Fort Sill Circular 300-21-01

Security

United States Army Fires Center of Excellence & Fort Sill (USAFCoEFS) Operations Security (OPSEC)

Department of the Army
Headquarters, USAFCOEFS
455 McNair Avenue, Suite 100
Fort Sill, OK 73503
30 November 2021

UNCLASSIFIED

Department of the Army
Headquarters, USAFCoEFS
455 McNair Avenue, Suite 100
Fort Sill, Oklahoma 73503
30 November 2021

Fort Sill Circular 300-21-01

Expires: 30 November 2022

Security

United States Army Fires Center of Excellence & Fort Sill (USAFCoEFS)
Operations Security (OPSEC)

History. This circular supersedes the USAFCoEFS Operations Security (OPSEC) Plan dated 2019.

Summary. This publication prescribes OPSEC guidance for all Fort Sill units and organizations assigned to United States Army Fires Center of Excellence & Fort Sill. This regulation is distributed and published solely through the Directorate of Human Resources, Administrative Services Division Homepage at: http://sill-www.army.mil/dhr/Admin_Svcs/Index.html

Supplementation. Supplementation of this circular is prohibited without prior approval from the Directorate Plans, Training, Mobilization and Security (DPTMS), Fort Sill, OK 73503.

Suggested Improvements. The proponent of this regulation is the DPTMS. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Directorate of Training, Mobilization, and Security.

Applicability. This Circular applies to all active component, reserve component, Department of Defense (DoD) civilian, and government contractor personnel assigned to USAFCoEFS.

MICHAEL J. KIMBALL
Colonel, GS
Chief of Staff,

HQ U.S. ARMY FIRES CENTER OF EXCELLENCE
OFFICIAL
FORT SILL, OK

JAMES A. MILLER
Director, Human Resources

DISTRIBUTION:
Fort Sill Intranet
30th ADA Bde
31st ADA Bde
75th FA Bde
428th FA Bde
434th FA Bde
MEDDAC
DENTAC
U.S. Army Garrison
HQs Detachment

1. References.

a. Army Regulation (AR) 530-1 (Operations Security), 26 September 2014

b. TRADOC Protection Plan 21-006, Appendix 3, 11 June 2021

c. ALARACT 289/213, Army OPSEC Training for External Official Presence (EOP) Sites Operators, 29 October 2013

d. AR 25-55 (The Department of the Army Freedom of Information Act Program), 19 October 2020

e. AR 190-45 (Law Enforcement Reporting), 27 September 2016

f. AR 360-1 (The Army Public Affairs Program), 8 October 2020

g. TRADOC Implementing Guidance for Integrating AT and OPSEC contained in FRAGOs 68 and 74 to OPORD 11-004, TRADOC Campaign Plan (TCP) 11-12

h. DoD Instruction 5200.48 (Controlled Unclassified Information (CUI)), 6 March 2020

i. Fort Sill Regulation 1-8 (Reporting Procedures), 1 October 2018

j. HQDA EXORD 018-17 Restricting Personal Electronic Devices (PEDs) at Training/Briefing Sessions in order to Mitigate Vulnerabilities and Reduce OPSEC Violations, 28 October 2016

k. HQDA EXORD 042-17 Personal Electronic Devices (PEDs) Level Designation Standardization at Training/Briefing Sessions in order to Mitigate Vulnerabilities in Cyberspace, 21 December 2016

l. AR 380-5 (Army Information Security Program), 22 October 2019

2. General.

a. This plan supersedes the USAFCoEFS Operations Security (OPSEC) Plan dated 2019 and prescribes OPSEC guidance for all Fort Sill units and organizations assigned to United States Army Fires Center of Excellence & Fort Sill. This plan applies to all active component, reserve component, Department of Defense (DoD) civilian, and government contractor personnel assigned to USAFCoEFS.

b. OPSEC considerations will be integrated into all operations, functions, and missions. OPSEC will enhance the mission by balancing operational effectiveness with the need for protecting critical and sensitive information.

c. OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

(1) Identify those actions that can be observed by adversary intelligence systems.

(2) Determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be used to adversaries.

