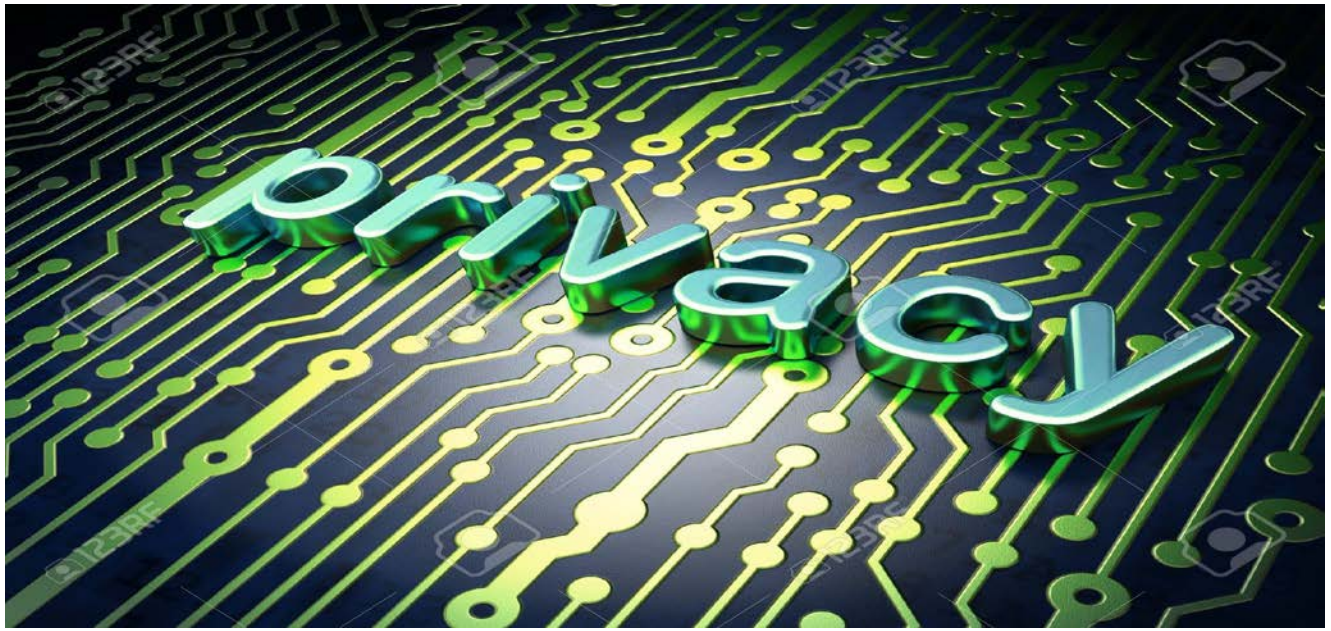

DON IT Conference East Coast

How the DON is protecting Your Privacy

Steve Muck, DON CIO

20 April 2016

Agenda

- Introduction
- Privacy Definitions
- PII Breach Trends, Metrics and Impact
- OPM Data Breach # 2
- Spear Phishing
- SSN Reduction
- Use of the DoD ID Number
- Handling PII in the office
- Your PII responsibilities
- What's New?
- Helpful Links

Definition of Personally Identifiable Information (PII)

"…information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a SSN; age; rank; grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical and financial information."

~ DoD Memo 21 Sep 07

PII and Non-sensitive PII

PII

PII may cause harm to an individual if lost/compromised

- **Financial information: bank account #, credit card #, bank routing #**
- **Medical Data: diagnoses, treatment, medical history**
- **Full or truncated Social Security number**
- **Place and date of birth**
- **Mother's maiden name**
- **Passport #**
- **Numerous low risk PII elements aggregated and linked to a name**

Non-sensitive PII

Non-sensitive PII includes business related PII, generally releasable under FOIA or authorized by DoD/DON policy

- **Pay grade/rank**
- **Office phone number**
- **Office address**
- **Office email address ***
- **Full name****
- **DoD ID / EDIPI**
- **DoD Benefits number**

***Note:* email phishing is a growing problem**

****Note: public release of names is causing increased security concern**

Identity Theft/Fraud Trends

- The Bureau of Justice Statistics reports ~ 7% of adults (12 million) were victims of ID fraud in 2012
- Government documents/benefits fraud (46%) most common, credit card: 13% (Source: FTC)
- 1 in 4 data breach victims became ID fraud victims (Source: Javelin Strategy & Research)
- Miami/Ft Lauderdale had highest incidence of identity fraud in 2012 (Source: FTC)
- 3 out of every 5 victims did not know the source of their fraud (Source: Javelin Strategy & Research)
- 85% of cases involved use of existing accounts such as credit card or bank accounts (Source: BJS)
- 29% of victims spent a month or more resolving credit problems (Source BJS)
- "Friendly Fraud" 1 in 7 ID thieves were known by their victims (Source: Javelin Strategy & Research)
- >50% of victims detected fraud using financial alerts, credit monitoring, or by monitoring their own accounts (Source: Javelin Strategy & Research)
- ID fraud of children and deceased individuals is a growing problem. Go to: http://www.youtube.com/attribution_link?a=RMkHNqw-_aU&u=/watch%3Fv%3DZcwN3FSLiTY%26feature%3Dem-share_video_user

