



WINTER 2009 Edition

**INSIDE THIS ISSUE:**

SECURITY & SUITABILITY REFORM . . . . .	P2
DEBRIEFINGS: Q&A. . . . .	P3
POSITION DESIGNATION SYSTEM . . . . .	P3
RESPONSIBILITIES LETTER. . . . .	P4
WEBSITES ACCESS. . . . .	P4

# The *Personnel & Document Security Division* Newsletter

## Information Security during the Transition Period

Departmental Administration (DA)  
Office of Security Services (OSS)  
Personnel & Document Security Division (PDSD)

**Need Assistance? Call us!**  
**(202) 720-PDSD**

*The change in administration, along with the departure of political appointees within our offices, provides us with an opportunity to review our internal policies for the protection of Classified National Security Information (CNSI) and Sensitive Security Information (SSI). It should also remind us to review how we handle and store Personally Identifiable Information (PII).*

For those of us that utilize such information, we should review our internal handling and storage practices, and, review the amount of holdings we currently have on hand. This is a good time to:

- Appropriately destroy any unwanted or unnecessary files.
- Conduct a "Security Sweep" of our offices to make sure classified information has not been stored inappropriately. This includes checking all desks, credenzas, bookcases, coffee tables, filing cabinets and other furniture.
- Discovered CNSI/SSI/PII information from the sweep requires proper handling, retention and/or destruction.

Please reference DM 3440-001 for further guidance or contact our staff. We will be happy to assist you to conduct a sweep and discuss the current requirements within your offices for the protection of this information.

As a reminder, we should make sure that the new administration is appropriately cleared before they are provided access to CNSI information. The Personnel Document Security Division will coordinate with the Office of Executive Resources to ensure new Appointees are appropriately vetted and briefed prior to access.

For assistance in these activities, please contact our staff; Keith McElfresh, Chief, Information Security Staff, (202) 260-0106, [keith.mcelfresh@usda.gov](mailto:keith.mcelfresh@usda.gov), or, Karen Maguire, Information Security Specialist, (202) 720-5712, [Karen.maguire@usda.gov](mailto:Karen.maguire@usda.gov).



# Security & Suitability Process Reform

A report from the Joint Security and Suitability Reform Team, December 08

*The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) calls for 90% percent of security clearance determinations to be made in 60 days (investigations in 40 days and adjudications in 20 days) by December 2009.*

Since the enactment of IRTPA, average timeliness for 90 percent of all clearance determinations reported has been substantially improved, from 265 days (in 2005) to 82 days (4th Quarter, Fiscal Year (FY) 2008).

To further improve timeliness and achieve the IRTPA goal of 60 days or better, a transformed process for making hiring and clearing determinations has been designed, as first described in the Initial Report on Security and Suitability Process Reform, dated April 30, 2008.

The April 2008 Report recommended that an Executive Branch governance structure is needed to ensure the hiring and clearing processes are effectively coordinated across the government. The necessary structure is provided by Executive Order 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, which was signed on June 30, 2008.

In December 2008, the Director of National Intelligence and Director of the Office of Personnel Management approved revised Federal Investigative Standards to implement the transformed process design. The revised standards will be used for both hiring and clearing investigations and are a vital piece of the reform effort. They require the use of automation to the greatest extent practicable, both to speed processing and to permit use of new tools. Initial implementation plans will be complete no later than March 2009.

Electronic submission through e-QIP has led to improved processing times for all types of investigations and dramatically reduced the overall error and rejection rates for completed standard investigative forms. A more comprehensive suite of branching questions will be included in the next-generation of e-QIP, which is targeted for deployment in December 2009.

