

# Personally Identifiable Information (PII) and Operations Security (OPSEC)

---

Cornerstone Spouses

October 2016

Samara Morales



Version

Point of Contact:  
Samara Morales  
703-784-9540



# Agenda

## Personally Identifiable Information

Recognize what types of information are considered Personally Identifiable Information (PII)

Identify the responsibilities for safeguarding and how to safely transmit PII

Illustrate appropriate disclosure of PII in respect to Social and Contact Rosters

## Operational Security

Recall the definition of Operational Security (OPSEC)

Characterize strategic ways to maintain OPSEC

Distinguish areas in daily life that are considered vulnerabilities

## Media

Name ways to maintain privacy on Publically Available Websites (PAWs)

Specify approaches to handle the media

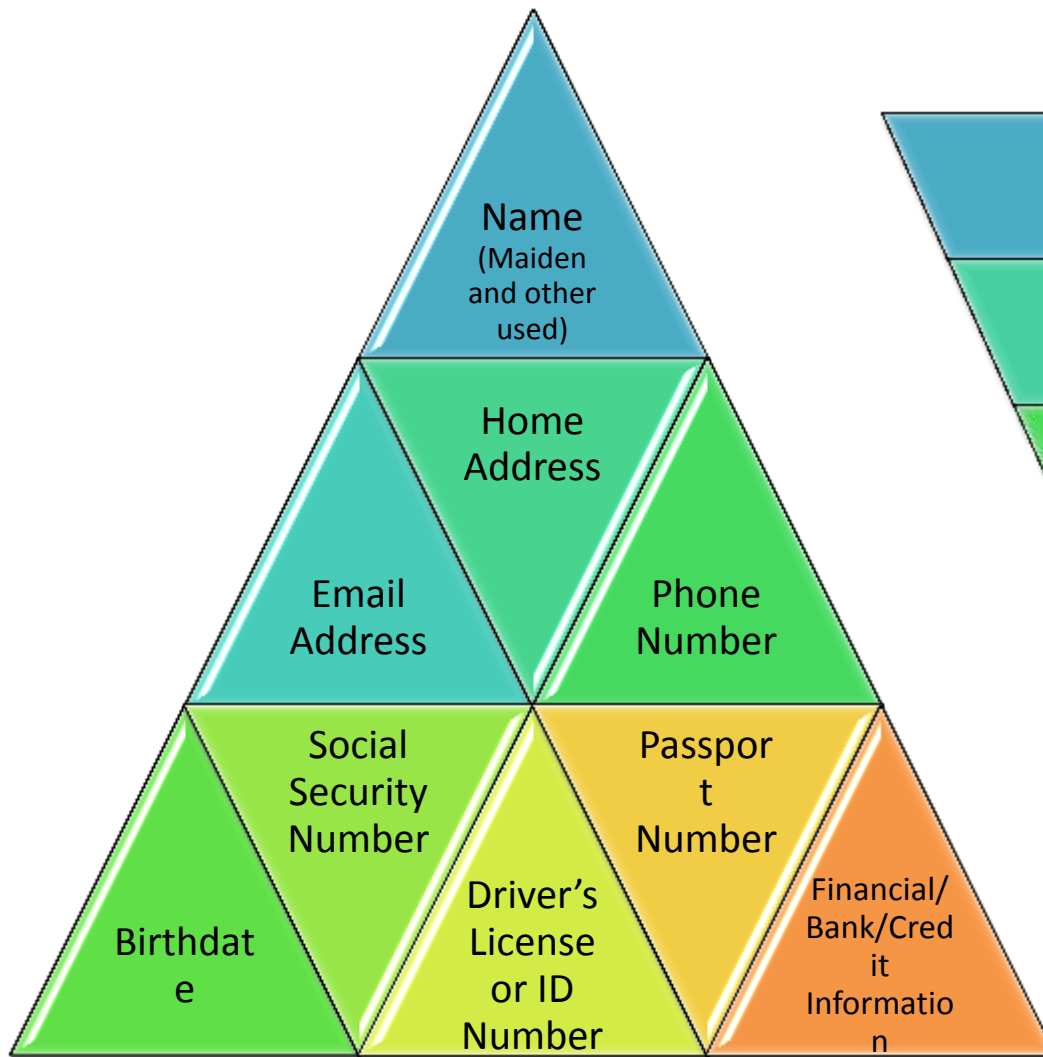
Identify features AOCT possesses that social media sites do not

