Privacy Awareness: Safeguarding PII

National Defense University
AY 2021 - 2022

Julie Hartmann, CIPP/US
Contractor Support to
NDU Privacy and Civil Liberties Office (PCLO)

Purpose & Objectives

- To provide an overview of **NDU's Privacy Program** and the **NDU Privacy and Civil Liberties Office**
- Outline the **safeguards** in place for the collection, use, maintenance and dissemination of personally identifiable information (PII) on NDU Systems of Records**.**

- NDU students will be made aware of and understand:
  - ✓ **What PII is collected** in NDU Systems of Records (SOR)
  - ✓ **What PII is prohibited** in NDU's on-prem and cloud IT environments
  - ✓ **What safeguards are in place** to protect PII
  - ✓ **How NDU reports** on PII
  - ✓ **How to request and make changes** to your PII
  - ✓ **What to do if you suspect a PII breach**

The Privacy Act of 1974

The Privacy Act of 1974 (5 U.S.C. 552a) is the key legislation governing federal records maintained on individuals. Its four objectives are:

1. To **restrict disclosure** of PII to those who need it to perform their federal duties
2. To grant people **access to their own** federal records
    - Must be submitted **IN WRITING** to the OSD/JS FOIA Center and be signed by requestor/owner of PII (can be faxed to (571) 372-0454)
    - Must include the name and number of the applicable NDU SORN *(DNDU01, September 21, 2010, 75 FR 57458)*
3. To **provide a process to correct** federal records that are inaccurate, irrelevant, or incomplete
4. To **establish "fair" regulations and practices** for the federal government's collection, maintenance, use, & dissemination of PII

Student PII in the NDU Environment

- **SSNs, DOBs, Fingerprints:** Used in JPAS (Clearance passing), Datamart (Transcripts), RAPIDS (CAC)
- **Biographical, Geo-location and Non-NDU Information and Data:** T
  sites; in
- **Passpo**
  Used in
  (DTS); in documents uploaded to Blackboard and O365; in on-premises network Shared Drives; in on-premises SharePoint libraries (not processes)

"What about my CAC number?"

☑ **PII, but "*approved for official DoD business*"**

Source: OSD/JS Privacy Office white paper, "DoD Identification Number," Jul 2019

Threats to Student PII =

Unauthorized **access**, **aggregation**, **alteration**, **disclosure**

Administrative Safeguards for Student PII

Fed, DoD, JS & NDU Governance	Baseline & Expanded Training
• Privacy Act of 1974 • OMB Circular A-130 • OMB Circular A-108 • DoDI 5400.11 • DoD 5400.11-R • DoDM 5400.11 v2 • DoDI 1000.30 • NDU RMF AR-1 • NDU Privacy Program Guidance	• Cyber Awareness Challenge course required for access to NDU IS • JS annual training includes: 1. *Privacy Act Awareness* 2. *OPSEC* 3. *Info/Records Management* 4. *Derivative Classification* 5. *Insider Threat* • **SOR-specific training, by role and responsibility, for PII handlers/Privacy Ambassadors** • NDU Privacy Program website for additional resources • Transparency via DoD/JS oversight and reporting requirements

NDU Transparency: SORNs & PIAs

A System of Records (SOR): Any DoD-controlled repository of records using unique IDs

SOR Notices (SORN): Descriptions of government approved SORs published in the Federal Register, as required by the Privacy Act of 1974 (5 U.S.C. 552a).

