OPSEC AWARENESS FOR FAMILIES: MILITARY INFO

Why Operations Security (OPSEC) for the Family

Adversaries see military family members as soft targets and an easy source of useful information. Family members, whether they know it or not, know a significant amount of sensitive military information. Family members who recognize and understand "what to protect," "how to protect it," and "why it requires protection" become engaged and proactive in safeguarding military critical information and indicators. This Smart Card is split into two categories; the front side discusses OPSEC as it pertains to protecting mission information and the back side focuses on how to apply OPSEC to your family, home and personal life.

What is OPSEC?

OPSEC is a warfighting capability used to identify and protect military "bits and pieces" of sensitive information from people who wish to do us harm. This sensitive information, if collected by an adversary, can provide them with indicators pointing to our future activities and give them an advantage. Its not being dramatic to state that lapses of OPSEC can (and have in the past) led to mission failure and even the death of military members. OPSEC protects this information.

What Do Family Members Know?

Simply by being associated with the military, possibly living on base or even accessing the base, family members know more about our units, missions and operations than we often give credit: Specifically, information such as:
- Pending deployment locations, date or purpose
- Installation access procedures (or changes)
- Security procedures and requirements for base or units
- Locations of sensitive facilities on base
- Morale and personnel issues within the unit
- Unit mission, capabilities, limiting factors, shortages, etc.

Unit Mission: What Not To Discuss and Reasons Why It Should Not Be Discussed

- Don't share specific information about the mission of assigned units
- Don't share specific dates and locations of deployments
- Don't list your service member's specific job on the internet
- Don't share your service member's exact location overseas
- Don't share anything about unit morale or equipment
- Don't share anything about deployment schedules or itineraries
- Don't share exact dates your service member is scheduled to return from deployment

NOTE: This is not an all-inclusive list.

But why shouldn't I talk about these things? Adversaries are experts at collecting and connecting "bits and pieces" of data. The small, seemingly harmless piece of information a family member provides may be the final puzzle piece. It can mean the difference between our military keeping the element of surprise and mission success… or failure. So, what can we talk about? Keep it simple. As a rule of thumb, the vaguer you are - the better. Generic answers are better than providing exact details. Avoiding certain topics isn't being rude, it about keeping our troops safe. Engage your local OPSEC POC for more information about specific OPSEC do's and don'ts for your unit.

How To Talk To Your Family About OPSEC

Service members are familiar with the term OPSEC; however, families may not understand what "OPSEC" means. Try to avoid using military acronyms, slang or terms. Sometimes the best way to talk about OPSEC is not to use the word "OPSEC". Instead, break it down and set guidelines and boundaries about what critical information is and what can/cannot be talked about and with whom. Explain why certain information should not be discussed. Discussions about OPSEC are not limited to spouse and children. Siblings and parents are proud and want to express their love and support, but they also need to be aware of the potential consequences of disclosing critical information. Additionally, this is not a one-time discussion but rather an ongoing reminder to be vigilant and protect unit critical information. OPSEC applies all year long, not only during deployments, exercise or big events.

Where Do I Go For Help?

Your unit should have an OPSEC Officer, reach out to them for specific questions.

MESA COUNTY Workforce Center

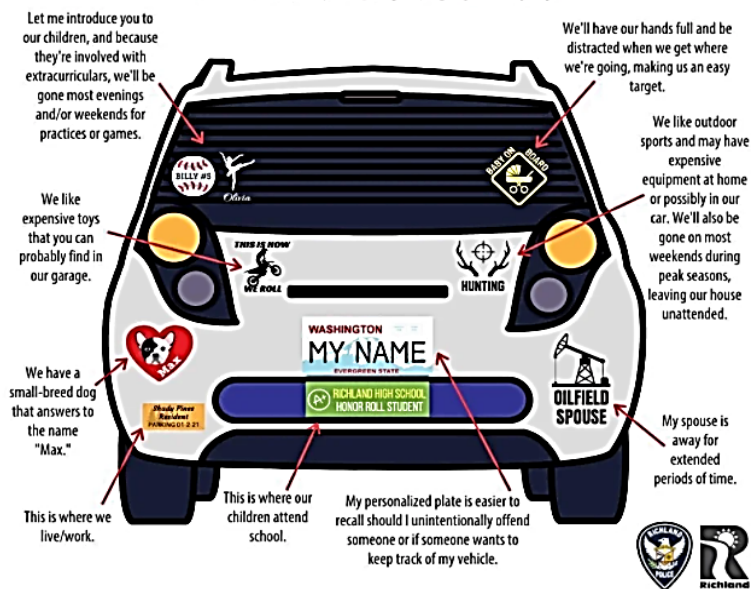Workforce Development *is* Economic Development

