

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, USAFCEFS
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 (USAFCEFS)
Operations Security (OPSEC)

History. This circular supersedes the USAFCEFS 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.

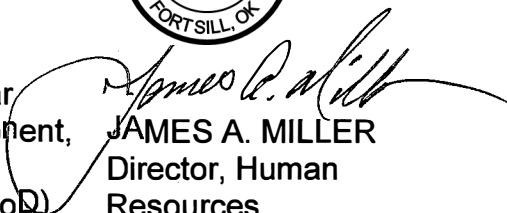
Suggested Improvements.

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 USAFCEFS.


MICHAEL J. KIMBALL
Colonel, GS
Chief of Staff,




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 III 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 III 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 devices 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 USAFCEFS 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/ioass/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



DEPARTMENT OF THE ARMY
UNITED STATES ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, UNITED STATES ARMY GARRISON FORT SILL
462 HAMILTON ROAD, SUITE 120
FORT SILL, OKLAHOMA 73503

AMIM-ISO-O

4 November 2021

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Fort Sill Operations Security (OPSEC) Critical Information List (CIL)

1. References:

- a. Army Regulation (AR) 530-1 (Operations Security), 26 September 2014
- b. AR 380-5 (Army Information Security Program), 22 October 2019
- c. Fort Sill Supplement 1 to AR 380-5 (Department of the Army Information Security Program), 1 November 2013

2. General:

a. Critical information consists of specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively to guarantee failure or unacceptable consequences for friendly missions accomplishment.

b. The OPSEC Officer, in conjunction with other staff officer's input, develops the organization's overall CIL which is then approved by the commander. It is the commander's intent that all organization personnel (Soldiers, Civilians, and DoD contractors), be aware of the organization's critical information and apply OPSEC to their daily tasks.

3. Critical Information List:

- a. Vulnerabilities and security measures of Fort Sill to include information systems.
- b. Sensitive non-public major Fort Sill events, times, locations, attendees, and security plans.
- c. Itineraries of General officers, Senior Executive Service officials, very important persons, and distinguished visitors outside of the greater Fort Sill area.
- d. Fort Sill critical assets, mission essential vulnerable areas, and the security measures and plans to protect them (preventing unauthorized photos, geo-tags, etc).

AMIM-ISO-O

SUBJECT: Fort Sill Operations Security (OPSEC) Critical Information List (CIL)


e. Protection and response capabilities of Fort Sill assets, activities, or Service providers on or off the installation.

f. Plans for initiation of contingency operations, deployment of units, or mobilization of units affecting Fort Sill facilities, or assets on or off the installation.

g. Fort Sill information sources that provide insights on doctrine, organization, training, materiel, leadership, education, personnel, facilities developments, lessons learned, or emerging Tactics, Techniques, and Procedures related to any ongoing operation.

h. Controlled Unclassified Information, which includes; For Official Use Only, Personal Identifiable Information, DoD Unclassified Controlled Nuclear Information, Law Enforcement Sensitive, Sensitive But Unclassified, Foreign Government Restricted, and Limited Distribution.

4. The point of contact for this memorandum is Mr. Terry A. Noel, Fort Sill OPSEC Program Manager at (580) 442-2532 or via email at terry.a.noel.civ@army.mil.


RHETT A. TAYLOR
COL, FA
Commanding

DISTRIBUTION:

Fort Sill Intranet

HQ Garrison

DES

DHR

DPTMS

DPW

DFMWR

PAIO

RMO

Safety Office

IMO

MICC

LRC

Welcome Center

Annex B (OPSEC Measures) to USAFCoEFS OPSEC Plan 2021

1. The United States Army Fires Center of Excellence (USAFCoEFS) Commanding General and United States Army Garrison Commander has approved the following OPSEC measures identified below for implementation to USAFCoEFS ongoing activities and planning for future operations. These OPSEC measures will be monitored by the FCoE and Installation OPSEC Officer and coordinators for compliance. In order to protect critical or sensitive information, as listed in base plan para 3 and Annex B, all personnel will abide by the following OPSEC measures:

a. General.

(1) Encrypt and digitally sign critical or sensitive information as indicated on the CIL when disseminated via e-mail within Army information systems. Digitally sign all e-mails that contain an active (embedded) hyperlink and/or attachment. When encryption is not a viable option, use a secure file transfer site such as AMRDEC SAFE, <https://safe.amrdec.army.mil/safe/>.

(2) When disposing of critical or sensitive information, destroy IAW proper procedures and regulations. DO NOT DISCARD IN TRASH OR RECYCLE BINS. Do not allow paper recycle bins in secure or sensitive areas.

(3) Protect sensitive and controlled unclassified information by at least one physical or electronic barrier (e.g., locked container or room, logical authentication or logon procedure) when not under direct individual control of an authorized user.

(4) Ensure that government conversations, web postings, bios, social media comments, or releases to the media and/or public receive appropriate OPSEC reviews prior to being disclosed.

(5) Do not wear security badge(s) outside secure areas. Avoid allowing pictures taken of security badge(s) and/or other sensitive information.

b. Training, conference and meeting security measures.

(1) Conduct training, meetings, briefings, and conferences in locations authorized and appropriate to the level and classification of information discussed at the location.

(2) The person in charge will:

(a) Notify the attendees of the classification or sensitivity of the meeting and any PED restrictions and/or information release requirements.

(b) Ensure each person attending the meeting has the appropriate access and the need to know.

(c) Ensure that notes taken and slides provided during the meeting are properly marked, handled, and destroyed afterwards as necessary appropriate to the level and classification of the meeting.

Annex B (OPSEC Measures) to USAFCoEFS OPSEC Plan 2021

(d) Inspect the area at the conclusion to ensure no sensitive information has been left behind.

(e) Avoid allowing sensitive information and security badges to be photographed.

c. Employee travel measures.

(1) Travel in civilian clothes whenever possible. Do not carry luggage, including briefcases, which identifies you as a member of the command.

(2) Use a passport or other ID instead of military orders whenever possible.

(3) Do not discuss assignments, duties, or reason for travel unless absolutely necessary (e.g., with security, customs, or immigration personnel).

(4) Do not use public or personal computers for Government business. If you use a public computer for personal business, understand your passwords and personal data are at risk of compromise. When using public computers, be sure to log off all accounts and clear history and cookies on exit.

d. Social networking measures.

(1) Take a close look at all privacy settings.

(2) Do not post sensitive information (to include CUI). Ask "What could the wrong person do with this information?" and "Could it compromise the safety of me, my family, or my unit?"

(3) Geo-tagging may reveal your location. Carefully check your privacy settings. Consider turning off the GPS function, as appropriate.

(4) Closely review all Army-related photos before they go online. Make sure they do not give away sensitive information (to include CUI) which could be dangerous if released. (For example, photos of your unit on a mission, sensitive equipment or areas, documents, briefing slides, security badges, etc., and what might be exposed in the background.)

(5) Talk to your family about operations security and what can and cannot be posted or discussed. Avoid disclosure of unnecessary potentially sensitive information outside the workplace.

(6) Avoid mentioning rank, unit locations, deployment dates, names, or equipment specifications and capabilities.

(7) If you do not want it made public, do not post it.

Annex B (OPSEC Measures) to USAFCoEFS OPSEC Plan 2021

(8) Ensure all official information released or posted to the public domain receives appropriate reviews IAW DoD and Army policies.

e. Visitor control and personnel security.

(1) Establish a visitor control system to coordinate and control all visits.

(2) Provide escorts for visitors and vendors who need access to restricted areas.

(3) Ensure escorts know proper escort procedures, limitations of disclosure, and other applicable controls involved in the visit. Challenge violators and report them to the security manager or OIC.

f. Communications security measures.

(1) Do not discuss or transmit sensitive information over wireless unsecure devices such as unofficial cell phones, computer data networks, or Bluetooth. Ensure your conversations are not overheard by those who may be nearby, who do not have a need to know.

(2) When discussing sensitive or critical information, make maximum use of secure communications. When an encryption feature is available on unclassified networks, encrypt e-mail messages containing sensitive information. When unavailable, use a secure file transfer site such as AMRDEC SAFE, <https://safe.amrdec.army.mil/safe/>.

