UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

Evaluating Holdings of Personally Identifiable Information (PII) and Eliminating Unnecessary Collections at the Department of Veterans Affairs

September 2007

EVALUATING HOLDINGS OF PERSONALLY IDENTIFIABLE INFORMATION (PII) AND ELIMINATING UNNECESSARY COLLECTIONS AT THE DEPARTMENT OF VETERANS AFFAIRS

Overview

The Department of Veterans Affairs (VA) is pleased to provide the Office of Management and Budget (OMB) this first report on VA's efforts to eliminate the unnecessary collection and use of the Personally Identifiable Information (PII). VA is committed to reducing the unnecessary collection and use of PII wherever feasible, and is devoting considerable resources to do so. In fact, VA began its efforts before the May 22, 2007, publication of OMB Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."

VA's mission is to serve America's veterans and their families with dignity and compassion and to be their principal advocate to ensure that they receive medical care, benefits, social support, and lasting memorials promoting the health, welfare, and dignity of all veterans in recognition of their service to this Nation. It is the second largest Federal Department, with over 235,000 employees. Among the many professions represented in the vast VA workforce are physicians, nurses, counselors, statisticians, architects, computer specialists, and attorneys. As advocates for veterans and their families, the VA community is committed to providing the very best services with an attitude of caring and respect.

VA comprises a Central Office (VACO), located in Washington, DC, and field facilities throughout the United States administered by its three major line organizations: the Veterans Health Administration (VHA), the Veterans Benefits Administration (VBA), and the National Cemetery Administration (NCA). Services and benefits are provided through a nationwide network of 155 hospitals, 881 outpatient clinics, 135 nursing homes, 46 residential rehabilitation treatment programs, 207 readjustment counseling centers, 57 veterans' benefits regional offices, and 125 national cemeteries. The current population of potential VA customers is almost 24 million veterans.

On May 22, 2007, OMB released OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information. It required Federal agencies to develop and implement a breach notification policy within 120 days while ensuring proper safeguards are in place to protect the information and to develop policies concerning the responsibilities of individuals authorized access to PII.

In response, VA initiated this Enterprise-wide effort to identify and evaluate its holdings of all types of PII and to eliminate all unnecessary collections. As one of the largest Federal agencies, VA currently retains a tremendous store of personal information. Although the initial focus of this effort has been on the unnecessary collection and use of the Social Security Number (SSN), this plan extends beyond the collection of SSNs and includes the unnecessary collection of all PII including Protected Health Information (PHI), Home Telephone Numbers, Personal E-mail Addresses, Mother's Maiden Name, etc.

PII is collected and maintained throughout VA in both paper and electronic format. This type of information serves the important functions of both distinguishing between veterans with similar names and verifying the identity of veterans seeking service and/or entitlements. VA must be particularly careful not to diminish its effectiveness in providing services to veterans as a result of this effort. A partial list of VA forms, systems, and processes containing PII has been assembled specifically in response to this effort. This list revealed over 800 items containing the SSN alone ranging from small uses such as Physical Access Controls, to much larger applications, such as SSNs used in the Veterans Health Information Systems and Technology Architecture (VistA).

