PEO EIS
ENTERPRISE INFORMATION SYSTEMS
DEPARTMENT OF THE NAVY

PEO EIS Portal Procedures for Safeguarding Personally Identifiable Information (PII)

Contract #N00178-04-D-4020 | **10 September 2010**

Submitted By:
Deloitte Consulting LLP
1725 Duke Street, Suite 300

Contents

1.Introduction

The Department of the Navy (DON), like many other federal agencies and departments, develops policy and procedures with the intent to make technology safer for all users and prevent breaches of sensitive information. Reference (a) states the loss of Personally Identifiable Information (PII) has impacted more than 200,000 Navy and Marine Corps personnel and the DON is taking efforts to reduce PII breaches and identify and report any mishandling of PII. The most common causes of PII loss, as stated in Reference (a) are human error, theft, postal, insider threat and hackers. Human error constitutes the majority of breaches and examples include material being erroneously posted, emails with attachments being improperly forwarded and site restrictions being unintentionally removed.

The loss of sensitive personal information is costly, time consuming to rectify, interferes with the DON mission and requires that all commands and content owners must take action to prevent the mishandling of PII. Compromised PII creates unnecessary risk of identity theft for our warfighters and the DON workforce, and could potentially adversely affect the DON's reputation. The careful management of personal information is critical for the DON.

1.1. References

(a). ALNAV 057/07 SECNAV WASHINGTON DC – Safeguarding PII from Unauthorized Disclosure
(b). ALNAV 070/07: SECNAV WASHINGTON DC– DON PII Annual Training Policy
(c). DTG 201839Z NOV 08 **–** Protecting Personally Identifiable Information on Department of the Navy Shared Drives and Application Based Portals
(d). SECNAVINST 5211.5E – DON Privacy Program Instruction
(e). SECNAVINST 5210.8D – DON Records Management Program
(f). PEO EIS Portal PII Spot Check Results

1.2. Enclosures

1. DON PII Spot Check Form
2. PEO EIS PII Spot Check Schedule

1.3. Scope

The PEO EIS Portal Procedures for Safeguarding PII applies only to PEO EIS Portal Area, Sub-area, and Site Collection content and does not cover paper records, laptops or desktops, electronic records not hosted within the portal, waste containers, burn bags, bulletin boards, and PDA devices. This document is not intended to contain technically-detailed information, but rather is meant to provide a policy and schedule for performing checks for PII, a method of capturing data on the results of the check, and provides a template for auditable results. This document outlines the processes for both manual and automated PII spot checks and provides information on implementing an automated solution for PII checks that would check 100% of data.

2.DOD PII Policy Guidelines

2.1. PII Safeguarding Guiding Policy

The PEO EIS Portal Team has reviewed relevant DON privacy and PII policies and documentation. The information gathered during this review was utilized to ensure the PEO EIS Portal Procedures for Safeguarding PII policy complies with DON privacy and PII policies and documentation. The relevant policies and documents are identified below:

- **DON CIO Website** - The DON Chief Information Officer (CIO) website states that lessons learned from various commands have demonstrated that implementing PII spot checks and aggressive corrective action where weaknesses are identified are essential to successful management of data.
- **ALNAV 057/07 and ALNAV 070/07; References (a) and (b) –** ALNAV policies created in an effort to minimize the mismanagement of PII. These policies assist Commanders, Commanding Officers and Officers-in-Charge with identifying weaknesses and ensure that basic PII safeguards are in place.
- **DTG 201839Z NOV 08; Reference (c) -** Protecting Personally Identifiable Information on Department of the Navy Shared Drives and Application Based Portals; reinforces current DON policy on reducing the number of incidences of mismanaged PII particularly in the case of shared drives and portals.
- **SECNAVINST 5211.5E; Reference (d) –** DON Privacy Program Instruction is the policy provided to guide leadership in privacy management practices and procedures to evaluate privacy risks in DON websites and unclassified non-national security information systems.
- **SECNAVINST 5210.8D; Reference (e)** – DON Records Management Program; provides policy on the creation, maintenance, use, and disposition of information as records in all media, including electronic, and establishing responsibility for the DON Records Management Program
- **PII Spot Check Form; Enclosure (1) -** The DON CIO form is the guide for PII assessment. Checklist line 17 (website guidance) is the only applicable checklist item for the PEO EIS Portal.