Breach Statistics

	FY 2012	FY 2013	FY 2014	FY 2015	FY 2016 (Jan only)
Number Impacted	1,780/mo	2,320/mo	2,557/mo	2,331/mo	598/mo
Number of "high risk" breaches	17/mo	24/mo	15/mo	14/mo	17/mo

Problem areas: # 1 Unencrypted email transmission
2 Misuse of command rosters

Good news: While the number of reported breaches has not changed, the number of affected personnel has been dropping.

OPM Data Breach #2

1. Hackers accessed OPM SF 85, 85p, 86 affecting ~21.5M DON personnel who submitted applications since 2000
2. PII elements include: name, SSN, residence and employment history; family, health, criminal, and financial information; and personal and business acquaintances.
3. Notifications will be sent to affected personnel later this month via U.S. mail. Mailings will take approx. 12 weeks.
4. Affected personnel are automatically enrolled in identity and restoration services 1 Sep. After notification opt in for credit monitoring services now good for ten years. Offered to spouses and minors.
5. **There has been no confirmation that ID fraud is occurring using the breached OPM data.**
6. For most current info go to: www.secnav.navy.mil/opmBreachDON/.
7. Expect changes from OMB regarding breaches and credit monitoring.

Credit Monitoring Services

CSID Protector Plus Includes:

- **Credit Monitoring:**
  Includes a TransUnion® credit report and tri-bureau monitoring for credit inquires, delinquencies, judgments and liens, bankruptcies, new loans and more
- **CyberAgent® Internet Surveillance:**
  Monitor websites, chat rooms and bulletin boards 24/7 to identify trading or selling of your personal information
- **Court and Public Records Monitoring:**
  Know if and when your name, date of birth and Social Security number appear in court records for an offense that you did not commit
- **Non-Credit Loan Monitoring:**
  Know if your personal information becomes linked to short-term, high-interest payday loans that do not require credit inquiries
- **Change of Address:**
  Monitor to see if someone has redirected your mail
- **Sex Offender Report:**
  Know if sex offenders reside in your zip code, and ensure that your identity isn't being used fraudulently in the sex offender registry
- **Social Security Number Trace:**
  Know if your SSN becomes associated with another individual's name or address
- **Identity Theft Insurance:**
  Reimburses you for certain expenses in the event that your identity is compromised with a $1,000,000 insurance policy
- **Identity Restoration:**
  Work with a certified identity theft restoration specialist to restore your ID and let you get on with your life. This service is available for affected individuals even if you do not enroll.

OPM Breach, What You Can Do Now

- Be more aware of phishing scams
- Routinely monitor your financial accounts
- Change your account passwords
- Change your security questions
- Review and increase privacy controls on social media sites
- Ensure personal computer security software is current
- Place a fraud alert on your credit file to let creditors know to contact you before opening a new account in your name.
- Pay close attention to the website URL before you click on it.
- If you are unsure whether an email or phone request is legitimate, try to verify it by contacting the company directly.

SSN Reduction

- **DON SSN Reduction Plan, Phase 3, is ongoing:**
  - Eliminate use of the SSN
  - Substitute the DoD ID number for the SSN when possible
  - Mask or hide the SSN from electronic displays or document output
  - All letters, memoranda, spreadsheets, electronic and hard copy lists and surveys must meet the acceptable use criteria (1 Oct '15)
- **Other SSN reduction efforts:**
  - Military Drug Testing Program: process accepts DoD ID on 1 March 2015
  - Navy Uniform Marking: policy now requires name only on clothing articles
  - JPAS
  - Medical: prescription filling process at Military facilities
  - BUPERS

DON Guidelines for Use of the DoD ID

- Presence or knowledge of an individual's DoD ID alone shall be considered as no more significant than presence or knowledge of that individual's name.
- The EDIPI/DoD ID by itself or with name is considered PII.
  - However, it is considered internal government ops related PII (e.g., work phone #, job title) and low risk. No breach if lost, stolen or compromised.
- The DoD ID shall only be used for DoD business purposes.
- The DoD ID may not be shared with other federal agencies unless a DoD/DON approved MOU is used.