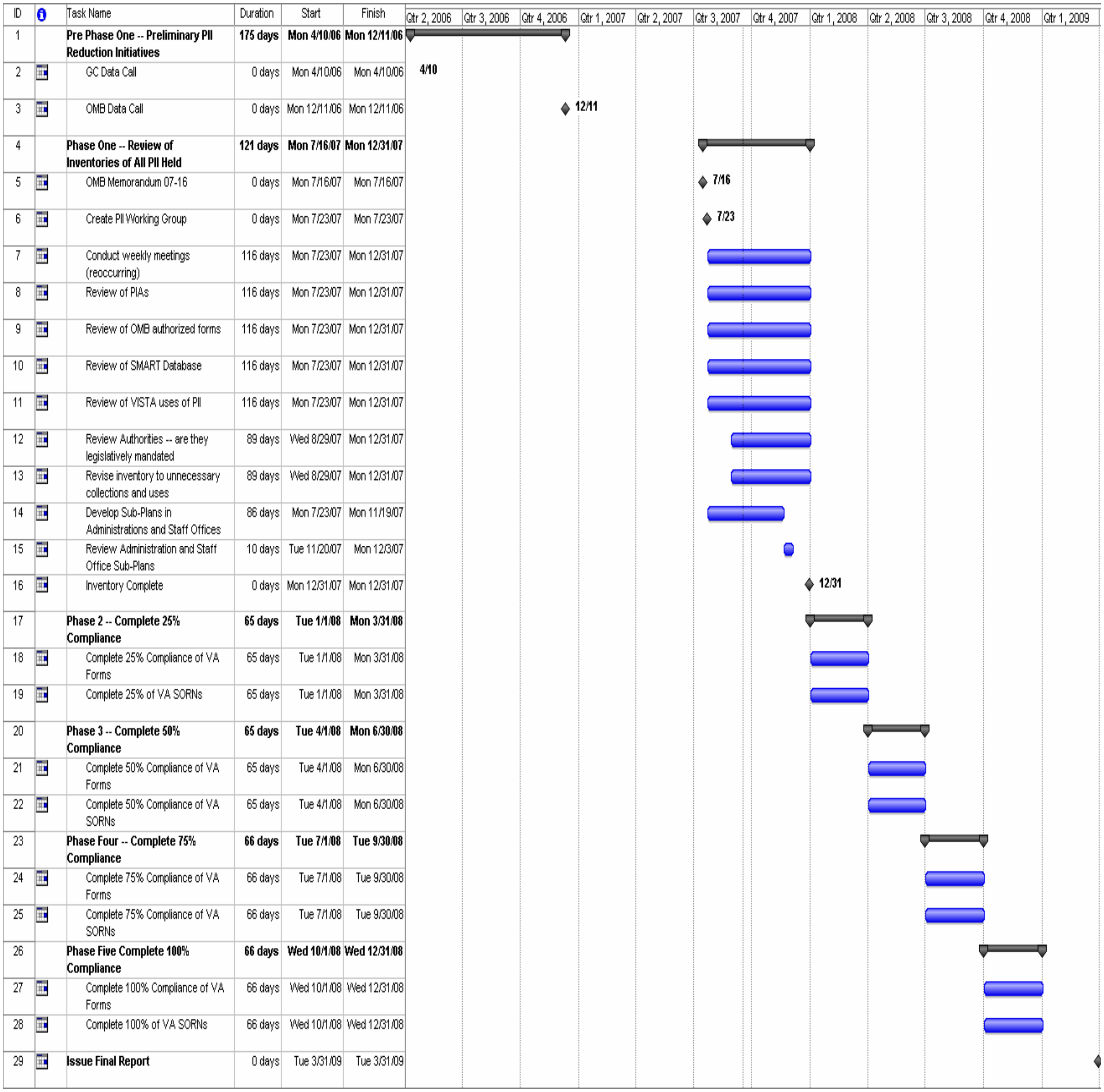
The scope of the VA Enterprise-wide effort will also include substantial coordination and interface with a number of other Federal agencies with whom the Department regularly interfaces. These agencies include the Social Security Administration (SSA), the Internal Revenue Service (IRS), the Department of Defense (DoD), and the Department of Education (ED). This effort will also require internal coordination between our own facilities throughout the country and the world.

When eliminating the PII now collected from any particular form or system, VA will be especially careful to consider the following:

- The systems in which the PII is contained
- The purpose served by collection and the uses of the PII
- Other forms populated using the form or system originally used for the collection
- System interfaces
- The costs and timeline for any modification.
- Policies or processes that must be changed as a result of the elimination

Figure 1 illustrates the preliminary plan to evaluate holdings of PII within VA and eliminate unnecessary collections within the Department.