OPSEC AWARENESS FOR FAMILIES: PERSONAL INFO

OPSEC and Criminals

OPSEC is a mindset of critical thinking and safe habits. Criminals seek information to determine any vulnerabilities and weaknesses that allow them to target your home. While their intent may not be readily known, there are some specific steps that can be taken to minimize their success.

- Do not post data to social media that could indicate your home will be vacant
- Do not put out trash that highlights purchased items that may tempt criminals
- Be aware of your surroundings
- Look for possible surveillance in your area
- Do not put bumper stickers on your car that may provide insight to your family
- Cross-cut shred all personal documents
- Educate kids about protecting information
- Disable location services on smartphones
- Check credit reports; set up fraud alerts

What information are you DRIVING around?

Let me introduce you to our children, and because they're involved with extracurriculars, we'll be gone most evenings and/or weekends for practices or games.

We'll have our hands full and be distracted when we get where we're going, making us an easy target.

We like outdoor sports and may have expensive equipment at home or possibly in our car. We'll also be gone on most weekends during peak seasons, leaving our house unattended.

We like expensive toys that you can probably find in our garage.

We have a small-breed dog that answers to the name "Max."

This is where we live/work.

This is where our children attend school.

My personalized plate is easier to recall should I unintentionally offend someone or if someone wants to keep track of my vehicle.

My spouse is away for extended periods of time.

BILLY #5 · Olivia · THIS IS HOW WE ROLL · HUNTING · MAX · WASHINGTON MY NAME EVERGREEN STATE · RICHLAND HIGH SCHOOL HONOR ROLL STUDENT · Shady Pines Resident PARKING 01.2.21 · OILFIELD SPOUSE · BABY ON BOARD

OPSEC and Travel

Consider OPSEC during personal travel, whether within the US or overseas. While many techniques from "OPSEC and Criminals" will carry over to this section, there are additional steps that should be taken to protect your family.

- Put mail and newspaper deliveries on hold; or have someone pick them up for you
- Ask a neighbor or family member to watch the house and turn on/off lights randomly
- Mow the lawn in advance so it doesn't become too high (and providing an indicator you are away)
- Never disclose alarm codes or duress passwords and keep valuables out of sight
- Do not hide keys outside the house
- Do not leave notes on doors or indicate the length of your absence on voicemails or electronic mail accounts
- Dress casually; dress down where appropriate; do not dress as an obvious American or tourist

OPSEC and Kids

Military families must take extra steps to ensure their child understands OPSEC. Kids have feelings of anger, sadness, and worry when their loved ones deploy. Kids want to express their heartache over another deployment or excitement of a parent's homecoming. While it might seem harmless, there could be consequences for sharing information. Sit down with your children and emphasize the importance of not sharing deployment details via social media or in public where potential criminals can overhear and use the data to target your family.

OPSEC and the Internet

Anytime you or your family connect online, you become susceptible to cyber threats. Unfriendly foreign governments, terrorists and criminals collect significant amounts of useful data and use a variety of approaches to befriend someone and gain sensitive information. Their methods have become very sophisticated and the internet has become the preferred method of gathering information. Simple steps will help protect your online presence:

- Create smart and strong passwords. Passwords should be at least 8 characters w/ upper case letters, lower case letters, numbers, and special characters. (16 hexadecimal passwords are the strongest)
- Do not share passwords with anyone or use the same password for multiple sites
- Never send sensitive personal information over e-mail or instant messaging tool
- When posting photo's, remember that a picture is worth a thousand words (Is the photo geotagged? Can it be misrepresented and used to do harm?)
- Check to ensure you have a secure connection (denoted by https://) when shopping/browsing online
- Do not respond to suspicious e-mails or click on unfamiliar links. Copy and paste the URL into your browser.
- Be cautious connecting to an open Wi-Fi. If you do, ensure to use a reputable VPN to keep your data secure.