*OPSEC Awareness Month*

# OPERATIONS SECURITY (OPSEC)


*January 2023*

# Table of Contents

NATIONAL OPSEC PROGRAM

Colleagues,

As you may be aware, January 2023 has been designated as National Operations Security (OPSEC) Awareness Month. The purpose of this designation is to bring attention to the importance of protecting sensitive data and other information critical to the mission of your institution. Operations Security practices keep critical information out of the hands of those who may want to do harm to not only your college or university, but also the students, faculty, and staff who are so integral to the success of your organization. In the attached document, *OPSEC Awareness Month Messaging Champion Communication Packet for Universities/Colleges January 2023*, we specifically address the protection of information, through OPSEC Awareness, for institutions of higher education.

The packet contains information for all members of the academic community, to include administrators, faculty, researchers, public safety personnel, and students. The packet is presented in an easy-to-read/understand format for those who may not be familiar with OPSEC concepts and practices, and provides resources and links to OPSEC-related tools and other resources that can strengthen your institution's security program. These resources can also be applied outside a college/university setting, and can enhance protection in the personal lives of your college or university's personnel and students, and their friends and families.

In an effort to raise OPSEC Awareness to an expansive community whose members may be new to OPSEC principles and/or practices, I encourage institutions of higher education to share these practices at OPSEC awareness events and through other promotional campaigns. We recognize that including your organization in the OPSEC community is critical to our nation's overall security posture. We also recognize that educating/introducing students to OPSEC practices and principles will result in a future generation of leaders with a greater understanding of threats posed by adversaries, and future leadership with the ability to recognize and mitigate those threats.

I invite you to get involved in National OPSEC Awareness Month 2023. The attached OPSEC Awareness Packet, Communications Supplement, and links will assist you. The Communications Supplement contains multi-use messages that you can use at your discretion, and can be incorporated into posters, social media posts, messaging boards, tabletop cards, or other materials your organization uses to communicate OPSEC Month messaging.

There are additional resources available through the NCSC's National OPSEC Program website (NOP Website Link) that will assist you in implementing National OPSEC Awareness Month messaging and creating or enhancing your ongoing OPSEC posture. Enhancing the OPSEC capabilities of our Nation's institutions of higher learning helps us all. Here's to a successful OPSEC Awareness Month this January and better protection of your organization all year round!

Sincerely,

*Rebecca Morgan*

Rebecca A. Morgan

Acting Director, National OPSEC Program

## What is OPSEC?

OPSEC stands for Operations Security. The plain English definition is: “A systematic process of identifying and protecting sensitive, critical information to deny or mitigate an adversary’s ability to access that information.” Universities and colleges are caretakers of valuable research and other institutional information, as well as personal, confidential, or private information belonging to students, faculty, and other employees that someone could use to harm an individual or your institution. These types of information include home addresses, travel plans, Social Security numbers, banking information, passwords, and more. Raising awareness among students and staff that their information may be targeted, and promoting appropriate OPSEC practices to mitigate the risk of compromise, are essential strategies for keeping such information secure and out of the hands of those seeking to use it for personal gain or other nefarious purposes. More importantly, individuals who understand that OPSEC is a continuous process are less likely to let their guard down as time progresses.

## Introduction to OPSEC Awareness Month 2023

The second annual OPSEC Awareness Month will be taking place during January 2023. Throughout the month, the Enterprise Threat-Mitigation Directorate (ETD) of the National Counterintelligence and Security Center (NCSC) will be sharing and promoting information related to this year’s themes: 1) Introduction to OPSEC, and 2) Protecting yourself and your peers by practicing OPSEC. While colleges and universities are not obligated to implement OPSEC programs, these themes provide an excellent opportunity to educate your community - especially students and staff - about keeping information safe in relatively basic terms that can be understood by recipients who may not be familiar with OPSEC practices.

