sole purpose of re-dating release pages is irrelevant.

### DATE CERTIFIED + REC’D BY OPM = FORM TIMELINESS

USDA is submitting 100% of all background investigation requests to the Office of Personnel Management (OPM) via e-QIP. In e-QIP, any corrections that are needed on questionnaires before they are released to OPM should be completed by the subject (rejected back via e-QIP) and therefore, the FIPC 391 is not a factor.

The only instance where the FIPC 391 should be utilized is to make corrections to a form that has been submitted to OPM after an OPM Correction Tech has requested additional information. For example, the subject did not initial a scratch-out/cross-out on a release form.

The intention of OPM in the future is to phase out the use of the FIPC 391 all together.

PDSD must submit all National Security requests to OPM within 14 calendar days; therefore, PDSD requests all agencies to submit their National Security requests to us in approximately 7 days to allow for processing time on our end. We recommend each agency prioritize their workload by processing all National Security requests in e-QIP first and utilize electronic fingerprint methods when possible (attaching the results to the submission package). When possible, obtain the fingerprint charts before initiating the employee so that there is no delay. IRTPA does not apply to Public Trust positions.

If you have any questions, please contact Carrie Moore, Acting Chief, Personnel Security Branch, at [carrie.moore@dm.usda.gov](mailto:carrie.moore@dm.usda.gov).

# Reciprocity and “Please Call” Reminders

Agency points-of-contact are reminded that prior to submitting an individual for a new background investigation, it is required that CVS be verified to ensure that the Subject does not have a previous background investigation that can be transferred via reciprocity to USDA.

If it is determined that the Subject has a previous investigation that meets all requirements (appropriate investigation type, form type, etc.), please ensure that the investigation was favorably adjudicated and that there are no please call indicators or other negative actions shown on the CVS record. If a “please call” notification is marked on an individual’s record, this cannot be ignored. The Agency POC must contact the provided information to verify the nature of the please call. **Note:** any action taken by an agency from the 79A with a response of 4 through 11 will automatically generate a “please call” indicator in CVS. This is why it is extremely important for the Agency POC to call and verify the information with the previous entity. A recent example that PDSD received involved a “please call” indicator that was not followed up on until the PDSD adjudicator contacted the agency upon receiving the reciprocity request. It was discovered that the case was never favorably adjudicated and that the individual had a previous security clearance revoked.

An agency POC should verify this information before submitting the reciprocity package to PDSD for action, thus saving working hours and aiding to the overall efficiency of service.

# Random TIDBITS

## EMPLOYEE SIGNATURES ON THE AD-1188

If you are submitting an initial request for access to Sensitive Compartmented Information (SCI), the employee must sign the Justification form (AD-1188) or the approval will not be processed. For questions concerning SCI requests, contact Valerie Ramirez at [valerie.ramirez@dm.usda.gov](mailto:valerie.ramirez@dm.usda.gov).

## e-VERIFY SELF CHECK

E-Verify Self Check is a voluntary, fast, free and simple service that allows an individual to check their own employment eligibility in the United States. USCIS is releasing the E-Verify Self Check service in phases. At this point the service is offered only to users that maintain an address and are physically located in Arizona, Colorado, the District of Columbia, Idaho, Mississippi, or Virginia. For more info, visit: <https://selfcheck.uscis.gov/SelfCheckUI/>.

## e-QIP: REVIEWING ATTACHMENTS

PDSD has had an influx of correction calls from OPM regarding e-QIP submissions submitted by our agency involving attachments. The attachments specifically (signature pages, OF-306 (Declaration of Federal Employment), resumes, etc.) have been the subject of most correction calls. This is due in part because there is no system validation capability for the attachments.

If all information is not included on the attachments, OPM will call PDSD for corrections. A recent example occurred when a Subject answered “yes” to one of the employment questions on the OF-306 and complete information was not provided as directed on the form (dates, address, etc). *Please note that OPM e-QIP processors will not take information from the security questionnaire to use in other areas of the submission package.* For example, on the aforementioned OF-306 issue, the information was on the security form, but OPM did not take that information and place it on the OF-306, rather PDSD had to provide it separately.

Please ensure that all attachments are reviewed closely and that if a Subject answers “yes” to a question on the OF-306, they complete the additional response needed in space provided on the second or back page. Likewise, please ensure signature pages are free of errors to include cross-outs and that the numbers are clearly legible. We have had similar problems where due to a Subject’s handwriting style, OPM has had difficulty distinguishing between digits on date of birth or social security number for example. For questions regarding e-QIP, please contact Lucy Lew at [lucy.lew@dm.usda.gov](mailto:lucy.lew@dm.usda.gov).



## SMARTPHONE THREATS

Smartphone's are vulnerable to identity theft, spying and fraud. Your phone holds an increasing amount of personal data on you. Researchers at getsafeonline.org have found that 67% of Smartphone holders do not have a password to lock their phones. That is a big NO NO. Just like your computer, you should have a password to be able to access your cell phone.

Touch screens are open to what they call "Smudge Attacks". The screens pick up all oils especially when putting in passwords, pins, or bank information. Ways of protecting yourself is start using screen cleaning wet wipes.

There are a number of ways that you can be a victim, but the most common way is through downloadable applications. Iphones do pre-screen their applications before giving the public access to them. The Android Market has no pre-screening process.

There is also another issue you should be aware of and that is GeoTags. Most people aren't aware of the security threats that GeoTags can cause to you and your family's privacy. When pictures are taken with your smartphone, it is more than just a picture; it is adding geo tags that show where you are at that exact time the picture is taken. It makes it easier for people to know when you are out, when no one is at home, and where you spend most of your time. Protect yourself by disabling your GPS feature on your phone while taking pictures. That will eliminate the Geo Tags being adding onto the pictures while using your smartphone.

# MALWARE

## TOP FIVE MOBILE MALWARES

- Android - DroidDream - the most recent and most advanced piece of malware hit apps and allowed product ID and userID from phones to be transmitted to remote server
- Android - Market Security Tool - the update sent to wipe rogue Android apps has already been hacked and injected with malware. Being distributed via 3rd party app stores in China.
- Zeus-in-the-mobile - a trojan working with the Windows virus Zeus, affecting Symbian and Blackberry handsets and aiming to steal online banking details.
- Android - Geinimi - similar to the market app attack, it took official apps, added malware and released them via Asian app markets. Could send SMSs, harvest phone data and make phone calls.
- Android - ADRD - another trojan that pirated official Android apps.

*Source: BullGuard*

## webSETS: Entry on Duty

The Entry on Duty (EOD) screen in the web-based Security Entry Tracking System (webSETS) is used by HR offices to track actions on Low Risk positions, such as NACI's, and to track Advance Fingerprint actions.

It is important for tracking and reporting purposes that all of the fields are updated appropriately, to include the "Employee Tasked" field (date the subject of investigation was initiated in e-QIP), the "Investigation Adjudicated" field (date the closed investigation was adjudicated), and the "Adjudication Decision" field (select the "Approved" or "Denied" button).

Incomplete records will result in inaccurate reports, especially those used to determine who has not been initiated for an investigation.

For questions regarding webSETS, refer to the user guide at <http://i2i.nfc.usda.gov/Publications/SETS/SETS.pdf> or contact Carrie Moore at [carrie.moore@dm.usda.gov](mailto:carrie.moore@dm.usda.gov).

## CONTACT US!

1400 Independence Ave, SW • RM S-310 • Washington, DC 20250-5050  
(202) 720-7373 • (202) 720-1689 (fax) • [pdsd@dm.usda.gov](mailto:pdsd@dm.usda.gov)