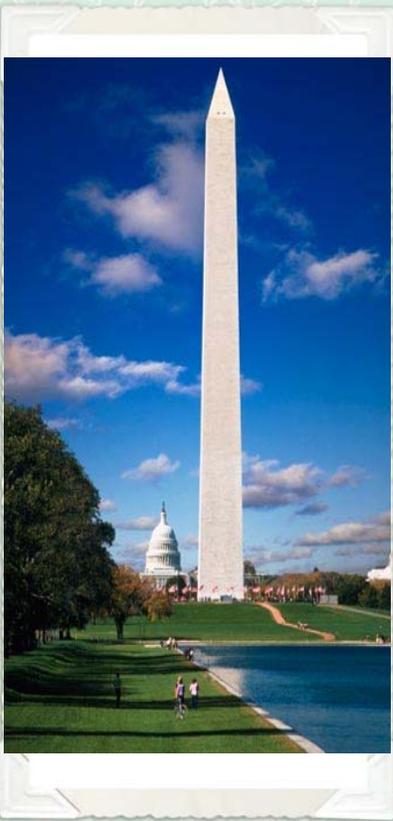
Today's technology enables the collection and processing of signatures through digital (unique codes generated in transmission) and electronic (captured using a pad and stylus) signatures. The use of these technologies on the application and electronic release authorizations, currently planned for February 2009, will eliminate the need for hardcopy submissions of signature pages.

An essential element of every investigation is the use of fingerprints to identify criminal history on record with the Federal Bureau of Investigation (FBI). A feasibility study assessing the use of existing and planned fingerprint scanning stations across the government to optimize the automation opportunities in processing investigative requests will be completed by February 2009.

Electronic adjudication (eAdjudication) is a viable technical means to automatically, electronically render hiring and clearing determinations in cases with no actionable issues. Approximately 25 percent of all Secret cases can be favorably eAdjudicated by applying computer coded business rules to the adjudicative decision process. Phased implementation is planned for clean case eAdjudication in DoD Industry, select DoD, and non-DoD, populations to improve timeliness and workflow between April 09 – Dec 09.

Continuous Evaluation (CE) includes an electronic review of scheduled updates of a subject's application information, Automated Record Checks (ARC), and an electronic assessment of the information acquired. The revised investigative standards replace the periodic reinvestigation model with CE annually for Tier Three (Top Secret or high risk positions) and at least once every five years for Tier Two (Secret, Confidential, or moderate risk positions).

To read the full report, visit <http://www.whitehouse.gov/omb/reports/>.



OSS/PDSD  
1400 Independence Ave, SW  
RM S-310  
Washington, DC 20250

(202) 720-7373  
(202) 720-1689 fax  
pdsd@usda.gov

## POSITION DESIGNATION SYSTEM

Recently, by memorandum from Acting Director Michael W. Hager, the Office of Personnel Management (OPM) introduced the new **Position Designation System (PDS)** and the **Automated Tool for Position Designation of National Security and Public Trust Positions** (Automated Tool).

Guidance for position designation has been provided in the Suitability Processing Handbook (SPH), and the SPH will be updated to reflect the new PDS. In the meantime, distribution of the PDS and the Automated Tool will be through OPM's Secure Portal.

As the head of security for USDA, and OPM's contact point in these matters, PDSD will be the custodian of the PDS and the Automated Tool. It will be our responsibility to limit the dissemination of the PDS and Automated Tool to those persons who require it due to their personnel security and/or suitability-related duties and/or those charged with position designation duties.

A separate notice will be sent out by PDSD to each mission area to designate their users in January 2009.



## DEBRIEFINGS:

### Frequently Asked Questions

Answers for departing Political Appointees, Senior Executive Service Personnel, and other departing USDA personnel who hold a security clearance.

**Question: How long does a security clearance remain in effect?**

**Answer:** Only as long as you are employed with USDA in a position that requires a security clearance and you have complied with any periodic reinvestigation requirement if appropriate.

**Question: When is a clearance terminated?**

**Answer:** A clearance is terminated when a person **permanently leaves a position at USDA for which the clearance was granted**. By federal regulation, upon your departure from USDA you are required to receive a security debriefing. Unless you are to remain employed with USDA as a Consultant or Volunteer (with an established agreement), you cannot carry the security clearance with you when you leave USDA.

**Question: Can a clearance be reinstated after it has been terminated?**

**Answer:** Yes. If you take a job requiring a security clearance within two years of departing USDA, the new employer may reinstate your clearance. If more than two years have passed, you will most likely be required to update the security forms for a periodic reinvestigation before a new clearance is granted.