Participation in OPSEC Awareness Month 2023 will be particularly useful in raising awareness among students and staff at your university, college, or institution about the importance of protecting sensitive information. By applying OPSEC strategies and guidelines to their everyday lives, students and staff can be better equipped to protect their information from those who would want to use that information for unintended purposes, or for purposes that may ultimately harm an individual, group, or organization. The enclosed awareness materials will help you identify activities and promotional information that can be shared with the members of your institution, to include marketing materials directed toward students and staff.

Lastly, federal government departments and agencies are required to implement OPSEC programs, and we use terms and phrases that are familiar, relevant, and culturally aligned to our programs and missions. We understand that, as colleges and universities with established security programs, you may already have implemented OPSEC principles and practices in some way, even if they are not under the banner of OPSEC. We encourage you to increase OPSEC awareness in the most effective

manner for your organization, including the use of terminology that reflects the culture of your organization or best suits your unique needs.

We are excited for the opportunity to share our OPSEC materials with a broader audience in the hope that you, and the ultimate target market (i.e., students and staff), find the awareness materials to be of educational value.

## Communications Goals and Desired Outcomes

The following list contains goals we believe would help strengthen your university, college, or institution's OPSEC program:

- Introduce your students and staff to the concept of OPSEC and its strategies.
- Inform students and staff about the importance of implementing OPSEC.
- Help students and staff to identify the private, personal, and/or institutional information that they would not want unauthorized people to have access to.
- Provide students and staff with the information they need to be able to employ OPSEC in their daily lives.
- Encourage students and staff to educate their friends, family, and other community members about OPSEC and how they can protect their information.
- Begin the process of developing a security mindset among students and staff, one in which they are skeptical but not paranoid, careful but not scared, and empowered to keep themselves and their private information safe.

Desired Outcomes: Students and staff within your university, college, or institution should 1) be familiar with the OPSEC cycle, 2) have the tools to implement OPSEC best practices, and 3) implement OPSEC best practices on a daily basis.

## Key Messages for OPSEC Awareness Month 2023

**Primary components of OPSEC that should be highlighted and understood:**

OPSEC is an analytic process and continuous cycle, with logical, easy-to-follow elements.

- OPSEC helps identify what information to protect, when to protect it, and how to protect it.
- OPSEC helps define the value of your private or personal information.
- OPSEC requires thinking from both friendly and adversarial perspectives.
- OPSEC helps develop a mindset and culture for safeguarding information.
- OPSEC denies critical information to adversaries when implemented properly.

**Further, there needs to be an emphasis on the role of teamwork and protecting your information as well as that of your friends and family. This includes the following points:**

- Everyone plays a role in effective Operations Security in an organization.
- Take care inside and outside your institution to protect information that an adversary could use to target you or your organization.
- Be aware of your surroundings – even online. Any information that is shared virtually can be used to exploit a vulnerability.
- Don't trade online convenience for security. Learn to recognize and report attempts to elicit information.

## Why Should Students Implement OPSEC?

With the proliferation of social media platforms and the emphasis society places on sharing one's life details with everyone on the Internet, there are many opportunities for someone to obtain the private, personal information of students and staff and use it for harmful purposes. Daily activities that seem harmless, such as posting a personal photo on Instagram, can make a student an attractive target to someone who wants their information. By employing the OPSEC strategies and guidelines, students and staff can better protect their private, personal information and keep themselves, their friends, and their families safe.

It is also important to understand that information collected on the Internet can be saved in perpetuity. Private companies, nation states, individual actors, and others collect and share (and, in certain cases, hack into databases) in order to obtain information. At that point, students and staff would not have control over their own information, which can now be used by any one of a number of bad actors to do individuals harm, either immediately or in the future.

## Opportunities to Implement OPSEC

**OPSEC and Student Foreign Travel (Study Abroad Programs)**

University study abroad programs offer students a unique opportunity to immerse themselves in another country's culture during their studies. While this should be viewed as a positive experience and something to be encouraged, it is important to understand that residing in another country comes with an increased likelihood that personal information may be stolen or compromised. Many countries have the capability to surveil foreign students traveling to (and within) their country, and any information stored on a phone, laptop, and other device could be monitored or collected at any time by a foreign government or other foreign actors. Identifying the information that may be unwittingly provided to a foreign government is vital to protecting a student's or staff member's information.