# Personally Identifiable Information

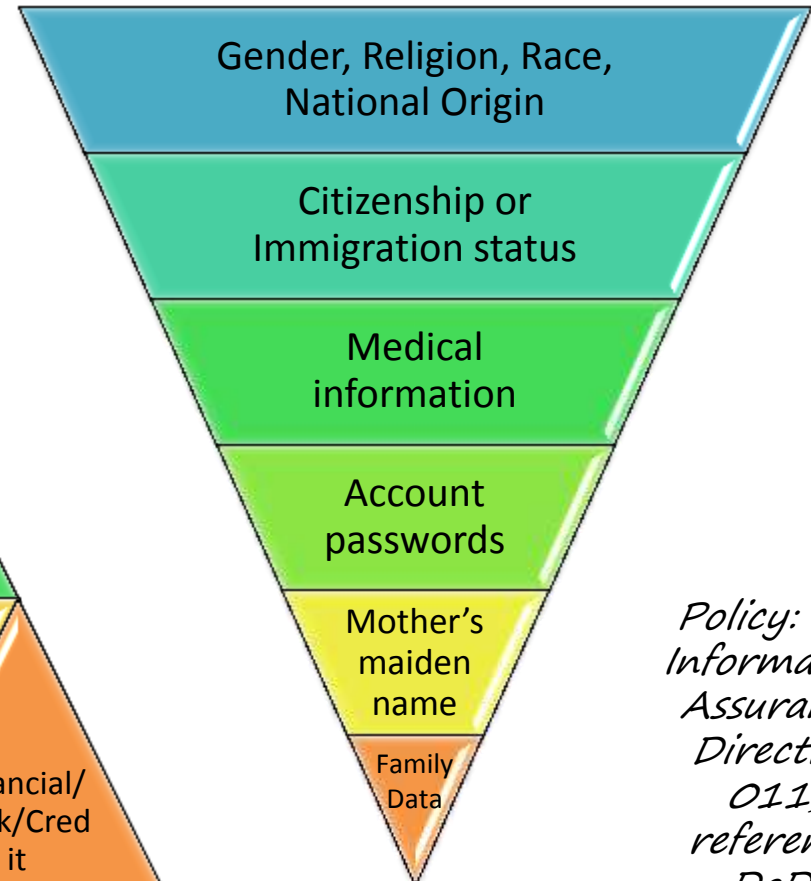


**A.K.A. PII**

# PII- What is it?



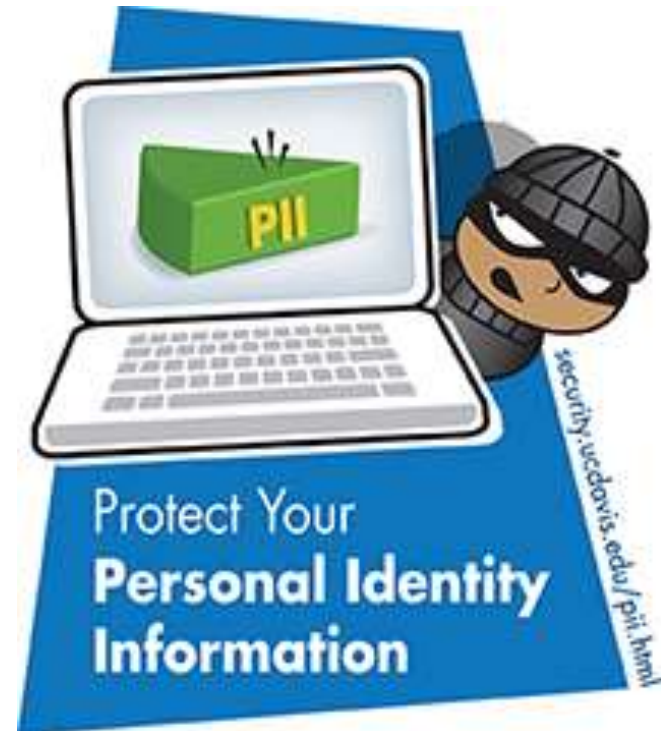
## Paired with....