- *NDU currently has one SORN for its USMS system*
- NDU SORNs are published by DPCLD at https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/OSDJS-Article-List/

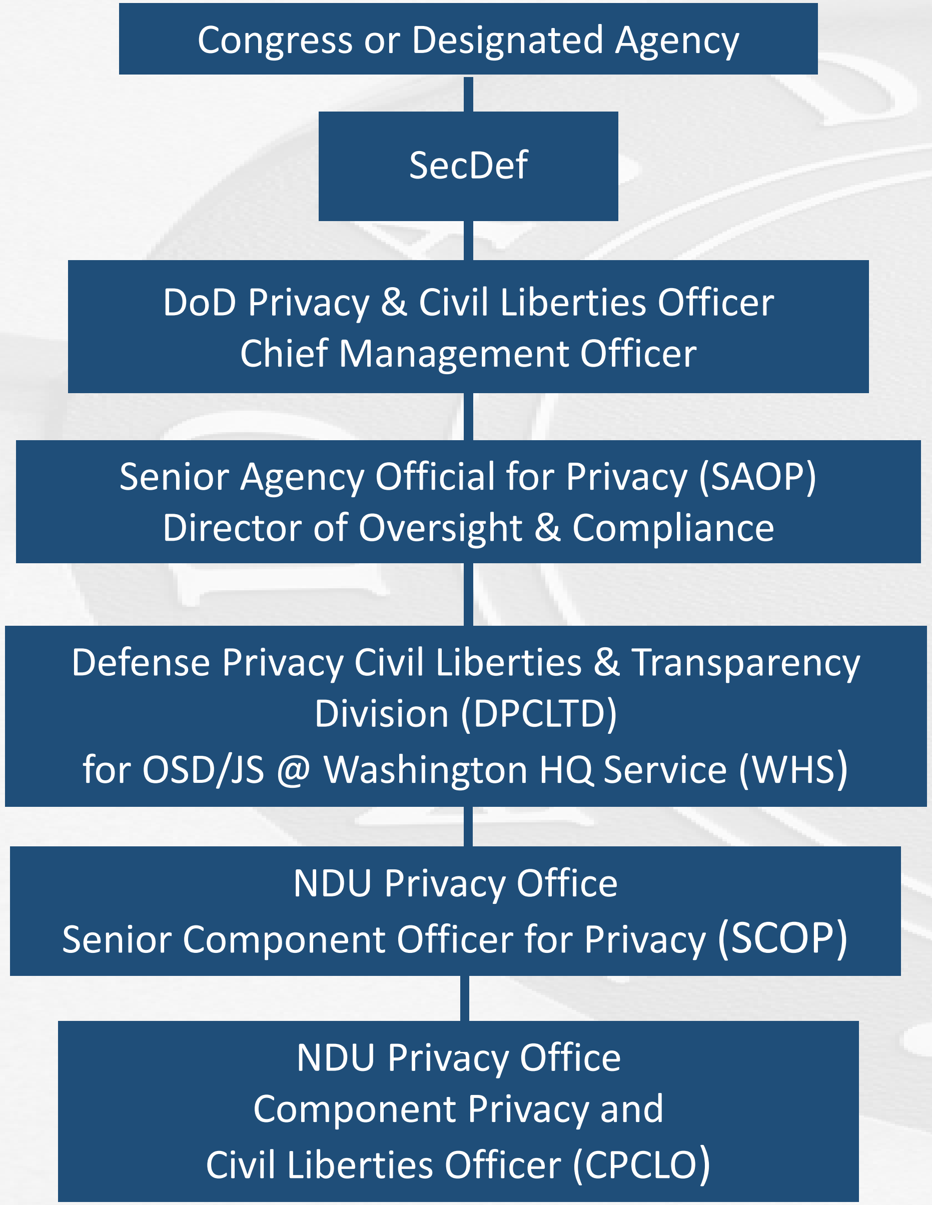
Privacy Impact Assessments (PIA): A tool required by the E-Government Act of 2002 to identify privacy risks in programs and SORs across their lifecycle.

- *NDU's NEIS PIA has been approved 31 AUG 2020*
- NDU PIAs are published by DPCLD at https://dpcld.defense.gov/Privacy/Privacy-Impact-Assessment/

Social Security Reduction Plan: DOD Instruction 1000.30, "Reduction of Social Security Number (SSN) Use Within DOD" requires components to evaluate how SSNs are used and to eliminate them if possible.