When traveling to another country, precautions such as considering the purchase of a different phone to use while abroad; the deletion of sensitive information from personal devices; and employing encryption measures are prudent OPSEC practices that enhance the security of students' information. Additionally, those who gain access to student information, especially logins and passwords to your institution's systems, increase your institution's risk in addition to their own. Raising OPSEC awareness

among students on foreign travel is a key component of protecting everyone's information.

Note: Similar issues apply to staff who are invited to international conferences, take sabbaticals in foreign countries, conduct research in foreign countries, etc.

### OPSEC and Social Media

Social media applications and websites such as Facebook, Twitter, Instagram, and TikTok are useful for staying in touch with friends and family as well as meeting new people. However, social media sites can be inherently dangerous when students and staff share information about their lives (and those of others). A photo posted to social media of an individual outside his/her home may appear to be a fun way to share information with your friends, but can quickly turn dangerous if an adversary were to use information from that photo to determine where you live. Applying OPSEC strategies to social media use is vital to protecting private, personal information. Students and staff should consider taking steps to protect themselves and their information, such as maximizing their privacy settings, disabling location services, and advising friends and family to do the same.

Users should also be aware that social media companies, whether they are US-based or foreign-owned, control *all* information shared on their platforms. Any information posted to a social media platform is by definition in someone else's possession, thereby creating risk. The only unknown is how the information will be shared, sold, or used by others.

## Students' Strengths and Weaknesses in Implementing OPSEC

### Student Strengths

Students have most likely been applying OPSEC strategies to their daily lives without knowing such actions fall under the umbrella of OPSEC. Many students receive instruction regarding online safety when they are younger, and continue to use those lessons today. Most students have been warned not to share personal information such as bank account info, credit card numbers, home addresses, and Social Security numbers. They have also been told not to click on suspicious text messages and emails or pop-ups on websites. These are important precautions, and students should remain vigilant. Adversaries won't ever stop trying to gain access to certain types of information, and letting one's guard down once is sometimes enough for an adversary to exploit a weakness.

Universities and colleges already have at least some information security protections for web-based student accounts and university email systems. Tools such as spam detectors and monitoring done by IT services also work together to protect students' (and the institution's) information.

### Student Weaknesses

The primary space where students tend to be the most at-risk and the least conscious of their actions is on the Internet and social media. Many students use the Internet and social media applications to connect with new people and friends without being careful about the information and data they are openly sharing. Very recently, it was found that

one of the most popular smartphone applications, TikTok, was transferring data from user phones and storing it in China. Information from large media companies such as Meta (formerly Facebook), Twitter, and others are especially at risk of having personal information of users stolen, sold, or leaked to adversaries.

Avoiding these websites and applications altogether is the best option for keeping personal information safe, but we understand how popular they are with the student population. To reduce their vulnerabilities, students should apply OPSEC strategies when utilizing these websites and applications, especially taking care to maximize their privacy settings so that sensitive, personal information is not inadvertently shared with those who might use it for harmful purposes.

**Student Best Practices**

As previously mentioned, students may already be proactively protecting their personal information, but students should continue to be careful when opening suspicious emails, text messages, and pop-ups. Students should also be careful with whom they share their personal information, both in-person and on the Internet.

In accordance with OPSEC best practices, students and staff should: 1) identify what information they consider to be private and personal 2) check where they have already shared this information and verify that the information is only posted in safe and necessary places 3) take steps to protect their information by implementing the OPSEC strategies discussed above.

Additional materials can be found on the NCSC website https://www.dni.gov/index.php/ncsc-what-we-do/operations-security and in the accompanying DIA manual.

## OPSEC Marketing Materials

The following marketing materials are available for use in your OPSEC awareness campaign.