Handling PII in the Office…

- FOUO privacy marking
- Hard copy paper storage
- Copier/Scanner/FAX
- Mail
- Email, Spreadsheets, electronic lists, memos, rosters
- Hard copy storage
- Shared drive
- Cloud service
- Social Media/People Search Engine
- Disposal

Your Privacy Responsibilities

- Safeguard PII to prevent unauthorized disclosure
- Report a breach/suspected breach to your supervisor
- Take annual PII awareness training
- Encrypt and digitally sign all email that contains PII
- Never store PII on a personal computer
- Collect only the minimum amount of PII to do your job
- Wherever possible, eliminate the use of Social Security Numbers
- Dispose of PII so that it is unrecognizable
- Never view a person's PII out of curiosity or to "help out" a coworker

Spear Phishing

- An estimated 91 % of cyber hacking attacks start with a phishing or spear-phishing email.
- Targeted victims lured to fraudulent websites, created to steal personal information, such as names, credit card and bank account numbers, social security numbers, and financial account logins and passwords.
- To foster trust emails contain details about the victim – name, postal address, employer, partial account number
- Mail-server spam and phishing filters stop 63 percent of phishing e-mails from even reaching in-boxes.
- 95 % of phishing e-mails pretend to be from Amazon, eBay, or popular banks. Targets can also be seasonal (e.g., IRS) or capitalize upon social trends (e.g.,Facebook).

SPEAR FISHING

A GROWING THREAT

What's New ?

- **Privacy Overlay – process for managing risk in IT systems**
- **Annual Privacy Training APP available: 1 Jun 2016**
- **Draft SECNAV 5211/13 and 5211/14 Breach Reporting Forms**
- **In progress: New Annual PII Awareness course. Avail: next FY**
- **DOD 14 Aug 14 CUI Memo / DON ALNAV DTG: _____**
- **DOD 28 Jan 15 Government Contract Compliance Responsibilities**
- **Email Encryption, go to:**
  http://www.doncio.navy.mil/ContentView.aspx?ID=3989
  https://www.google.com/work/apps/government/products.html#gmail

  Customize your "Home" screen to make encryption easier, go to:
  http://www.doncio.navy.mil/ContentView.aspx?id=5565
- **Social Media Safeguards, go to:**
  http://www.defense.gov/documents/WEB_Guide_to_Keeping_Your_Social_Media_Accounts_Secure_2015.pdf

What's New (continued…)

- New hire for DON CIO Privacy Information specialist onboard
- (New) Privacy Tip: How To Protect Yourself From Medical Identity Theft
- (Updated) Privacy Tip for Tax Identity Theft
- (Updated) Privacy Tip for office moves
- Complete list of Privacy Tips available at: http://www.doncio.navy.mil/ContentView.aspx?ID=906
- Taxpayer Guide to Identity Theft available online at: http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft
- Command recipients receive the first DON Excellence Award for Privacy
- New FTC Identity Theft resource at: https://www.identitytheft.gov/

Helpful Links

- **Secure Access File Exchange (SAFE): http://www.doncio.navy.mil/Products.aspx?ID=3544**
- **Ways to find your DoD ID number: http://www.doncio.navy.mil/ContentView.aspx?id=3792**
- **Contractor's requirements under PA, FOIA and HIPAA: http://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Privacy-Contract-Language**

DON Privacy POCs

STEVE MUCK
DON CIO
Compliance Branch Head
Phone: (703) 695-1297
Email: steven.muck@navy.mil

ROBIN PATTERSON
OPNAV DNS-36
Navy Privacy Act Program Manager
Phone: (202) 685-6545
Email: robin.patterson@navy.mil

STEPHANIE CLEARWATER
HQMC C4 CYBERSECURITY DIVISION
PII/PIA Analyst
Phone: (571) 256-8868
Email: stephanie.clearwater@usmc.mil

STEVE DAUGHETY
DON CIO Privacy Lead
Phone: (703) 697-0045
Email: steve.daughety1@navy.mil

CRYSTAL MANLEY
OPNAV DNS-36
Phone: (202) 685-6583
Email crystal.manley.ctr@navy.mil

BARBARA FIGUEROA
DON Forms Manager (DNS-15)
Phone: (703) 614-7585
Email: barbara.figueroa@navy.mil

SALLY HUGHES
HQMC ARSF
Head, FOIA/PA
Phone: (703) 614-3685
Email: sally.hughes@usmc.mil

DEBORAH CONTAOI
HQMC ARSF
Privacy Act/SORN SME
Phone: (703) 692 2445
Email: deborah.contaoi@usmc.mil

Don Free
DON CIO
Privacy Information Specialist
Phone: (703) 695 1955
Email: donald.free@navy.mil

www.doncio.navy.mil/privacy