

SUMMER

2006

P D S D



## Personnel & Document Security Division

USDA/DA/OPPM/PDSD

# Thank you Marty Brumback!

After over 31 years of service at USDA, Marty Brumback, Chief of PDSD, is retiring at the end of July.

They say that no company ever employs a good man - they just borrow him for a couple of years in his life before he moves on to better and more enjoyable things. USDA was lucky enough to have Marty Brumback for over 31 years! It is with heartfelt appreciation and sadness that we bid farewell to our Chief, Marty Brumback, as he retires on July 30<sup>th</sup> after nearly 32 years of federal service.

After beginning his career as an investigator with the former U.S. Civil Service Commission, Marty transitioned to a career with USDA in the employee relations field. Marty's pre-PDSD career included various specialized positions in the Office of Personnel, Agricultural Marketing Service, Economics Management Staff, and Agricultural Research Service as he developed an in-depth knowledge of human resources.

Marty brought his wealth of experience to what is now the PDSD in November 2001 and led a revitalization of the personnel and information security programs in USDA, resulting in receipt of the Office of Personnel Management's prestigious Guardian Award in November 2002 for "commitment and excellence in safeguarding National Security and Public Trust."

His noteworthy accomplishments include the modernization of the personnel security database, implementation of the e-Clearance initiative across USDA, oversight of USDA's original classification authority, and development of an information security regulation and manual. Marty's most important and lasting achievement has been the leadership and knowledge he has imparted over the past 18 months as an integral member of the advisory group tasked with implementing



Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors.

His institutional knowledge of USDA and his tireless work ethic have been invaluable to the HSPD 12 effort, and will ensure that USDA implements this important security initiative in a common-sense, cost effective manner. Marty, we anticipate you will devote the same diligence and enthusiasm to your future retirement activities and we wish you joy and peace as you transition to a new chapter in your life. Farewell and happy trails, boss!

HSPD-12 TOWN HALL MEETING...PAGE 2

JUST HOW SAFE IS YOUR HOTEL INTERNET ACCESS?...PAGE 3

THE LATEST IN E-QIP ...PAGE 4

EXECUTIVE ORDER 13381 EXTENDED ...PAGE 5

*Our decisions affect national security...can we afford to be wrong?*



## OPM Reiterates Its Commitment to Processing Security Clearances

The U.S. Office of Personnel Management (OPM) told the House and the Senate on May 17, 2006 of the considerable progress OPM is making in enhancing the speed and reducing the backlog of Federal personnel security investigations. Kathy Dillaman, Associate Director of OPM's Federal Investigative Services Division, stated "In 2006 alone, we expect to process more than 1.7 million investigations. Thanks to the cooperation of Federal agencies and advancements in technology, we are making great strides in improving the timeliness of investigations and reducing our caseload."

Dillaman said OPM and the major clearance granting agencies have made steady progress in meeting the four main requirements of OPM's background investigation performance improvement plan. The four requirements are improving accuracy of workload projections, enhancing timeliness and quality of agency investigations requests, enhancing timeliness of investigations, and enhancing timeliness of adjudications. Dillaman cautioned Congress about a rising inventory of pending investigations due to access problems involving third-party record information by stating, "Investigations cannot be closed without such information, and we continue to experience significant delays in obtaining information from Federal, State, and local record systems."

## HSPD-12 TOWN HALL MEETING

The USDA HSPD-12 Program Team will host the 2<sup>nd</sup> USDA HSPD-12 Town Hall session.

The session will be held in Washington, DC, at the South Building, Jefferson Auditorium, from 9:00 am to 3:30 pm on Thursday July 27th. An agenda will be distributed in the coming weeks, so check the HSPD 12 website at <http://hspd12.usda.gov/>.

Persons interested in attending should RSVP to [egov@usda.gov](mailto:egov@usda.gov) and put in the subject line: "RSVP HSPD-12 Town Hall."

