Disclaimer: This publication is offered to you conditioned upon your acceptance without modification of the following terms, conditions, and notices: All content herein is for the user's convenience and informational purposes only. While such content is believed to be of practical value, neither the Department of the Navy nor Naval Services FamilyLine make any representation as to the suitability, reliability, completeness, or accuracy of the information herein. All information is provided "as is" and without warranty of any kind. The Department of Defense, Naval Services FamilyLine, and their respective employees and volunteers shall have no liability whatsoever for any losses that may occur as a result of applying the information contained herein. Though no license to the intellectual property herein is granted, fair use is encouraged. Thus you may quote or disseminate this document in whole or part with credit to its creators but it shall not be resold or used for advertising or product endorsement purposes. Trademarks appearing herein belong to their respective owners and no affiliation with or sponsorship by such owners is claimed.
What is OPSEC?

OPSEC keeps potential adversaries from discovering our critical information. As the name suggests, it protects operations – those planned, in progress, and already completed. Mission success depends on secrecy and surprise, which allows the Navy to accomplish the mission quickly and with less risk.

One way to support your Sailor is to recognize the importance of appropriately sharing the Navy story.

Without strong, capable families, our Sailors cannot be prepared to do what they must to defend our nation and further our objectives abroad. Because families are such a big part of our Navy, it is crucial that, should you choose to share your story, you follow certain guidelines to preserve OPSEC and propriety. Remember that OPSEC is more than not sharing classified information, it is also about being aware that it is just as critical not to share unclassified, but sensitive, information that could be used by our adversaries.

How does OPSEC apply at home?

You might have heard the saying that “Loose Lips Sink Ships” and today “Loose Tweets Sink Fleets.” Social media amplifies operations security risks because it enables information to be shared publicly with greater speed and at an increased volume. OPSEC violations commonly occur when someone shares information with people they do not know well (like their Twitter followers,) or if their social media accounts have loose privacy and security settings. OPSEC can blend seamlessly from military duty into personal lives. At home, the health and safety of family members are as critical to unit morale and, ultimately, mission success as are the bullets and bombs needed to destroy the enemy. OPSEC use at home protects loved ones and military missions as forces deploy worldwide. It also protects family members from becoming an indirect target of adversaries or criminals, who would see your spouse’s absence as an opportunity or weakness for their own gain.

Families of Sailors need to be especially careful when it comes to discussing current deployments, scheduled movements, and current or future locations. Instead of saying, “My son, IT2 Any Sailor, is in Any Unit at Naval Station Anywhere in Any City, Japan,” you should rephrase it to say, “My Sailor is deployed in the Pacific.” Instead of saying, “My Sailor will be back in 53 days”
you should say “My Sailor is coming home.” You should also limit the personal information you post about yourself or your Sailor.

Family members should be careful who they friend on social media and who follows them. Not everyone who wants to be your friend or follower is necessarily who they claim. Only allow people that you actually know in real life into your social circles.

As a family member of a Sailor, you should feel free to post about pride and support for service members, port call information after it has been released to the media, general status of the location of a ship at sea (e.g., operating off the west coast, as opposed to 45 minutes nm north of San Diego) and posts from official Navy social media presences.

OPSEC is a family affair. All family members and loved ones are part of the OPSEC team and need to protect the Navy's information to ensure our safety. Discuss OPSEC with all family and close friends and, if there is ever a question, ask for clarification. It is important that all members of your family review their security and privacy settings and keep them as restrictive as possible.

<table>
<thead>
<tr>
<th>Dangerous</th>
<th>Safer</th>
</tr>
</thead>
<tbody>
<tr>
<td>My son, IT2 Any Sailor, is in Any Unit at Naval Station Anywhere in Any City, Japan.</td>
<td>My Sailor is deployed in the Pacific.</td>
</tr>
<tr>
<td>My daughter, Any Sailor, is aboard USS John C. Stennis. She's coming home in 53 days.</td>
<td>My daughter’s ship is coming home in a couple of months.</td>
</tr>
<tr>
<td>My family is in Houston, Texas.</td>
<td>I’m from Texas.</td>
</tr>
</tbody>
</table>

**CYBERSECURITY**

One of the best features of social media sites is the ability to connect people from across the world in spontaneous and interactive ways. However, this also opens its users and their systems to security weaknesses. Information shared on the internet can provide adversaries such as terrorists, spies, and criminals with information that may be used to harm you or disrupt your command's mission. Remember, hacking, configuration errors, social engineering and the sale/sharing of user data means your information could become public at any time.
All types of information are sought for nefarious reasons and our enemies are not just pursuing the military member to get it. They are interested in the family members for the information that they may not realize they possess. The military has always closely guarded its classified information, but unclassified information could be just as damaging if an enemy with the intent to do harm gains additional insight. Others can piece together small bits of ordinary, unclassified information like puzzle pieces to gain a clearer picture of U.S. intentions and actions. These OPEC concerns are most vulnerable through social media platforms.