2.2. DON PII Safeguard Policy Requirements Overview

The relevant requirements gleaned from the DON privacy and PII policies and documentation are summarized below. These requirements have driven the content of this PII safeguarding document and are intended as a guide for commands to check for PII weaknesses. The actual PII plan or policy is to be tailored to meet the specific needs of the command.

- Perform spot checks for PII semi-annually
- Check at least 25% of content of sites or data within its root and Site Collections
- Record auditable results and retain for up to three years
- Should PII be found, corrective action must be taken to remove the data and resolve problem areas where weaknesses are found and report PII breaches to the DON CIO Privacy office
- Submit auditable results to local Privacy Act office

2.3. Defining PII

PII of concern is information which carries some risk-of-harm to an individual or to the command should the information be accessed by unauthorized personnel. PII of this nature is considered to be "sensitive" and must be protected.

Sensitive PII, as Reference (d) and Enclosure (1) state, includes but is not limited to:

- Full Social Security number (SSN)
- Date and place of birth
- Personal financial information
- Personal medical information
- Passport numbers
- Financial, credit, and medical data
- Security clearance level
- Leave balances; types of leave used
- Home address and telephone numbers (including home web addresses)
- Mother's maiden name; other names used
- Drug test results and the fact of participation in rehabilitation programs
- Family data
- Religion, race, national origin
- Performance ratings and pay pool information
- Names of employees who hold government-issued travel cards, including card data
- Any non-sensitive PII listed contextually with sensitive information

The following PII is normally considered to be not sensitive for all employees and contractors and is releasable to the public:

- Full name
- Work phone
- Work email
- Code
- Rank
- Work location
- Badge number
- Assigned position

Although the above stated PII is not considered to be sensitive, all non-sensitive PII must be examined in its context of use. If non-sensitive PII is contextually associated with sensitive information, the PII would then be considered sensitive. For example, if a list of only names (normally not sensitive PII) is in a folder marked 'Employees who failed a drug test', this would be considered sensitive PII and would not be allowed to be posted on the PEO EIS Portal.

3.PEO EIS Portal PII Safeguard Procedures

3.1. Overview

In an effort to ensure PII is not stored on the PEO EIS Portal and to be in compliance with DON policy on PII spot checks of content, the PEO EIS Portal will conduct semi-annual PII spot checks of content within its root and Site Collections. Auditable records will be developed and maintained for three years and will be stored on the PEO EIS Portal within the PMW-270 program area. Should PII be found on the portal, corrective action will be taken to appropriately remove the data, take necessary steps to prevent future mishandling of PII and breaches are to be reported to the DON CIO Privacy Team.

Checks for PII within the PEO EIS Site Collections can either be a manual process or an automated process. An automated solution is a best practices option where technically feasible and cost effective as it provides 100% coverage of a PII check with little to no man hours to implement. The manual process is more labor intensive and only checks about 25% of portal data, but in some instances, may be the best or only option for the spot check.

3.2. Semi-Annual PII Spot Check Execution

Automated Process - An automated PII spot check process would be implemented based on requirements of the specific software and would be according to guidelines specified in section 2.2 of this document. The automated spot check would be implemented and results compiled and reported by the PEO EIS Portal Team. There are two software applications which are DADMS approved and currently being implemented in DON portal systems, which could be utilized by PEO EIS, however, other automated solutions could be considered as well.