(3) Limit reading file distribution to personnel with need to know. Control distribution of unclassified sensitive information in accordance with distribution markings for technical and operational information (FOUO, CUI, Restricted, PII, etc).

(4) Enforce strict compliance with command information systems policies on the use of all computer systems.

(5) Limit mission-related email to only official DoD accounts.

(6) Log off computer or remove CAC when away from work area.

(7) Prohibit unauthorized hardware or software on Army systems.

(8) Limit use of personally owned devices, to include mobile devices, to only those documents that are approved for public release. Do not download CUI or other distribution-restricted documents and files to your personally owned devices. This includes emailing the documents and files to a commercially owned email account.

(9) Do not process sensitive information on publicly available computers (e.g., those available for use by the general public in kiosks or hotel business centers).

Annex B (OPSEC Measures) to USAFCoEFS OPSEC Plan 2021

(10) When using portable devices, encrypt wireless connections with virtual private network (VPN).

(11) Transmit fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.

g. Smart phones, fitness devices, and other PEDs may monitor your location and microphone.

(1) Carefully review privacy settings, and limit apps that have access to, and may be revealing your location and/or microphone.

(2) Do not allow these devices in secure areas, and consider restricting their use in deployed areas as appropriate.

(3) Consider turning off Bluetooth when not in use.

h. Need to know and the insider threat.

(1) All personnel will limit sharing of critical and sensitive information (to include CUI) to only those personnel who have an official "need to know".

(2) Recognize the common signs of the insider threat, to include OPSEC violations, and report them to your supervisors or security personnel.

(3) POC is the Fort Sill OPSEC Program Manager, at (580) 442-2532.

Annex C (OPSEC Assessments) to USAFCoEFS OPSEC Plan 2021

The OPSEC assessment is an analysis of an operation, exercise, test, or activity to determine the overall OPSEC posture and to evaluate the degree of compliance of subordinate organizations with the published OPSEC program, OPSEC plan, or other form of OPSEC guidance.

At each level, the organization's OPSEC Officer conducts OPSEC assessments of subordinate units using the published OPSEC guidance to determine if the unit being assessed is implementing higher headquarters-directed and their own OPSEC policies and procedures. The OPSEC officer submits a written assessment with results and recommendations to the assessed unit commander or commander who directed the assessment.

OPSEC Officers will ensure that assessments are conducted for their units as part of their commands' Organizational Inspection Programs (OIPs) or similar assessment programs. This does not preclude assessments being conducted other than as part of the. CIP. A formal OPSEC checklist will be developed and tailored to the organization's needs.

Fires Center of Excellence OPSEC Checklist for units down to battalion is contained in Appendix 1 to this Annex.

Fires Center of Excellence OPSEC Checklist for staff organizations is contained in Appendix 2 to this Annex.

The CDID's and TCM's checklists are contained in Annexes D and E respectively.

Methodology. Identify non-compliance and determine root causes. Assess vulnerabilities from likely threats and hazards and recommend mitigating actions. Coach, teach, and mentor during assessments with the intent on bringing unit into compliance. **Assessment Terminology:**

Observation. Standards not met. An observation must be supported by a regulatory requirement. Follow-up is required until standards are met.

Annex C (OPSEC Assessments) to USAFCoEFS OPSEC Plan 2021

Neutral Comment. Standards met. Improvements could be made to enhance the Protection Program.

Sustain. Exceeded standards. This action enhances the command's Protection Program and should be sustained.

Best Practice. An element of the Protection Program exceeded standards and should be shared with other organizations to improve their security programs.

POC for this Annex is the FCoE OPSEC Officer, (580) 442-0852, or the Installation OPSEC Program Manager at (580) 442-2532

Encls

Appendix 1 - Unit OPSEC Assessments Appendix 2 - Staff Coordinator Checklist

Annex D (Army Capability Developments Activities) to USAFCoEFS OPSEC Plan 2021

1. TRADOC organizations and activities are directed by AR 530-1 Operations Security, to ensure that OPSEC measures are incorporated into Army Capability Development activities to include concepts for doctrine, organizations, and materiel.
2. Currently many TRADOC organizations are developing new doctrine, organizations, and materiel. Many of these organizations contain Soldiers, Civilians, and contractors. Regardless of the type of personnel involved in the development, all are responsible for OPSEC.
3. The Fires Center of Excellence Combat Development (CDID) is incorporated into this OPSEC plan or will have a separate OPSEC plan or annex. Each CDID will appoint an OPSEC officer in writing and provide Level II training.
4. If contractors are involved in the capability development activity, the government is responsible for identifying the critical program information, providing the threat assessment, making the final risk assessment decisions, ensuring OPSEC guidelines are included in the contract, and evaluating contractors' performance in meeting the OPSEC requirements.
5. AR 25-2, "Information Assurance" (IA), is an important reference in developing an OPSEC program and its goal is to protect unclassified, sensitive, and classified information stored, processed, accessed, or transmitted by information systems. These systems exhibit inherent security vulnerabilities. The steps to be taken to protect information must be included in the earliest phases of the system acquisition, contracting, or development lifecycle. Failure to implement IA security measures may compromise the new program to foreign and competitor collection activities. Violation of established measures may result in disciplinary measures as spelled out in the regulation for military, civilian, and contractor personnel.
6. The Fires Center of Excellence OPSEC officer will maintain a list of capability development activities under the commander's authority and assist in achieving compliance as necessary and ensure each has a copy of this annex.
7. For an example checklist to assist in compliance see enclosure 1 to Annex D.

OPERATIONS SECURITY (OPSEC)

Administrative Information

- The Army protects critical information from unauthorized release to adversaries
- Army personnel may discuss critical information with unified action partners with a need to know
- Authorized Commanders, their representatives, and public affairs officials may release critical information to the public when:
 - The Commander determines there is a requirement to release the information, and
 - Public affairs guidance authorizes release

HQDA COVID-19 Critical Information List

- Pre-decisional Army deliberations on potential policies, plans, and activities related to the Army's response to COVID-19
- Number of Army personnel (Soldiers, Army Civilians, Contractors, Family members, Retirees) with COVID-19 or in isolation, quarantine, or possibly infected
- Army vulnerabilities and gaps created by COVID-19
- Potential (pre-decisional) COVID-19 impacts to Army training, operations, exercise, and modernization efforts
- Pre-decisional Army capabilities potentially available to support DSCA efforts to counter COVID-19, including but not limited to:
 - Units, task organization, capacity/beds to provide inpatient and outpatient care
 - Isolation, diagnosis, and treatment capacity
 - Critical shortages of sensitive medical items
 - Shortages of medical personnel by AOC/MOS/ASI
 - Facilities for quarantine of personnel (military/civilian) returning from overseas

HQDA COVID-19 OPSEC Mandatory Measures

- Move all work on the Army COVID-19 Campaign Plan to SIPR due to the sensitive nature of the content
- Restrict pre-decisional COVID-19 deliberations to personnel with a need to know; non-disclosure agreements required for HQDA-level planning
- Never release internal planning documents to the public or media
- Only OSD/ASLs will release numbers of confirmed COVID-19 cases that are aggregated at DoD/Service levels - do not release numbers of people in isolation, quarantine or possibly infected
- Ensure all messages intended for public audiences receives both public affairs and OPSEC review prior to release
- Use Army-approved collaboration methods, applications, and portals; minimize sending documents by email
- Encrypt NIPR COVID-19 email communications; use only government email networks (e.g. outlook/OWA)
- Commands will submit reports on COVID-19 positive personnel on NIPR; HQDA will report aggregated confirmed case data on SIPR
- When teleworking, do not participate in COVID-19 planning within hearing of family members; do not print COVID-19 planning products at home
- Monitor organizational and Soldier and family readiness group external official presence social media accounts for OPSEC



HQDA EOC, Army COVID Campaign Plan
Strategic Narrative OPT,
usarmy.pentagon.hqda-cs-g-3-5-7.list.damo-
so-covid-19-strategic-c@mail.mil

OPERATIONS SECURITY (OPSEC)