Figure 1: VA's Five-Phase Plan



ID	Task Name	Duration	Start	Finish
1	**Pre Phase One -- Preliminary PII Reduction Initiatives**	**175 days**	**Mon 4/10/06**	**Mon 12/11/06**
2	GC Data Call	0 days	Mon 4/10/06	Mon 4/10/06
3	OMB Data Call	0 days	Mon 12/11/06	Mon 12/11/06
4	**Phase One -- Review of Inventories of All PII Held**	**121 days**	**Mon 7/16/07**	**Mon 12/31/07**
5	OMB Memorandum 07-16	0 days	Mon 7/16/07	Mon 7/16/07
6	Create PII Working Group	0 days	Mon 7/23/07	Mon 7/23/07
7	Conduct weekly meetings (reoccurring)	116 days	Mon 7/23/07	Mon 12/31/07
8	Review of PIAs	116 days	Mon 7/23/07	Mon 12/31/07
9	Review of OMB authorized forms	116 days	Mon 7/23/07	Mon 12/31/07
10	Review of SMART Database	116 days	Mon 7/23/07	Mon 12/31/07
11	Review of VISTA uses of PII	116 days	Mon 7/23/07	Mon 12/31/07
12	Review Authorities -- are they legislatively mandated	89 days	Wed 8/29/07	Mon 12/31/07
13	Revise inventory to unnecessary collections and uses	89 days	Wed 8/29/07	Mon 12/31/07
14	Develop Sub-Plans in Administrations and Staff Offices	86 days	Mon 7/23/07	Mon 11/19/07
15	Review Administration and Staff Office Sub-Plans	10 days	Tue 11/20/07	Mon 12/3/07
16	Inventory Complete	0 days	Mon 12/31/07	Mon 12/31/07
17	**Phase 2 -- Complete 25% Compliance**	**65 days**	**Tue 1/1/08**	**Mon 3/31/08**
18	Complete 25% Compliance of VA Forms	65 days	Tue 1/1/08	Mon 3/31/08
19	Complete 25% of VA SORNs	65 days	Tue 1/1/08	Mon 3/31/08
20	**Phase 3 -- Complete 50% Compliance**	**65 days**	**Tue 4/1/08**	**Mon 6/30/08**
21	Complete 50% Compliance of VA Forms	65 days	Tue 4/1/08	Mon 6/30/08
22	Complete 50% Compliance of VA SORNs	65 days	Tue 4/1/08	Mon 6/30/08
23	**Phase Four -- Complete 75% Compliance**	**66 days**	**Tue 7/1/08**	**Tue 9/30/08**
24	Complete 75% Compliance of VA Forms	66 days	Tue 7/1/08	Tue 9/30/08
25	Complete 75% Compliance of VA SORNs	66 days	Tue 7/1/08	Tue 9/30/08
26	**Phase Five Complete 100% Compliance**	**66 days**	**Wed 10/1/08**	**Wed 12/31/08**
27	Complete 100% Compliance of VA Forms	66 days	Wed 10/1/08	Wed 12/31/08
28	Complete 100% of VA SORNs	66 days	Wed 10/1/08	Wed 12/31/08
29	**Issue Final Report**	0 days	Tue 3/31/09	Tue 3/31/09

Efforts Currently Underway

The Department is committed to reducing its collection and use of the PII wherever and whenever possible, and has already devoted considerable effort to doing so. A brief description of efforts currently underway follows and a detailed listing of initiatives already accomplished is found in Figure 2.

In June 2007, VA drafted a memorandum calling for the assembly of a working group of Staff Office and Administration representatives charged with devising a plan within their respective areas of responsibility for the eliminating the unnecessary collection and use of PII. This group held its first meeting in July 2007. Subsequently, several Administration and Staff Office groups have begun to assemble information regarding the efforts that have been made and those efforts that are planned to reduce the use of PII in their respective areas. The primary focus of these efforts to date has been on the elimination, where possible, of use of the SSN as it presents the most significant danger to identity theft. Going forward, these efforts will be expanded to include collection and use of all types of PII.