- Power Grep 3.5.2 - DADMS Approved
  DADMS 55317

- DT Search Desktop 7.54 - DADMS Approved
  DADMS 53409

The PEO EIS Portal Team will compile results based on data provided by the software and report the results to the PMW-270 Program Manager. If PII is found, a record of how much data, what type of data (SSN#s, home addresses, etc.), how many user have access to the area in which it was found and any other important data relevant to the description of the data will need to be recorded.

Manual Process - The PEO EIS Portal Team Program Manager (PM) will notify the government leads of areas of responsibility scheduled to be spot checked at least 60 days prior to the due date of the results of the scheduled spot check. The Portal Team Program Manager will task the action to perform the spot check and will provide guidance on spot check procedures. Spot checks are to be initiated by program area government leads and performed by assigned area content administrators or POCs (roles and responsibilities outlined in section 3.3).

The personnel assigned to check the portal for content will need to:

- Check 25% of sites, a listing of sites which need to be checked will be provided by the PEO EIS Portal Team and Program Manager
- Check 25% of the root according the PEO EIS Portal PII Spot Check Schedule, Enclosure (2)

The PII spot check will involve opening folders and documents to review for PII as defined in section 2 of this document. The PEO EIS Portal Team will determine how many sites need to be checked for each semi-annual spot check, in order to meet the requirement of checking 25% of sites. A spot check list will be created by the PEO EIS Portal Team and provided to program area managers prior to implementing each spot check. The list will include all Site Collections, My Sites and portal areas that need to be checked and will consider new sites and areas that have been added to the portal since the last spot check. Over the course of two years, the entire root and all Site Collections are scheduled to be checked.

POC spot check personnel will be provided with instructions on how to conduct the spot check, a list of areas and sites to check and the template for reporting the results as the spot check date approaches. The POCs will be requested to complete the PEO EIS Portal PII Spot Check Results Table (Table 1.) and return to the PEO EIS Portal Team Program Manager for compilation of auditable results. The PEO EIS Portal Team will be responsible for compiling the data into an auditable report, posting the results on the PMW-270 area of the portal and forwarding a copy of the final report to the local Privacy Act Office. A detailed list of Site Collections, My Sites and areas checked are to be available with the auditable results and posted on the PMW-270 area of the portal.

Results of the manual spot check will be reported to the PMW-270 Program Manager. The program area spot check POC or government lead will provide the completed PEO EIS Portal PII Spot Check Results Table (Table 1.) to report the results of the spot check. The data that will be provided is as follows:

- Site or area name and URL checked
- Date the site or URL was checked
- Indication if PII was found
- POC performing the area or site spot check
- Comments or action taken (if required)
- If PII is found, indicate how much data, what type of data (SSN#s, home addresses, etc.), how many user have access to the area in which it was found and any other important data relevant to the description of the data

Table 1. – PEO EIS Portal PII Spot Check Results Table

Area/Site Name and URL	Date	PII Found	POC	Comments / Response

3.3. Roles and Responsibilities

PEO EIS Portal Program Manager

- **Automated Process**
  - Coordinate with DON CIO to appropriately respond to any reports of PII
- **Manual Process**
  - Engage with area PMs to task with PII spot check in their area of responsibility
  - Provide clear instructions to the PMs on how to conduct the PII spot check
  - Provide PEO EIS Portal PII Spot Check Results Table (Table 1) as a format for results gathering
  - Receive results of the spot check provided by the PMs
  - Coordinate with DON CIO to appropriately respond to any reports of PII

Program Manager/Government Lead

- **Automated Process**
  - No action
- **Manual Process**
  - Assign PII spot check POC and spot check personnel
  - Enforce the PII spot check implementation
  - Provide results of the spot check to the PEO EIS Portal PM
  - Report any found PII to the PEO EIS Portal PM and take necessary action to remove the data and resolve the weakness

