The Purple Dragon

Special Edition | **Joint Information Operations Warfare Center**
Joint OPSEC Support Element (JOSE) | **Spring 2020**

COVID-19 and OPSEC Considerations

Operations Security (OPSEC) must remain a priority as senior leaders take steps to address COVID-19 and actions enabling the force to continue missions. During this time of social distancing and unprecedented number of teleworkers, senior leaders must utilize their staffs and OPSEC practitioners to identify new threats, indicators, and vulnerabilities created by minimal staffing and the use of non-standard communications methods. Commanders must continually ensure their current OPSEC measures are reviewed for effectiveness, and if necessary, develop and implement new OPSEC measures to prevent inadvertent disclosures or new vulnerabilities.

How commanders conduct business during the coming weeks will be of great interest to our adversaries who continually monitor our efforts and seek new avenues to gain sensitive and critical information. To successfully mitigate unacceptable risk to activities, intentions and capabilities; the following is a list of items that senior leaders should consider adding to their organization's critical information lists to deny sensitive information to our adversaries:

- Rosters, manpower shortages, or changes
- Changes to schedules and timetables
- Shortfalls and vulnerabilities in readiness
- Information related to sensitive mission areas affected by COVID-19
- Information regarding loss of capability or degradation
- Changes or modifications to tactics, techniques, and procedures
- Limitations or reduced capabilities
- Changes in force composition or disposition

Leaders should also consider:

- Placing emphasis on members knowing their unit Critical Information List (CIL) and how to protect items on it
- Updating and sharing threat information surrounding the pandemic (i.e. COVID-19 scams and other social media techniques)
- Directing members to not discuss readiness and operational limitations
- Ensuring members are aware that social media sites should not include work info
- Ensuring computer and communication devices are configured to encrypt
- Placing emphasis on members encrypting e-mails that contain sensitive or critical information

Strong OPSEC measures are a key to denying adversaries access to sensitive information.

Inside This Issue

Joint Information Operations Warfare Center
Joint OPSEC Support Element (JOSE)
2 Hall Blvd, Suite 217
JBSA LACKLAND, TX 78236

Editorial Staff – Email: js.jbsa.jiowc.mbx.jose@mail.mil
Phone: (210) 977-5192 DSN 969-5192
http://www.facebook.com/JIOWC.OPSEC.Support

Maintaining our Essential Secrecy during COVID-19

Commanders / Directors are reminded that OPSEC directly impacts military readiness. The need to maintain essential secrecy of operations and contingency plans, including current and future operational activities and events is a mission assurance imperative. We must remain OPSEC vigilant!

Commanders / Directors should consider the following to support maintaining essential secrecy across the force:

- Refer to the DoD CUI Index w/ Categories worksheet to aid with understanding and determining the categorical types of information their teleworking workforce typically and/or potentially will process while using personal and/or government furnished computing devices. See the DoD CUI Program: https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx
- Conduct a thorough information protection review to readily know which teleworkers process CUI with a *low, moderate, or high* impact on confidentiality
- Direct a teleworking *security* review with those individuals who process CUI with moderate-to-high confidentiality impact in order to mitigate concerns before an incident arises
- Remind Teleworkers:
    - To review the newly issued DoDI 5200.48, *Controlled Unclassified Information*
    - To review the unit's Critical Information List
    - To avoid or limit storing / saving / printing CUI, especially on personal computing devices
    - Review home network and device security configuration and privacy settings
    - Think about unclassified data aggregation that could result in the disclosure of CUI or even classified information
    - To think before they post / share to social media; pictures / videos of a teleworking "office" environment could reveal national security-related work products and/or personal privacy information
    - That information security incidents resulting in a classified "spillage" could result in the computing device(s) being seized by law enforcement officials; accessing a DoD web site / portal required acceptance of the terms contained in the DoD Notice and Consent Banner

Eight Things Senior Leaders Can Do To Improve Their OPSEC Program

1. Provide your specific OPSEC guidance to staff and family members
2. Ensure Organization Critical Information List is current (within one year)
3. Ensure organization OPSEC guidance is current and published
4. Ensure local/mission specific OPSEC training is being conducted
5. Ensure personnel are encrypting emails containing OPSEC CIL or CUI
6. Ensure OPSEC is incorporated into planning, plans and orders
7. Assess your organization's OPSEC program for effectiveness
8. Post OPSEC guidance and CIL on SharePoint so members can access

OPSEC Frustrates The Adversary & Saves Lives!

