Personnel & Document Security Division

PDSD Newsletter

Volume 19 First Quarter FY08

planning, building & implementing SETS

In this Issue:

The Personnel & Document Security Division (PDSD) has been working with the National Finance Center (NFC) to create a modernized Security Entry Tracking System (SETS).

SETS will be used to track all background investigations, including those completed by HR offices and PDSD, on USDA employees and contractors. The new system will include additional features to track security briefings, Sensitive Compartmented Information (SCI) access, and reciprocity actions.

Authorized users will also have access to a variety of reports to aid them in their reinvestigations tasking, obtain clearance listings, suitability listings, etc.

The first version of the new SETS is anticipated to be released around early November 2007. The use of this new system will be mandatory as the previous version will no longer be active.

A training module in AgLearn is currently being created for the new system.

All users will be required to successfully complete this training prior to being granted access. We anticipate the training module will be launched in late October.

Do you require access to SETS?

ALL SETS users must fill out the "**SETS User Access & Acknowledgement**" form in order to gain access to the new system. PDSD will ensure the request is justified and the role selection is correct prior to forwarding it on to NFC. We will use these requests to notify individuals when the AgLearn training is available. A supervisor must sign off on each form acknowledging the access is required in the performance of duties.

If you need this form emailed to you, please contact Carrie Moore at carrie.moore@usda.gov.

USDA/ASA/OSS/PDSD (202) 720-7373 (202) 720-1689 fax
www.usda.gov/da/pdsd

security management

HSPD-12 MATTERS

DASO Contractor Implementation Project

Over the summer, PDSD worked with OPPM's Procurement Policy Division and Communications Resources, Inc. (CRI) to prepare draft procedures for implementing the requirements of HSPD-12 as it pertains to contractor employees. The team is now in the process of initiating those procedures through the Departmental Administration Staff Offices (DASO) Contractor Implementation Project.

For the initial phase of this project, PDSD worked with two contract companies and a USDA/college partnership group to identify contractors and begin the process for initiating background investigations. As of September 24th, background investigations have been initiated for 100 percent of the identified contract employees.

The DASO Contractor Implementation Project will continue into FY 2008 and is expected to ultimately become the primary procedural template USDA-wide for managing and maintaining contractor employee data under HSPD-12 requirements.

If you would like additional information about this Project or HSPD-12 requirements for contractor employees, please contact Eileen Gibbons at (202) 720-7373 or by email at Eileen.Gibbons@usda.gov.

Welcome to PDSD…

LaJoya "Joy" Assent is our new Information Security Specialist in the Personnel and Document Security Division. Joy has most recently worked for the U. S. Army Materiel Command as a Security Specialist and comes to us very well regarded with a solid background in information, industrial, and personnel security. We are very fortunate to have someone of Joy's caliber join PDSD. Joy can be reached at Lajoya.assent@usda.gov.

Eileen Gibbons began working in PDSD in May 2007 on a detail from the Office of Security Services' Protective Operations Division where she worked as a Management Analyst. She has recently become a permanent member of PDSD personnel security team. Eileen is responsible for developing and implementing processes within PDSD to manage the contractor NACI program for DASO, as well as processing and adjudicating DASO contractor investigations. We are excited to have her join our team. Eileen can be reached at Eileen.gibbons@usda.gov.

PDSD Bulletins

The following PDSD Bulletins are available for viewing at:
http://www.usda.gov/da/pdsd/bulletins.htm

#07-04: **Required Foreign Country Releases for Canada and Australia**; This bulletin became effective August 1, 2007

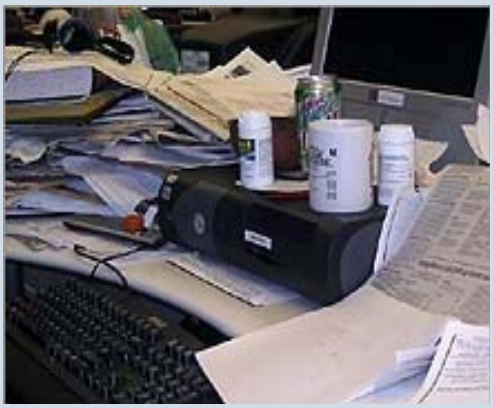
#07-05: **OPM Investigations Reimbursable Billing Rates for Fiscal Year 2008;** This bulletin becomes effective October 1, 2007. An updated price listing attachment has been added to this bulletin as of October 2, 2007 due to an increase in FBI rates.

