PRIVACY 100: STAND DOWN TRAINING - What you Need to Know about Safeguarding Protected Personal Information/Personally Identifiable Information (PPI/PII)

DEFINITIONS: WHAT IS PPI/PII???

» PPI stands for Protected Personal Information

- PPI stands for Protected Personal Information.
- PII stands for Personally Identifiable Information.
- PPI and PII are interchangeable at this time.
- Definition: Information which can be used to identify a person uniquely and reliably, including but not limited to name, social security number, address, telephone number, e-mail address, mother’s maiden name, etc.

STAND DOWN

- This STAND DOWN training is designed to focus on the importance of PRIVACY and to ensure all DON personnel (military, civilian, and contractor) are aware of the vital role they must play in ensuring that PPI/PII is properly protected from unauthorized disclosure.

YOU NEED TO KNOW ABOUT PRIVACY BECAUSE…

- It’s information we are collecting, maintaining, distributing and disposing of about you!
- It also requires you to take precautions when collecting, maintaining, distributing, and disposing of PPI/PII required by your job.
- It’s a factor in developing best business practices.
- It contains both civil and criminal penalties for non-compliance.

VA's BIG BREACH

- The VA's loss of thousands of records on veterans was well publicized, costly, and brought to the forefront the need to shore up actions to protect privacy data.
- It resulted in strong Presidential and Congressional Interest.
- As a result, Office of Management and Budget (OMB) to established working groups to address better protections, notification protocols, costs, actions to be taken against employees, etc. Their inputs are due by 1 Oct 06.

Why are you here for training?

- **The Office of Management and Budget (OMB) issued a memo on May 22, 2006, to Heads of Departments and Agencies entitled "Safeguarding Personally Identifiable Information." It directed agencies to train their employees on their responsibilities to safeguard personally identifiable information and was precipitated by the massive VA Breach.**

- **ALNAV 059/06, Safeguarding Personnel Information, issued on 15 Jul 06 told DON to comply. This was reiterated in the Marine Corps by MARADMIN 330/06 of 21 Jul 06, entitled "Notification of Responsibilities Regarding the Safeguarding of Protected Personal Information."**

- **NAVADMIN 208/06 of 25 Jul 06, entitled "Navy Policy on Handling of Privacy Act Information" reiterated the need to ensure training, and identified a three phase plan designed to improve privacy.**

Why are you here for training? con't

- To understand the important role you play in ensuring privacy is properly protected.
- To get you involved in identifying best business practices to protect privacy.
- To make you aware of consequences for non-compliance.
- To ensure you understand privacy because KNOWLEDGE IS POWER!

DON PA RESPONSIBILITIES

- Establish rules of conduct for collecting, maintaining, distributing, and disposing of personal information.
- Publish PA system of records notice in the Federal Register for all approved privacy collections of information.
- Ensure we collect only data that is authorized by law.
- Only share data with those individuals having an official need-to-know.

DON PA RESPONSIBILITIES

- Establish and apply data safeguards to protect information from unauthorized disclosure.
- Allow individuals to review records about themselves for completeness and accuracy.
- Allow individuals to amend their personal records regarding factual information that is in error.
- Keep a record of disclosures made outside of DOD to authorized “routine users” described in the PA system notice.

Examples of Personal Data which is Privacy Sensitive and Requires Protection

- **Financial, credit, and medical data**
- **Security clearance level**
- **Leave balances; types of leave used**
- **Home address and telephone numbers (including home web addresses)**
- **Social Security Number**
- **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**
- **Names of employees who hold government-issued travel cards, including card data**

LOSS OF PPI/PII

- Can be embarrassing.
- Can cause emotional distress.
- Can lead to identity theft, which is costly to the individual and to the Government.
- Can impact our business practices.
- Can result in actions being taken against the employee.
- Can erode confidence in the Government’s ability to protect information.

DEPSECDEF MEMO

- On 15 Jun 2005, DEPSECDEF issued a memo entitled, “Notifying Individuals When Personal Information is Lost, Stolen, or Compromised.”
  - It requires DoD activities to notify individuals within 10 days after the loss or compromise of protected personal information is discovered.
  - The notification would advise individuals of what specific data was involved, the circumstances surrounding the loss, theft, or compromise, and what protective actions the individual can take. when personal information is lost, stolen, or compromised.