Anyone using social media should choose passwords that are unique and difficult to guess for each account. You should not share passwords or security questions. Regularly update your anti-virus software and operating system to install the latest security patches for all devices, and beware of links, downloads, and attachments. Look for HTTPS://, the lock icon or a green browser bar that indicates active transmission security before logging in or entering sensitive data (especially when using Wi-Fi hotspots or public Wi-Fi). Consider using a Virtual Private Network (VPN) when using public Wi-Fi. Also, make certain that your personal Wi-Fi is secured with a unique password.

Following are some examples of critical information that you are urged you to review and protect before, during, and even after, your spouse's deployment. Remember, do not send critical information to anyone, including friends and relatives, via e-mail, text, or social media messaging as they easily intercepted.

Critical information you should protect:

- Dates, times, length of deployments, to include departure and arrival dates, using ship's name in correspondence and “Tiger Cruise” information.
- Places, names, ranks
- Deployment status
- Numbers of people, parts, or aircraft
- En route stop locations-Port visits
- Hotels and room numbers
- Personal information, addresses, and family names and addresses
- Numbers and names of children
- Social security numbers
- Bank and credit card information
- Address and telephone numbers

Other considerations:
- Military ID cards indicate you are military-affiliated—use your driver’s license instead when possible.
- Do not send critical information to relatives or others via email or text, as it is easily intercepted.
- Be vigilant about what information you share with friends and family over the phone.
- Do not share critical information via social media.
- Military/government documents, including the military ID, should not be photocopied without proper authorization.
- Teach OPSEC to your children: tell them what NOT to say when answering the telephone and give them safety tips to use when at home alone.

**PERSONAL SECURITY (PERSEC)**

Personal Security is not only important for family members but is a part of overall security for the command. OPSEC and cybersecurity concerns are both relevant to personal security. Areas of personal security also include daily personal security, managing your digital footprint, and home security.

**Daily Security**

It is important to always be aware of both your surroundings and how you may inadvertently share information about your status as a military family member. Here are some key personal security considerations.

- Military ID cards indicate you are military-affiliated. When possible, use your driver’s license instead.
- Military decals (official and unofficial) on your vehicle also indicate your military affiliation.
- Military/government documents, including the military ID, should not be photocopied without proper authorization.
● Always be aware of your surroundings.
● When parking, be sure to park under lights and as close to your destination as possible.
● When approaching your vehicle, look around it before unlocking doors.
● When loading your vehicle, have doors you are not using locked. Also, do not leave your handbag or other personal items unattended in a cart or unlocked vehicle.
● When securing children in seats, stay vigilant of your surroundings and who may be approaching your vehicle.
● When leaving a building, take note of both who is in the parking lot and who may follow you out of the building.
● When driving, if you see someone following you, do not go home. Drive to a busy, well-lit area and try to find a police officer or some other person. If you fear for your safety, call 911.
● As much as possible, avoid deserted and dark areas when you are alone.
  ○ When walking/running/biking never cover both ears with headphones or use earbuds in both ears. You need to be able to hear if a person or driver is approaching you.
  ○ Consider carrying a personal self-defense product.
  ○ If you have serious concerns about your personal safety, report it to the appropriate authorities with your local government.
  ○ Ridesharing.
  ○ Before getting into a rideshare vehicle, ask the driver’s name and who they are there to pick-up. Do not provide them with either the name of the driver you are expecting or your name.
  ○ If there is anyone other than the driver in the vehicle, do not accept the ride.
  ○ If you did not schedule the rideshare, do not get in the vehicle.
  ○ Make sure that you are dropped off in a safe, well-lit location.
  ○ When possible, do not ride alone.