*Policy: MC Information Assurance Directive 011; reference DoDI 5200.1-R*

# Where is it found/how is it transmitted?

- Copy Machine
- Fax Machine
- Filing cabinets
- Mail
- Unsecure websites
- Text/Email
- Verbally



# Who has access to PII?

Commanding Officer (CO)

Family Readiness Officer  
(FRO)/ Deputy FRO

Adjutant

Chaplain

Family Readiness Assistant(s)\*

Executive Officer/Sergeant  
Major (XO/SgtMaj)

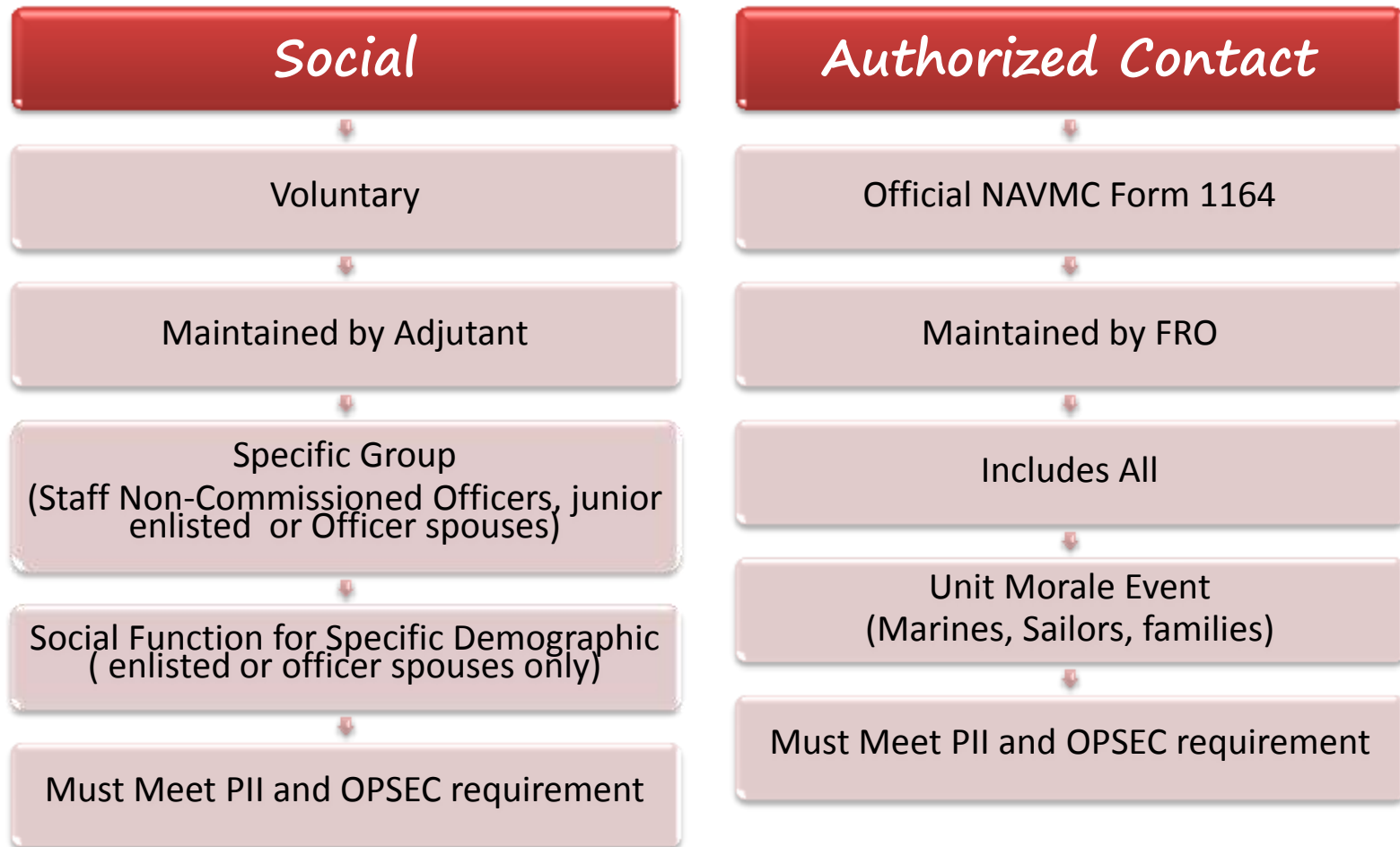
Single Marine Program  
Representative (SMP Rep)