IS YOUR DESK CLEAN?

A clean desk enhances security. It is a crucial element in protecting classified and sensitive or personal information from disclosure. USDA office space is frequented by visitors, consultants, vendors, cleaning crews, maintenance and fellow employees. Please keep your workspace neat. If it is messy, you may not notice when something important is missing.

At the end of each duty day, desks, chairs, credenzas, bookcases, etc., should be cleared of all working materials to the degree necessary to ensure the security of classified and sensitive or personal information. Because of the many different office environments that exist within each organization, individual office and division chiefs should determine the exact extent the desks and surrounding areas should be kept clear. The following tips will assist you in making your desk a clean desk:

Throughout the day:
-Lock sensitive documents and computer media in drawers or filing cabinets and secure classified materials in security containers approved for the storage of classified material.
-Secure your workstation before walking away.



Do not post sensitive documents in your work areas. Examples include:
-User IDs & Passwords
-Forms and rosters with personal information such as social security numbers
-Contracts
-Account numbers
-Employee records

At the end of the day, take a moment to:
-Tidy up and secure classified or sensitive material.
-Lock drawers, file cabinets and offices as appropriate.
-Secure expensive equipment (laptops, PDAs, etc.).

PHASED PERIODIC REINVESTIGATION (PPR)

The Personnel and Document Security Division (PDSD) would like to remind agencies that there is no longer an absolute requirement for coverage of references and neighborhoods in reinvestigation cases when there is no security concerns admitted on the Standard Form (SF) 86 or developed during the investigation. The Office of Personnel Management (OPM) developed the PPR in response to these new changes.

PDSD has been receiving a high number of full scope Single-Scope Background Investigations (SSBI-PR's) for reinvestigations. Agencies should be using the new Phased Periodic Reinvestigation (PPR) if the subject does not disclose anything of a security concern on their SF-86. Agency points-of-contact are asked to review the SF-86 before requesting the PPR. The Personnel Security Branch will complete a second review for any self-disclosed security concerns upon receipt and notify the submitting agency if a change to the SSBI-PR is required.

Any PPR that develops information of a security concern during the course of the investigation will be expanded by OPM to meet the full SSBI-PR requirements. The Case type for PPR is 19 and it is available for Priority Service (A) or Standard Service (C). Please refer to Federal Investigations Notice 07-05 for billing rates.

OPM will continue to offer the full scope SSBI-PR with full coverage and issue resolution. OPM will no longer offer an SSBI-PR that does not include issue resolution. The Case type for the SSBI-PR is 18. The SSBI-PR is available for Priority Service (A) or Standard Service (C).

It is imperative that all e-QIP submissions include all required items uploaded into e-QIP (scanned releases and signature pages, resume, SF 171 or OF 612, etc.) to ensure timely processing of investigation requests. USDA personnel experiencing difficulties with scanning documents into e-QIP should contact Vet Thorpe, Senior Personnel Security Specialist, at (202) 720-4390 or Arviet.Thorpe@usda.gov for assistance.

SECRET OF SUCCESS

Since 1974, the Government Accountability Office has published no less than 74 reports on issues plaguing the federal security clearance process -- the most recent was released in September 2006. More than three decades after the first report, the clearance process still suffers from many of the same problems, as witnessed by an estimated backlog of roughly 180,000 cases at the Defense Department alone.

Procedures for investigating and adjudicating security clearance applications are founded on a largely paper-based system that dates back to World War II. Backlogs and delays cost the government as much as $1 billion in lost productivity every year, and they prevent the government and contractors from hiring people who are desperately needed in the war on terror.