OPSEC Do's and Don'ts for Teleworking

Operations Security (OPSEC) actions play an important role in defending networks and protecting critical information and indicators. The following tips and best practices can help you protect sensitive information from adversary exploitation or collection while teleworking:

DO

- Follow your organization's OPSEC and telework guidance
- Know your organization's OPSEC Critical Information List (CIL)
- Ensure operating systems and anti-virus software are up-to-date
- Take reasonable steps to minimize the risk of access by unauthorized personnel (e.g. reading, discussing, or leaving sensitive information unattended)
- Familiarize yourself with newly published DoDI 5200.48, *Controlled Unclassified Information*
- Study and know what must be protected: OPSEC Critical Information, For Official Use Only (FOUO), Controlled Unclassified Information (CUI), and Personally Identifiable Information (PII)
- Familiarize yourself with adversary information collection methodology
- Ensure computers and mobile devices are configured to sign and encrypt e-mails
- Always encrypt Controlled Unclassified Information (CUI) such as OPSEC critical information, FOUO, and PII data sent on computers and mobile devices
- Use your organization-approved file sharing service/capability to share files with others
- Use your organization's approved communication and collaboration methods for official business
- Use DoD SAFE to share large files/videos (i.e., over 10 MB) with DoD and non-DoD recipients
- Vary the start times of conference calls to avoid always beginning at the same time
- Use approved voice and collaboration tools and limit collaboration via cell phone when possible
- Mute your microphone during conference calls unless actively speaking when possible
- Disconnect from conference calls immediately when the call ends
- Talk to your family members and friends about OPSEC and protecting their personal information
- Ensure unclassified documents requiring protection are appropriately marked and safeguarded

DON'T

- Use personal email accounts for official business
- Encrypt unclassified e-mails that don't require additional protection
- Send Controlled Unclassified Information (CUI) such as OPSEC critical information, FOUO, and PII or other sensitive information through unencrypted e-mails or to personal accounts
- Discuss critical or sensitive information on unsecure phones or talk around information
- Allow unauthorized individuals to use government-issued devices
- Use personal cloud/file sharing/storage accounts for official business
- Use any non-DoD approved instant messaging applications to share DoD information
- Store Controlled Unclassified Information (CUI) such as OPSEC critical information, FOUO, and PII on non-government equipment
- Work from public locations or transportation where others can "shoulder surf"

Protecting Sensitive Unclassified E-Mails

Be the strongest link and think Operations Security (OPSEC) when sending emails on unclassified DoD networks. Did you know that encrypting e-mails is an effective OPSEC measure to protect e-mails from being read by unintended recipients or being compromised? It's a known fact that business conducted on DoD networks provides opportunities for sensitive information to be read when not encrypted.

You can identify what sensitive unclassified information requires protection by reviewing your organization's and higher headquarters' Critical Information List (CIL). OPSEC critical information is defined as information about friendly (U.S., allied, and/or coalition) activities, intentions, capabilities, or limitations an adversary seeks in order to gain military, political, diplomatic, economic, or technological advantage. Such information, if revealed to an adversary, may prevent or complicate mission accomplishment when not protected. Commanders and senior leaders approve these lists so their personnel know what to protect since everything can't be protected.

Encrypting emails is not new to the DoD, but the number of personnel working from home is greater than has been seen in the past due to COVID-19, thus making it important to ensure all personnel teleworking know how to encrypt when working from home. The policy to encrypt applies to all unclassified emails sent from DoD-owned, operated or controlled systems or accounts to include desktops, laptops, and mobile devices. OPSEC assessments conducted by the Joint OPSEC Support Element found that when personnel failed to encrypt emails, they usually fell into one of three categories: individuals did not configure their devices to encrypt, personnel did not know what to encrypt, and personnel did not know how to encrypt.