PEO EIS Portal Team

- **Automated Process**
  - Install software and initiate the automated PII spot check
  - Tabulate and post results of the spot check as directed by the PEO EIS Portal PM
- **Manual Process**
  - Create spot check instructions, a new list of sites and areas to check and the template for reporting the results prior to each spot check
  - Determine how many sites need to be checked to meet the 25% requirement
  - Assist program area POCs in the spot check by responding to questions and providing guidance as needed
  - Tabulate and post results of the spot check as directed by the PEO EIS Portal PM

Program Area Spot Check POC/Administrator

- **Automated Process**
  - No action
- **Manual Process** Perform the spot check of data according to the instructions provided by the PEO EIS Portal PM
- Tabulate the results using the PEO EIS Portal PII Spot Check Results Table (Table 1) or similar format and return results to area PM for review

3.4. PEO EIS Portal PII Response

If PII is found on the portal, the following steps must be taken promptly:

- The spot check POC will contact the PEO EIS Portal Team to seek assistance on how to proceed
- If it is determined the breach is significant, the PEO EIS Portal Team will lock the area from all users
- The spot check POC will not delete any data until directed to do so by the PEO EIS Portal Program Manager
- The PEO EIS Portal Team will respond to each incidence of reported PII on a case by case basis

If PII is discovered, the PEO EIS Portal team will report the incident to the PEO EIS Portal Team Program Manager immediately for direction on how to proceed to address the specific instance of PII discovery. Generally, if the PII is considered a significant breach, the PEO EIS Portal Team will close the area to all users and individuals of compromised information must be notified prior to the information being removed from the site. If the data is considered a low risk breach, meaning few users have access to the information and the information is minimally invasive, the content should be removed from the portal and the recycle bin by either the PEO EIS Portal Team or the spot check POC. If PII is found, and the documentation is deemed to be official documentation, as define in Reference (e), respond as directed in Reference (c). The PEO EIS Portal Team Program Manager will contact DON CIO PII points of contact as indicated in Reference (b) to report the discovery and obtain guidance on any additional required action to address the specific instance of PII.

3.5. Recurring Communication with Users on PII Policy

As part of its Continuous Process Improvement, to increase the effectiveness of Portal PII safeguarding procedures, the PEO EIS Portal Team identified that many users are not aware the PEO EIS Portal is not accredited to allow PII. In an effort to inform the user community of the DON and the PEO EIS Portal PII policy and restrictions, the PEO EIS Portal Team will send out communications to its users semi-annually and post announcements on the PEO EIS Portal Program Area Homepages, with portal PII policy guidance. The policy guidance will be in accordance with References (a), (b), (c), (d) and (e) to include a list of sensitive information which constitutes PII and is not allowed to be posted on the portal. Additionally, updated DON policy will be relayed to the user community as it is released.

4. Continuous Process Improvement

4.1. Overview

As part of a continuous process improvement for the PEO EIS Portal Procedures for Safeguarding PII, following each implementation, the PEO EIS Portal Team will perform an assessment of the effectiveness of the plan and create lessons learned for future improvement of the process. The assessment of the effectiveness of the plan will include but are not limited to the activities below:

- Assess the effectiveness of the manual process and consider process improvement benefits of an automated PII process
- Assess effectiveness of interaction with POCs performing the check
- Assess adherence, clarity and timing of the instructions and data provided to the area POCs
- Assess efficiency in the POC reporting process
- Assess action taken in response to reports of found PII

Should this Continuous Process Improvement assessment reveal opportunities to significantly improve these PII safeguard procedures, lessons learned will be documented. Lessons learned will be accompanied by recommendations to update this plan that can be used to improve subsequent spot checks. Each PII Spot Check will therefore be concluded with a set of recommendations made to the PEO EIS Portal PM for approval. If approved, they will be incorporated into the next spot check procedure. In this manner, this PII Safeguard Procedure plan has incorporated outcomes of lessons learned from the previous spot checks performed.