(3) Select and execute the measures that eliminate or minimize known vulnerabilities to an acceptable level of risk associated with friendly actions to adversary exploitation.

d. IAW AR 530-1, organizations will maintain Level II OPSEC Officers at Battalion and higher to manage their command OPSEC programs. Level Ill OPSEC instructors are required to train and certify these Level II OPSEC Officers. Units may request support through the Installation OPSEC Program Manager or the FCoE OPSEC Officer. Brigade Commanders may request at least two Level II OPSEC Officers be certified to be Level Ill through the Installation OPSEC Program Manager to maintain the Level II requirement prescribed in AR 530-1.

e. Improper handling and destroying of Controlled Unclassified Information (CUI) is a significant trend and pose an OPSEC vulnerability across the command. CUI is included as one of the Critical Information that must be protected by OPSEC measures.

f. HQDA released EXORD 018-17 (ref I) on 28 October 2016. The EXORD directed effective immediately, IAW Army policy, AR 360-1 and AR 530-1 (Reference A), personnel using Personal Electronic Devices (PEDs) at training/briefing sessions where PEDs are restricted, are prohibited from publishing and/or sharing official Army information covered in the training/briefing session, without expressed permission from the chain of command, in order to mitigate army vulnerabilities and reduce operations security violations. Soldiers and Department of the Army Civilians who violate these prohibitions may be subject to appropriate disciplinary, administrative, or other corrective actions.

(1) PEDs are devices that communicate, send, receive, store, reproduce, and display voice and/or text communication or data. These include, but are not limited to, cellphones, smartwatches, laptops/tablets, cameras, and other devises that are transmitting a signal. This includes government issued devices. Exercise devices such as Fitbits, may not be in wireless mode where PEDs are restricted.

(2) Introducing PEDs into any training/briefing session will be managed at unit level. Commanders will provide secure storage for personnel to secure PEDs if they are inadvertently brought to a training/briefing session where PEDs are restricted.

3. Sensitive Information

a. **Sensitive information**. Sensitive information is information requiring protection from disclosure that could cause a compromise or constitute a threat to national security, an Army organization, activity, family member, Department of the Army (DA) Civilian, civilian supporting military personnel, or DoD contractor. Examples of sensitive information include, but are not limited to, the following types of information:

(1) Serious Incident Reporting will be IAW AR 190-45 (paragraph 8-1) and USAFCoEFS Regulation 1-8.

(2) For Official Use Only (FOUO) information, information protected by the Freedom of Information Act (FOIA) and AR 25-55.

(3) Information protected by the Privacy Act of 1974 (5 USC 552a), to include the Health Insurance Portability and Accountability Act (HIPAA). The Privacy Act includes protection of Personally Identifiable Information and is protected under HIPAA.

(4) Unclassified information that requires special handling (for example, Sensitive But Unclassified, Limited Distribution, Encrypt For Transmission Only, and scientific and technical information protected under the Technology Transfer Laws and Arms Export Control Act. This includes information with a distribution restriction statement IAW DA Pam 25-40, Chapter 17.

(5) Controlled Unclassified Information (CUI). CUI is unclassified information to which access or distribution limitations have been applied according to national laws, policies, and regulations of the U.S. Government. It includes U.S. information that is determined to be exempt from public disclosure according, but not limited to, DODD 5230.25, DODD 5400.7, AR 25-55, AR 340-21, AR 530-1, and so on, or that is subject to export controls according to the International Traffic in Arms Regulations or the Export Administration Regulations. Because CUI does not qualify for formal classification, it should be afforded OPSEC measures for additional protection because of its vulnerability as unclassified information.

(6) Law Enforcement or Drug Enforcement Administration Sensitive Information.

b. **Critical Information**. Critical information is defined as information important to the successful achievement of U.S. objectives and missions or which may be of use to an adversary of the U.S. Critical information consists of specific facts about friendly Capabilities, Activities, Limitations (includes vulnerabilities), and Intentions (CALI) needed by adversaries for them to plan and act effectively so as to degrade friendly mission accomplishment. It is vital to a mission that if an adversary obtains it, correctly analyzes it, and acts upon it; the compromise of this information could prevent or seriously degrade mission success. Critical information can either be

classified or unclassified depending upon the organization, activity, or mission. Critical information that is unclassified requires OPSEC measures because it is not protected by the requirements provided to classified information. Critical information can also be an action that provides an indicator of value to an adversary and places a friendly activity or operation at risk. The USAFCoEFS Critical Information List (CIL) is contained in Annex A. Each organization will develop a CIL for specific operations they are planning or executing.

c. Official Army information includes information listed on Critical Information Lists (CIL) created IAW AR 530-1, OPSEC. Official Army information also includes pictures and other information presented in training/briefing sessions that includes critical and other sensitive Army information.