VA has implemented an enterprise encryption solution that protects hard drives, encrypts e-mail messages across VA, and encrypts removable storage devices. VA has discontinued the use of thumb drives with few exceptions until delivery of the more secure, auto-encrypting devices has been made.

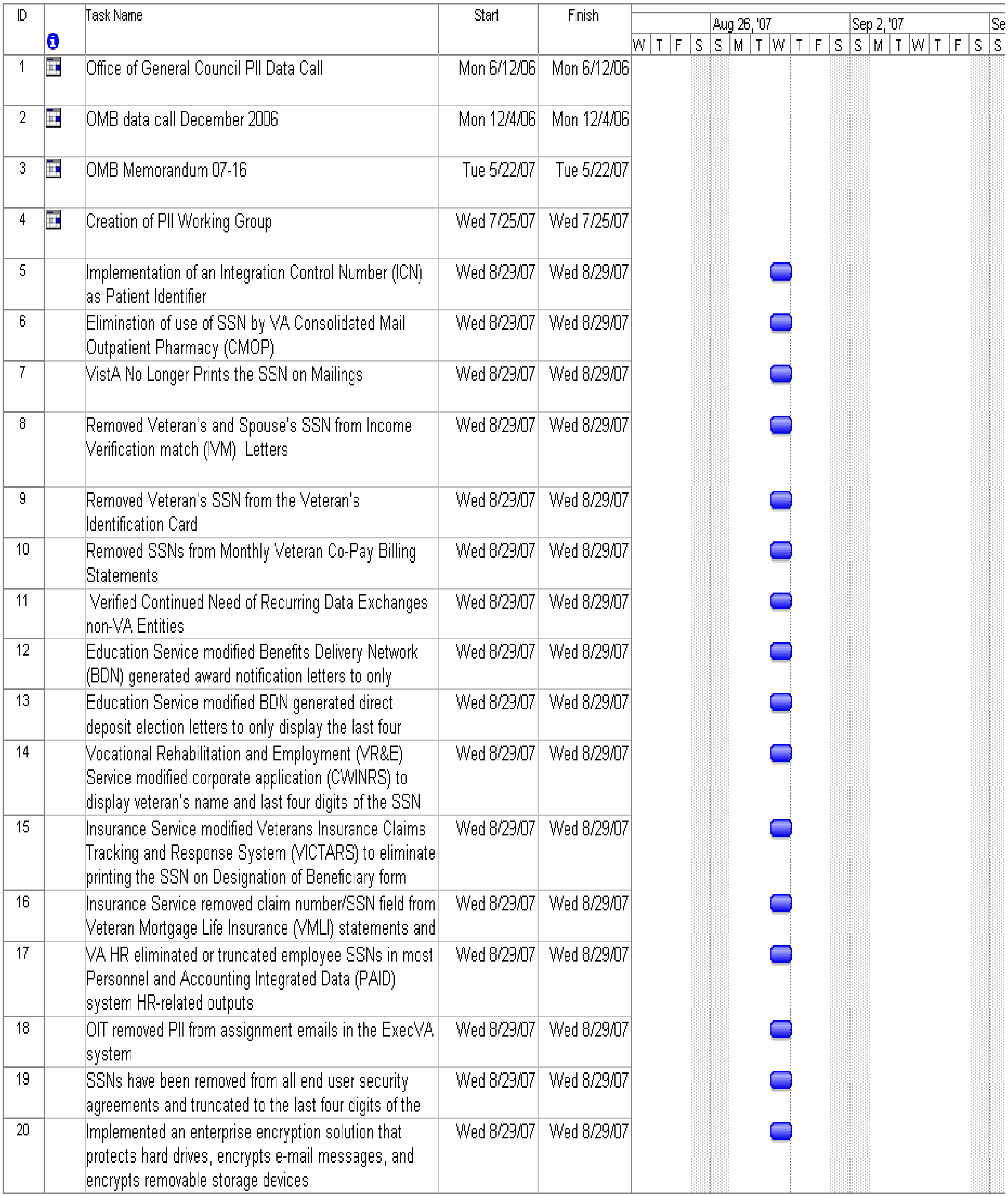
To ensure that VA continues to provide the care and services to each veteran’s unique needs, it is critical for VA to be able to distinguish between them. This is particularly true for VA’s role in providing healthcare where a case of mistaken identity could be catastrophic. Traditionally, PII and in particular the SSN has been VHA’s primary identifier used to make the determination of unique identity. With the increased risk to our veterans, associated with the use of PII, VA has already taken a number of steps to reduce the use of the SSN, and in some cases, VA has eliminated use of the SSN for identifying veterans.