UNCLASSIFIED//FOUO

This guidance applies specifically to
HQDA - all ACOMs, ASOCs, and DRUs
are strongly encouraged to tailor this
guidance for their commands

Annex E (OPSEC Guidance for TRADOC-Capability Managers TCMs) to USAFCoEFS OPSEC Plan 2021

1. TCMs are directed by AR 530-1, Operations Security, to provide acquisition managers with operational considerations so that OPSEC is addressed throughout the lifecycle of any acquisition program. This requirement has been directed because of the TCM's unique relationship with both the operational and acquisition components of the Army.
2. AR 530-1 states that acquisition activities are particularly vulnerable in the OPSEC area and recent studies showed 75 percent of U.S. acquisition programs had countermeasures initiated against them within 3 years of full-scale development.
3. The "Acquisition Lifecycle" consists of five phases. They are Concept Refinement, Technology Development, System Development, Demonstration, Production and Deployment, and Operations and Support. There are three milestones associated with the lifecycle. They are Milestone A at the end of phase 1, Milestone B at the end of phase 2, and Milestone C at the end of phase 3.
4. Each acquisition program or activity is required to have considerations addressed in the CDID OPSEC guidance that should be developed as early as possible in the acquisition lifecycle. Both the government and contractor have shared responsibilities for development of the OPSEC plan. This may be an Annex to the CDID's plan. It will cover, at a minimum, the TCM's critical information, and the measures to protect that information.
5. AR 25-2 "Information Assurance" (IA) is an important reference in developing an OPSEC program and its goal is to protect unclassified, sensitive, and classified information stored, processed, accessed, or transmitted by information systems. These systems exhibit inherent security vulnerabilities. The steps to be taken to protect information must be included in the earliest phases of the system acquisition, contracting, or development lifecycle. Failure to implement IA security measures may compromise the new program to foreign and competitor collection activities. Violation of established measures may result in disciplinary measures as spelled out in the regulation for military, civilian, and contractor personnel.
6. TCM's provide operational considerations to the acquisition manager for each program under their responsibility and use the accompanying checklist to document this support. Considerations from the operational context will greatly improve the OPSEC posture and compliance.

Annex F (OPSEC Information Posting Process) to USAFCEFS OPSEC Plan 2021

1. General. Only information of value to the general public and which does not require additional protection may be posted to publicly accessible Websites or other public media. Information requiring additional protection such as FOUO information, information -not specifically cleared and approved for public release, or information of questionable value to the general public and for which worldwide dissemination poses an unacceptable risk to DOD, including to military personnel and civilian employees, is not releasable to the public.

2. Review, approval, and release personnel must be trained IAW paragraph 4 and knowledgeable with the rules governing FOUO information as well as pertinent security classification guides (SCGs). Must also be familiar with the aspects of the organization's operations CIL, the organization's vulnerabilities and the pertinent threat so he/she can properly assess the nature of the risk inherent in posting information. Review personnel may need to consult with subject matter experts on areas that they are not familiar with.

3. Clearance review of content. Review of content for sensitivity and distribution controls, including sensitivity of information in the aggregate; includes review for CIL, FOUO information, PII, unclassified information pertaining to classified programs, copyrighted material, and material creating conflicts of interest. Use the OPSEC Decision Flow Chart in Figure 1 below as a guide. This is a formal process and must be documented per local policy.

4. FOUO. FOUO information is exempted from release by the FOIA. FOUO information, if disclosed, would cause harm to an interest protected by one or more of the FOIA exemptions and it may not be posted to a publicly accessible Website.

5. Unclassified information pertaining to classified programs. The clearance-review procedures for unclassified information pertaining to classified programs proposed for posting to publicly accessible Websites must take into account the likelihood of classification by compilation. Consulting the program SCG may be required to determine the likelihood that the information - if compiled or aggregated with other information likely to be contained on publicly accessible Websites - will reveal an additional association or relationship that meets the standards for classification.

6. Operations Security for official EOP Sites:

a. Commanders will designate members of their organizations responsible for posting content to the official online presence and make sure those individuals are current on all required EOP OPSEC training. (See Base Order para 7.f.)

b. Make sure all content is submitted to and approved by the commander or the organization's release authority.

c. Make sure all content is posted in accordance with organization Public Affairs guidance and Army regulations.

Annex F (OPSEC Information Posting Process) to USAFCoEFS OPSEC Plan 2021

d. Monitor your social media presence and make sure external social media users are not posting sensitive information on your official presence sites.

Annex G (Integrating Antiterrorism and Operations Security into the Contract Support Process) to USAFCoEFS OPSEC Plan 2021

1. References:

- a. AR 525-13, Antiterrorism, 3 Dec 2019
- b. AR 530-1, Operations Security (OPSEC), 26 Sep 2014
- c. TR 5-14, Acquisition Management and Oversight, 14 Feb 2018
- d. Desk Reference, 25 Jan 12, subject: Integrating Antiterrorism and Operations Security into the Contracting Support Process

2. General. References a., b., and d. require AT and OPSEC integration into the contracting process. AT and OPSEC considerations must be taken into consideration during the development of the requirement and must be given full consideration during the execution of both pre-award and post-award tasks. Each contract has unique AT and OPSEC considerations. There is not one model that fits all contracts. This document supplements the acquisition management and oversight processes described in reference c. and describes TRADOC implementing guidance for integrating AT and OPSEC into the pre-Acquisition Management and Oversight (AMO) and post-award acquisition processes-.

3. FCoE Implementing Guidance.

- a. The Requiring Activity (RA) will:
 - (1) Include the requiring activity's appointed or servicing OPSEC Officer in the development of contract requirements.
 - (2) Encourage RA's appointed or servicing OPSEC Officers' participation in the Functional Review Board (FRB) process (reference c.).
 - (3) Include a "Contract Requirements Package AT/OPSEC Review Cover Sheet" in addition to the required documentation for all service contract requirements as prescribed in Chapter 5 of reference c.

Annex G (Integrating Antiterrorism and Operations Security Into The Contract Support Process) to USAFCoEFS OPSEC Plan 2021

a. Administrative Contract Review Board (ACRB) chairs will ensure that OPSEC Officers from an echelon above the RA serve as a member of the ACRB (reference c.).

b. Directorate of Resource Management offices or the respective office charged with orchestrating the Executive Contract Approval Board (ECAB) will ensure OPSEC Officers from an echelon above the RA serve as members of the ECAB (reference c.).

c. The RA's appointed OPSEC Officers will ensure that OPSEC actions are integrated into relevant contract support requests by performing both pre-award and post-award tasks IAW reference c).

d. OPSEC Officers supporting the ACRB and/or ECAB will ensure that contract OPSEC language and clauses are sufficient and ensure that a properly executed "Contract Requirements Package AT/OPSEC Review Cover Sheet" is included.

4. OPSEC Considerations.

As a minimum, the following OPSEC measures will be considered for all contracts. All AT, OPSEC and other security-related language and clauses should be consolidated into one section (e.g., *Security Requirements*) of the contract. This is not an all exclusive list of measures and not all measures may be applicable.

a. The User Activity (UA) Level II OPSEC Officer or next higher will ensure contracts are properly developed and executed IAW ALARACT 015/2012 requirements.

b. Level II OPSEC Officers will become involved in the contracting process early on from the initial planning through to the contract execution and monitoring (refer to pages 7-9 of desk reference).

c. Level II OPSEC Officers will use the five-step OPSEC process to identify critical information, vulnerabilities, risks, and mitigations required.

d. Level II OPSEC Officers will ensure OPSEC mitigations are included in the contract. Using the Cover Sheet, Level II OPSEC officers will work with their Antiterrorism and Security Officers to identify OPSEC training requirements and OPSEC SOP/Plan requirements (coversheet, section 11, item numbers 6 and 7).

e. Note that all contracts will not require their own OPSEC SOP/Plan, and will usually fall within the unit's OPSEC Program. For contracts that require their own

Annex G (Integrating Antiterrorism and Operations Security Into The Contract Support Process) to USAFCoEFS OPSEC Plan 2021

OPSEC Standing Operating Procedure/Plan, the contractor shall develop an OPSEC Standing Operating Procedure (SOP)/Plan within 90 calendar days of contract award, to be reviewed and approved by the responsible government OPSEC Officer, per AR 530-1, Operations Security.

f. This SOP/Plan will specify the government's critical information, why it needs to be protected, where it is located, who is responsible for it, and how to protect it. In addition, the contractor shall identify an individual who will be an OPSEC Coordinator.

g. The contractor will ensure that this individual becomes OPSEC Level II-certified per AR 530-1. When using the Standard Contract Provisional Clause Text Applicability and/or PWS Language #6, ensure that the contractors are either required to comply with the unit's OPSEC plan, or produce their own OPSEC SOP/Plan IAWAR 530-1, Chapter 6.

h. When using the Standard Contract Provisional Clause Text Applicability and/or PWS Language #7, ensure that contractors receive OPSEC Level I training at least within the first 30 days, annually, and pre-deployment.

i. Before a contract is released to the public, Level II OPSEC Officers will ensure that the PWS or SOW does not contain critical information from their unit's EEFI/CIL, or provide details that may be aggregated with other public information to show friendly sensitive or classified capabilities, activities, limitations, intentions, and/or vulnerabilities.