Commanding Officer/Senior  
Enlisted Spouse (CO/SES)\*

Command Team Advisor(s)\*

**\*Represents an appointed position**

# Social vs. Authorized Contact Rosters



# Transmitting PII

1

**Select Upload Method**: DoD CAC users choose the CAC option, all others choose the non-CAC option. All non-CAC users will be required to verify their email address.

2

**Sender Uploads Files**: The sender fills out their information and then adds files and recipients to the package.

3

**Recipient Downloads File**: Recipients will receive an email with a link and unique password to download the package. After the recipient has downloaded files in the package, their password will become invalid and the files will be removed from the site.



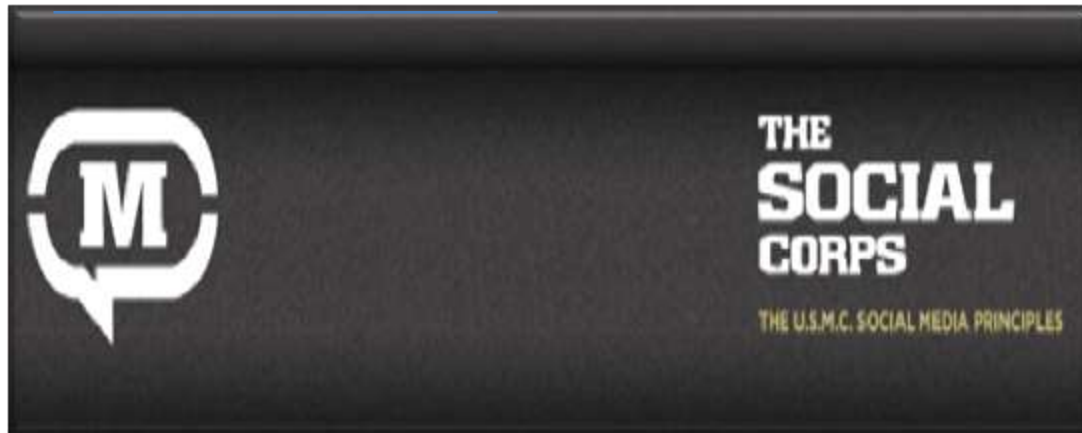
*\*Per Department of Navy (DON) CIO, message DTG 171625Z Feb 12, PII may not be transmitted via fax/unencrypted email\**

Website: <https://safe.amrdec.army.mil/safe/>



# Did you know?

*PII must adhere to SECNAVINST 5720-47B DON Policy for Content of Publicly Accessible Websites*



For more information on the Marine Corps' social media policy:

<http://marines.dodlive.mil/social-media/>

# Operations Security (OPSEC)



# OPSEC, what is it?

- Operations Security (OPSEC)
- Policy: MCO 3070.2A
- Keeping adversaries from discovering critical information to include operations; enemies want the information!!
- Protecting critical information



# Critical Information

- Military movement information, such as dates and locations
- Unit information; such as size, issues, morale
- Security/Equipment data, such as tactics or defenses
- Pictures that could be interpreted differently than intended
- Names and information of Command Team Members, Marines, co-workers, family

# Ways to maintain OPSEC

- Secure: Emails coming from Gmail, Yahoo, or other web domains, might not be secure. Be aware of emails from unknown or suspicious sources.
- Careful: Do not talk about or email/post details about troop movement, missions, logistics, numbers, locations, or homecoming dates.
- Protective: Do not discuss critical information details outside of your immediate family and especially not over the telephone or internet.
- Private: Keep your social media profiles on restricted settings, and be cautious of accepting invitations to connect from people you may not know.
- Photo conscious: If you take or receive a photograph of Marines involved in any military operation or exercise, you should not post the photograph unless it has been released by the Marine Corps or Department of Defense.