**Question: I was hoping to take my security clearance with me upon my departure from USDA to make it easier to continue working. Is this permissible?**

**Answer:** No. Once you are no longer employed with USDA you no longer have an "active" security clearance and cannot access classified information. The clearance would have to be reinstated by another entity before you could have access to classified information. Please have your gaining security office contact the Personnel and Document Security Division (PDSD) at (202) 720-7373 or [pdsd@usda.gov](mailto:pdsd@usda.gov) and your prior clearance information will be verified on USDA letterhead.

**Question: If I decide not to receive a security debriefing upon my departure can I maintain my security clearance?**

**Answer:** No. As soon as PDSD is notified that an employee has departed without receiving a security debriefing, the security clearance is automatically "administratively withdrawn" and the security clearance is no longer valid.

We hope this answers your questions. You may contact the Personnel and Document Security Division for additional information if necessary at 202-720-7373.

# "Responsibilities Letter"

updated December 17, 2008



TO: ALL USDA EMPLOYEES WITH ACCESS TO CLASSIFIED INFORMATION

FROM: Susan Gulbranson Chief  DEC 17 2008

SUBJECT: Responsibilities of Employees Cleared for Access to Classified Information

When you signed your non-disclosure agreement, you were accepting responsibility for properly safeguarding classified information affecting the national security, military, economic, and/or foreign relation interests of the United States. Such access is an important responsibility and you must take every precaution against the unauthorized disclosure of any classified information.

Listed below are several required security measures for handling and safeguarding classified materials:

1. To receive classified information, an individual must have a security clearance equal to the level of the classified information being received and must possess a mission related "need-to-know." Classified information shall not be disclosed to any individual merely by virtue of his/her position. Likewise, the possession of a security clearance does not equate to a de facto need-to-know.
2. Classified information must never be discussed over standard telephone lines. Discussions of classified information should only be conducted where facilities or conditions are adequate to prevent unauthorized access to the information. You must ensure that when discussing classified information, the area is clear of any personnel that do not possess a security clearance and mission-related need-to-know.
3. Under no circumstances may you store classified information in your desk, vehicle, or at your personal residence.
4. Requirements for properly distributing or transmitting classified documents are addressed within Departmental Manual 3440-001, "Classified National Security Information Program Manual," Chapter Six. All classified material (**Top Secret, Secret, or Confidential**) must be stored in a GSA approved safe; **Top Secret** material must be further protected by locating the safe in a secure area approved by PDSO.
5. Publication of any classified information in an unclassified publication is strictly prohibited.

For additional information and assistance regarding information security, please visit our website at [www.usda.gov/da/pdsd](http://www.usda.gov/da/pdsd) or contact PDSO at (202) 720-7373.



Revised 12/08

## STEPS TO GAINING ACCESS TO webSETS

Personnel who require access to the new web-based Security Entry Tracking System (webSETS) as part of their official duties involving background investigations and adjudications, must complete the following tasks prior to receiving access approval from PDSO:

- 1) Complete the "**webSETS User Request & Acknowledgement**" form and have it approved by your Mission Area Personnel Officer.
- 2) Fax the completed form to PDSO at 202/720-1689. If approved, PDSO will contact NFC to create a new account or modify your existing account. By agreement, NFC will only grant webSETS access on requests received and endorsed by PDSO.
- 3) The user will receive an email from PDSO notifying them that they have been tasked for webSETS training in **AgLearn**.
- 4) Upon successful completion of webSETS training in **AgLearn**, the user must fax their completion certificate to PDSO at 202/720-1689.
- 5) The user will receive an email from PDSO requesting they sign and fax back the "**Rules of Behavior**" form.
- 6) Once the "**Rules of Behavior**" form is received, PDSO will send the user the "**Welcome to webSETS!**" email notifying them of their User ID, the link to access webSETS, and help information.
- 7) The user will log into webSETS using their existing NFC password or a new password assigned to them by their Agency Security Officer. PDSO can only issue or reset passwords for DA personnel.

Questions concerning access to webSETS or working within webSETS should be directed to Carrie Moore at 202/720-3487 or [carrie.moore@usda.gov](mailto:carrie.moore@usda.gov).

\*\*\*\*\*

Visit us on the web!

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