5. OPSEC Training.

a. For contracts that have contractor employees, including subcontractor employees, assigned for 30 days or more; those employees must complete Level I OPSEC training within 30 calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever applies, and annual OPSEC awareness training if they remain over 365 days.

b. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee to the COR (or to the contracting officer if a COR is not assigned) within 35 calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever applies.

Annex H (Terms) to USAFCoE&FS OPSEC Plan 2021

ACOM	Army Command. An Army force, designated by the Secretary of the Army, performing multiple Army Service Title 10 functions (3013b) across multiple disciplines. Command responsibilities are those established by the Secretary.
Adversary	Those individuals, groups, or organizations that must be denied critical information to maintain friendly mission effectiveness. Adversaries may include hostile countries, terrorists and allied intelligence agencies.
AIS	Automated Information System
AR	Army Regulation
ASCC	Army Service Component Command. An Army force, designated by the Secretary of the Army, comprised primarily of operational organizations serving as the Army component of a combatant command or a sub-unified command. If directed by the combatant commander, an ASCC serves as a Joint Forces Land Component Command (JFLCC), or Joint Task Force (JTF).
CALI	Capabilities, Activities, Limitations, and Intentions.
CIL	Critical Information List
Collection Threat	Collection of information on U.S. Army activities may be conducted by adversaries using various intelligence collection methods. These pieces of information provide an accurate portrayal of the commands overall intentions and/or operations.
C2	Command and Control
C2W	Command and Control Warfare
COMSEC	Communications Security. This material is controlled and managed under a separate set of security standards and procedures from those that apply to other classified information. The loss of U.S. COMSEC information and materials can seriously damage the national interest.
Critical Information	Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act to guarantee the failure of friendly mission accomplishment.

DA	Department of the Army
DCSINT	Deputy Chief of Staff, Intelligence. Security and Intelligence Section located at USARC and at other headquarters.
DOD	Department of Defense.
DRU	Direct Reporting Unit. An Army organization comprised of one or more units with institutional or operational support functions, designated by the Secretary of the Army, normally to provide broad general support to the Army in a single, unique discipline not otherwise available elsewhere in the Army.
EEFI	Essential Elements of Friendly Information (EEFI). Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities and activities, so they can obtain answers critical to their operational effectiveness.
EOC	Emergency Operations Center
Essential Secrecy	The condition achieved from the denial of critical information to adversaries.
FOIA	Freedom of Information Act. Allows people to gain access to non-classified information from government agencies.
FOUO	For Official Use Only. Information that often has Social Security Numbers or other information that could harm the soldier if released.
FPCON	Force Protection Condition. A system that provides procedures for terrorism analysts to assess the terrorist threat and for commanders to determine appropriate security measures based on the assessed threat of terrorist attack.
Imagery Intelligence Threat (IMINT)	Collection of information by photographic, infrared, or radar imagery. Images can be gathered either by individuals or by remote means, such as aircraft or satellite. This method is valuable because it provides analysts with clues to other areas requiring examination. The IMINT includes unauthorized duplication of documents.
Indicators	Friendly detectable actions and open source information that can be interpreted or pieced together by an adversary to derive critical information.
IO	Information Operations

Measurement and Signature Intelligence (MASINT)	Scientific and technical intelligence obtained by quantitative and qualitative analysis of data derived from technical sensors to identify any distinctive features associated with the source, emitter, or sender. It is technical in nature.
Military Deception	Actions executed to mislead foreign decision-makers, causing them to derive and accept desired appreciation of military capabilities, intentions, operations, or other activities that evoke foreign actions that contribute to the originator's objectives. Deception is an effective OPSEC measure that can be employed given prior coordination (e.g., cause adversary intelligence collection efforts to fail to target friendly activities, create confusion or misinterpretation of information obtainable from open sources).
Observables	Actions that convey indicators exploitable by adversaries but that must be carried out regardless, to plan, prepare for and execute activities.
Operations security compromise	The disclosure of sensitive or critical information which has been identified by the Command and all higher headquarters as jeopardizing the unit's ability to execute its mission or to adequately protect its personnel and/or equipment.
OPSEC	Operations Security. A program meant to deny our adversaries access to any critical information.
OPSEC Measure	Methods and means to gain and maintain essential secrecy about critical information.
Operations security planning guidance	Guidance that serves as the blueprint for OPSEC planning by functional elements throughout the organization. It defines the critical information that requires protection from adversary, appreciations, taking into account friendly and adversary goals, estimated key adversary questions, probable adversary knowledge, desirable and harmful adversary appreciations and pertinent intelligence system threats. It also should outline tentative OPSEC measures to ensure essential secrecy.
Operations security vulnerability	A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision-making.
PAO	Public Affairs Office
SAEDA	Subversion and Espionage Directed against the U.S. Army.

SBU	Sensitive but Unclassified. Unclassified information that is readily available and which could be used against the Army or its personnel.
Sensitive Information	Any information, the loss, misuse, or unauthorized access to, or modification of which could adversely affect the national interest or the conduct of Federal programs, but which has not been specifically authorized under an Executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy (PL 100-235, 8 Jan 88).
Signals Intelligence (SIGINT)	Collection of information by interception of electronic signals from communications equipment or non-communicative devices that emit an electronic signal, such as a radar beacon. It includes interception of communication and the interception and analysis of communication between pieces of equipment (e.g., LAN).
TDA	Table of Distribution and Allowances. A document authorizing equipment and personnel for a garrison unit.
TDY	Temporary Duty
THREATCON	Threat Condition. Used for commanders to determine appropriate security measures based on the assessed threat of terrorist attack and provides procedures for terrorism analysts to assess the terrorist threat.
USARC	United States Army Reserve Command
Vulnerabilities	Friendly actions which provide indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making. Vulnerabilities exist when three conditions exist; adversary has capability to collect indicator, and adversary has time to process (report, analyze, take planning action), and the adversary must be able to react.