4. The Intelligence Collection Threat.

a. Known threat. The intelligence threat consists of multiple and overlapping collection efforts targeted against all sources of Army information, capabilities, and activities. The major threat collection disciplines to USAFCoEFS elements fall into these areas:

(1) Human intelligence (HUMINT) threat. The HUMINT threat has become increasingly important to all of our adversaries human sources can gain access to information not accessible to other collection assets. HUMINT employs overt, covert, and clandestine operations to achieve worldwide collection objectives. Overt collection operations gather intelligence information from open sources. Threat HUMINT collectors include official diplomatic and trade representatives, visitors, exchange students, journalists, and military personnel legitimately in the U.S. Greed, financial gain, alcoholism, drug abuse, sexual perversion, marital infidelity, and financial indebtedness are among the human failures exploited by threat HUMINT collectors. Disenchanted idealists are also a fertile source of information. Another recruitment technique involves misrepresentation of status or the "false flag" approach. A threat agent will attempt to pass himself off as an agent of a U.S. agency or of a friendly government to solicit cooperation.

(2) Open source intelligence (OSINT) threat involves the collection and analysis of freely available information, such as that presented in the media, or available in libraries or the internet. Open source information includes photographs, newspapers, magazine advertisements, government and trade publications, contract specifications, congressional hearings, computers and other public media. Up to 80 percent of the adversary's intelligence needs can be satisfied through access to open sources without risk and at minimum cost. In recent years, the Internet has become an ever-greater source of open source information for adversaries of the U.S. Websites sites in particular, especially personal Websites sites of individual Soldiers (to include Web logs or "blogs" and social networking sites or SNSs), are a potentially significant vulnerability. Sharing what seems to be even trivial information online can be dangerous to loved ones and the fellow Soldiers and Civilians in the unit.

America's enemies scour blogs, forums, chat rooms, and personal Websites sites to piece together information that can be used to harm the U.S. and its Soldiers. It's important to know that social media is a quickly evolving means of distributing information and that means OPSEC is more important than ever before. Other sources for open source information include public presentations, news releases from units or installations, organizational newsletters (both for official organizations and unofficial organizations, such as alumni or spouse support groups), and direct observation.

(3) Signals intelligence (SIGINT) threat. The SIGINT threat incorporates communications intelligence (COMINT), electronics intelligence, and foreign instrumentation signals intelligence. Communications intelligence has the greatest impact on the day-to-day performance of Army missions. It derives information from the study of intercepted electromagnetic communications. Prime sources of valuable COMINT include clear voice or non-encrypted telephone and radio communications. Adversaries, especially nation states with intelligence services, use various intercept platforms and have a worldwide COMINT capability. Other adversaries without these sophisticated capabilities will use commercially available technology to obtain COMINT which can be effective when properly utilized.

(4) Technical intelligence (TECHINT). Technical intelligence is derived from the collection and analysis of threat and foreign military equipment and associated material for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages. Adversaries seek TECHINT on U.S. equipment and material in order to learn their vulnerabilities and counter U.S. technological advantages. As an example, adversaries want to know the vulnerabilities of U.S. vehicles and armor protection in order to conduct effective improvised explosive device attacks against U.S. forces.

(5) OPSEC measures. There are a variety of good habits that everyone should practice and make part of their routine. Vulnerabilities exist when friendly actions and information can be observed and processed to allow an adversary to react in a way harmful to our mission. Critical information can be compromised and used against our forces today. Our adversaries' collection capabilities depend largely on failure to follow established procedures or carelessness on the part of our personnel. Throwing sensitive but unclassified information in the trash provides adversaries an opportunity to gain information about our activities. Posting sensitive information onto public Websites allows our adversaries to obtain valuable information. Proper OPSEC measures will decrease detection of critical information about our CALI. See Annex B for the specific USAFCoEFS OPSEC specific measures.