Details of the historical lessons learned are outlined in Appendix A of this document.

Appendix A

Lessons Learned and Recommendations

PII Spot Check Ending 28 May 2010

Implement schedule for Root Site Spot Check

- **Previous Process:** The initial PII spot check of the portal reviewed a random sampling of 25% of content located within the root site and a complete check of 25% of Site Collections and My Sites hosted within the portal. The Site Collection and My Site check was found to be systematic and effective and needs no further review of process at this time. The random sampling of the root site areas was conducted by the PEO EIS Portal Team and several administrative POCs from different top level areas. POCs were instructed to perform a spot check for PII within their area of responsibility of the portal, but were given no designated set of areas to check.
- **Lesson Learned:** While a random sample spot check of the root site was appropriate for the first spot check, a more systematic procedure should be in place going forward. In order to ensure all areas of the root site are reviewed, but not redundantly reviewed, over the course of two years, a listing of areas and sub-areas and schedule for when they should be checked should be developed.
- **Recommendation:** Create a schedule for checking the root top level program areas and sub-areas so that within a two year time frame, all areas will be reviewed for PII. The area spot check schedule has been created and is represented in this document as Enclosure 2.

Engage Program Areas in performing the Spot Check

- **Previous Process:** In the previous PII spot check, the PEO EIS Portal Team performed most of the content review to ensure it was completed within the time constraints required and to minimally impact the area managers.
- **Lesson Learned:** A few program area administrators were asked to assist in the spot check and it was found that some were not aware of the DON PII policy regarding portal content or what was posted within the portal areas in which they are responsible. While some teams have a designated POC who manages portal content within the area of responsibility, some teams have little governance over posted content. By involving program area managers, it is hoped that awareness and governance of content within the areas reviewed will improve, particularly as it relates to PII. Program areas may not have full awareness of the content that is stored on the portal within their area of responsibility and thus may not know if there is PII.
- **Recommendation:** Prior to implementing the next PII spot check, engage with program area leads scheduled to perform in the next spot check to assist in designating a PII spot check POC and provide instructions to assist designated POCs in the implementation of the spot check. Review DON PII policy as necessary with

designated POCs. Refer to the root site schedule (Enclosure 2) for a list of areas scheduled to be checked next.

Implement recurring PII communications to improve user awareness of DON and PEO EIS Portal PII restrictions

- Even within the small group of area POCs that assisted the PEO EIS Portal Team with the initial PII spot check, it was discovered several did not know PII was not allowed on the Portal. Communications to educate the user community on DON PII policy as it relates to portals has been identified as needing to be implemented.
- **Previous Process:** Previous to the initial PII spot check, there were limited communications to the portal user community regarding PII on the portal.
- **Lesson Learned**: Many users are not aware PII is not allowed on the portal. Even with the small group of area POCs that assisted our PII spot check, it was discovered some did not know PII was not allowed.
- **Recommendation:** Communicate with users that PII is not allowed on the portal. In an effort to remind all portal users PII is not allowed on the PEO EIS Portal, the Portal Team will send out email messaging to the user community and post announcements on the Program Area Homepages. Messaging will inform users PII is not allowed to be posted due to portal security accreditation, explain what constitutes PII (as outlined in section 2 of this document) and provide updates in DON policy on PII as it is set.

Enclosure 1 - PII SPOT CHECK FORM (as Referenced in ALNAV 070/07 and located at web address http://privacy.navy.mil/)

This form is an internal document and will be used by command leadership to assess the level of compliance in the handling of Personally Identifiable Information (PII) as delineated by law and or specific DoD/DON policy guidance. Commands should tailor this form to fit their specific requirements. For additional guidance and information contact the Command Privacy Official at XXX-XXXX. This Spot Check form is an auditable record and shall be kept on file for three years by the Privacy Official. **Ref: ALNAV 070/07: SECNAV WASHINGTON DC 042232Z OCT 07.**

PII of concern is information which carries some risk-of-harm to an individual or to the command should the information be accessed by unauthorized personnel. PII of this nature is considered to be "sensitive" and must be protected. SENSITIVE PII includes but is not limited to: Social Security number (SSN), date and place of birth, personal financial information, personal medical information.