Annex I (Risk Assessment Worksheet) to USAFCoEFS OPSEC Plan 2021

Risk Assessment Worksheet

Vulnerability/ Indicator	Threat H/M/L	Vulnerability H/M/L	Impact H/M/L	Risk H/M/L	Y/N	(T) OPSEC Measure	Residual Risk

Risk= Impact x (Threat x Vulnerability)

LOW	Threat: No adversary has demonstrated an intent, or no adversary is assessed to have the capability to advance <u>Against friendly objectives</u> .
	Vulnerability: Potential for exploitation is negligible.
	Impact: No personal injury, property loss less than \$1,000, delays less than 15 minutes, no effect on the integrity of the system, no effect on government or harm to the reputation of, or the Nation public services, no embarrassment or harm to the reputation of, or the Nation.
	Risk: It is improbable an adversary would exploit an existing vulnerability and the resulting impact would be insignificant

MEDIUM	Threat: An adversary has demonstrated both intent and capability to act against similar friendly objectives
	Vulnerability: Potentially exploitable by multiple collection disciplines requiring significant Corroboration of data.
	Impact: Injuries requiring hospital treatment or observation, property loss greater than \$5,000 but less than \$10,000, delays greater than 30 but less than 60 minutes, moderate embarrassment or harm to the reputation of or the Nation
	Risk: It is possible an adversary could exploit an existing vulnerability and the resulting impact would be manageable

HIGH	Threat: An adversary has demonstrated both intent and capability to act against friendly objectives
	Vulnerability: Potentially exploitable by multiple collection disciplines requiring virtually no corroboration of data.
	Impact: Death, property loss greater than \$1,000,000, delays lasting longer than 25 hours, catastrophic embarrassment or harm to the reputation or the Nation
	Risk: There is no doubt an adversary could exploit an existing vulnerability and the resulting impact would be irreparable

Annex J (Threat Assessment Worksheet) to USAFCoE&FS OPSEC Plan 2021

Threat Assessment Worksheet

[illegible]

UNCLASSIFIED

**Annex K (Personal Electronic Device (PED) Vulnerability Mitigation) to
USAFCoEFS OPSEC Plan 2021**

1. References:

- a. AR 530-1, Operations Security (OPSEC), 26 SEP 14
- b. HQDA EXORD 018-17 Restricting Personal Electronic Devices (PEDs) at training/briefing sessions in order to mitigate vulnerabilities and reduce OPSEC violations, 28 OCT 16
- c. HQDA EXORD 042-17 PEDs level designation standardization at training/briefing sessions in order to mitigate vulnerabilities in cyberspace, 21 DEC 16

2. Situation.

a. Information transmitted or posted via cyberspace is a growing concern, as it is available for all to see, including our adversaries. PEDs pose unique potential vulnerabilities to our critical and sensitive information when they are used to record and release information presented in Army training, briefings, meetings, operations, and other official events.

b. PEDs include privately owned and government issued devices. They 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 devices that are transmitting a signal. Exercise devices such as Fitbits are also considered PEDs and may not be in wireless mode or be able to communicate/pair with host device, where PEDs are restricted.

c. Critical and sensitive information includes information listed in the command's Critical Information List (CIL), Controlled Unclassified Information (CUI), For Official Use Only (FOUO), Personal Identifiable Information (PII), and other information IAW this order, AR 530-1 (OPSEC), and Army guidance.

d. This annex establishes TRADOC guidance on the use of PEDs during Army events, meetings, training, and briefings; as well as procedures for releasing or posting that information.

3. Mission. Units will determine level of PED restrictions and control their use at Army training, briefings, meetings, operations and other official events; in order to mitigate vulnerabilities and reduce OPSEC compromises.

UNCLASSIFIED

UNCLASSIFIED

**Annex K (Personal Electronic Device (PED) Vulnerability Mitigation) to
USAFCoEFS OPSEC Plan 2021**

4. Execution.

a. Introducing PEDs into any event will be managed at the lowest appropriate level. This may be subject to local command guidance. Prior to, or at the beginning of the event, the person in charge of the event will issue an appropriate announcement, posting, or other guidance clearly identifying the specific PED level for the event. This can be accomplished by annotating the PED level on a training schedule, posting at a room or building entrance, as an introduction slide, or verbal instruction. Sample placards are in enclosure.

b. The following PED levels are designated:

(1) PED 0: No PEDs allowed. *(This is used when the use of PEDs present a security concern, or are otherwise, not appropriate. Refer to local security policies and procedures.)*

(2) PED 1: Specified PEDs are allowed. *(This is used when a PED may be brought in; however, its use may be limited and/or powered down as applicable. Use this for events where the PED may be a distraction, and/or critical or sensitive information is vulnerable to compromise.)* Event organizers or OIC needs to provide specific instructions for attendees that have PEDs present.

(3) PED 2: All PEDs allowed. *(No restriction as to presence or use. This is the primary default for most non-sensitive events.)*

c. When PEDs are inadvertently brought to an event where PEDs are restricted and local storage is not available, the person in charge of the event will direct personnel to leave and secure their device.

d. Personnel using PEDs at Army training, briefings, meetings, operations, and other official events, where PEDs are restricted, are prohibited from publishing and/or sharing the information covered without express permission from the chain of command. Soldiers and Department of the Army Civilians who violate these prohibitions may be subject to appropriate disciplinary, administrative, or other corrective actions as applicable.

UNCLASSIFIED

UNCLASSIFIED

**Annex K (Personal Electronic Device (PED) Vulnerability Mitigation) to
USAFCoEFS OPSEC Plan 2021**

e. The lowest level of command with authority to grant express permission to publish official Army information is the company commander, provided appropriate level of reviews are conducted IAW Army and unit policy.

5. Sustainment. No TRADOC resources are provided.

6. Command and Control. POC for this Annex is FCoE OPSEC Officer, (580) 442-0948, or the Installation OPSEC Program Manager at (580) 442-2532.

Enclosures: PED Level placards.

UNCLASSIFIED

TRADOC Protection
Higher Headquarters Assessment (HHA)
Operations Security (OPSEC) Benchmarks

Appendix 1 to Annex C (Unit Checklist) to USAFCoEFS OPSEC Plan 2021									
Unit OPSEC Officer:									
Assessor:									
Date:									
BENCHMARK #	BENCHMARK CATEGORY	BENCHMARKS	SUSTAIN, NEUTRAL, or OBSERVATION	REFERENCES					
OPSEC 1	OPSEC Officers	OPSEC Officer appointed at each level of command down to battalion-level or equivalent sized organization. 1. Designated in writing by the Commander (or equivalent), or their official designee. 2. Appropriate rank/grade level. 3. OPSEC Level II Trained		AR 530-1, (paras 2-18, 3-2, and 4-2)					
OPSEC 2	OPSEC Document	Unit has published an OPSEC Plan, Order, SOP, Policy, or other procedural format, that protects the unit's sensitive and/or critical information. 1. In writing, signed by the Commander (or equivalent), or their official designee. 2. Clearly defines unit's critical information and the measures to protect them. 3. Based upon the 5 Step OPSEC Process. 4. Reviewed at least Annually.		AR 530-1, (paras 2-18, 2-19, and 3-2)					
OPSEC 3	Critical Information	Unit's critical information is identified and widely distributed. 1. A Critical Information List (CIL) is approved by the Commander (or equivalent), or their official designee. 2. Known by all personnel assigned to unit. 3. Reviewed at least Annually. Unit's critical information is protected.		AR 530-1, (paras 2-18, 2-19, 3-2, B-2, and Appendix C)					
OPSEC 4	OPSEC Measures	1. OPSEC measures are approved by the Commander (or equivalent). 2. Known by all personnel assigned to unit. 3. Measure are coordinated and synched with supported organizations and other security programs. 4. Measure are executable, adhered to, and effectively protect the unit's critical information. 5. Unauthorized Disclosures 6. Random Security Measures are implemented to deter improper handling of CUI and other critical and sensitive information based on the published CIL.		AR 530-1, (paras 2-18, 2-19, 3-2, and B-6, and Appendix F)					
OPSEC 5	OPSEC Oversight and Assessments	OPSEC officer provides OPSEC guidance and oversight to subordinate units and staff. OPSEC Assessments are conducted of organization, exercises, and current/future operations, to determine if sufficient OPSEC posture and compliance. 1. OPSEC Officer observes unit activities and provides OPSEC oversight to organizations. 2. The command and subordinate units are assessed at least annually or as part of Command Inspection Program (CIP) to determine OPSEC posture and compliance. (Documented) 3. Unit uses a published OPSEC checklist. 4. Corrective actions are taken and/or best practices are shared.		AR 530-1 (paras 3-2, 5-3, 5-4, and Appendix H)					
OPSEC 6	OPSEC Level I Training	All personnel receive OPSEC Level I training. 1. All personnel know their OPSEC officer, the threat, the unit's CIL, and the OPSEC measures to protect their critical information. 2. All newly assigned personnel receive initial training within first 30 days of arrival. 3. Deploying and redeploying personnel receive OPSEC training specific to area of operations. All information released to the public or posted to public websites receive OPSEC reviews to ensure critical information is not disclosed.		AR 530-1, (para 4-2)					
OPSEC 7	OPSEC Reviews	1. OPSEC documents states which products automatically go to the OPSEC officer or appropriate reviewer for review. 2. All personnel that review, approve, or post unit releases are EOP trained. 3. OPSEC reviewers use published CIL to review releases. 4. Web site reviews conducted at least quarterly. 5. When critical information is found inadvertently released, corrective actions are taken.		AR 530-1, (paras 2-18, and 2-19, and Chapter 5), Army ALARACT 289/213					
OPSEC 8	Coordination and integration with other Security Programs	OPSEC is coordinated and integrated with the command's other security programs such as PS, IA, and AT. 1. OPSEC Document staffed with command's security programs. 2. OPSEC Officer participates in, an OPSEC and/or Protection working group. 3. OPSEC Officer receives current threat warnings and integrates threat analysis into the OPSEC process.		AR 530-1, (paras 2-18, 2-19, 3-2, B-3, and Appendix G)					
OPSEC 9	OPSEC in Contracts	Command's contracts have appropriate OPSEC reviews to ensure critical information is protected. 1. OPSEC Officers utilizes AT/OPSEC Cover Sheet. 2. OPSEC Officer ensures that unit's OPSEC compliance is addressed in the PWS. 3. OPSEC Officer ensures that OPSEC training is addressed in PWS. 4. OPSEC Officer ensures PWS does not release critical information from the CIL.		AR 530-1, (para 2-18, and Chapter 6)					
OPSEC 10	Annual OPSEC Reports	Command receives subordinate reports, prepares, and submits the Command's Annual OPSEC Report for the fiscal year (FY) to their HHQs. (Documented) 1. Subordinate units down to BN are submitting. 2. Reports are compiled, analyzed, and submitted to HHQs by suspense dates.		AR 530-1, (Appendix I)					