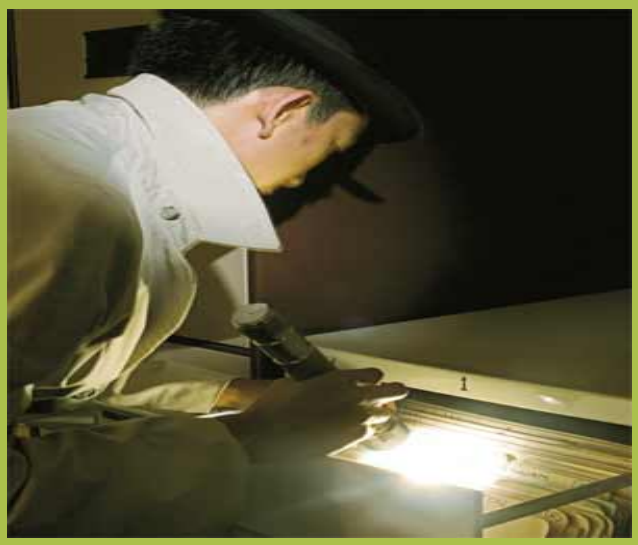
Fortunately, there is new momentum for a solution. Director of National Intelligence Mike McConnell and James Clapper, Undersecretary of Defense for Intelligence, recognize that in order to stem the detrimental effects on national security, this anachronistic system must be reinvented. In his recent One Hundred Day Integration and Collaboration Plan, McConnell said the intelligence community must "build on best practices in risk management."

The security clearance backlog can be addressed immediately by leveraging commercial technology, analytics and data in four pivotal areas:

- Electronic verification of information on applicants' Standard Form 86.
- Risk segmentation and pre-investigation of applicants for more effective allocation of investigative resources.
- Case management software to enhance the monitoring and visibility of investigations.
- A persistent reinvestigation process that can be triggered by automatically flagging high-risk or derogatory information contained in public and government records.

GovExec, September 5, 2007
http://www.govexec.com/dailyfed/0907/0905

Potential Espionage Indicators



An excerpt from DIA phamphlet, *Espionage*

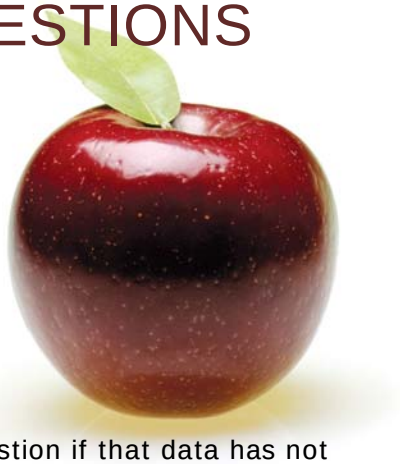
Several of the spies involved in confirmed espionage cases share a number of characteristics in varying degrees. The fact that an individual exhibits one or more of the following indicators does not automatically mean that he or she is engaged in espionage. However, based upon the situation, such factors can be cause for concern and may merit further investigation to determine whether espionage is a possibility. Even where espionage is not present, several of the characteristics may be indicative of problems in suitability or security, which we cannot ignore.

Behavior patterns of possible significance that should be reported include the following:

-Unexplained affluence in the absence of some legitimate source of increased income
-Frequent unreported unofficial travel overseas
-Showing unusual interest in information outside the job scope
-Keeping unusual work hours/excessive voluntary overtime
-Frequent and high volume reproduction of documents/taking classified material home
-Unreported or concealed contacts with foreign nationals, or foreign government, military, or intelligence officials
-Attempting to gain new accesses without the need to know
-Unexplained absences
-Indicators of emotional, mental or nervous disorders

You should report the behavior patterns above or other suspicious activity to Susan Gulbranson, Chief, Personnel and Document Security Division, or John Loveless, Chief, Personnel Security Branch, at (202) 720-7373.

Learning Corner
FREQUENTLY ASKED QUESTIONS in e-QIP



1. *I cannot login to e-QIP. What should I do?*

   Contact the *e*-QIP representative for your Agency.

2. *What does the Submit button do?*

   The **Submit** button saves the data you have entered for an individual question or for the section of the question on the current screen.

3. *What does the Reset button do?*

   The **Reset** button clears (removes) any data just entered for the current question if that data has not been saved (submitted).

4. *What is TLS 1.0?*

   A browser setting that must be selected prior to successful operation of the *e*-QIP system. The TLS protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

5. *Does every request have to be reviewed and approved by both a Reviewer and an Approver?*

   No. If an Approver initially reviews and approves a request, that request does not also have to be reviewed by a Reviewer. If a request is reviewed and approved by a Reviewer initially, that request must be approved by an Approver. The Approver is the final authority.