PII that is releasable to the public in accordance with law (5 USC §552) or regulation (5 CFR §293.311 or 32 CFR §310.22) or is commonly used in the work environment (OSD 15041-07) is not considered to be of risk to an individual nor to the command. PII of this nature is NOT "sensitive". All non-sensitive PII must be examined in its context of use. Context of use can make non-sensitive PII (a list of 'just names') sensitive if the list is contextually associated with sensitive information (list of 'just names' in a folder marked "Employees who failed a drug test").

The following PII is NORMALLY considered to be NOT SENSITIVE for all employees and contractors: name, work phone, work email, code, rank, work location, badge number, and assigned position.

ADMINISTRATIVE

1. Name of the individual assigned to conduct this spot check is _____

2. Area of responsibility checked (Bldg/Floor) _____ (Code) _____

3. Date spot check conducted _____

PAPER RECORDS

1. Has the command developed a PII records disposal program? _____

2. ____ Number of personnel onboard ____ Number of personnel that received PII training in last 12 months

Ref: GENADMIN: DON CIO WASHINGTON DC 181905Z DEC 08

3. ____ Number of PII breaches reported this calendar year ____ Number of personnel notified

4. Does the command have a SSN reduction plan in place? _____

5. Spot check 10 % of burn bags within your area of responsibility. Ensure that if they contain PII that they are secure from unauthorized access by individuals who do not have a need to know. **Ref: SECNAVINST 5211.5E 8.b. (1) through (3) – pg. 19**

Number of bags checked ____ Number of bags containing PII and not secured ____

6. Spot check 10 % of recycle containers within your area of responsibility. Ensure that no PII has been placed inside, awaiting disposal. **Ref: SECNAVINST 5211.5E 8.b. (1) through (3) – pg. 19**

Number of containers checked ____ Number of containers containing PII ____

7. Spot check 10 % of waste containers within your area of responsibility. Ensure that no PII has been placed inside, awaiting disposal. **Ref: SECNAVINST 5211.5E 8.b. (1) through (3) – pg. 19**

Number of containers checked ____ Number of containers containing PII ____

8. For static bulletin boards disseminating/displaying command information, check for the presence of PII. PII should only be available to individuals with a need to know. **Ref: SECNAVINST 5211.5E 18.d. (6) – pg. 47**

Number of boards checked ____ Number of examples of where PII was found ___

ELECTRONIC RECORDS/HARDWARE

9. For Non-NMCI networks: Is your activity currently using "Mobile Armor" to protect DAR on non-NMCI laptops, desktops and removable storage media? If no, when will a DAR product be implemented? If using other than Mobile Armor, provide date that a DON CIO waiver was granted? _____

10. For NMCI networks: Have you verified with your IAM that the data at rest encryption solution has been pushed to all NMCI laptops and desktops? (Note: laptops must be plugged in to the NMCI network to receive the push) _____

Ref: GENADMIN: DON CIO WASHINGTON DC 091256Z OCT 07

11. Has a check in /check out log for all laptops and portable electronic equipment been created and implemented for all such devices that contain PII on >24 individuals and that are transported outside a secure government space. Does the supervisor maintain this log and can it be produced upon request. **Ref: DONCIO 171952Z APR 07**

_____

12. Spot check at least 10% of PDA/Blackberries within your area of responsibility. Ensure the time out function is enabled and each unit is password protected. **Ref: SECNAVINST 5211.5E 18.d. (5) – pg. 47**

Number of units not in compliance ____ Not applicable, AOR has no PDA's _____

13. Spot check 10% of laptops within your area of responsibility. Ensure all data is encrypted, the time out function is enabled and each unit is password protected. **Ref: SECNAVINST 5211.5E 18.d. (5) – pg. 47**

Number of laptops checked ____ Number of laptops not configured as required _____

14. Search and spot check 25% of files on the shared drives within your area of responsibility. Ensure that no PII has been posted.