**CONTRACT REQUIREMENTS PACKAGE ANTITERRORISM/OPERATIONS SECURITY REVIEW COVER
SHEET**

Requirements Package Title _____

Date _____

Section I.

Purpose of cover sheet: To document the review of the requirements package, statement of work (SOW), quality assurance surveillance plan and any applicable source selection evaluation criteria for antiterrorism (AT) and other related protection matters to include, but not limited to: AT, operations security (OPSEC), information assurance (IA)/cyber security, physical security, law enforcement, intelligence, foreign disclosure.

Army policy requirement: A signed AT/OPSEC cover sheet is required to be included in all requirements packages except for supply contracts under the simplified acquisition level threshold, field ordering officer actions and Government purchase card purchases. Command policy may require this form for supply contracts under the simplified acquisition level threshold.

Mandatory review and signatures: The requiring activity antiterrorism officer (ATO) must review each requirements package prior to submission to the support contracting activity to include coordination with other staff elements for review as appropriate per section II below. If the requiring activity does not have an ATO, the first ATO in the chain of command will review the contract for considerations. An OPSEC and InfoSec Officer review is also mandatory.

Section II. Standard Contract Language Provision/Contract Clause Text Applicability and/or Additional SOW Language. If standard contract or clause language found on page 2 (Section IV) of this form is sufficient to meet specific contract request requirements, check "yes" in block below and include this language in the SOW. If standard contract text (provisions or clauses) or clause language does not apply, check "no." If the standard SOW language applies, but is not in of itself sufficient, check "yes" and "SOW" and include both the standard language and additional contract specific language in the SOW. If standard contract text or clause language is not desired, but there is related contract specific language in the SOW, check "no" and "SOW." If yes is marked for items 1, 3, 4, 7, 8, 12 or 13, training is required. Mandatory training must be measured as a deliverable and evaluated in the QASP.

	ATO Reviewer	OPSEC Reviewer	IAT Reviewer	SOW / PWS
1. AT level 1 training (general)	Yes	N/A	N/A	N/A
2. Access and general protection policy and procedures	Yes	N/A		N/A
2a. For contractor requiring Common Access Card (CAC)	N/A	N/A		N/A
2b. For contractor not eligible for CAC, but requires access to DoD facility or installation.	Yes	N/A		N/A
3. AT awareness training for US based contractor personnel traveling overseas.	N/A	N/A		N/A
4. iWATCH training	Yes	N/A		N/A
5. Army Training Certification Tracking System (ATCTS) registration for contractor employees who require access to government information systems.	N/A	N/A		N/A
6. For contracts that require a formal OPSEC program.	N/A	Yes		N/A
7. Requirement for OPSEC training	Yes	Yes		N/A
8. Information assurance/information technology training	N/A	N/A		N/A
9. Information assurance/information technology certification	N/A	N/A		N/A
10. Contractor Authorized to Accompany the Force clause	N/A	N/A		N/A
11. Contract requiring performance or delivery in a foreign country	N/A	N/A		N/A
12. Handling/Access to Classified Information	N/A	N/A		N/A
13. Threat Awareness Reporting Program	Yes	N/A		N/A
14. Delivery of Food and Water	N/A	N/A		N/A

Section III. ATO Remarks:

Section III OPSEC Remarks: Contractor is required to take OPSEC Level I Training

Section III IAT Remarks:

Antiterrorism Review Signature: I am an ATO (Level II Certified or trained AT coordinator) and have reviewed the requirements package and understand my responsibilities in accordance with Army Regulation 525-13, *Antiterrorism*.

Reviewer _____ (Typed or printed name, rank/civ grade)	COCHRAN, BILLY, JAMES, 111	Date: _____
Signature: _____		Phone Number: _____

Operations Security Review Signature: I am OPSEC level II certified and have reviewed the requirements package, and it is in compliance with Army Regulation 530-1, *Operations Security*.

Reviewer _____ (Typed or printed name, rank/civ grade)	Signature: _____	Date: _____
		Phone Number: _____

Information Assurance Review Signature: I am either IAM-II or IAT-II (can be higher) certified and have reviewed the requirements package and it is in compliance with DOD 8570.01-M and DOD 8580.1 (elevate to IAM-III/IAT-III if necessary).

Reviewer _____ (Typed or printed name, rank/civ grade)	Signature: _____	Date: _____
		Phone Number: _____

Section IV. Standard Contract Language/Contract Clause Applicability and/or Additional SOW Language.