- *NDU's SSN Justification Memo for USMS/DataMart approved on 28 Jun 2019 (3 years)*

Reporting & Accountability



Congress or Designated Agency

SecDef

DoD Privacy & Civil Liberties Officer
Chief Management Officer

Senior Agency Official for Privacy (SAOP)
Director of Oversight & Compliance

Defense Privacy Civil Liberties & Transparency Division (DPCLTD)
for OSD/JS @ Washington HQ Service (WHS)

NDU Privacy Office
Senior Component Officer for Privacy (SCOP)

NDU Privacy Office
Component Privacy and
Civil Liberties Officer (CPCLO)

- ✓ **Social Security Number Fraud Prevention Act Report –** *Documents sent via postal mail that use SSN, and justification* **Annually to Congress*

- ✓ **Executive Orders 13636 and 13691 Privacy and Civil Liberties Assessments Report –** *Efforts to mature tech-neutral cybersecurity framework and maximize sharing of threat info with private sector* **Annually to DHS*

- ✓ **Computer Matching Reports –** *Activities re: sharing of PII by the SORs of two or more fed agencies* **Annually to DOJ and OMB*

- ✓ **Privacy and Civil Liberties Section 803 Report** – *SORNs, PIAs, breaches, SSN use, issuances, rule exemptions, achievements and complaints* **Semi-annually to Congress via OMB*

- ✓ **Federal Information Security Modernization Act (FISMA) Report – ***Information security incident and data breaches* **Per incident and quarterly (new) to Congress via DHS*

Physical Safeguards for Student PII

Facilities	✓ Must be locked ✓ Access controlled via physical token, door key or door code ✓ Monitored by Security personnel, paper logs, cameras
Hardware	✓ Kept in locked facilities ✓ Access controlled via facility doors, physical token, and/or password ✓ Never left unattended ✓ Gov devices under hand-receipt; turned in for destruction
Electronic Files	✓ Stored on secured devices; always under your control ✓ No CDs or thumb drives on gov devices ✓ Printed on secured devices while user is present; printed with PII coversheet ✓ Destroyed beyond reconstruction: overwritten, Degaussed, permanently deleted
Paper Files	✓ Stored in marked folders and locked cabinets ✓ Never left unattended; faxed with PII coversheet ✓ Can be sent by secure courier ✓ Destroyed beyond reconstruction: Burned or shredded