Digital Security
It is important to manage your personal digital footprint. As previously noted, digital platforms are easily compromised and the information can be used to negatively impact operational security, but your personal security risks can also be elevated. To manage your digital footprint,
follow the recommendations under “Cybersecurity” regarding WiFi, passwords, protecting critical information, etc. Here are some additional practices to consider implementing.

- Geo-tagging: Make sure that your geo-tagging/location finders are turned off unless you have a specific need for them. Remember that these can be accessed both to locate you in the moment and to learn your patterns.
- When you take pictures, be sure your GPS feature is turned off. If it is turned on then your pictures will be tagged with your location and when shared, others can use that information to identify your specific location.
- Regularly review your security and privacy settings on all social media accounts. Ensure that they are set so that only your friends and approved followers can view your information. Consider limiting who can find you, friend you, and follow you via social media.
- Periodically review your friend and follower lists. Remove or block those that you do not know personally on any account where you share personal information about your life.
- When using a fitness tracking app, be aware that these can be accessed and used to locate you and establish your patterns and habits. This information can be used by those who intend to do harm.
- Do not send critical information to relatives or others via e-mail, text, or social media messaging as it is easily intercepted.
- Be vigilant about what information you share with friends and family over the phone.
- Do not share critical information via social media.

Home Security
In addition to paying attention to your surroundings when you are not at home, it is important to assess your home in terms of security. Here are some key security recommendations.

- Exterior lighting is a primary deterrent. Ensure that all areas around your home are lighted. Motion lights are a good option for many areas, but it is recommended that front door lights always be left on after dark.
- Ensure you have locks that are affixed with long screws (longer than the ones that typically come with the lockset). Bolt locks add an additional level of security.
● If you use remotely controlled locks, make certain that you have the maximum security settings possible.
● Always lock your doors, even when you are at home during the day.
● Do not leave garage door openers in your vehicle when it is parked outside of the garage.
● Do not leave house keys in your vehicle.
● Lock all the windows when you are not at home and at night.
● Do not hide keys outside. If you are concerned that you may need access to your home, give spare keys to a trusted neighbor or friend.
● Have a plan for your children to know where to go and who to find in the event of an emergency.
● Make sure your children understand and know-how and when to call 911.
● Teach OPSEC to your children: teach them what NOT to say when answering the telephone and give them safety tips to use when at home alone.
● When traveling, stop your mail and newspapers and have someone check your home to pick-up any packages that may be delivered. Address any other items that may leave signs that you are out-of-town.
● When traveling, consider putting lights on timers to maintain patterns of activity in your home.
● Ensure that ladders and tools that could be used to break into your home are not left outside. Secure them inside your garage or a locked shed.
● Make sure you have properly functioning smoke and carbon monoxide detectors and that the batteries are changed with the change of time each spring and fall.
● Make sure you have a home evacuation plan in the event of a fire and ensure that everyone knows the plan. Practice the plan at least once a year.
● If possible, consider using a home security system.

ADVERSE INCIDENTS

Remember that OPSEC is a vital element in protecting missions and service members and their loved ones and our cybersecurity and personal security practices are a part of overall OPSEC. All of us play a vital role in ensuring that we deny our adversaries potentially useful information. We cannot afford to let our guard down, whether we are on or off duty. This includes adverse incidents when many people are seeking information about what has occurred.
When Sailors are killed, wounded, or missing in action, it is hard to control the flow of information distributed through social media platforms. While it is difficult to prepare for these situations, it is important to know that social media can play a role (good or bad) in the handling of a serious illness, injury, or death.

According to the Department of Defense (DoD) Personnel Casualty Matters, Policies and Procedures, no casualty information on deceased military or DoD civilian personnel may be released to the media or the general public until 24 hours after notifying the next of kin regarding the casualty status of the member. In the event of a multiple loss incident, the start time for the 24-hour period commences upon the notification of the last family member.

Do not post on social media or discuss adverse incidents until the information has been publicly released by the official DoD or Department of the Navy (DoN) sources, to help prevent family members learning of their service member's injury or death through unofficial channels. If approached or contacted by friends or family asking about an incident, explain that you cannot and will not discuss the incident.

Journalists' jobs are to report the news, which includes adverse incidents. The media may look at command, Sailor, DoN civilian, and family member social media to get more information. Should you be contacted by a member of the media, simply refer them to your command's public affairs officer.

For more information reference 2019 Navy Social Media Handbook.  