The purpose of the HSPD-12 Town Hall session is to facilitate a coordinated and collaborative effort on the HSPD-12 implementation at USDA by bringing together the key stakeholders who are collectively responsible for ensuring the Department's compliance with the HSPD-12 directive. There will be the opportunity for the Agency HSPD-12 teams to ask questions and raise issues or concerns.

All persons with a role in implementing HSPD 12 in their agency are encouraged to attend.

July 27th

9am-3:30pm

A

B

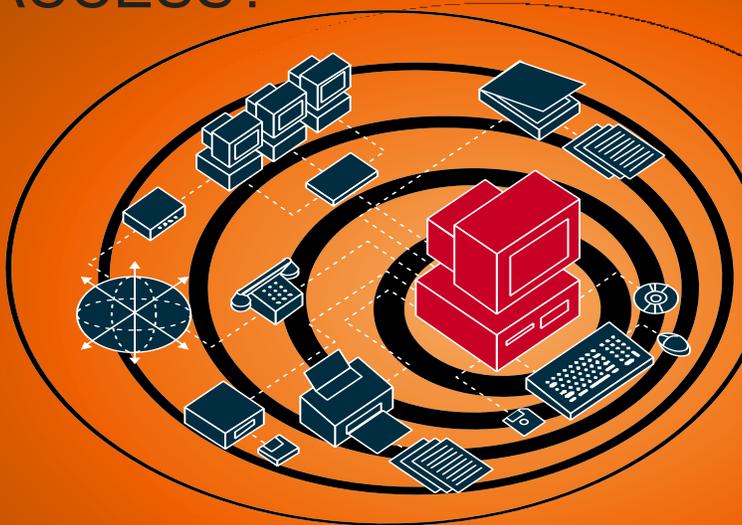
C

SCI stands for Sensitive Compartmented Information.

## of Requesting Access to SCI

- A.** Submit a 'Request for Personnel Security Services' form and a Justification form. Ensure the 'Justification' form clearly answers the SCI related questions on page 2 (Instructions) to include what compartments are required and the request is authorized by a Senior Executive Service (SES) employee.
- B.** The employee's background investigation must be current (completed within 5 years). If the investigation is not current, request an updated investigation. An SSBI is required for initial TS/SCI requests and SSBI-PR for reinvestigations.
- C.** The employee's Standard Form (SF) 86 questionnaire **MUST be completed and signed by the employee within 2 years**. If the employee has not completed an SF-86 within 2 years, an updated form **MUST** be submitted with the 'Request for Personnel Security Services' form.

# JUST HOW SAFE IS YOUR HOTEL INTERNET ACCESS?



## CELLULAR PHONE VULNERABILITY

Your Cellular Phone has three Major Vulnerabilities:

1. *Vulnerability to monitoring of your conversations while using the phone.*
2. *Vulnerability of your phone being turned into a microphone to monitor conversations in the vicinity of your phone while the phone is inactive or turned off.*
3. *Vulnerability of "cloning" or the use of your phone number by others to make calls that are charged to your account.*

Remember that your cell phone is a radio transceiver. Your voice is transmitted through the air on radio waves. The safest way to avoid your phone from being turned on remotely and used as a listening device is to remove the battery before any sensitive or classified discussions take place in the room. Do not talk around sensitive or classified subjects. Eavesdroppers targeting your number may eventually derive a conclusion and determine your subject and issues. Cloning is the process whereby a thief intercepts the electronic serial number and mobile identification number and programs those numbers into another telephone to make it identical to yours. Cloning resulted in approximately \$650 million dollars worth of fraudulent phone calls in 1996. Police made 800 arrests that year for this offense. Cloning occurs most frequently in areas of high cell phone usage – valet parking lots, airports, shopping malls, concert halls, sports stadiums, and high traffic areas. Do not leave your phone unattended. Use them sparingly and never discuss sensitive and classified information on a cell phone. Always review your cell phone bill carefully to identify cloning early.