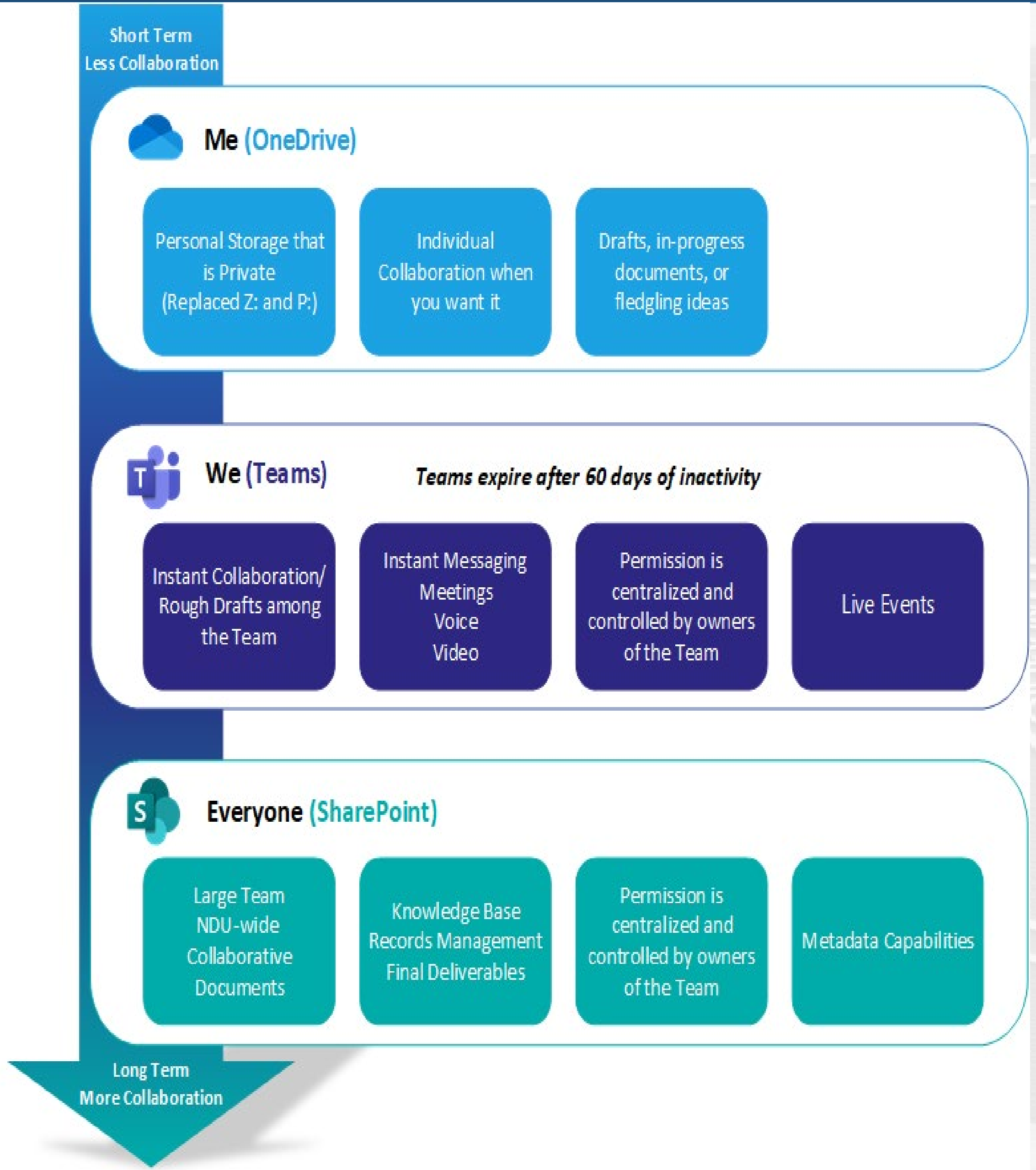
Technological Safeguards for Student PII

Facilities	✓ Monitored by electronic access logs ✓ Access controlled via permission settings, security groups, CAC certificates
Hardware	✓ Accessed via PKI certificates & authentication ✓ Devices set to “time out” (sleep, log off) ✓ Gov device use monitored; security patches kept up to date ✓ Passcode, fingerprint or facial scan used to open locked personal devices
Electronic Files	✓ Stored as encrypted and/or with password ✓ Emailed/transferred digitally signed and encrypted with a PII e-coversheet ✓ Access on “need to know” basis, controlled by security groups ✓ Monitored/scanned for PII by ITD ✓ Labeled using “PII” and/or “CUI”
Paper Files	✓ Watermarks and clearance levels printed on documents ✓ Faxing and emailing scanned hard copies requires CAC on network multi-use printers

NATIONAL DEFENSE UNIVERSITY
PRIVACY & CIVIL LIBERTIES OFFICE

NATIONAL DEFENSE UNIVERSITY

Privacy Best Practices – Storing and Sharing PII



Short Term
Less Collaboration

Me (OneDrive)

Personal Storage that is Private (Replaced Z: and P:)

Individual Collaboration when you want it

Drafts, in-progress documents, or fledgling ideas

We (Teams)

Teams expire after 60 days of inactivity

Instant Collaboration/ Rough Drafts among the Team

Instant Messaging
Meetings
Voice
Video

Permission is centralized and controlled by owners of the Team

Live Events

Everyone (SharePoint)