All of these situations can be corrected by commanders and directors taking the following actions: **First**, get involved and make an active effort to ensure your organization's computer devices are properly configured to send encrypted emails and personnel are informed on how to configure their personal devices for encryption. **Second**, ensure personnel are trained on what to encrypt and made aware of your higher headquarters' and your organization's CIL. Controlled Unclassified Information, such as For Official Use Only, Personally Identifiable, and OPSEC Critical Information and other sensitive technical data must be encrypted. **Lastly**, ensure your staff and personnel are trained on how to encrypt. Having personnel knowing the difference between digitally signing an email and encrypting an email can significantly impact an organization on what's being protected. Remind personnel not to encrypt every e-mail since this can have an equally damaging effect by increasing the bandwidth across DoD networks.

Configuring My Computer to Telework

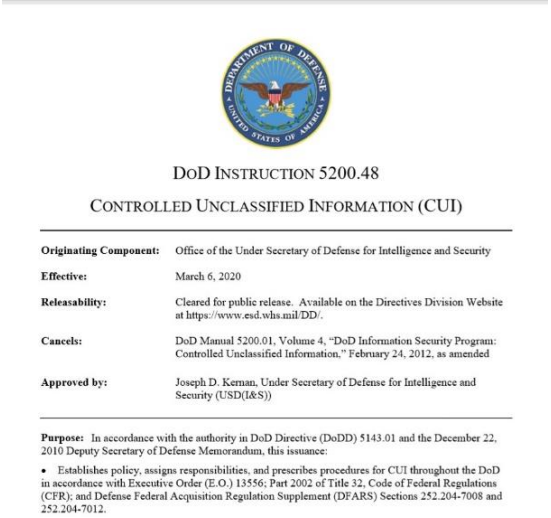
For help configuring your computer to read your CAC or troubleshooting go to:

https://public.cyber.mil/pki-pke/

New DoDI 5200.48, Controlled Unclassified Information

DoD issued a new DoD Instruction 5200.48, *Controlled Unclassified Information (CUI)*, effective 6 March 2020 to replace DoD Manual 5200.01, Volume 4, "*DoD Information Security Program, Controlled Unclassified Information*," February 24, 2012. This publication identifies Operations Security (OPSEC) as a category in the DoD CUI registry and is available at https://www.esd.whs.mil/DD/. A list of all DoD CUI registry categories aligned to the CUI National Registry can be found on Intelink at:

https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/CUI/Forms/AllItems.aspx



DoD INSTRUCTION 5200.48

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Originating Component:	Office of the Under Secretary of Defense for Intelligence and Security
Effective:	March 6, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Cancels:	DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information," February 24, 2012, as amended
Approved by:	Joseph D. Kernan, Under Secretary of Defense for Intelligence and Security (USD(I&S))

Purpose: In accordance with the authority in DoD Directive (DoDD) 5143.01 and the December 22, 2010 Deputy Secretary of Defense Memorandum, this issuance:

- Establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoD in accordance with Executive Order (E.O.) 13556; Part 2002 of Title 32, Code of Federal Regulations (CFR); and Defense Federal Acquisition Regulation Supplement (DFARS) Sections 252.204-7008 and 252.204-7012.

Protect Yourself While On Social Media

Social media is an easy way to stay connected to friends and family, but you should be wary of the information you publish on these sites and who can view the material on such sites. If you have social media accounts, it is important to appropriately set up your account security settings, as well as limit certain types of information published on your account. Realize that even with correctly implementing your security settings, your information can still be used against you.