Source: Air Force Special Security Office Courier Newsletter, Fall 2005

Worldwide business travel is inevitable in order to accomplish the business of USDA. Aside from receiving foreign travel briefings for safe travel, our personnel must be reminded of the continuing technological threat. Since many travelers carry laptops with them, some may choose to use their in-room television Internet access. However, it's more appealing to use your wireless keyboard from the comfort of your bed or couch. Not a bad idea in the eyes of the hotel industry; however, for security some issues must be addressed to raise your awareness.

Many hotels offer this unique Internet access service through in-room television sets and provide a wireless keyboard so their guests can surf the web, pay bills, or check email while in their pajamas. Through a series of studies, these networks have been found to put your personal protection and identity at risk of theft. Researchers have release reports citing these networks are often poorly configured and allow for uncontrolled accessibility with minimal effort.

Through a few simple steps one particular researcher was able to "subvert the TV system in the hotel to the point where you can do things, such as, identify who else is staying in the hotel by viewing their folios, and furthermore, by tricking the TV in the room into believing it was in another room." (Piazza) For most, this may not seem to be a big threat because the only things they have disclosed on their folios are hotel expenses. What they don't realize is this is minor compared to what these potential information perpetrators can do. More severe may be, watch you type an email, pay bills, or conduct other online activities without your knowledge. Even more amazing it that "it didn't take any serious hardware or software for (the researcher) to discover or exploit these weaknesses." (Piazza). As simple as it sounds, all that is required is the built-in infrared transmitter that most laptops have and a piece of software for Linux that is available through a multitude of open sources.

Some hotels have a data line you can connect your laptop to which gives you internet access and the capability of answering your emails. Beware of these also! The hotel has a server set up in which all the data flows through before it goes to the email recipient. The server can be collecting and saving the information before sending out.

The good news is these security deficiencies have been addressed and many hotel Internet systems have already installed systems that block this type of probing. While some may have these new systems, some may still be vulnerable to this unlawful snooping. There isn't a real answer to the issue of using the hotel data line.

The safest practice is to not answer sensitive emails from a hotel or use encryption software to better protect your information.

Sources: Piazza, Peter Arming the Road Warrior, Security Management, January 2006, pg. 81, and the Air Force Special Security Office Courier Newsletter, Winter 2006

## e-QIP Version 2.0 Debuts!

OPM unveiled use of the e-QIP 2.0 version on Wednesday, July 5<sup>th</sup>. The long-awaited enhancement to the e-QIP program has been fully tested and is available for use by all current e-QIP users. The newest version features several significant changes including, single screen navigation, templates for the Agency Use Block, communication tools, easier administration, a new Help Desk role, and improved reporting. Early feedback from recently trained agency e-QIP users has been very positive and it is anticipated that the enhancements will allow for faster processing of investigative forms and improved workload management. If you have any questions about the e-QIP 2.0 version, please contact Vet Thorpe at (202) 720-4390.

# THE LATEST IN e-QIP

Subject's certification and release pages must be uploaded in e-QIP 2.0 because the system will not allow you to release the form to PDS unless pages are uploaded. Signature page dates may be changed using a FIPC 391 upon contacting the Subject of investigation and letting him/her know that you are changing the date; draw a single line through the current date and put a new date, then your agency's SON, your initials and date. Keeping an eye on the date subject signs the form and taking the appropriate action will enable PDS to meet OMB's timeliness goal of 14 days.

## USDA e-QIP USAGE MEETS 100% PARTICIPATION GOAL

The PDS met an important Office of Management and Budget (OMB) goal of submitting all national security investigative requests electronically via the Office of Personnel Management's Electronic Questionnaires for Investigations Processing (e-QIP) system in May 2006, which was up from 98% in the 2<sup>nd</sup> Quarter of Fiscal Year 2006.