Since that issuance

- Navy and Marine Corps have reported over 25 losses
  - Most involved lost or stolen laptops, computers, thumb drives, etc.
  - Some involved paper records not being properly disposed or paper documents being misplaced or stolen.
  - Notifications to affected persons is time-consuming and costly.
  - Congress is interested in privacy breaches.

Breach Notification Procedures

- We are required to inform affected personnel within 10 days of discovering the breach.
- Detailed instructions on Breach Notification are being vetted and will be disseminated shortly and posted at http://privacy.navy.mil.

WHY DO WE COLLECT PERSONAL INFORMATION ABOUT YOU???

- We need it to
  - hire you
  - retain you
  - pay you
  - separate you
  - compensate you
  - locate you
  - educate you
  - discipline you
  - rate you
  - provide services to you
  - ETC

TRANSPARENCY

- This is the “in” word to describe what our Privacy Program should look like – it should be transparent to anyone who wants to know what records we are maintaining, how we are maintaining those records, disseminating information from those records, and disposing of those records.

How do you know what kinds of records we are maintaining on you?

- We tell you…
  - When soliciting PPI/PII information directly from you we provide you with a Privacy Act Statement (PAS) that identifies the authority for collecting the information; the purpose; routine uses, and whether disclosure of the information is voluntary or mandatory.
  - We also publish our Privacy Act systems of records notices in the Federal Register and on http://privacy.navy.mil.

We give you the right to:

- Request copies of the records we are maintaining on you.
- To designate a person to have access to information about you: parent, spouse, friend, attorney, congressman, colleague, etc.
- To seek amendment of any factual inaccuracies (not opinions).
- To understand how long records will be maintained before being accessioned or destroyed.
- Appeal any denial of information.