- Establish and maintain connections with people you know and trust; review your connections on a regular basis
- Assume anyone can see information you post about your activities, location, and personal and professional life
- Don't post Controlled Unclassified Information (CUI) such as OPSEC critical information, FOUO, and PII on social media
- Don't post that you are teleworking as this can make your home a target
- Make sure you family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data
- Avoid posting or tagging images of you or your family that clearly show your face
- Avoid posting pictures that gives away PII such as license plates or addresses
- Be aware of adversary collection methods on social media and share with family members and friends
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points
- Avoid participating in social media games where you provide family personal information
- Use direct "hard-line" ethernet connection vs wireless connectivity whenever possible

DEFEND THE DODIN

Do your part to protect the Department of Defense Information Network (DODIN) while teleworking

Network Utilization Do's & Don'ts

DO

- ✓ Log off of your VPN connection at the end of the work day
- ✓ Verify your local internet connection before calling your IT service desk if you're having connectivity issues
- ✓ Use your organization-approved file sharing service/capability to share files with others
- ✓ Use your organization's approved communication and collaboration methods for official business
- ✓ Use DoD SAFE to share large files/videos (i.e., over 10 MB) with DoD and non-DoD recipients
- ✓ Limit all non-mission-essential activity on government-furnished equipment (GFE) (e.g., social networking, audio and video streaming, personal shopping)
- ✓ Digitally sign government emails
- ✓ Study and follow the Acceptable Use Policy for government systems
- ✓ Request assistance from knowledgeable co-workers for tips before calling your IT help desk
- ✓ Consider providing alternate phone numbers – other than your office phone number – on email correspondence, out of office replies, and/or voicemail for contact while teleworking
- ✓ Work offline when possible
- ✓ Use approved voice and other collaboration tools
- ✓ Disconnect from conference calls immediately when the call ends

DON'T

- ✓ Use your GFE for non-essential activity (e.g. social networking, audio and video streaming, personal shopping
- ✓ Use internet-based, unofficial audio and video on demand streaming services or websites
- ✓ Email large files of videos
- ✓ Dial into phone or video conferences unless invited
- ✓ Leave applications running that you're not actively using (e.g., email, video, voice, etc.)

Cyber Security Do's & Don'ts

DO

- ✓ Reboot your machine prior to establishing a VPN connection
- ✓ Use GFE when possible
- ✓ Ensure your GFE is patched with the latest updates
- ✓ Ensure your personal devices are updated with the latest operating system and security patches
- ✓ Follow your organization's GFE use and handling instructions
- ✓ Report loss or theft of GFE to your security point of contact and IT service desk immediately
- ✓ Close all applications you're not actively using
- ✓ Configure your home Wi-Fi according to best practices; change the password and enable encryption
- ✓ Study and know the difference between For Official Use Only (FOUO), Controlled Unclassified Information (CUI), and Unclassified information
- ✓ Familiarize yourself with adversary attack methodology (e.g., COVID-19 maps,COVID-19 spear phishing attacks)
- ✓ Report suspicious activity or behavior to your chain of command
- ✓ Follow your organization's specific cybersecurity guidance
- ✓ Install "McAfee Total Protection" antivirus software (free to DoD employees) on your personal computer available on public.cyber.mil