5. Taskings/Responsibilities.

a. All USAFCoEFS assigned personnel. Operations security is everyone's responsibility. Failure to properly implement OPSEC measures can result in serious

injury or death to our personnel, damage to weapons systems, equipment, and facilities, loss of sensitive technologies and mission failure. OPSEC is a continuous process and an inherent part of military culture, and as such, must be fully integrated into the execution of all operations and supporting activities. To avoid conflict with contract requirements, contractor personnel will always coordinate accomplishment of OPSEC taskings and responsibilities with their respective COR and Contracting Officer. All DA personnel (active component, reserve component to include DA Civilians), and contractor personnel will -

(1) Know what their organization considers to be critical information, where it is located (Annex A), and how-to protect it (Annex B). Protect from disclosure any critical information and sensitive information to which they have personal access. Personnel who fail to comply with these orders, directives, or policies to protect critical and sensitive information may be punished under violations of a lawful order under Uniform Code of Military Justice (UCMJ), Article 92, or under other disciplinary, administrative, or other actions as applicable. Personnel not subject to the UCMJ who fail to protect critical and sensitive information from unauthorized disclosure may be subject to administrative, disciplinary, contractual, or criminal action.

(2) Know who their OPSEC Officer is and contact that person for questions, concerns, reviews, or recommendations for OPSEC related topics.

(3) Encourage others, including Family Members and Family Readiness Groups (FRG) to protect critical and sensitive information.

b. Commanders, Commandants, Directors, down to battalion levels.

(1) Are responsible for ensuring that their units' activities or plans integrate and implement OPSEC measures to protect their command's critical information in every phase of all operations, exercises, tests, or activities.

(2) Are responsible for issuing orders, directives, and policies to protect their commands' critical and sensitive information in order to clearly define the specific OPSEC measures that their personnel should practice.

(3) Ensure PED guidance is followed at all briefings and PED classification signs are posted and visible for all attendees.

(4) Will coordinate and synchronize their OPSEC program or OPSEC measures with USAFCoEFS security programs (Antiterrorism/Physical Security/Information Security/Emergency Management).

(5) Will ensure all official information released to the public, to include official, news releases, unit public Web pages, external official presences (social networking sites, Facebook, etc.), professional publications, or any other information that is released to the public, receive an OPSEC review prior to dissemination.

(a) Ensure all Webmasters, public affairs specialists, or anyone who reviews, approves, or posts information for public release via command Websites complete mandatory OPSEC training (paragraph 7.f.).

(b) Ensure that all external official presences (EOP) sites (social networking sites, Facebook, etc.) receive approval, and be registered on the external presences list, maintained on the Army Social Media Directory. These sites will be reviewed at least quarterly to ensure compliance IAW Annex F.

(c) OPSEC reviews will be conducted prior to releasing information to the public IAW Annex F. This includes print, FOIA requests, media, and Web to include social media.

(6) Incorporate OPSEC reviews into all contracts using the Antiterrorism /Operations Security (AT/OPSEC) in Contracting Cover Sheet for Integrating AT and OPSEC into the Contract Support Process IAW TRADOC Implementing Guidance for Integrating AT and OPSEC (reference E) and Annex G.

(7) Appoint an OPSEC Program Manager (PM)/Officer/Coordinator, in writing, with responsibility for supervising the execution of proper OPSEC within their organization.

(8) Establish a Brigade Level OPSEC Working Group to review its OPSEC processes, procedures, and programs to assist the command in developing OPSEC policy and attend the quarterly Installation Working Group (WG).

(a) The OPSEC PM and Installation OPSEC Program Manager will establish an Installation OPSEC WG. The OPSEC WG will be conducted in conjunction with the installation force protection WG (Antiterrorism, Emergency Management, OPSEC, and Physical Security). Attendance is mandatory for OPSEC Officer(s) assigned at the Brigade (BDE) level. All other OPSEC Officers are invited to attend as their mission allows. The TRADOC OPSEC PM will host a quarterly TRADOC OPSEC WG. The OPSEC PM will participate in this WG and will disseminate the minutes to all assigned FCoE OPSEC Officers.

(b) The BDE/Directorate OPSEC Officer will establish OPSEC WGs. The OPSEC WG will discuss OPSEC issues as they pertain to their specific BDE/Directorate. Attendees will include leadership representative and subordinate unit OPSEC Officers or their designated representative.

(c) All OPSEC WGs will meet at least quarterly to review its OPSEC processes, procedures, and programs and to assist the command in developing OPSEC policy. Topic examples are CIL updates, annual OPSEC report, OPSEC plan, dumpster dives, trash/recycling bins, OPSEC awareness, and OPSEC award program.

Memorandum will be maintained to indicate date of WG, attendees/non attendees,

and issues discussed. This memorandum will be reviewed during the Organizational Inspection Program (OIP).