**Graphic Logo**

**OPERATIONS SECURITY**


***"Protect What's Yours"***

**Social Media Posts**

The following messages may be used as-is, or edited to include your organizational branding. They are suitable for posters, social media (Tweets), school hallway messaging boards/monitors, tabletop cards, or any other manner your school may use to communicate OPSEC messaging. Some of the messages may be more applicable than others in addressing OPSEC-related content. Consider your "target market" when selecting and/or editing certain messages.

When you travel abroad, that foreign government might gain access to everything on your phone. Identifying the information that you could unwittingly provide to a foreign government is vital to protecting private, personal information that you would never want them to have. #THINKOPSEC

That super cute selfie you just posted may contain more private information about you than you think. Would you want the world to have your personal information? Switch social media settings to private so only people you know can see what you post. #THINKOPSEC

Sometimes sharing is not caring. Giving information to people who don't need it may impact your personal and professional life in the future. #THINKOPSEC

Educating your family about how OPSEC can affect THEM is key to maintaining FAMILY OPSEC. Your personal information can be used against you. Protect your family. #THINKOPSEC


Any information that is shared online can be used to exploit a vulnerability. #THINKOPSEC before posting to social media!

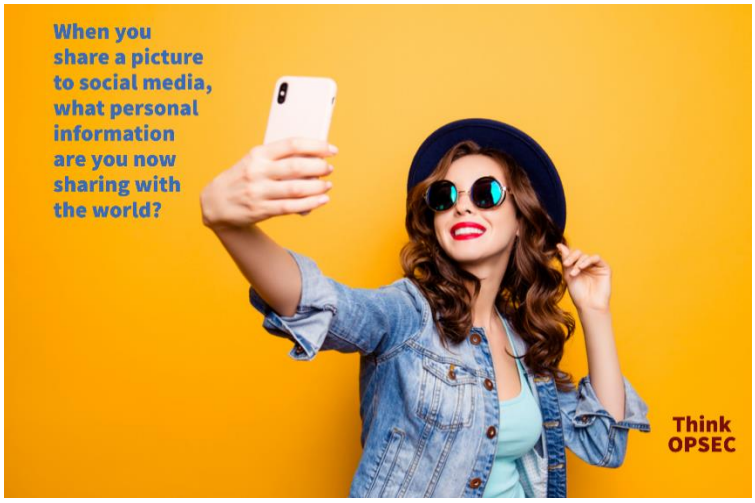
| | |
|---|---|
| Remember in *Home Alone* when the burglar posed as a police officer in order to scope out the McCallisters? The McCallisters shared their home security features and even the details of their trip to Paris with the fake officer, leaving Kevin as their only defense. #THINKOPSEC | **OPERATIONS SECURITY**<br>  <br>***"Protect What's Yours"*** |
| Any information that is shared online can be used to exploit a vulnerability about either you or your family. #THINKOPSEC before posting or answering questions about your life online. |  |

## Multi-Use Messages

The following multi-use messages may be used as-is, or edited to include your university/college logo. They are suitable for posters, social media (Tweets), school hallway messaging boards/monitors, tabletop cards, or any other manner your school may use to communicate OPSEC awareness messaging.


Everything you put on the Internet stays there forever. Do you know what information about you is currently out there?
Think OPSEC


WHEN YOU DELETE A SUSPICIOUS EMAIL FROM AN ADDRESS YOU DON'T RECOGNIZE AND INFORM YOUR SCHOOL'S IT DEPARTMENT ABOUT THE INCIDENT
Think OPSEC


When you share a picture to social media, what personal information are you now sharing with the world?
Think OPSEC


Don't over think it! Protecting your information is not rocket science!
Think OPSEC


TAKING A NEW PHONE WHEN VISITING A FOREIGN COUNTRY SO THAT THE GOVERNMENT CAN'T ACCESS YOUR DATA AND INFORMATION
Think OPSEC


When you travel abroad, all information on your phone now belongs to that foreign government.
Think OPSEC

**Awareness Posters**

Following are sample OPSEC awareness posters available for your use. They can be used as-is, or modified to suit your unique needs. These and other posters can be downloaded from the NCSC website at Operations Security (dni.gov).