6. *What happens when I enter rejection comments and reject a request?*

   When a request is rejected, the system automatically generates a new request with the same form and group for the Applicant, with a new request number. The Applicant's access to *e*-QIP is automatically re-instated for the new request. When the Applicant logs into the new request, he/she may review the rejection comments from the ***Select Investigation Request*** window. All data will be present from the old request except for the Part 2 yes/no answers, which will have to be completed again. (This is because the answers to these questions may have changed from the time the first request was released and the time the second request is released.)

7. *I don't see the form that I need to initiate for the Applicant (e.g., SF85).*

   In the Forms selection box, you will see only those forms which your Agency is authorized to initiate within *e*-QIP. If you have a question about this, contact OPM.

8. *What is a quick way to find a specific request?*

   If you know the Request ID or SSN, enter the Request ID or SSN into the ***Manage Request*** sidebar panel on the right side of the screen and click the desired button.

9. *Does Version 2.0 of e-QIP allow me to use the browser's Back button?*

   In general, the Back button may be used. However, you should NOT use the Back button ***if the use of the back button crosses a change of agencies***. In that event, errors may occur.

10. *What does Cancel/Terminate a request do?*

    If a request is cancelled, it can be re-instated to its last event state by certain roles. If a request is terminated (for example, by the system when a time limit is met) the request may not be re-instated. An Initiator would have to initiate a new request at that time if desired.

Use the following address to mail e-QIP attachments and fingerprints to OPM:

e-QIP Rapid Response Team
OPM-FIPC
PO BOX 618
Boyers, PA 16020

When using Federal Express:

e-QIP Rapid Response Team
OPM-FIPC
1137 Branchton Road
Boyers, PA 16020

OPM Unveils Technology to Speed Clearance Processing

Completed background investigations for security clearances will be sent via electronic transfer under a pilot project initiated by the Office of Personnel Management. Under the pilot, OPM, which conducts 95 percent of background investigations, will electronically deliver the results of such reviews to the Army Central Personnel Security Clearance Facility for adjudication of the applications under its jurisdiction.

The use of technology has been cited as critical to reducing the time necessary to transfer documents across agencies. Currently, most background investigation results are delivered through the mail or other hand-delivery methods. Electronic transfer will reduce delivery time by seven to 13 days and will provide savings on postage and personnel, according to OPM. "OPM has worked diligently over the past two years to increase the speed with which federal employees receive their security clearance," said OPM Director Linda Springer. "Through electronic transfer, agencies will have instant access to completed background investigations, ensuring more timely and efficient adjudication of clearance cases."

The program will enable the Army's clearance facility to process adjudication cases electronically through the Clearance Adjudication Tracking System. That system can manage cases more efficiently, in part by automatically prioritizing them based on OPM codes. The system helps eliminate staff costs associated with the current paper-based environment, OPM said.

Under a 2004 anti-terrorism law, agencies are required to ensure by 2009 that 90 percent of applications get adjudicated within 60 days of the date investigators receive the forms. Within that time, the investigations phase could take 40 days at most, and the process of deciding whether to accept or reject the application could take a maximum of 20 days, according to the law.

"OPM is looking at one small segment of the clearance process that can be more easily fixed," said Evan Lesser, director of ClearanceJobs.com, which matches clearance-holding job seekers with top hiring companies. "The government is saying that things are improving, but we are not seeing it trickle down yet."

Lesser pointed to a request-for-information posted last week on the Federal Business Opportunities Web site, in which the Office of the Director of National Intelligence, the Defense Department and OMB sought input from vendors on potential ways to reduce clearance delays. "This is probably the most remarkable thing to come about with the security clearance backlog in years," Lesser said.

According to the information request, the agencies are seeking a defined industry solution on how to speed clearance processing in compliance with the law. The agencies are hoping to have the new system in place by Dec. 31, 2008, the request stated.

GOVEXEC, August 21, 2007, http://www.govexec.com/story_page.cfm?filepath=/dailyfed/0807/082107b1.htm