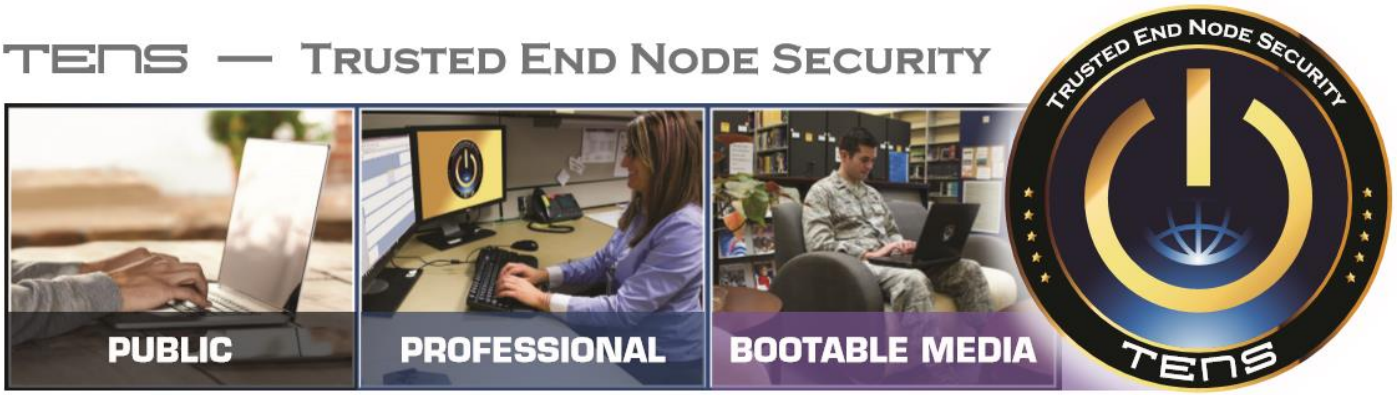
DON'T

- ✓ Leave your computer unlocked when unattended
- ✓ Use untrusted internet or Wi-Fi connections
- ✓ Open suspicious email
- ✓ Auto-forward or forward sensitive information, OPSEC CI, CUI, FOUO, PII, and protected health information (PHI) from official email accounts to personal email accounts

DoD Secure File Access Exchange (SAFE)

DoD SAFE is an effective tool to protect an organization's sensitive information when encryption is not available or members can't get the e-mail encryption to work with outside organizations and partners. DoD SAFE, located at https://safe.apps.mil, is a web-based tool that provides authenticated DoD CAC users and guests (unauthenticated users) the capability to securely send and receive large files, including files that are too large to be transmitted via email. Guests can receive files from CAC users and (only if CAC users requested files) send files to CAC users. Notification is achieved via email.

DoD SAFE has an authorization to operate under DISA and is approved for transfer of For Official Use Only (FOUO), Personally Identifiable Information (PII), and Protected Health Information (PHI) data. DoD SAFE utilizes the latest web browser encryption transport protocols to secure files when they are in transit. Files uploaded into SAFE can be encrypted at rest if the sender selects the corresponding check box on the DoD SAFE site. DoD SAFE users are responsible for ensuring they encrypt FOUO, PII, PHI data and information found on Critical Information List (CIL). DoD SAFE is for UNCLASSIFIED information. For additional information go to https://dl.cyber.mil/dcs/pdf/unclass-DoD_SAFE_FAQs_v1.2.pdf.



Trusted Node Security (TENS) is a family of products focused on providing network access in the most secure way possible. By booting from read-only media and installing nothing, TENS creates a temporary RAM-based, secure end node on almost any computer. Check it out at https://www.spi.dod.mil/lipose.htm

Free Antivirus Software for PC and MAC Platforms

The DoD Antivirus Software License Agreement from McAfee allows active DoD employees and authorized government contractors to utilize the antivirus software for personal device protection. Home use of the antivirus products will not only protect personal PCs, but will also potentially lessen the likelihood of malicious threats being introduced to the workplace and compromising DoD networks. Defense Information System Agency (DISA) Home Use is now being offered to government employees and defense contractors with an approved .mil email address.

McAfee Internet Security

As a member of the DoD government and defense contractor community, you can now take advantage of a free one-year subscription to McAfee Internet Security for your PC or MAC at no cost. This subscription gives you proactive security for your home PC by preventing malicious attacks and keeping you safe while you surf, search, and download files online. McAfee's Internet Security service also continuously delivers the latest software, so your protection is never out-of-date.

By installing McAfee Internet Security on your home system, you'll not only be protecting your PC from malicious threats, but you'll also help your organization strengthen its IT security against transferable viruses and spyware.

Be advised, DISA Home Use licensing for McAfee Internet Security is for personal/privately purchased devices only. Do not install McAfee Internet Security on Government Furnished Equipment (GFE).

Additional Information/Download

Go to https://cyber.mil/covid19 (CAC enabled) for additional information on MACAFEE Home Solutions and how to download for PC and MAC platforms.

Like US on Facebook!
https://www.facebook.com/Joint.OPSEC.Support/