In addition, our rate of deficient submissions was 3%, which also exceeded OMB's goal of having 5% or fewer forms submitted with deficiencies. PDS continues to strive to meet the timeliness goal submitting e-QIP forms within 14 days of subject's signature on the release pages. We have reduced our average number of days by half from the 2<sup>nd</sup> Quarter, but it remained at 33 days on average for May 2006.

## e-QIP Training Provided to USDA Agencies

Arviet Thorpe of the PDS staff presented hands-on training related to the e-QIP program in Minneapolis, MN in May 2006. Attendees included security and human resources personnel from the Animal and Plant Health Inspection Service (APHIS) and the Food Safety and Inspection Service (FSIS). This training enhanced both agencies processing of background investigation forms and enables them to be among the first USDA agencies to pilot the program for use of the electronic Standard Form 85, "Questionnaire for Non-Sensitive Positions."

PDS has held four classroom-training sessions in May and June 2006 regarding use of e-QIP version 2.0. These sessions also included guidance for processing the SF-85, "Questionnaire for Nonsensitive Positions." Attendees included representatives from Agricultural Research Service, APHIS International Service, Departmental Administration, FSIS, Foreign Agricultural Service, Farm Service Agency, Food and Nutrition Service, Forest Service, National Finance Center,

Office of the Chief Financial Officer, Office of the Inspector General, Office of the Chief Information Officer, Office of the Secretary, Natural Resources Conservation Service, and Rural Development. This training is critical because the 2.0 version of e-QIP features important enhancements to the overall e-QIP navigational system, plus the SF-85 will be the primary security questionnaire used for identity proofing and conducting background investigations for the employees and contractors who will need a USDA biometric ID card to perform their work.

The PDS will offer two, one-day training sessions on September 6 and September 7, 2006. Each day will feature a session related to e-QIP and a session related to processing investigative forms. Persons interested in attending the training sessions should contact either Vet Thorpe or Susan Gulbranson on (202) 720-7373. Priority will be given to new Personnel Security Points of Contact, human resources personnel with responsibility for processing SF 85s, and persons who have not previously attended a similar training session.

Federal Agents from the Department of Homeland Security's Office of Inspector General arrested a Border Patrol agent on August 4, 2005 in Escondido, California who was suspected of being an illegal immigrant and smuggling other illegal immigrants into the United States. Assisting in the arrest were the Escondido police, the North County gang unit, and the U.S. Immigration and Customs Enforcement (ICE) agents.

The 28-year-old, Oscar Antonio Ortiz of San Diego, completed an application to work for the Border Patrol on October 31, 2001 and claimed he was born in Chicago, IL. On his application, he admitted to using drugs and being arrested on suspicion of smuggling. Ortiz previously served in the U.S. Navy and worked on navigational equipment on the attack ship Tarawa.

Ortiz was hired and assigned to the El Cajon field station located 35 miles east of San Diego. Ortiz and another Border Patrol agent became the targets of an undercover investigation after they were overheard on telephone conversations discussing the smuggling of migrants into the United States through a border area near Tecate. He stated he had smuggled several dozen people into the country and he had been paid fees ranging from \$300 to \$2,000 a person.

During his initial background investigation for employment, the Office of Personnel Management, which handles background checks for most federal agencies, could not verify his citizenship. When the results of his investigation were forwarded to INS, the adjudicator asked Ortiz to provide proof of his citizenship. Ortiz managed to produce a forged birth certificate and INS did not verify the document. A subsequent investigation resulting from the undercover investigation revealed Ortiz was a citizen of Mexico (born in Tijuana) and the birth certificate Ortiz presented actually belonged to another person who was born one month before him. Border Patrol agents are required to be U.S. citizens and they are required to carry firearms.