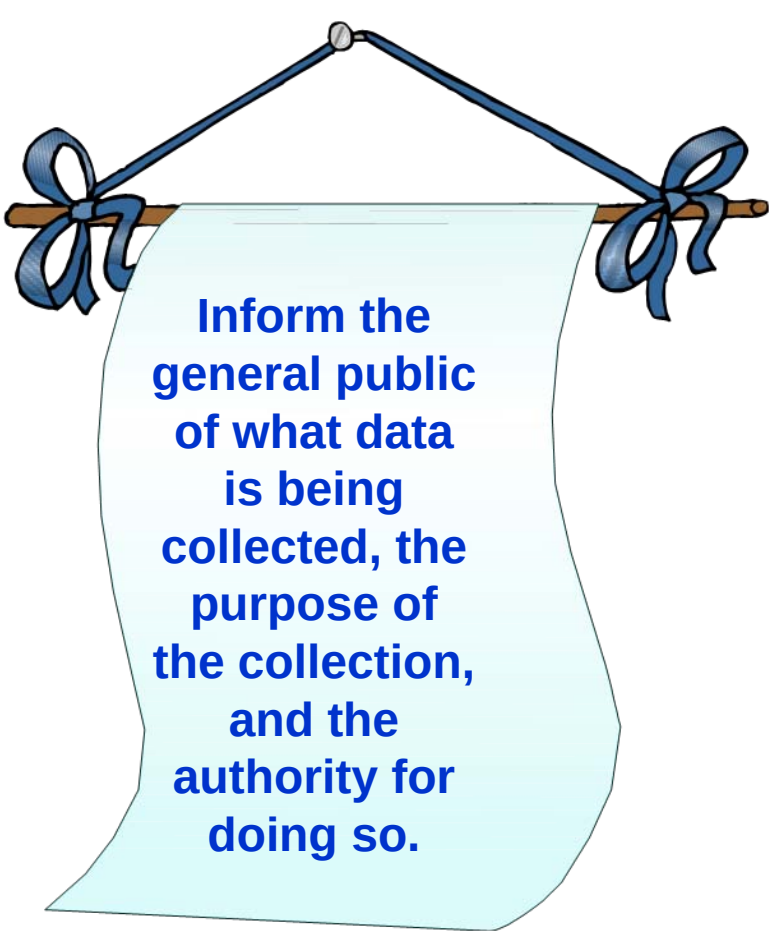
PRIVACY ACT SYSTEMS OF RECORDS NOTICES

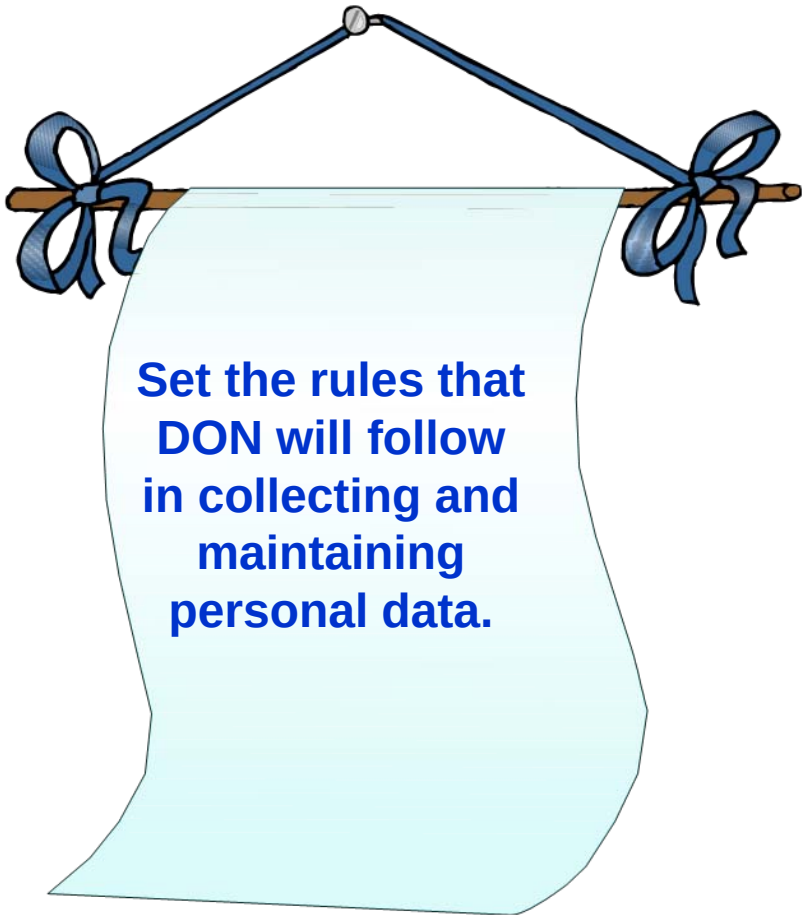
- With the passage of the Privacy Act, Executive Branch agencies had to identify “systems of records” that allowed for the collection of information that was retrieved by a person’s name and/or personal identifier.

- Today, the DON has over 250 approved Privacy Act systems of records which identify the kinds of records we can maintain on you. They are listed at http://privacy.navy.mil.

What purpose does a Privacy Act Systems of Records Notice serve?

- **It serves to:**





OVERVIEW OF PA SYSTEMS OF RECORDS

- We maintain systems of records that are unique to a specific activity, such as the Naval Academy, Naval Criminal Investigative Service, Navy Exchange Command, Navy Personnel Command, Naval Inspector General, etc.
- We maintain systems of records that can be used by any Navy and/or Marine Corps activity – called Umbrella systems.
- We sponsor systems that cover all of DoD and its services and components (DoD Birth Defects Registry).
- We also use Government-wide systems of records, such as those created by OPM – civilian personnel records; Dept of Labor – workmen's comp; etc.

Releasability

- Because we generally collect information about you from you – most of our systems of records for which you are the subject are releasable to you in their entirety.

COLLECTING PPI/PII

- If you collect it – you must protect it!
- If in doubt – leave it out – do you really need the entire SSN or will the last 4 digits serve as a second qualifying identifier?
- Just because we've always done it that way doesn't mean this remains the best business practice.

When Moving from Paper to Electronic Records – Think Privacy

- **Moving from a paper process into an electronic process requires you to identify any risks that would subject personal information to compromise. In other words, yesterday's SOP when moved from paper to an electronic means may open us up to a potential privacy breach.**
  - **For Example: Promotion lists for FLAG OFFICERS containing full names and SSNs were sent to Congress in paper form and placed in the Congressional Record which was not readily available/accessible. Once the Congressional Record was placed on the Internet, its contents were available for all to see. This resulted in credit cards being opened up on those FLAG OFFICERS which resulted in identity theft.**
    - **Result: We had to change our business practice.**

Think Privacy – con't

As we move from the paper environment to the electronic environment we must factor in safeguarding of personal information.

- The fact we have always done it this way may no longer be feasible.
- We need to address whether collection and maintenance of "all" that information we previously collected is "relevant and necessary" and whether we can maintain "timely and accurate" information.
- As we move into electronic records that collect and maintain PPI/PII, we need to conduct a Privacy Impact Assessment (PIA) to mitigate vulnerabilities. Your CIO should know about this and be able to provide you guidance.