Large Team
NDU-wide
Collaborative Documents

Knowledge Base
Records Management
Final Deliverables

Permission is centralized and controlled by owners of the Team

Metadata Capabilities

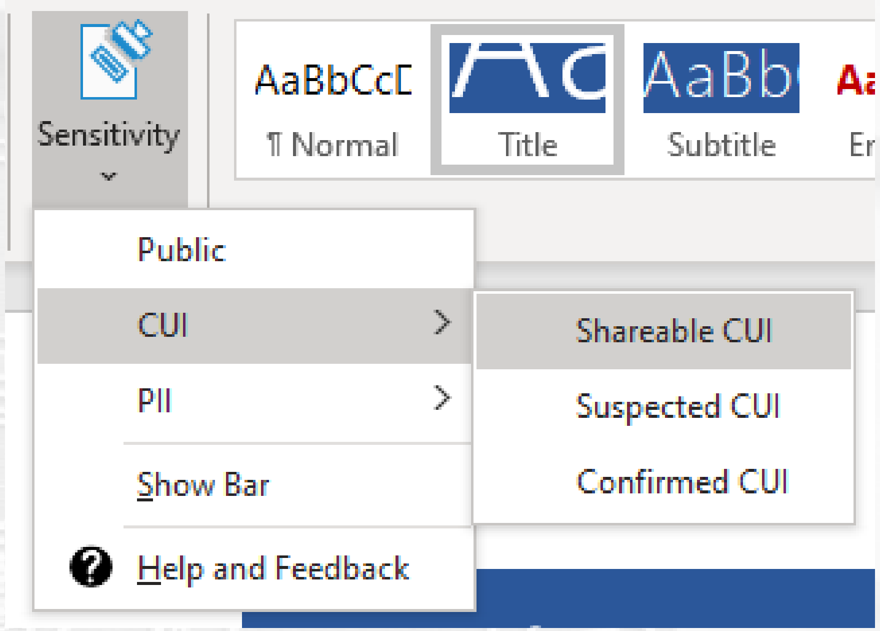
Long Term
More Collaboration

- **Properly labeled documents can be shared using**:

  DoD SAFE – the preferred method for sharing PII electronically
  - Web-based tool that provides authenticated DoD CAC users and unauthenticated users the capability to securely send and receive files and communication. (https://safe.apps.mil/)
  - If the recipient's email address is personal or the business email is located outside of the DoD environment, utilize DoD SAFE to send
- **Microsoft Teams**
- **Email** - should there be a need to transmit PII via email
  - Include "CUI" in the subject line of the email
  - PII included in any of the document types from Microsoft Suite can be protected with a password
  - Encrypt and digitally sign the email to those with a CAC

Privacy Best Practices – Applying Sensitivity Labels

- **Label Office documents that contain PII or Controlled Unclassified Information (CUI) using the O365 Sensitivity Labels**
  - **Suspected PII or Suspected CUI**
    - Treated as if they may have PII/CUI based on programmed criteria
    - Encrypted and protected exactly like officially marked documents
    - These labels are applied automatically
    - *Do not apply these labels yourself*
  - **Confirmed PII or CUI**
    - Officially marked documents
    - Includes PII/CUI headers and footers
    - Encrypted and protected throughout their lifecycle regardless of location
    - **When e-mailed**:
      - NDU recipients may edit and save the content, but cannot print
      - ***External recipients may only view the content***
  - **Shareable PII or CUI**
    - Officially marked documents
    - Includes PII or CUI headers and footers
    - ***Only used to display PII or CUI in a Teams meeting or share outside of NDU using a secure method (DOD SAFE, CAC Encrypted E-mail)***
  - **Public**
    - Clears an improperly labeled document
    - Justification required



Breach Reporting

Who is required to report? All NDU Faculty, Staff and Students ***who become aware of a suspected breach***

What should be reported?