(9) Conduct OPSEC assessments IAW Annex C.

(a) The OPSEC assessment is an evaluation process, conducted annually of an organization, operation, activity, exercise, or support function to determine if sufficient OPSEC measures are in place to protect critical information. An OPSEC program assessment may include self-assessments, program reviews as part of the inspector general inspection, or higher headquarters assessments specifically addressing OPSEC. The OPSEC assessment determines the overall OPSEC posture and degree of compliance by the assessed organization with applicable OPSEC plans and programs. The OPSEC assessment team should be composed of the OPSEC PM/Officer and appropriate subject matter experts from throughout the organization.

(b) Units will use the Appendix 1 (Unit OPSEC Assessment Checklist) to Annex C of this plan to conduct assessments (or checklists, if differing OPSEC requirements apply to different subordinate organizations) as part of the OIP/command inspection program (CIP).

(c) This doesn't preclude OPSEC assessments from being conducted other than as part of the annual CIP. Organizations are encouraged to request OPSEC assessments from Installation to assist in strengthening their OPSEC posture.

c. Director, Capability Development and Integration Directorate (CDID). In addition to the requirements previously discussed in this plan:

(1) Integrate OPSEC into doctrine and Army education and training as appropriate. This includes, but is not limited to, courses, training support packages, Soldier training publications, and combined arms training strategies.

(2) Incorporate OPSEC measures into Army capability development activities, to include concepts for doctrine, organizations, and materiel IAW Annex D.

(3) Ensure that Army Capability Managers (ACMs) provide acquisition managers with operational considerations so that OPSEC is addressed throughout the lifecycle of any acquisition program IAW Annex E.

d. General Staff (G-1, G-2, G3/5/7, G4, G-6, and G8). In addition to the requirements previously discussed in this plan:

(1) Appoint an OPSEC coordinator in writing to serve as a member of the OPSEC WG meetings. Ensure maximum participation in all OPSEC WG meetings.

(2) Coordinators will be responsible to coordinate and track the OPSEC training for all personnel assigned to their staff section (military, Civilian, and contractors).

This includes ensuring all personnel complete Level I Initial OPSEC training within first 30 days of assignment and Annual OPSEC training each year.

(3) Coordinators will, as appropriate, conduct OPSEC reviews of documents and apply suitable OPSEC measures to contracts in order to protect classified or sensitive information (Chapters 4 and 6 of AR 530-1 and Annex F of this plan).

(4) Coordinators will track all active contracts within organization and ensure contractors are complying with AT and OPSEC requirements.

e. G-33. In addition to the requirements previously discussed in this plan:

(1) G-33, Current Operations. Serves as primary office of responsibility for the development, organization, and administration of the command OPSEC program. Assigned to the G-33, the FCoE OPSEC Officer/Program Manager is responsible for implementation of the command OPSEC program and performs duties and responsibilities IAW AR 530-1 and appropriate references.

(2) Prepare and disseminate annual FCoE OPSEC Report to TRADOC, due in October.

(3) Annual update/review of FCoE CIL and OPSEC Plan in conjunction with the Installation OPSEC Program Manager (PM).

(4) Prepare and coordinate OPSEC Level II courses based on needs of organizations to ensure personnel meet the requirements of AR 530-1 and Appendix 1 of Annex C of this plan.

(5) Conduct OIP inspections and staff assistance visits (SAVs).

(6) Foreign Disclosure section serve as the Fort Sill proponent for disclosure approval to foreign nationals and students.

f. DPTMS. In addition to the requirements previously discussed in this plan:

(1) Serves as primary office of responsibility for the development, organization, and administration of the Installation OPSEC program. Installation OPSEC PM is responsible for the implementation of the Installation OPSEC program and perform duties and responsibilities IAW AR 530-1.

(2) Installation OPSEC PM conducts OPSEC briefings for incoming personnel to the Installation during the Start Right Program.

(3) Protection division update the Installation OPSEC PM and OPSEC Working Group, as appropriate with the current threat assessment and/or specific threat activity.

(4) Conduct or coordinate appropriate OPSEC reviews of command Website IAW Annex F.

g. Chief Public Affairs Officer (PAO)/Webmaster. In addition to the requirements previously discussed in this plan:

(1) Public Affairs Website content and command information product reviews are the responsibility of the PAO. Other organizations are responsible for ensuring that the content on their publicly accessible Web pages contain only releasable information.