- 1. AT Level I training.** This standard language is for contractor employees with an area of performance within an Army controlled installation, facility or area. All contractor employees, to include subcontractor employees, requiring access Army installations, facilities and controlled access areas shall complete AT Level I awareness training within 30 calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable and annually thereafter. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee, to the COR or to the contracting officer, if a COR is not assigned, within 05 calendar days after completion of training by all employees and subcontractor personnel. AT level I awareness training is available at the following website: <http://jko.jten.mil>
- 2. Access and general protection/security policy and procedures.** This standard language is for contractor employees with an area of performance within Army controlled installation, facility, or area. Contractor and all associated sub-contractors employees shall provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. Contractor workforce must comply with all personal identity verification requirements (FAR clause 52.204-9 or NAF Clause BI.142, Personal Identity Verification of Contractor Personnel) as directed by DOD, HQDA and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.
- 2a. For contractors requiring Common Access Card (CAC).** Before CAC issuance, the contractor employee requires, at a minimum, a favorably adjudicated National Agency Check with Inquiries (NACI) or an equivalent or higher investigation in accordance with Army Directive 2014-05. The contractor employee will be issued a CAC only if duties involve one of the following: (1) Both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely; (2) Remote access, via logon, to a DoD network using DoD-approved remote access procedures; or (3) Physical access to multiple DoD facilities or multiple non-DoD federally controlled facilities on behalf of the DoD on a recurring basis for a period of 6 months or more. At the discretion of the sponsoring activity, an initial CAC may be issued based on a favorable review of the FBI fingerprint check and a successfully scheduled NACI at the Office of Personnel Management.
- 2b. For contractors that do not require CAC, but require access to a DoD facility or installation.** Contractor and all associated sub-contractors employees shall comply with adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (TSDB) (Army Directive 2014-05/AR 190-13), applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative), or, at OCONUS locations, in accordance with status of forces agreements and other theater regulations.
- 3. AT Awareness Training for Contractor Personnel Traveling Overseas.** This standard language required US based contractor employees and associated sub-contractor employees to make available and to receive government provided area of responsibility (AOR) specific AT awareness training as directed by AR 525-13. Specific AOR training content is directed by the combatant commander with the unit ATO being the local point of contact.
- 4. iWATCH Training.** *This standard language is for contractor employees with an area of performance within an Army controlled installation, facility or area.* The contractor and all associated sub-contractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity ATO). This locally developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR. This training shall be completed within 30 calendar days of contract award and within 05 calendar days of new employees commencing performance with the results reported to the COR NLT 30 calendar days after contract award.
- 5. Army Training Certification Tracking System (ATCTS) registration for contractor employees who require access to government information systems.** All contractor employees with access to a government information systems must be registered in the ATCTS (Army Training Certification Tracking System) at commencement of services, and must successfully complete the DOD Information Assurance Awareness prior to access to the IS and then annually thereafter.
- 6. For contracts that require a formal OPSEC program.** The contractor shall develop an OPSEC Standing Operating Procedure (SOP)/Plan within 90 calendar days of contract award, to be reviewed and approved by the responsible Government OPSEC officer. This plan will include a process to identify critical information, where it is located, who is responsible for it, how to protect it and why it needs to be protected. The contractor shall implement OPSEC measures as ordered by the commander. In addition, the contractor shall have an identified certified Level II OPSEC coordinator per AR 530-1.
- 7. For contracts that require OPSEC Training.** Per AR 530-1 Operations Security, the contractor employees must complete Level I OPSEC Awareness training. New employees must be trained within 30 calendar days of their reporting for duty and annually thereafter. OPSEC Awareness for Military Members, DoD Employees and Contractors is available at the following website: <http://cdsetrain.dtic.mil/opsec/index.htm>
- 8. For Cyber Awareness (Information assurance (IA)/information technology (IT)) training.** All contractor employees and associated sub-contractor employees must complete the DoD Cyber awareness training before issuance of network access and annually thereafter. All contractor employees working IA/IT functions must comply with DoD and Army training requirements in DoD 8570.01, DoD 8570.01-M and AR 25-2 within six months of appointment to IA/IT functions. DoD Cyber Awareness Challenge Training is available at the following website: <https://ia.signal.army.mil/DoDIAA/>
- 9. For Cyber (Information assurance (IA)/information technology (IT)) certification.** Per DoD 8570.01-M, DFARS 252.239.7001 and AR 25-2, the contractor employees supporting Cyber (IA/IT) functions shall be appropriately certified upon contract award. The baseline certification as stipulated in DoD 8570.01-M must be completed upon contract award.
- 10. For contractors authorized to accompany the force.** DFARS Clause 252.225-7040 or NAF Clause BI.143, Contractor Personnel Authorized to Accompany U.S. Armed Forces Deployed Outside the United States. The clause shall be used in solicitations and contracts that authorize contractor personnel to accompany US Armed Forces deployed outside the US in contingency operations; humanitarian or peacekeeping operations; or other military operations or exercises, when designated by the combatant commander. The clause discusses the following AT/OPSEC related topics: required compliance with laws and regulations, pre-deployment requirements, required training (per combatant command guidance), and personnel data required.
- 11. For Contract Requiring Performance or Delivery in a Foreign Country, DFARS Clause 252.225-7043 or NAF Clause BI.144, Antiterrorism/Force Protection for Defense Contractors Outside the US.** The clause shall be used in solicitations and contracts that require performance or delivery in a foreign country. This clause applies to both contingency and non-contingency support. The key AT requirement is for non-local national contractor personnel to comply with theater clearance requirements and allows the combatant commander to exercise oversight to ensure the contractor's compliance with combatant commander and subordinate task force commander policies and directives.
- 12. For contracts that require handling or access to classified information.** Contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret" and requires contractors to comply with— (1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); (2) any revisions to DOD 5220.22-M, notice of which has been furnished to the contractor.
- 13. Threat Awareness Reporting Program.** For all contractors with security clearances. Per AR 381-12 Threat Awareness and Reporting Program (TARP), contractor employees must receive annual TARP training by a CI agent or other trainer as specified in 2-4b of AR 381-12.
- 14. For contracts that require delivery of food and water.** This standard language is for contractor employees with an area of performance delivering food and water within an Army-controlled installation, facility or area. The supplies delivered under this contract shall be transported in delivery conveyances maintained to prevent tampering with and / or adulteration or contamination of the supplies, and if applicable, equipped to maintain a prescribed temperature. All delivery vehicles will also be subject to inspection at all times and all places by the Contracting Officers Representative, Post Veterinarian, and / or Law enforcement Officials. When the sanitary conditions of the delivery conveyance have led, or may lead to product contamination, adulteration, constitute a health hazard, the delivery conveyance is not equipped to maintain prescribed temperatures or the transport results in product "unfit for intended purpose", supplies tendered for acceptance may be rejected without further inspection. As the holder of a contract with the Department of Defense, it is incumbent upon the awardee to insure that all products and/or packaging have not been tampered or contaminated. Delivery conveyances will be locked or sealed at all times, except when actively loading or unloading. Unsecured vehicles will not be left unattended. All incoming truck drivers will provide adequate identification upon request. In the event of an identified threat to an installation, or a heightened force protection/Homeland Security threat Level, the contractor may be required to adjust delivery routes to minimize vulnerability risks and enable direct delivery to DOD facilities.

Appendix 2 to Annex C (Staff Coordinator's Checklist) to USAFCoEFS OPSEC Plan

Staff Coordinator's Checklist

Appendix 3a to TRADOC OPSEC Annex, Unit OPSEC Assessment Checklist as of 04 Jun 20				
BENCHMARK #	BENCHMARK CATEGORY	BENCHMARKS	SUSTAIN, NEUTRAL, or OBSERVATION	REFERENCES
OPSEC 1	OPSEC Officers	OPSEC Officer appointed at each level of command down to battalion-level or equivalent sized organization. 1. Designated in writing by the Commander (or equivalent), or their official designee. 2. Appropriate rank/grade level. 3. OPSEC Level II Trained		AR 530-1, (paras 2-18, 3-2, and 4-2)
OPSEC 2	OPSEC Document	Unit has published an OPSEC Plan, Order, SOP, Policy, or other procedural format, that protects the unit's sensitive and/or critical information. 1. In writing, signed by the Commander (or equivalent), or their official designee. 2. Clearly defines unit's critical information and the measures to protect them. 3. Based upon the 5 Step OPSEC Process. 4. Reviewed at least Annually.		AR 530-1, (paras 2-18, 2-19, and 3-2)
OPSEC 3	Critical Information	Unit's critical information is identified and widely distributed. 1. A Critical Information List (CIL) is approved by the Commander (or equivalent), or their official designee. 2. Known by all personnel assigned to unit. 3. Reviewed at least Annually.		AR 530-1, (paras 2-18, 2-19, 3-2, B-2, and Appendix C)
OPSEC 4	OPSEC Measures	Unit's critical information is protected. 1. OPSEC measures are approved by the Commander (or equivalent). 2. Known by all personnel assigned to unit. 3. Measure are coordinated and synched with supported organizations and other security programs. 4. Measure are executable, adhered to, and effectively protect the unit's critical information.		AR 530-1, (paras 2-18, 2-19, 3-2, and B-6, and Appendix F)
OPSEC 5	OPSEC Oversight and Assessments	OPSEC officer provides OPSEC guidance and oversight to subordinate units and staff. OPSEC Assessments are conducted of organization, exercises, and current/future operations, to determine if sufficient OPSEC posture and compliance. 1. OPSEC Officer observes unit activities and provides OPSEC oversight to organizations. 2. The command and subordinate units are assessed at least annually or as part of Command Inspection Program (CIP) to determine OPSEC posture and compliance. (Documented) 3. Unit uses a published OPSEC checklist. 4. Corrective actions are taken and/or best practices are shared.		AR 530-1 (paras 3-2, 5-3, 5-4, and Appendix H)
OPSEC 6	OPSEC Level I Training	All personnel receive OPSEC Level I training. 1. All personnel know their OPSEC officer, the threat, the unit's CIL, and the OPSEC measures to protect their critical information. 2. All newly assigned personnel receive initial training w/in first 30 days of arrival. 3. Deploying and redeploying personnel receive OPSEC training specific to area of operations.		AR 530-1, (para 4-2), and TRADOC OPSEC Plan
OPSEC 7	OPSEC Reviews	All information released to the public or posted to public websites receive OPSEC reviews to ensure critical information is not disclosed. 1. OPSEC documents states which products automatically go to the OPSEC officer or appropriate reviewer for review. 2. All personnel that review, approve, or post unit releases are EOP trained. 3. OPSEC reviewers use published CIL to review releases. 4. Web site reviews conducted at least quarterly. 5. When critical information is found inadvertently released, corrective actions are taken.		AR 530-1, (paras 2-18, and 2-19, and Chapter 5), Army ALARACT 289/213, and TRADOC OPSEC Plan)
OPSEC 8	Coordination and integration with other Security Programs	OPSEC is coordinated and integrated with the command's other security programs such as PS, IA, and AT. 1. OPSEC Document staffed with command's security programs. 2. OPSEC Officer participates in, an OPSEC and/or Protection working group. 3. OPSEC Officer receives current threat warnings and integrates threat analysis into the OPSEC process.		AR 530-1, (paras 2-18, 2-19, 3-2, B-3, and Appendix G)
OPSEC 9	OPSEC in Contracts	Command's contracts have appropriate OPSEC reviews to ensure critical information is protected. 1. OPSEC Officers utilizes AT/OPSEC Cover Sheet. 2. OPSEC Officer ensures that unit's OPSEC compliance is addressed in the PWS. 3. OPSEC Officer ensures that OPSEC training is addressed in PWS. 4. OPSEC Officer ensures PWS does not release critical information from the CIL.		AR 530-1, (para 2-18, and Chapter 6), and TRADOC OPSEC Plan
OPSEC 10	Annual OPSEC Reports	Command receives subordinate reports, prepares, and submits the Command's Annual OPSEC Report for the fiscal year (FY) to their HHQs. (Documented) 1. Subordinate units down to BN are submitting. 2. Reports are compiled, analyzed, and submitted to HHQs by suspense dates.		AR 530-1, (Appendix I)