MORE BEST PRACTICES

- **When you receive an email and it contains personal information about another individual, do not forward that document to others without first assessing whether each recipient has an official need to know.**
- **Use training to educate your personnel on Privacy.**
  - **Ensure all newly assigned personnel receive orientation training on the Privacy Act so they fully understand their role in ensuring that personal information is protected from unauthorized disclosure.**
  - **Ensure all personnel receive refresher training once a year or more often should they be involved in a breach (loss) of personal information.**
  - **Ensure that supervisors take Privacy Act training 102 from http://privacy.navy.mil.**
  - **Ensure all personnel who deal with personal information contained in a Privacy Act system of records are properly trained on the systems notice and the safeguards addressed therein and the restrictions regarding access to the information.**

Protecting PPI/PII

- **Think about ways to ensure that PPI/PII is properly protected.**
- **Think about your computer, memory stick, PDA, etc., and what PPI/PII information you store on it. What would you do if they were stolen?**
- **Think about emails – if you receive emails that contain PPI/PII – are they properly marked alerting you to treat them as FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE – Any misuse or unauthorized access may result in both civil and criminal penalties? Do you properly mark your emails?**
- **Think privacy when you create documents, do you need to include the entire SSN or will the last four digits work?**
- **Think privacy and do not include the entire SSN in the subject line of an email for all to see.**

Protecting PPI/PII – con't

- Think privacy and do not place PPI/PII in public folders in Outlook for others to see.
- Think privacy and do not place PPI/PII information on public web sites.
- Think privacy and identify ways to ensure PPI/PII is not compromised!

DISPOSAL OF PPI/PII

- Don’t assume that documents containing PPI/PII that are placed in a recycle bin are being shredded prior to being recycled..
  - Recent audits confirmed that documents containing PPI/PII were not properly disposed of.
- Best practice – cross cut shredding.
- Dispose of PPI/PII in a manner that does not result in a privacy breach.

MAINTAINING INFORMATION

- If you maintain information that is retrieved by a person's name and/or personal identifier, you must identify a Privacy Act system of records that permits that collection and follow the rulemaking set forth in the systems notice.
- All PA systems of records notices are listed at http://privacy.navy.mil.

DISTRIBUTING INFORMATION

- Under the Privacy Act, individuals who have an official need to know may have access to that portion of a record.

- If a disclosure is being made outside the Department of Defense, the systems notice must identify the recipient and why they are receiving it. For example, to the Department of Veteran's Affairs for the purpose of providing medical care.

- All disclosures outside the Department of Defense require a disclosure accounting (I gave it to _____ for this purpose on _____).

DON PA RESPONSIBILITIES

- Upon written request, provide a copy of the record to the subject of the file.
- Maintain only accurate, timely, and complete information.
- When directly soliciting personal information, provide a PA Statement that addresses the authority for the collection, purpose for the collection, routine uses that will be made of the information, and whether collection is voluntary or mandatory.

DON PA RESPONSIBILITIES

- Follow the guidance set forth in the PA systems notice regarding release/withholding of information.
- With some exceptions provided for in the PA, make no disclosure of information without the record subject's written consent.
- When contracts are awarded that involve PA data, ensure the contract contains the appropriate Federal Acquisition Regulation (FAR) privacy clauses.

WHAT ARE YOUR RESPONSIBILITIES???

- As an employee, you play a very important role in assuring DON complies with the provisions of the Privacy Act. Accordingly,
  - DO NOT collect personal data without authorization.
  - DO NOT distribute or release personal information to other employees unless they have an official need-to-know.

WHAT ARE YOUR RESPONSIBILITIES???

- DO NOT be afraid to challenge “anyone” who asks to see PA information for which you are responsible.
- DO NOT maintain records longer than permitted under records disposal.
- DO NOT destroy records before disposal requirements are met.
- DO NOT place unauthorized documents in PA systems of records.

WHAT ARE YOUR RESPONSIBILITIES???

- DO NOT commingle information about different individuals in the same file.
- DO NOT transmit personal data without ensuring it is properly marked. Use ‘FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE.’
- DO NOT use interoffice envelopes to mail Privacy data.
- DO NOT place privacy data on shared drives, multi-access calendars, the Intranet or Internet that can be accessed by individuals who do not have an official need to know.

WHAT ARE YOUR RESPONSIBILITIES???