(2) Provide policy and propriety reviews of information for public release. Advise staff to conduct OPSEC and security reviews before providing information for public release.

(3) Consider the security of classified/sensitive/close-hold information when preparing command information, public information, and community relations activities.

(4) Review Public Affairs-managed Website content and command information products so they contain only publicly releasable information. PAO will assist organizations with content review before posting, as requested.

(5) Coordinate print/broadcast materials that may have OPSEC implications before public release/announcement.

(6) Conduct an OPSEC review before release of information concerning the command and command programs/projects IAW Annex F.

(7) Appoint an OPSEC coordinator to serve as a member of the OPSEC WG. Ensure maximum participation in all OPSEC WG meetings.

6. Concept of Implementation.

a. Office of Primary Responsibility (OPR). The command, unit, or activity operations officer is the staff OPR for OPSEC. However, the success or failure of OPSEC is ultimately the responsibility of the Commander, and the most important emphasis for implementing OPSEC comes from the chain of command.

(1) Operations security is an operations function that protects critical information and requires close integration with other security programs.

(2) A unit or organization's commander, operations officer, and the OPSEC Officer must consider OPSEC in all unit activities to maintain operational effectiveness.

(a) Unit actions are a primary source of indicators collected by adversaries. The commander, advised by the OPSEC Officer, controls these actions, assigns tasks, and allocates resources to implement OPSEC measures.

(b) By constantly observing activities, the OPSEC Officer can evaluate these measures for their effectiveness and their impact on operational success.

(3) In an organization without a specified operations staff, the element with primary responsibility for planning, coordinating, and executing the organization's mission activities will be the OPR for its OPSEC program.

(4) While the OPSEC Officer is responsible for the development, organization, and administration of an OPSEC program, the commander's emphasis and support from the chain of command are essential to ensure the proper implementation of an OPSEC program.

(a) To apply OPSEC to plans, operations, programs, projects, or activities, units will utilize the 5-Step OPSEC Process IAW AR 530-1 to identify, analyze, and protect their critical and sensitive information.

(b) Exercises, Tests, and Systems Development. Brief OPSEC requirements to planners, participants, and support personnel. OPSEC measures are command-directed actions executed by individuals who must be aware of their responsibilities. Emphasize the adverse results of a failure to maintain effective OPSEC, particularly for long-term undertakings such as research development test & evaluation programs.

(5) Organizations and activities will ensure that OPSEC measures are incorporated into Army Capability Development activities to include concepts for doctrine, organizations, and materiel. See Annex D.

(6) Army Capability Managers (ACMs) will provide acquisition managers with operational considerations so that OPSEC is addressed throughout the lifecycle of any acquisition program. See Annex E.

7. OPSEC Training.

a. General. For OPSEC to be effective, all Army personnel (Soldiers; DA Civilians, and government contractor personnel) must be aware of OPSEC and understand how OPSEC complements traditional security programs. All personnel must know how to apply and practice OPSEC in the performance of their daily tasks. OPSEC must become a mindset of all Army and Government contractor personnel, and be performed as second nature. To accomplish this level of OPSEC vigilance, OPSEC training programs must be action and job-oriented, enabling the workforce to put into

practice the knowledge and tactics, techniques, and procedures they learned in training. Training should maximize the use of lessons learned to illustrate OPSEC objectives and requirements. In order to ensure accomplishment of training, commanders will include OPSEC training as part of their organizations' annual training guidance. Fort Sill SharePoint contains references and training at:

Operations Security - Home (army.mil)

b. Training Programs. Commanders and leaders, their OPSEC Officers, program managers, and assigned personnel receive OPSEC training as outlined below:

Operations Security Level I Training. The target audience for Level I is all Army personnel (the total workforce consisting of Soldiers, DA Civilians, and DoD contractors). To avoid conflict with contract requirements, contractor personnel will always coordinate accomplishment of OPSEC taskings and responsibilities with their respective CORs and Contracting Officers. Level I training is composed of initial, annual, and continual awareness training:

(1) Initial operations security awareness training. All newly assigned personnel within the first 30 days of arrival in the organization (this includes accessions and initial entry programs) must receive initial training. Newcomers will receive OPSEC Training during the Start Right Program at Fort Sill. OPSEC Officers at the unit level will conduct Pre-deployment and Re-deployment training IAW AR 530-1.