The Veterans Benefits Administration (VBA) has completed the following actions that to identify and eliminate the unnecessary collection and use of PII:

- Verified continued need of 831 recurring data exchanges that provide Privacy Act protected data to non-VBA entities;
- Updated and strengthened procedures for handling changes to address and direct deposit information to ensure proper verification of identity of individual requesting changes;
- Issued standardized Work-at-Home/Flexi-Place procedures that require individuals to ensure protection of PII. (Additionally, individuals are prohibited from downloading or saving PII to their computer’s hard drive);
- Issued new shipping procedures to ensure that any hard-copy documents containing PII are sent via carrier that offers package tracking.

The Office of Information and Technology (OI&T) has stripped all PII from assignment e-mails in the “ExecVA” system. These e-mails are used to include the issue description including all of the veteran's PII. Only those persons with the appropriate rights and a username and password

Figure 2: PII Elimination Accomplishments



ID	ℹ	Task Name	Start	Finish
1	▦	Office of General Council PII Data Call	Mon 6/12/06	Mon 6/12/06
2	▦	OMB data call December 2006	Mon 12/4/06	Mon 12/4/06
3	▦	OMB Memorandum 07-16	Tue 5/22/07	Tue 5/22/07
4	▦	Creation of PII Working Group	Wed 7/25/07	Wed 7/25/07
5		Implementation of an Integration Control Number (ICN) as Patient Identifier	Wed 8/29/07	Wed 8/29/07
6		Elimination of use of SSN by VA Consolidated Mail Outpatient Pharmacy (CMOP)	Wed 8/29/07	Wed 8/29/07
7		VistA No Longer Prints the SSN on Mailings	Wed 8/29/07	Wed 8/29/07
8		Removed Veteran's and Spouse's SSN from Income Verification match (IVM) Letters	Wed 8/29/07	Wed 8/29/07
9		Removed Veteran's SSN from the Veteran's Identification Card	Wed 8/29/07	Wed 8/29/07
10		Removed SSNs from Monthly Veteran Co-Pay Billing Statements	Wed 8/29/07	Wed 8/29/07
11		Verified Continued Need of Recurring Data Exchanges non-VA Entities	Wed 8/29/07	Wed 8/29/07
12		Education Service modified Benefits Delivery Network (BDN) generated award notification letters to only	Wed 8/29/07	Wed 8/29/07
13		Education Service modified BDN generated direct deposit election letters to only display the last four	Wed 8/29/07	Wed 8/29/07
14		Vocational Rehabilitation and Employment (VR&E) Service modified corporate application (CWINRS) to display veteran's name and last four digits of the SSN	Wed 8/29/07	Wed 8/29/07
15		Insurance Service modified Veterans Insurance Claims Tracking and Response System (VICTARS) to eliminate printing the SSN on Designation of Beneficiary form	Wed 8/29/07	Wed 8/29/07
16		Insurance Service removed claim number/SSN field from Veteran Mortgage Life Insurance (VMLI) statements and	Wed 8/29/07	Wed 8/29/07
17		VA HR eliminated or truncated employee SSNs in most Personnel and Accounting Integrated Data (PAID) system HR-related outputs	Wed 8/29/07	Wed 8/29/07
18		OIT removed PII from assignment emails in the ExecVA system	Wed 8/29/07	Wed 8/29/07
19		SSNs have been removed from all end user security agreements and truncated to the last four digits of the	Wed 8/29/07	Wed 8/29/07
20		Implemented an enterprise encryption solution that protects hard drives, encrypts e-mail messages, and encrypts removable storage devices	Wed 8/29/07	Wed 8/29/07