ENCL 1 to Annex D to USAFCoEFS OPSEC Plan 2021

ARMY CAPABILITY DEVELOPMENTS ACTIVITIES INSPECTION CHECKSHEET

Answer Yes, No or Not Applicable (NA) to each of the items. _____

Name of the Capability Development Activity: _____

Date of Contact: _____

ITEM	YES	NO	N/A
1.1. Is a list of all CDIDs under the organization available for review?			
1.2. Have the OPSEC officers been appointed and trained for each and are orders signed by the commander available for review?			
1.3. Are their OPSEC Plans that incorporate CDID OPSEC considerations?			
1.4. Are copies of the OPSEC Plans available for inspection?			
1.5. Have the OPSEC Plans been periodically reviewed to ensure they do not need to be adjusted?			
1.6. If contractors are involved in the combat development activity, has the government conducted an evaluation of the contractor's OPSEC requirements, and have recommendations for improvements been annotated?			
1.7. Have any OPSEC compromises for the combat activity occurred since the last inspection and were they reported to higher headquarters as required?			

NOTES:

PED
LEVEL

0

NO PEDS ALLOWED

PED
LEVEL

1

**SPECIFIED PEDS
ARE ALLOWED**

PED

LEVEL

2

ALL PEDS ALLOWED

ENCL 1 to Annex D to USAFCoEFS OPSEC Plan 2021

ARMY CAPABILITY DEVELOPMENTS ACTIVITIES INSPECTION CHECKSHEET

Answer Yes, No or Not Applicable (NA) to each of the items. _____

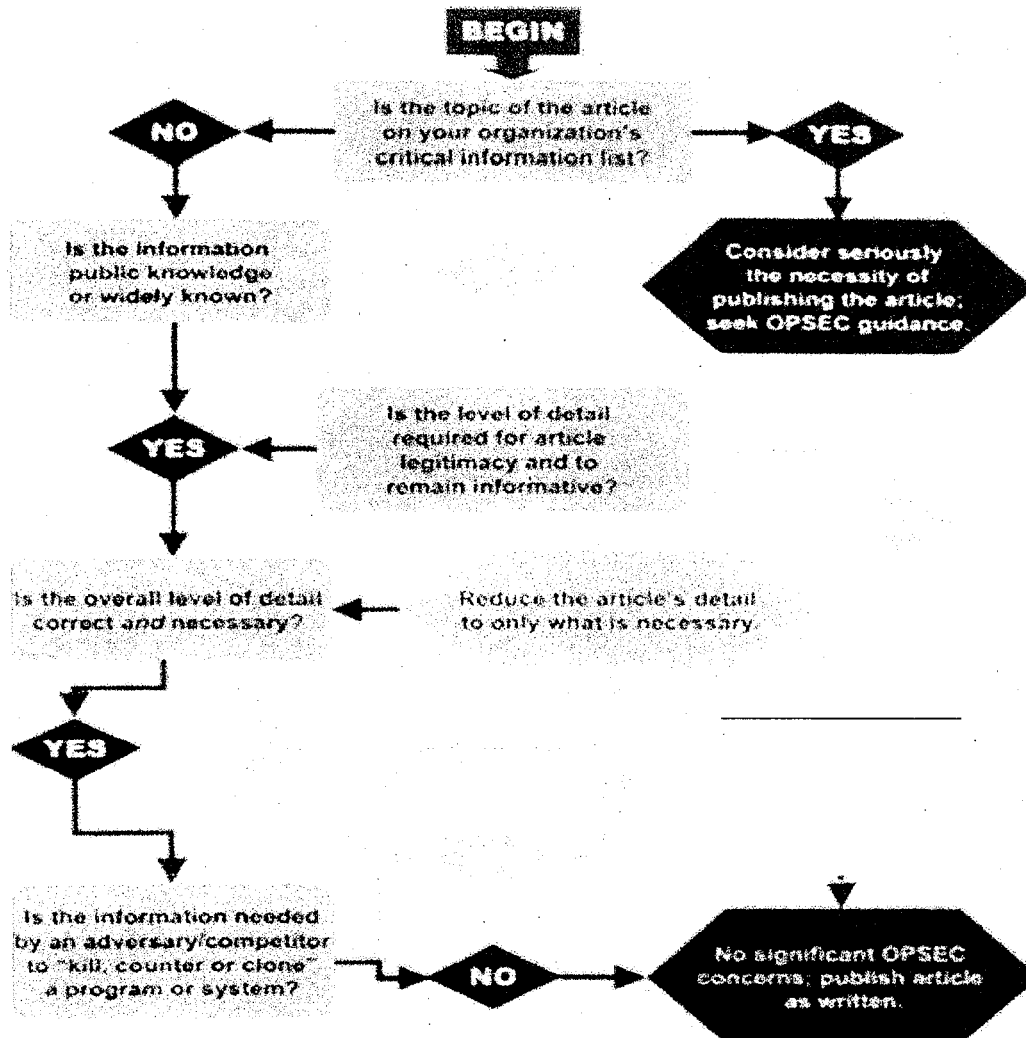
Name of the Capability Development Activity: _____

Date of Contact: _____

ITEM	YES	NO	N/A
1.1. Is a list of all CDIDs under the organization available for review?			
1.2. Have the OPSEC officers been appointed and trained for each and are orders signed by the commander available for review?			
1.3. Are their OPSEC Plans that incorporate CDID OPSEC considerations?			
1.4. Are copies of the OPSEC Plans available for inspection?			
1.5. Have the OPSEC Plans been periodically reviewed to ensure they do not need to be adjusted?			
1.6. If contractors are involved in the combat development activity, has the government conducted an evaluation of the contractor's OPSEC requirements, and have recommendations for improvements been annotated?			
1.7. Have any OPSEC compromises for the combat activity occurred since the last inspection and were they reported to higher headquarters as required?			

NOTES:

OPSEC Decision Flowchart For Article Reviews



www.ioss.gov

Designed to help writers and reviewers make informed decisions about the content of articles and the need for assistance from an operations security (OPSEC) perspective. For guidance, consult OPSEC program manager.