Number of files checked ____ Number of files containing PII ____

15. Are all computer hard drives physically destroyed when sent to disposal? _____

16. Are copier/printer machine hard drives sanitized or destroyed prior to disposal?

_____

WEBSITES

17. Spot check 25% of AOR web sites (internal and external), searching for PII that is available to individuals who do not have a need to know. **Reference: SECNAVINST 5720.47B 7.d. (1) – pg. 4**

Number of sites checked ____ Number of records with PII ____ N/A, no AOR web site _____

Enclosure 2 - PEO EIS PII Spot Check Schedule

Program/Competency Area	Approx. Site Count	5/31/2010	11/30/2010	5/31/2011	11/30/2011
MySites	934	25% (234) - Checked	25%	25%	25%
Site Collections for All Areas	303	25% (76) - Checked			
BLII (One-Net) Engineering	62	Checked	Remainder		
Acquisition			x		
Communications /PR			x		
Engineering			x		
IA Operations			x		
Integrated Master Schedule		Checked			
Legal		Checked			
Logistics		Checked			
Meeting and Conferences		Checked			
Migration		Checked			
One-Net Admin		Checked			
One-Net C&A		Checked			
One-Net Deployables		Checked			
One-Net LRI		Checked			
One-Net Deployables		Checked			
One-Net Standards		Checked			
Operational Guidance		Checked			
PC Refresh		Checked			
PIERS		Checked			
Production		Checked			
Reference Documents		Checked			
Tier IV		Checked			
DASN ALM	12		x		
ESOL	13	Checked			
ESol Team		Checked			
Oracle Applications Suite Analysis		Checked			
Resource Documents		Checked			
Senior Leadership		Checked			
FPPS	3		x		
GCSS-MC	1		x		
Navy ERP	3			x	

NGEN	33		Remainder		
Acquisition Documents			x		
Business Operations			x		
Network Operations			x		
NGEN Competencies			x		
NGEN IPT			x		
Program Control			x		
Program Manager/Deputy Program Manager				x	
SE&I Gov				x	
Service Delivery				x	
Strategy				x	
T&E				x	
Technical Director				x	
Transition/CRM				x	
NMCI	73		Remainder		
Acquistion			x		
Budget			x		
Business Operations			x		
Contracts		Checked			
Cost Baseline			x		
CTR Community & Resources			x		
Engineering			x		
FY06 Portal Deliverables				x	
Legacy Environment				x	
Legal				x	
Logistics				x	
New Business				x	
NMCI CoOP BCA Project				x	
PAO				x	
PCO					x
Pre-Production and Deployment					x
Program Management					x
Security					x
Senior Leadership					x
Service Delivery IPT					x
STEAG					x
Test & Evaluation					x
PEO EIS Competencies	31			Remainder	
Acquisition		Checked			
Business Process Solutions				x	

Engineering				x	
Financial Management				x	
ITSM COE				x	
Operations					x
PAO					x
PEO EIS Competency Leads Team					x
Program Management Competency Board					x
Technical Authority					x
Total Force Management		Checked			
Welcome to PEO EIS		Checked			x
PEO-IT Archive	33				Remainder
PMW 270	1		x		
CMMS			x		
JALIS			x		
DON JCIS			x		
Portal Support	2		x		
Sea Warrior	25	Checked		Remainder	
1.0 Finance				x	
2.0 Contracts		Checked			
4.0 Logistics & Fleet Support		Checked			
5.0 Engineering				x	
6.0 Program Management				x	
8.0 Corporate Operations		Checked			
Other	11		x		