(2) At a minimum, all Army personnel must receive annual OPSEC awareness training. This training must be updated with current information and tailored for the unit's specific mission and critical information. Face-to-face or in-person training by a Level II-trained OPSEC officer is the preferred method of instruction. Army OPSEC Level I (Newcomers and Refresher) Web Based Training is available online at https://www.lms.army.mil/. Search "Army OPSEC Level I" in the search box to complete course and meet this requirement. Command emphasis and monitoring of training status in DTMS will help ensure maximum participation.

(3) Level I training is provided/tracked by the organization's OPSEC officer/coordinator. The intent and focus of initial training will be on the following areas:

(a) Understanding the unit's CIL in Annex A.

(b) How adversaries seek information on our capabilities, intentions, and plans.

(c) Specific guidance on how to protect critical information through the OPSEC measures in Annex B.

(d) End state. Each individual should have the requisite knowledge to safeguard critical information and know the answers to the following questions:

(1) What is my unit or organization's critical information?

(2) What critical information am I personally responsible for protecting?

(3) How is the threat trying to acquire my critical information?

(4) What steps am I/are we taking to protect my/our critical information?

(5) Who is my OPSEC officer/coordinator?

c. Continuous Operations Security Awareness Training. Operations security awareness training must be continually provided to the workforce, reemphasizing the importance of continuous and sound OPSEC practices.

(1) This training consists of, but is not limited to, periodic OPSEC news releases in local command publications, OPSEC posters in unit areas, OPSEC information bulletins on unit bulletin boards, and OPSEC awareness briefings by unit commanders at commander's calls. OPSEC awareness products can be obtained through the Interagency OPSEC Support Staff (IOSS) at https://www.iad.gov/ioss/index.cfm.

(2) Operations security training will also be provided to deploying and redeploying units, to include FRGs.

(3) Family members of non-deploying units also require an appropriate level of OPSEC training and awareness. Provide Family Members appropriate OPSEC training and awareness products on a regular basis. This can be done through FRG meetings or by providing flyers and training material for Soldiers to take home.

d. Operations Security Level II Training. All appointed OPSEC Officers or OPSEC PMs will attend the DA OPSEC Officer/PM or IOSS equivalent certification course.

e. Units will maximize use of the DA OPSEC Course taught by local Level III OPSEC Instructors. Coordinators are highly encouraged to attend. Units will maximize use of the HQDA OPSEC Course taught by local Level III OPSEC Instructors (if available), or request a MTT thru OPSEC Officer. TRADOC G-33 will coordinate MTTs directly with the proponent.

f. Operations Security Level III Instructor Training. The OPSEC Support Element (OSE), The 1st Information Operations (10) Command, is the proponent. OPSEC Program Managers at installations where TRADOC has the Senior Commander can request training to the TRADOC OPSEC officer. As resources allow, TRADOC will coordinate with the OSE for training and certification. Candidates must be actively assigned in a command OPSEC officer role, and be available to the command to train their Level II OPSEC officers.

g. Web Release OPSEC Training. All Soldiers, DA Civilians, and contractors who post, review, or maintain information or documents for official purposes on a public domain (External Official Presence site) must receive mandatory OPSEC training

annually.

h. Additional Training. Army OSE offers additional courses that can increase the knowledge, skills, and abilities of OPSEC personnel. Army OSE milSuite site at: https://www.milsuite.mil/book/groups/army-opsec-support-element-ose/activity

ANNEXES:

Annex A - USAFCoEFS Critical Information List
Annex B - USAFCoEFS OPSEC Measures
Annex C - USAFCoEFS OPSEC Assessments
Appendix - 1 (Unit Checklist)
Appendix - 2 (Staff Coordinator's Checklist)
Annex D - Army Capability Developments Activities
Enclosure 1 to Annex D
Annex E - USAFCoEFS Capability Managers
Annex F - USAFCoEFS OPSEC Information Posting Review Process
Enclosure 1 - OPSEC decision flow chart
Annex G - (Integrating AT and OPSEC into the Contracting Support Process)
Appendix 1 - AT/OPSEC Coversheet
Annex H - Terms
Annex I - Risk Assessment Worksheet
Annex J - Threat Assessment Worksheet
Annex K - Personal Electronic Device (PED) Vulnerability Mitigation
Enclosure 1 to Annex K - PED Level Placards