- DO NOT create a new system of records without first consulting your Privacy Officer or CNO (DNS-36).

- DO NOT hesitate to offer recommendations on how to better effectively manage privacy data.

YOUR INSIGHT COUNTS!!! YOU DEDICATION TO PROTECTING PRIVACY IS PARAMOUNT TO OUR SUCCESS!!!

REVIEW BUSINESS PRACTICES

- Review how information is stored and transmitted, as a breach, loss or compromise of information is costly to the government, to the individual whose identity is at risk, and to the individual who is involved in the loss/ compromise/theft.

- Individuals who use laptops, blackberrys, etc., must comply with DON directives/guidance on how to prevent loss.

LOSS OF PRIVACY INFORMATION

- If you lose personal information, you must report that loss immediately to the head of your organization, as there are distinct reporting requirements that must be followed.
- When in doubt, contact DNS-36 at 202-685-6545.

CONTRACTORS

- AS WE MOVE INTO A BLENDED WORKFORCE, WE MUST ENSURE THAT OUR CONTRACTORS UNDERSTAND THAT THEY TOO MUST COMPLY WITH OUR PRIVACY PROGRAM AND FOLLOW THE SAME RULES AS IF THEY WERE A GOVERNMENT EMPLOYEE.

PENALTIES

- There are criminal penalties addressed in the Privacy Act. They are based on knowing and willfully:
  - Obtaining records under false pretenses.
  - Disclosing privacy data to any person not entitled to access.
  - Maintaining a system of records without meeting public notice requirements.
- Result: Misdemeanor criminal charge and a fine of up to $5000.

PENALTIES

- Courts may also award civil penalties for:
  - Unlawfully refusing to amend a record.
  - Unlawfully refusing to grant access to a record.
  - Failure to maintain accurate, relevant, timely, and complete information.
  - Failure to comply with any PA provision or agency rule that results in an adverse effect on the subject of the record.

PENALTIES FOR THESE VIOLATIONS INCLUDE:

Actual damages

Payment of reasonable attorney's fees

Removal from employment

How will I know if the data that I handle is Privacy Act protected data?

- **Privacy data should be marked: "For Official Use Only – Privacy Sensitive: Any misuse or unauthorized disclosure may result in both civil and criminal penalties."**
- **Be aware that privacy data may not always be marked as such. If you have questions about whether data is protected under the Privacy Act, ask your supervisor or your Privacy Officer.**

WHAT'S ON THE HORIZON FOR PRIVACY?

- WE WILL BE ISSUING INFORMATION ASSURANCE GUIDANCE (DON CIO).
- WE WILL CONTINUE TO UPDATE OUR PA SYSTEM OF RECORDS NOTICES.
- WE WILL LOOK FOR WAYS TO ELIMINATE THE OVER-COLLECTION OF SSNS.
- WE WILL DEVELOP MORE TRAINING MODULES AND OFFER TRAINING ON NAVY KNOWLEDGE ONLINE (NKO).
- WE WILL BE PERFORMING MORE PRIVACY IMPACT ASSESSMENTS ON OUR PA SYSTEMS AND REPORTING THE RESULTS TO OMB.

WHAT'S ON THE HORIZON?

- OMB WILL BE ISSUING NEW GUIDANCE.
- EXPECT STRONGER LEGISLATION TO PROTECT PRIVACY.
- LOOKING TO ADD PRIVACY TRAINING TO OUR ANNUAL SECURITY TRAINING.
- DEVELOP MORE BEST PRIVACY PRACTICES.
- REVISE SECNAVINST 5211.5E.

PRIVACY TOOLBOX

- HTTP://PRIVACY.NAVY.MIL: ONE STOP SHOPPING TO PRIVACY ISSUANCES, POLICIES, GUIDANCE, SYSTEMS OF RECORDS NOTICES, ETC
- SECNAVINST 5211.5E, DON PRIVACY PROGRAM
- YOUR LOCAL COMMAND'S IMPLEMENTING PRIVACY INSTRUCTION

THINK PRIVACY

- YOUR ATTENTION TO PRIVACY SERVES EVERYONE!
- FACTOR PRIVACY IN YOUR WORKPLACE!
- DEVELOP BEST PRACTICES!

- PLEASE DIRECT ANY QUESTIONS TO YOUR PRIVACY OFFICER OR TO DORIS LAMA, CNO (DNS-36), 202-685-6545, DORIS.LAMA@NAVY.MIL