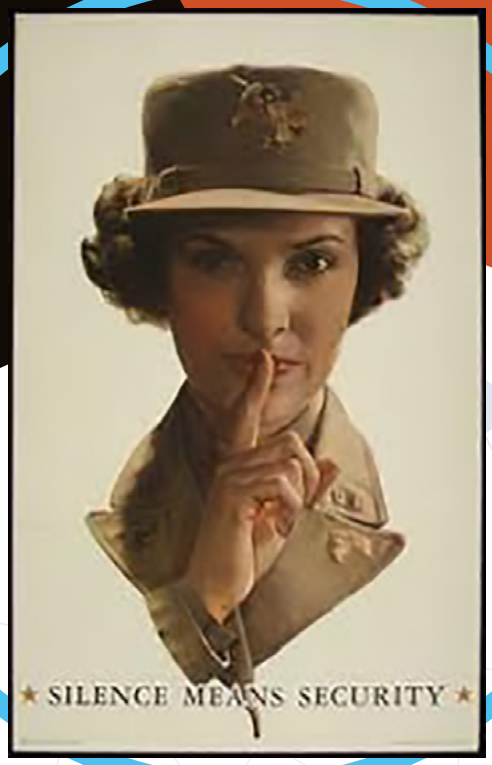
LIS SOLUTIONS MONTHLY NEWSLETTER JUNE 2022



HOW OPSEC APPLIES TO YOU

As a professional working in the government contracting, your role in protecting critical and sensitive information is crucial to your organization's success. Adversaries will try to obtain any information they can to use it against you or to damage our National Security. It is important to remember that OPSEC is not an arbitrary set of rules. It is a process and a strategic method of denying access and protecting information from our adversaries.

WHAT IS OPSEC?

Operational Security (OPSEC) is a systematic and proven process by which potential adversaries can be denied information about capabilities and intentions. This is done by identifying, controlling, and protecting generally unclassified evidence involved in the planning and execution of sensitive activities. The process involves five steps:

1. Identification of critical information
2. Analysis of threats
3. Analysis of vulnerabilities
4. Assessment of risks
5. Application of appropriate countermeasures

WHY IS OPSEC IMPORTANT TO GOVERNMENT, BUSINESSES, AND PEOPLE?

There is an old saying: "If you have nothing to hide, you have nothing to fear."

The truth is that we all have things we want to hide—like sensitive personal data. OPSEC is important to government agencies and large-scale businesses because they have may have multi-billion-dollar projects that need to be secure. But individuals also need to sufficiently protect their information and understand the full personal and professional impact of that information being compromised.

Adversaries are always looking for vulnerabilities in their targets. Here are some of the personal identifiers that you should be protecting and the ways bad actors can try to gain information about you:

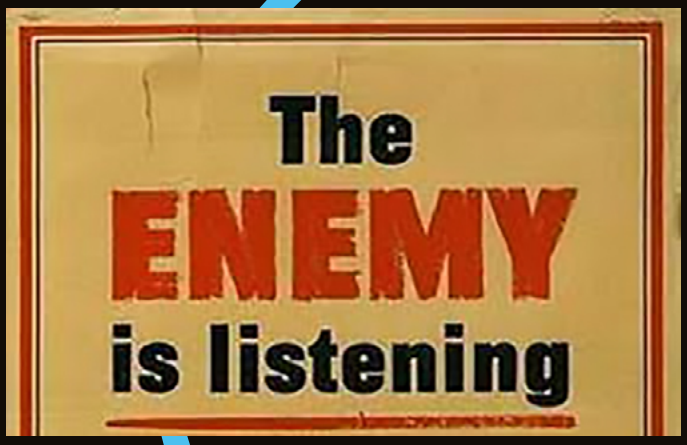
- Full Name
- Location
- SSN/NI number
- Date of Birth
- Email Accounts and Passwords
- Mother's Maiden Name
- Online Digital Footprint
- Employment Information
- Financial Information
- Mobile/Work Telephone Numbers
- Social Media Information/Posts
- Family/Friends/Colleagues

It is extremely important to protect all personal data so that you can protect yourself, your privacy, and U.S. National Security from threats, risks, and vulnerabilities. For any data that is lost, compromised, or suspected to be compromised, you are to report it to your security professionals at LIS Solutions at security@lissol.com immediately.

PROTECT YOUR SOCIAL MEDIA ACCOUNTS

Here are some simple steps that you can take to protect yourself and others

- Avoid oversharing online. Protect your critical information and ensure your family and friends don't post personal details.
- Enable the highest privacy setting available.
- Be selective of friend and connection requests.
- Turn off location settings and avoid check-ins, especially in real time.
- Avoid clicking on suspicious messages, links, or posts.
- Report concerns. If you see something, say something.
- Use strong, complex passwords for all your accounts and two-step authentication when available.



HOW MUCH INFORMATION ARE YOU REALLY SHARING?

What you or your family and friends share on social media can provide an adversary with important information about our connections, habits, and careers. This can support their efforts of elicitation, recruitment, social engineering, targeting, and more—putting us, our families, our organizations, and our missions at risk.

OPSEC, is a proven risk-analysis process that helps protect critical information and determine the value of unclassified information, but awareness is key. Using the OPSEC process, we can deny the adversary information they need to compromise our operations.

Keep in Mind:
Remember, before posting anything, or sharing information, or logging into a system, think before you act. It is okay to ask if this is safe or how posting/sharing information will harm you or others. Take that extra step to protect and safeguard data and information. Be situationally aware of your environment and surroundings and ensure that you are not being watched or overheard by anyone. Finally, do not discuss details like timelines, detailed locations, or movements, specific names, ranks, job titles, budgets, current or future operations, or most importantly our security procedures. This information can be vulnerable and can cause risk to you and others.

Helpful Resources:

- https://csrc.nist.gov/glossary/term/operations_security
- https://cdse.usalearning.gov/course/view.php?id=227
- https://www.army.mil/article/249435/be_opsec_aware_before_you_share
- https://www.tripwire.com/state-of-security/security-data-protection/opsec-everyone-not-just-people-something-hide/