- PII posted on public-facing websites, social media sites, O365
- PII sent via e-mail unencrypted or to unauthorized recipients
- PII hardcopies provided to individuals without a need to know or “found” without a handler
- Loss of electronic devices or media on which PII is stored
- PII used by any NDU Faculty or Staff member for unofficial business

What actions are required?

- STOP THE LEAK as soon as possible (if you are able)
- REPORT IT IMMEDIATELY to your Dean of Admin/Dean of Students AND the IT Help Desk at Help-IT@ndu.edu or privacy@ndu.edu

What are the repercussions for NDU Students who breach PII security?

- At minimum, to complete a Privacy/PII refresher course and submit a certificate to their Deans
- Deans must report disciplinary actions to the NDU SCOP within 15 days of breach

How are those affected notified?

- If notification is required, by mail from NDU within 10 days of the decision

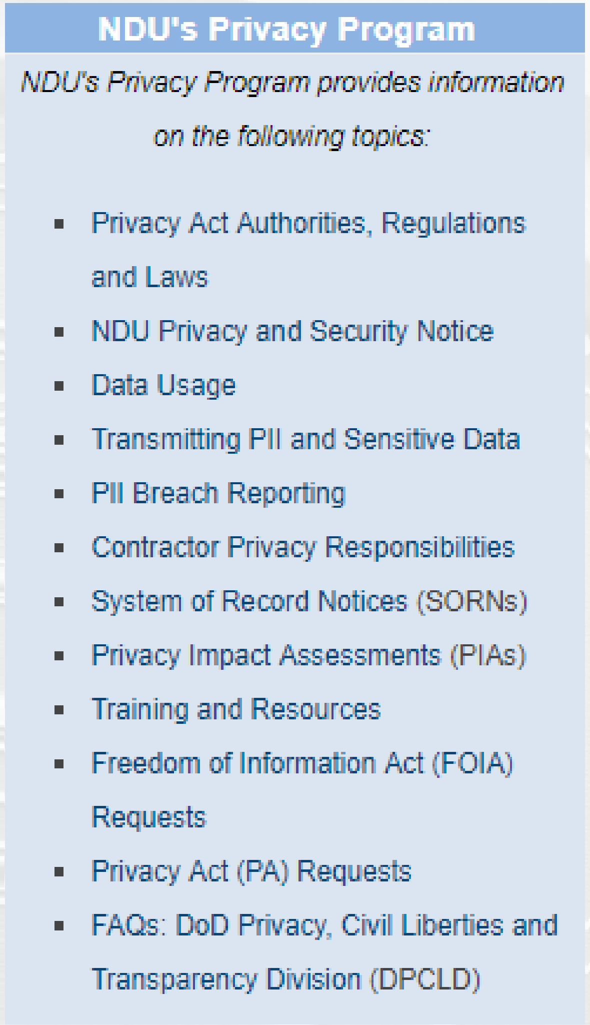
Resources

NDU’s Privacy Program:
https://www.ndu.edu/About/Privacy

NDU’s Privacy and Civil Liberties Office:
privacy@ndu.edu

DoD Defense Privacy and Civil Liberties Division (DPCLTD)
(703) 571-0070
https://dpcld.defense.gov/

DoD Inspector General
FOIA/Privacy Office
(703) 699-5680
http://www.dodig.mil/Programs/Privacy-Program/



NDU's Privacy Program

NDU's Privacy Program provides information on the following topics:

- Privacy Act Authorities, Regulations and Laws
- NDU Privacy and Security Notice
- Data Usage
- Transmitting PII and Sensitive Data
- PII Breach Reporting
- Contractor Privacy Responsibilities
- System of Record Notices (SORNs)
- Privacy Impact Assessments (PIAs)
- Training and Resources
- Freedom of Information Act (FOIA) Requests
- Privacy Act (PA) Requests
- FAQs: DoD Privacy, Civil Liberties and Transparency Division (DPCLD)