On January 27, 2006, Ortiz plead guilty in federal district court in San Diego to conspiring to bring in illegal aliens, making a false claim to United States citizenship, making a false statement in the acquisition of a firearm, and being an illegal alien in possession of a firearm. Ortiz admitted that he had brought in over 100 aliens into the United States. He was scheduled for sentencing on May 12, 2006 in San Diego, CA. Results of the sentencing have not been posted. Each charge carries a prison sentence between 3-10 years.

Because of this case, the Border Patrol has made changes to its employment background screening process. All prospective employees for the Border Patrol are now required to provide birth certificates, which are checked independently with the issuing agency or a database. This case highlights the importance of document verification, especially in positions of National Security.

Related Links:

[www.usdoj.gov/usao/cas/pr/cas60127.2.pdf](http://www.usdoj.gov/usao/cas/pr/cas60127.2.pdf)

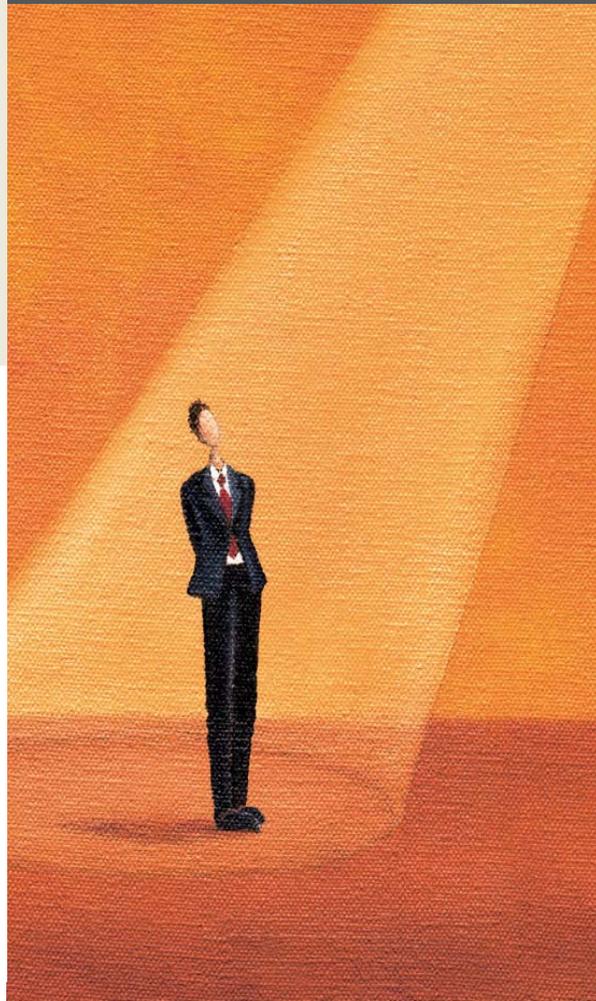
[www.nbcsandiego.com/print/4816916/detail.html](http://www.nbcsandiego.com/print/4816916/detail.html)

<http://washingtontimes.com/functions/print.php?StoryID=20051117-111242-2476r>

[www.nctimes.com/articles/2005/08/05/news/inland/21\\_17\\_498\\_4\\_05.prt](http://www.nctimes.com/articles/2005/08/05/news/inland/21_17_498_4_05.prt)



## THE IMPORTANCE OF PROPER INVESTIGATIONS



### Financial Considerations: Is your Government Travel Charge Card current?

The Department of Agriculture has a “Zero Tolerance Policy” on misuse and abuse of the travel charge card, as outlined in Departmental Regulation 2300-001, Government Travel Card Regulation.

Employees undergoing an investigation with USDA will be contacted if their credit report or agency reports any misuse or delinquent balance on their government issued charge card. It is the card holders responsibility to keep their account current and paid as agreed.



*nurture*

And reap the benefits.