# Ways to maintain OPSEC cont.



- Ensure that the information you post/tweet/write/talk about has no significant value to the enemy



- Always assume that the enemy is reading/listening to the information you provide



- Be careful about discussing information in public settings - Clubs/Bars, airports, restaurants, gyms, public transportation, shopping, or online: Anywhere people can eavesdrop on a conversation



- Avoid public (online or real life) speculation about future missions (“they’ll probably start building up here, next”)

# Ways to maintain OPSEC cont.

## Safeguard Indicators such as:

- Plans, schedules, maps, locations
- Deployment dates/ Large troop movements
- Increase in field exercises
- Ceremonies
- Privately Owned Vehicle (POV) storage
- Large number of wills and power of attorneys being processed

## Do not post:

- Photos with indicators in the background or filenames and file tags with sensitive data
- Links that imply endorsement, such as charitable sites
- Anything that you wouldn't be comfortable with if it became public knowledge
- Information that is political in nature

# The Don'ts of OPSEC

- Discuss future destinations
- Discuss future operations or missions
- Discuss dates and times of exercises
- Discuss readiness issues or numbers
- Discuss specific training equipment
- Discuss people's names and billets in conjunction with operations
- Speculate about future operations
- Spread rumors about operations
- Assume the enemy is not trying to collect information on military operations, you or your family



# Vulnerability

An enemy can physically observe your paraphernalia, track your daily activities, or they can listen to your phone conversations and monitor your Internet/e-mail activities to get information.



# Siri and Google Now



- According to French Network and Information Security Agency, Siri and Google Now can silently take orders from a hacker across the room who isn't even uttering a word.
- Radio signals transmitted from an antenna can be used to eavesdrop on conversations

# Siri and Google Now cont.



Protect against hackers!

- Disable Siri or Google Now access from the lock screen
- Better shielding on headphone cords
- Add an electromagnetic sensor
- Approved to create own “wake words” to launch virtual personal assistant







# OPSEC measures you should practice daily:

- Be aware of your surroundings
- Keep sensitive discussions in designated secure areas
- Keep a need-to-know attitude (if they don't need to know, don't tell them)
- Safeguard sensitive but unclassified information
- Be mindful of security of publicly available websites



*“On the internet, nobody knows you’re a dog”*

# Why the Authorized Organizational Communication Tool?

						
View Photos	✓	✓	✓	✓	✓	✓
View Videos	✓	✓	✓	✓	✓	✓
Access Documents	✓	✓	✓	✓		✓
Participate in Forums	✓	✓				✓
Official USMC Website						✓
P/W Requirement meets DOD standards						✓
Information is verified/validated						✓
Open only to Marines & family members						✓

Avoid the rumor-mill: use the Marine Corps' safe, secure portal for dissemination of authorized and official family readiness information

# OPSEC measures you should practice daily:

- Be aware of your surroundings
- Keep sensitive discussions in designated secure areas
- Keep a need-to-know attitude (if they don't need to know, don't tell them)
- Safeguard sensitive but unclassified information
- Be mindful of security of publicly available websites

# Dealing with the media

- You are under NO OBLIGATION to speak with the media
- If you choose to speak, you cannot speak on behalf of the command or the Marine Corps
- Do not give specific information to reporters (ex: troop movement or family location)
- Notify the Commander or the FRO that you have been approached
- Refer the media representative to the unit Public Affairs Officer (PAO)



# Additional Trainings

- For additional safety related trainings for yourself or family please contact your installation MCFTB office.
- Classes include:
  - Social Networking Safety
  - Safe and Sound at Home
- Additional OPSEC training
  - Website: [www.marinenet.usmc.mil](http://www.marinenet.usmc.mil)
- Course Information: Name: Uncle Sam's OPSEC, Code: OPSECUS001
  - 45 minutes in length
  - Certificate is generated
  - Meets annual training requirements for Marines, Contractors and DoD Civilian Employees



*Please see the handouts for more information on how to access MarineNet as a DEERS family member without a Common Access Card (CAC).*



# Questions