can see the PII in the system. All user accounts and rights are first approved by the Office of the Secretary before they are created.

The Office of the Inspector General (OIG) completed an analysis of the use of PII in general and put in place processes to de-identify the large data sets. In those instances where there is an absolute need for PII, OIG will use small samples of data under rigorous controls by senior managerial staff.

The OIG CIO conducted training for all OIG managers in May 2007 and has regularly disseminated policy and procedure reminders to all staff during the past 12 to 15 months.

As part of their policy review last year, all OIG employees were enrolled in a “New Rules of Behavior” certification, which places an emphasis on protecting PII. OIG is also conducting a purge of paper throughout its offices, which will result in the shredding of documents no longer needed.

In parallel with this effort to eliminate the unnecessary collections of PII the Department formed an Information Protection Steering Committee (IPSC) as a governance body comprised of OI&T Executive leadership, including the CIO, and Information Protection program stakeholders. The IPSC serves the purpose of deliberating and providing recommendations for decision-making as it pertains to the VA Information Protection Program. The IPSC meets once a month to acquire project status, discuss business issues, prioritize activities, and discuss risks associated with the project. These discussions and decisions made by the IPSC are essential to ensuring the delivery of the project outputs and attainment of the outcomes. The IPSC’s initiatives include the following:

- By September 15, 2006, VA encrypted 18,000+ laptops. Simultaneously, the Department developed and implemented procedures to ensure that all laptops contain applied updated security policies and have removed all sensitive information not authorized on the devices.

- In April 2007, VA Directive 6601, **Removable Storage Media**, was signed by the Secretary. It mandates that VA allow only FIPS 140-2 certified encrypted Universal Serial Buses (USBs) thumb drives to be used within the Department. In addition, a port security and device control technology will be implemented to enforce adherence to the directive. This technology will: allow the use of only VA authorized removable storage, restrict the transfer of information to removable storage media, and thwart any attempt to introduce malicious code via USB ports.

- In September 2007 the Department rescinded VA Directive 6601 and published VA Handbook 6500, **Information Security Program**, which. VA Handbook 6500 contains specific guidance on the use of **“Mobile/Portable/Wireless and Removable Storage Media and Device Security”** including mandating the use of FIPS 140-2 certified encrypted USB thumb drives contained in VA Directive 6601.

- The Department has also established levels of standardization for Blackberrys, SmartPhones and other mobile devices. Older versions of mobile devices that do not support encryption or content protection are being retired and replaced with versions that support VA’s IT Security Policies. The Department implemented Blackberry content protection on a majority of its devices. IT Memorandum 07-01, **Standardization of Blackberry Devices, SmartPhones, and Other Mobile Devices** (currently in concurrence), will restrict the use of non-government mobile devices, allowing their use only if VA can monitor their use to verify they follow IT Security Policies. VA is also in the process of deploying Trust Digital which will encrypt SmartPhones.

- The Remote Enterprise Security Compliance Update Environment (RESCUE) project will address the security of information that is transmitted and stored by VA remote access users. This initiative will require Government Furnished Equipment (GFE) laptops and desktops that connect to the VPN to undergo a compliance check to verify that the device has been encrypted, patched, received antivirus updates, and that the HIPS is active. If the laptop or desktop is not compliant, it will be quarantined and moved to a secure virtual desktop. Other Equipment (OE) will only be able to utilize the virtual desktop and will not be able to gain access to network shares.

