

Text for Bureau of Naval Personnel PII Safeguarding Brief to DON CIO, January 2009

Slide One: Bureau of Naval Personnel PII Safeguarding

Hello, this is Dave German. I am the Privacy and Freedom of Information Act Officer for the Bureau of Naval Personnel, often also referred to as "BUPERS", PERS or simply the Bureau. I will refer to our organization as PERS throughout this brief.

I am going to provide you with a presentation summing up the journey that PERS has taken in the past two and a half years regarding our Privacy Act Program and the safeguarding of Personally Identifiable Information, generally referred to as "PII".

Slide Two: Historical Overview

Let's first take a quick historical overview. Most people will agree that the Veteran's Administration PII Breach in May of 2006 was a cornerstone incident that set off alarm bells within the Federal Government with respect to the protection of PII.

Unfortunately, it didn't take long for PERS to have our own major PII Incident. In June of 2006, a Navy Contractor uploaded a file containing PII on 28,000 Navy military members and their dependents to the public-facing side of his company's website.

This incident resulted in a Manpower, Personnel, and Training Enterprise PII Task Force Initiative consisting of a review of our Privacy Act System of Records Notices, a review of our Information Technology Security, and an initial review of our business processes to determine if less PII could be used while still executing vital Navy functions. This process incorporated input from all levels in our chain of command.

Slide Three: Actions

PERS took some specific actions in order to strengthen our safeguarding of PII. First, we held a massive Privacy Act training stand-down to ensure that all of our employees knew what was expected of them. Shortly after, we met with

all Division-level leadership and asked them to review our business processes and to remove the collection and use of PII where it was not necessary. We also purchased several industrial-sized shredders and bought and distributed "red shred bins" for placement of PII material to be shredded before it left each building. We printed and distributed thousands of privacy posters, and long-term, we revamped our Privacy Act Instruction.

Slide Four: Privacy Act Instruction

The BUPERSINST 5211.6, our Privacy Act and Safeguarding of PII" instruction was approved in April of 2008 after a long review process by many players within the BUPERS organization. The new instruction expanded beyond the scope of the Privacy Act and ventured into the larger issue of PII safeguarding.

For starters, the instruction created two new NAVPERS forms that we felt were critical as part of our safeguarding program. The NAVPERS Form 5211/14 was created to ensure that personnel traveling off base with PII on portable devices were getting approval from their chain of command, that they were capturing an inventory of what PII they were taking with them, and requiring a check-back-in procedure to ensure that the PII and portable device was accounted for. The second form generated, the NAVPERS Form 5211/15, created a checklist for Department Privacy Coordinators to utilize when they did monthly random reviews of workspaces. This completed form was turned into the Head Privacy Officials for review each month along with any additional comments by email from the Department Privacy Coordinators. The instruction also required that the PERS CIO/Information Assurance Office conduct Privacy Impact Assessments or PIAs of our automated computer systems. A BUPERSNOTE 5239, initiated by our CIO Office was signed along with the instruction providing guidance to the organization regarding when encryption was required, and what encryption solutions were acceptable.

Slide Five: Employee PA/PII Training

Training, training, training - is critical. We saturate our employees with training: First, a new employee receives training when they first check-onboard, they sign a NAVPERS Form 5211/13 verifying that they have received training. We also speak each month at the new employee orientation

training, of course we also have each employee complete annual training requirements. Finally, we regularly provide offices with guidance in response to specific issues or concerns regarding the handling of PII.

Slide Six: Privacy Team

One lone voice can not do it all, repeat one lone voice can not do it all. This has been the overriding lessons learned with respect to the PII safeguarding issue here at PERS. PERS created a Privacy Team consisting of individuals in the roles as Contracting Officer/Contractor POC, Records Manager, CIO, Security Manager and Department Privacy Coordinators.

Department Privacy Coordinators conduct monthly random office visits to ensure that employees are following requirements at set forth in the Navy training products. The Department Privacy Coordinators work within their divisions to solve PII business process concerns and report to the Head Privacy Officer when an issue is not resolved. Department Privacy Coordinators assist the Head Privacy Officer during annual training events. Commander, Navy Recruiting Command has a different field structure due to their large spread of commands with oversight handled by regional and district-level officials.

Slide Seven: CNPC PII Breach Summary

As you can see, Commander Navy Personnel Command has been able to reduce PII Breach Incidents to two in the past calendar year with only eight impacted individuals.

Commander Navy Personnel Command completed a security upgrade to our CD Service Record providing encryption and password protection for CDs that are mailed to individuals.

Slide Eight: Challenges

Balancing the use of PII and leveraging technology while simultaneously protecting the PII is the big challenge. PII is deeply integrated in automated systems and is needed by other DOD and non-DOD agencies to effect pay, benefits and the like.

One size does not fit all as command construct and varying business processes will impact specific actions that

leadership must take in order to safeguard PII within their organizations. Clearly, PERS Leadership has shown a commitment to take many actions that have strengthened our organization's safeguarding of PII.

Slide Nine: Contact

Here is my contact info if you have questions. I hope my presentation has been helpful. Thank you for your time.