



# P&RCIO NEWSLETTER

SERVING THE P&R COMMUNITY  
VOLUME 3, ISSUE 4



SUMMER 2011

## Personnel and Readiness Information Management (P&R IM) Document Migration: A Case for Knowledge Management (KM)

### POINTS OF INTEREST:

- P&R IM Document Migration: A Case for KM
- The Evolution of Cyber Sabotage
- Records Management (RM) at P&R

As many agencies prepare to move their offices under Base Realignment and Closure (BRAC) 133, the organization of shared electronic drives has become increasingly important. P&R IM addressed this growing need by beginning a KM initiative in the spring of 2010. The immediate purpose of the initiative is to organize and clean up an overgrown electronic folder system based on Records Management policy; however, the larger goal is to encourage streamlined strategies that enable the adoption of insights and collaboration across the organization's capabilities and among Government agencies.

Many organizations are plagued with knowledge loss due to employee turnover and stove-pipe programs. These issues create problems for employees trying to access information that they need but may not have authored. P&R IM was encumbered by a legacy system that needed to be maintained, but for which many of the original file owners were no longer available. With over 400,000 files, P&R IM document management was not a simple task. After planning and mapping out a new electronic folder structure, the P&R IM KM Team launched its file migration effort in mid-May 2011. For the next four and a half months, the KM team will work closely with P&R IM users to facilitate file migration from the old, unorganized network drives to the new S: (shared) and R: (restricted) drives and eContent document repository.

Document management allows Knowledge Managers to identify what information can be shared for collaborative purposes and what information needs to be protected. At P&R IM, the electronic drives separate shareable information located on the S: drive from restricted information protected by verified permission sets on the R: drive. In this way, P&R IM can still encourage collaboration and knowledge exchange while protecting its sensitive information.

The categorization of information is an important first step, especially when it comes to Records Management (RM) policy. At any time, an organization can be asked to produce a record or be checked for disposition schedule compliance. P&R IM uses a document management system with synchronizer technology to help move record documents from the new S: drive to the eContent document archive. eContent stores final record documents in a searchable and secure repository to make them easier to find and manage in accordance with RM policies.

Technology is only part of the solution, as is strong management support. Maintained organization and compliance depends on the continuous training of employees and guidance from Knowledge Managers. Since its inception, the KM team at P&R IM has communicated extensively with its user base regarding the overall KM effort and the migration process. Over the coming months, the KM Team will provide

the entire organization with comprehensive, hands-on training so that users can begin migrating their electronic files to the new shared drives. During these training sessions, the KM Team will review the folder structure, help locate the folders for which users are responsible, confirm permissions for the restricted drive, and walk users through navigating the document search capability, eSearch. In this way, all users will have personal, hands-on knowledge of their files and will be comfortable with the folder structure prior to the BRAC move.

Document management and the Mark Center move are just the beginning of the KM initiative. Organizations must constantly review their processes and build on their collaborative tools in order to stay efficient. The P&R IM KM Team will continue exploring and implementing proven best practices to embed a strong KM practice within the organization. These efforts include hosting quarterly KM Collaboration Forum sessions to share resources and best practices with other agencies and developing a set of resources designed to foster inter-agency collaboration.

The P&R IM KM Team invites you to take a moment to explore the offerings in the link below. If you have any questions regarding the migration, the Collaboration Forum, or KM at P&R IM, please contact [CIOsupport@osd.pentagon.mil](mailto:CIOsupport@osd.pentagon.mil).

If you would like to learn more about KM and P&R IM's migration initiative, please visit the following link from a Government computer:  
[https://www.intelink.gov/wiki/Portal:Personnel\\_and\\_Readiness\\_Information\\_Management\\_Knowledge\\_Management](https://www.intelink.gov/wiki/Portal:Personnel_and_Readiness_Information_Management_Knowledge_Management)



## The Evolution of Cyber Sabotage: Growing Incidences of Cyber Attacks

From retail to banking, recent attacks at Sony, Public Broadcasting Service (PBS), Citigroup, EMC's security arm RSA, email marketing giant Epsilon, and defense contractor Lockheed Martin, among others, have left no doubt that cyber threats are a formidable concern in the digital space. Any organization can become the target of amateur and professional hackers who run the gamut from recreationally defacing publicly accessible websites to breaking into seemingly secure systems to retrieve corporate secrets and sensitive data that could have serious consequences in the wrong hands. In the past, an organization could fall victim to being knocked offline for several hours in the face of a denial of service attack, but now every website presents an opportunity for hackers to try to break into companies' information technology (IT) assets to retrieve or expose as much data as possible, knowing that the damage has become much more multi-faceted.

In the Epsilon attack, hackers were privy to millions of verified email addresses that will most likely be used in phishing attempts in order to trick end users into disclosing personal information. While exposed email addresses pose a small but manageable threat, they do not compare to security attacks such as the attack on the RSA; in this case, data was stolen



about SecurID, a very common security system employed by a range of global clients, including the United States (U.S.) Government and the Department of Defense (DoD). RSA customers were notified, but some speculated that the

attack on Lockheed was related, exposing vulnerable systems around the world for significant amounts of time.

In May 2011, the White House unveiled policy framework on cyber security asserting that the U.S. has the right to use military force against cyber threats in order to defend itself. A key tenet of the policy is rumored to view foreign adversary cyber attacks on the U.S. in the same light as physical attacks with similar methods of retaliation. The DoD is quickly fine-tuning policy to redefine what constitutes an act of war in this age of cyber threats. With an increasing dependence on IT, the U.S. Government, the DoD, its allies, and the private sector must work together to protect their infrastructures. It is no longer simply a possibility that sophisticated groups of hackers, fueled by an adversary, could cause significant physical damage to remote systems. That scenario is now a reality with immediate and often significant impacts.

Sources:  
[http://www.nextgov.com/nextgov/ng\\_20110531\\_5712.php?oref=topnews](http://www.nextgov.com/nextgov/ng_20110531_5712.php?oref=topnews)  
<http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html>  
<http://online.wsj.com/article/SB10001424052702304563104576355623894502788.html>

## Records Management (RM) at Personnel and Readiness (P&R)

Federal employees, including those at P&R, create, receive, and use records daily in performing their jobs. A Federal record is Federal property and legally defined as:

“[Any recorded information], regardless of medium or format, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business, and either preserved or appropriate for preservation as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government...”<sup>\*</sup>

Understanding basic RM policies and requirements can help us manage them more effectively. In its simplest terms, RM is the organized process for creating, maintaining, and using records, and for disposing or preserving them in accordance with approved records disposition schedules. All records have life cycles, and



Federal agencies are responsible for establishing and maintaining an efficient and effective program for the management of the agency's records during each life cycle phase.

Sound RM practices are essential to achieving proper documentation of the activities of the Federal government as referenced in the definition above. Appropriately implemented, a RM program contributes to the streamlining of work processes, supports the agency's mission by

ensuring documents are easily accessible, contributes to more efficient agency decision-making, and demonstrates agency accountability, credibility, and responsiveness to the public.

P&R recently completed a baseline assessment of its RM program and practices and is in the process of implementing the recommendations from that review. On May 24, 2011, the P&R RM Working Group (RMWG) was formally chartered to facilitate and maintain communication, coordination, and collaboration in the development and sustainment of a compliant P&R RM program. For more information, please contact [CIOsupport@osd.pentagon.mil](mailto:CIOsupport@osd.pentagon.mil).

<sup>\*</sup>Source: United States Code: Title 44, Chapter 33, "Disposal of Records: § 3301. Definition of records, <http://www.archives.gov/about/laws/disposal-of-records.html#def>