- The Department is in the process of procuring a technology that will encrypt the transmission of passwords and information sent over the network. This Enterprise procurement will enable the Department to standardize on terminal emulator applications such as IFCAP, ETA, CPRS, VistA and VistA Mail.

- Public Key Infrastructure (PKI) is an Enterprise solution meant to protect sensitive information contained within email messages. This solution is used for internal and external email correspondence. This past spring VA began deploying an Enterprise solution to encrypt and secure emails, documents and files. This initiative, titled the **Rights Management Services** (RMS) initiative, compliments the PKI initiative. RMS has the ability to encrypt messages and restricts permissions to forward, save and print messages. RMS will be fully deployed across the Department by September 2007.

I. VA’s Enterprise-Wide Plan for the Elimination of the Unnecessary Use of PII

Because VA is comprised of three Administrations with three very different missions and a consolidated Office of Information and Technology that controls most information technology (IT) functions, the VA Enterprise-wide plan to eliminate the unnecessary use of PII is divided into several sub-plans based on functional areas. Each of the sub-plans will roll up into the Enterprise-wide plan to eliminate the unnecessary use of PII.

VA shares data with many government agencies and private organizations. This is done to verify income in order to determine benefits eligibility, to transmit health data to third parties, to confirm a veteran’s or dependent’s status, to report income of employees, to verify education, etc. Because of the varying and complex nature of VA data sharing, each administration must also coordinate with other agencies and private organizations regarding the impact of eliminating PII, and, if necessary, replacing PII with another unique identifier. This effort has already begun through VA’s participation in the Interagency Best Practices Collaborative and participation in

Office of Personnel Management's task force that was chartered to create a new Unique Employee Identification Number (UEID).

A plan to eliminate the unnecessary collection and use of PII throughout the Department has been developed. The plan will evolve as we move through the process and learn more about what data is in specific systems, and how that information is cross referenced within the Department, and matched with data in other Government systems.

Between October 2007 and March 2009, VA intends to fully implement a plan to review and then eliminate the unnecessary use and collection of all types of PII. The Plan consists of well-defined tasks and milestones designed to carry-out a complete overhaul of VA's use and collection of PII. This plan will provide specific procedures for all Department business owners to eliminate the collection and maintenance of any type of unnecessary PII as appropriate.

As already noted, VA shares a great deal of data with other government agencies and private organizations. This data sharing will make it necessary for each administration to coordinate with other agencies and private organizations about the impact of eliminating PII, and if necessary, replacing it with another unique ID. VA has already begun this through participation in the Interagency Best Practices Collaborative and participation in OPM's task force that was chartered to create a new Unique Employee Identifier (UEID).

The VA plan to eliminate unnecessary collections of PII will be based on sub-plans which are focused on the different missions and functions of our three Administrations and our various Staff Offices. Each of the Department's sub-plans will be aggregated by the Office of Privacy and Records Management into VA's overall plan. This attachment provides a snapshot of the plan in its current state and an overview of the plan to eliminate unnecessary collections of PII within VA's Administration and Staff Offices as they fit into VA's overall plan. The plan will evolve as we move through the process and learn more about what data is in specific systems, and how that information is cross referenced within the VA Enterprise, and matched with data in other Government systems.

By the end of March 2009, the Office of Privacy and Records Management will issue a final report on its findings, including discussion of the instances when the use and/or collection of PII were identified as unnecessary.

A. Phase One

During the first quarter of fiscal year (FY) 2008, VA will complete a full review of its inventories of PII held in all VA systems. VA's PII Reduction Workgroup has established a preliminary set of Tasks for the Department's Administrations and Staff Offices to accomplish during this first portion of implementing the initiative to eliminate the unnecessary collection of all PII. These tasks reside in a living document that is subject to change as the initiative develops. The preliminary tasks identified by the Workgroup include:

- Issuance of data calls to all administrations and staff offices requiring them to review and update all new and existing Privacy Act System of Records Notices (SORNs) and all VA forms that collect PII.