## *Is your U.S. passport really valid?*

Planning on taking a trip abroad? Be sure to check that expiration date carefully! Some countries require that your U.S. passport is valid not only for the duration of your visit, but also for three to six months after your entry or return from their country. Here is a list of some countries that have special passport expiration rules:

**\*\*\*Passport must be valid for an additional six months**

Brazil  
Ecuador (including the Galapagos Islands)  
Indonesia  
Israel  
Malaysia  
Paraguay  
Romania  
Singapore

**\*\*\*Passport must be valid for an additional three months**

Cambodia  
Denmark (including Greenland)  
Fiji  
Switzerland

There are many others. Some countries count their expiration windows from the date of entry into their country, others from the scheduled departure date. For additional information, check the U.S. Department of State's listing of foreign entry requirements at

[http://travel.state.gov/travel/tips/brochures/brochures\\_1229.html](http://travel.state.gov/travel/tips/brochures/brochures_1229.html)

If you need to renew your passport, the State Department says to allow for six weeks for renewal. The turnaround times for passports is faster in the slower months of September and December. For an additional \$60, you can expedite the renewal process to two weeks.

New passport rules are scheduled to take effect for travel to and from the Caribbean, Bermuda, Panama, Mexico, and Canada. As of December 31, 2006, a passport or other secure documentation will be required for all AIR or SEA travel to or from Canada, Mexico, Central and South America, the Caribbean, and Bermuda. As of December 31, 2007, a passport or other secure documentation will be required for all LAND border crossings to or from these countries.

Holders of TS/SCI access are reminded to report ALL unofficial foreign travel to Carrie Moore, Senior Personnel Security Specialist at 202-720-3487 or [carrie.moore@usda.gov](mailto:carrie.moore@usda.gov). You will be asked to complete the "Foreign Travel Request" form (AD-1196) and you will be notified if a travel briefing, conducted by the State Department, is required.

# Executive Order 13381 extended

## STRENGTHENING PROCESSES RELATING TO DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED NATIONAL SECURITY INFORMATION

Executive Order 13381 was extended by President George W. Bush on June 29, 2006. The order was amended to extend its duration until July 1, 2007. E.O. 13381 states, "To the extent consistent with safeguarding the security of the United States and protecting classified national security information from unauthorized disclosure, agency functions relating to determining eligibility for access to classified national security information shall be appropriately uniform, centralized, efficient, effective, timely, and reciprocal." To view the entire order, go to <http://www.whitehouse.gov/news/releases/2005/06/20050628-4.html>.

## SF-85 Success Story!



Effective June 26, 2006, FSIS' Human Resources initiated the first USDA electronic SF-85, "Questionnaire for Non-sensitive Positions" using the e-QIP system. FSIS' use of the electronic SF-85 will enhance USDA's compliance with Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors. Other agencies that have been authorized to use the SF 85 include the National Finance Center, Office of Executive Resources, Office of the Chief Information Officer, and the Office of Inspector General. In the near future, the PDSO will rollout to other USDA agencies authority to use the SF-85, which will further enhance USDA's compliance with Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors. Full implementation of the e-QIP program improves the quality of investigative submissions, the timeliness of background investigations, reduces the length of time required to obtain a national security clearance, and complies with a portion of the Presidential e-Government initiative, e-Clearance.

### Notice to Industry

## Resumption of DoD Investigations

The Defense Security Service stopped accepting industry applications for all security clearance on April 28<sup>th</sup> due to lack of funding and the high volume of applications. This agency provides security support services to the Defense Department, federal government contractors, and other authorized parties. On May 16<sup>th</sup>, funding was identified to begin processing initial Secret requests immediately. Requests for initial Top Secret and reinvestigations are pending the receipt of additional funding.

Need to send a  
fax to the  
Personnel  
Security Branch?

Please use this fax  
number!  
**202/720-1689**

### CONTACT US!



1400 Independence Ave, SW, RM S-310  
Washington, DC 20250-9305  
202-720-7373 tel 202-720-1689 fax  
<http://www.usda.gov/da/pdsd/>  
[pdsd@usda.gov](mailto:pdsd@usda.gov)