- Establishment of regularly scheduled PII Reduction Workgroup meetings to oversee and facilitate this review through the use of an established set of criteria, to determine whether particular uses and collections of PII can be eliminated or must be maintained.

- Based on the review described above, the Workgroup will develop and issue policies mandating a permanent reduction in the collection of PII data throughout the agency. This will include annual reviews of existing SORNs and VA forms to ensure that changes have not been mistakenly made to those information collections.

- Regular communication of these policies and all new changes to all employees via daily employee news feeds, on-line training vehicles, and through cooperation and coordination with Office of Oversight and Compliance assessment team visits.

- Administration and Staff Office Sub plans.
    - Because each VA Administration and Staff Office will be responsible for its methodology for complying with the mandate to eliminate the unnecessary collection, holding and use of PII, each will develop its own sub-plan.

B. Phase Two

Phase Two of the Plan will take place during the 2nd Quarter of FY 2008. During this phase VA anticipates it will implement the procedures approved during Phase One and will transition 25% of all Privacy Act Systems of Record and VA Forms into compliance with reduction plan.

C. Phase Three

Phase Three of the Plan will take place during the 3rd Quarter of FY 2008. During this phase VA anticipates it will implement the procedures approved during Phase One and will transition 50% of all Privacy Act Systems of Record and VA Forms into compliance with reduction plan.

D. Phase Four

Phase Four of the Plan will take place during the 4th Quarter of FY 2008. During this phase VA anticipates it will implement the procedures approved during Phase One and will transition 75% of all Privacy Act Systems of Record and VA Forms into compliance with reduction plan.

E. Phase Five

Phase Five of the Plan will take place during the 1st Quarter of FY 2009. During this phase VA anticipates it will implement the procedures approved during Phase One and will transition 100% of all Privacy Act Systems of Record and VA Forms into compliance with reduction plan. A final report will be issued before the end of the second quarter of FY 2009.

II. Issues

One of the main challenges VA faces in eliminating of the unnecessary collection and use of PII is the need to balance resources among high priority projects. Currently, a cultural change is underway within the Department. Long-term VA employees are accustomed to using PII to authenticate veterans, as well as VA employees, contractors, volunteers. Much education and retraining will be required to break the habit of using PII as the primary way to verify identity. PII is relied upon quite heavily as a positive unique identifiers at VA. There are many system changes needed before VA can implement new unique identifiers that are not based on PII. It will be a challenge to find reliable unique identifiers without these new identifiers eventually causing the same challenges as are currently present.

III. Oversight and Monitoring

We understand that one of the keys to the success of this very complex any effort will be the designation of one Office with primary oversight responsibility. To this end the Office of Privacy and Records Management (OPRM) has been designated as the responsible office for oversight of the plan, VA Administrations and Staff Offices will be required to: designate a representative to the Workgroup who will attend the regularly scheduled meetings and serve as the point of contact for all business related to the plan; provide updates to OPRM on a regularly scheduled basis; and to provide updates to VA senior executives on the progress of their plans. Thirdly, OPRM will compile a quarterly report on the progress of the VA plan to eliminate the unnecessary use of PII and submit it with the quarterly FISMA filing.

IV. Summary

VA has already taken a very large step forward in its efforts to evaluate its holdings of Personally Identifiable Information (PII) and to eliminating all unnecessary collections. As a part of this initiative, VA has worked diligently to develop tools, monitoring capabilities, and policies and guidance to ensure the protection of all forms of PII. These steps, coupled with our future plans, will help VA maintain a culture where appropriate uses of PII are fully protected and all information about our Nation’s veterans is treated with the highest level of confidentiality and the utmost respect.