U.S. Army Tank-automotive and Armaments Command (TACOM) Operations Security (OPSEC) Plan

July 2023

Revised FY23 edition, supersedes all previous publications of this plan.

Distribution Approved for Public Release; Distribution Unlimited, per AR 380-5. OPSEC Review conducted per AR 530-1 and TACOM OPSEC Plan.

Table of Contents

1. References 5
2. Introduction 5
   a. Purpose 6
   b. Mission 6
   c. Critical Information 6
   d. OPSEC Program 7
3. Responsibilities 9
   a. TACOM Commander 9
   b. TACOM Deputy Chief of Staff G-2 10
   c. TACOM OPSEC Officer 10
   d. TACOM PAO 11
   e. TACOM Deputy Chief of Staff G-6 Corporate Information Office/Webmaster 12
   f. Detroit Arsenal Tenant Organizations 12
   g. TACOM Personnel 12
4. Indicators and Risks 14
5. OPSEC and the Family 16
6. Service Support 16
7. Command and Signal 17
   a. Command Responsibility 17
   b. OPSEC Monitoring 17
   c. OPSEC Surveys 17
   d. Signal 18
ANNEX A – OPSEC and Social Media
ANNEX B – Glossary of Acronyms

1. References:

a. AMC-M 530-1, Operation Security (OPSEC) for Headquarters, U.S. Army Material Command (HQ AMC)

b. AR 530-1, Operations Security

c. DoDM 5205.02, DoD Operations Security (OPSEC) Program Manual, Incorporating Change 2, effective 29 October 2020

d. DoDD 5205.02E, DoD Operations Security (OPSEC) Program, Incorporating Change 2, effective 20 August 2020

e. AR 380-5, Army Information Security Program

f. AR 25-2, Army Cybersecurity

g. AR 360-1, The Army Public Affairs Program

h. AR 25-1, Army Information Technology

i. DoDI 5200.48, Controlled Unclassified Information (CUI)

j. Information Security Oversight Office (ISOO) memorandum, CUI Notice 2019-03: Destroying Controlled Unclassified Information (CUI) in paper form, 15 July 2019

k. TACOM, AMTA-IN memorandum TACOM Policy 20-10, TACOM Policy for the Use of Antiterrorism (AT); Operations Security (OPSEC); Information Assurance (IA); Information Security (INFOSEC) Review Cover Sheet (STA Form 255), 19 June 2020

l. Headquarters, Department of Army (HQDA) Office of the Provost Marshal General Desk Reference; (Integrating Antiterrorism (AT)/OPSEC into the Contract Support Process), Initial: January 2012; Reissued: March 2020, 5th Edition

2. Introduction. OPSEC awareness and execution is crucial to Army success and is applicable to TACOM personnel, missions and supporting activities daily, from routine duties to planning, testing, exercise and evaluation phases through force deployment, recovery, and reconstitution. While traditional security programs are designed to deny adversaries access to classified information, an OPSEC Plan provides guidance on how to deny adversaries access to critical information and indicators of sensitive information.

While it is impossible to avoid all risks and protect everything, OPSEC provides a methodology to manage the risk. Specific aspects of military planning and execution are detectable; the key is to delay the detection for as long as possible so that the adversary does not have time to negatively influence TACOM mission execution. Unlike tactical operations, OPSEC, in support of the research, development, engineering, testing, acquisition and logistics process, is often easier to apply and implement. Tenant organizations and subordinate locations may require a unique approach to OPSEC, depending upon the function of the organization.

a. Purpose. The purpose of an OPSEC Plan is to develop a process that identifies the critical information (military plans, operations and supporting activities of an organization) and the indicators that can reveal those plans. Identification of this information allows for the development of measures to eliminate, reduce or conceal those indicators to prevent and/or limit the adversary's access that information. Application of OPSEC will attempt to deny adversaries access to information and technologies that are sensitive and, if disclosed, could seriously impact TACOM's mission and operations.

b. Mission. Provide guidance and processes to TACOM personnel, allowing for OPSEC measures to be incorporated into all facets of TACOM planning and execution. OPSEC is a process of identifying critical information (CUI, legacy FOUO, etc.) and analyzing friendly actions attendant to military operations and activities to:

(1) Identify those actions that are observable by adversary intelligence systems.

(2) Determine indicators and vulnerabilities an adversary intelligence system might obtain to be able to interpret or piece together to derive critical information in time to use against U.S. and/or friendly missions posing an unacceptable risk.

(3) Select and execute measures that eliminate or reduce the risk to friendly actions and operations or reduce to an acceptable level.

c. Critical Information. Critical information is specific facts about friendly capabilities, activities, limitations and intentions, or CALI. CALI is sought by adversaries, enabling them to plan and act effectively, causing failure or unacceptable consequences for the mission. Army operating forces use the doctrinal term "essential elements of friendly information" (EEFI). EEFIs are critical aspects of a friendly operation that, if known by a threat would subsequently compromise, lead to failure, or limit success of the operation and therefore should be protected from enemy detection. The corresponding term in joint doctrine is "critical information." Department of Defense

(DoD) and the service components are now using the term "Critical Information List" (CIL) for the purpose of standardization. The Army will continue to use the term EEFI in modified purpose related to CILs. The Army and joint definitions describe processes with the same objective, to protect information that can impede or prevent the force from accomplishing its mission. This OPSEC Plan will use the term critical information. Critical information can either be classified or unclassified, depending upon the organization, activity, or mission. Classified critical information requires OPSEC measures for additional protection because it can be unintentionally revealed by unclassified indicators. Critical information and CILs that are unclassified specifically require OPSEC measures because this information is not protected by the requirements pertaining 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(s) at risk. CILs are phrased as questions that the adversary is likely to ask about CALI. The use of CILs is an effective way to ensure the widest dissemination of a unit or organization's critical information while protecting classified and sensitive information. The answers to CILs are critical information that must be protected, are not releasable to the public or in the public domain and will not be posted to publicly accessible websites or sent over the Non-classified Internet Protocol Router Network (NIPRNet) or internet unencrypted. In some rare occasions, answers to CILs may be classified. An adversary relies upon detectable activities and open sources for information about the command's mission. Operations (training, testing, exercises and development) involve many detectable (observable) activities and significant amounts of open-source information. As world conditions change, an ally today may be tomorrow's adversary or competitor.

d. OPSEC Program. An OPSEC Program utilizes a five-step process. These steps provide a framework for the systematic and continuous process necessary to identify, analyze and protect critical and sensitive information. The process considers the changing nature of critical information and the threat and vulnerability assessments throughout the operation. When classified or unclassified-sensitive undertakings, such as operations, exercises, or field tests of military systems are planned and executed, acting routinely can often result in adversaries gaining information which can harm the mission by piecing together the various critical indicators that are observable. The five step OPSEC process includes:

Fig. 1 – 5 Step OPSEC Process

(1) Step One: Identify Critical Information. This step answers specific questions about what information must be protected and why. Adversaries collect information pertaining to U.S. DoD activities and technologies to further their own agendas. Even pieces of unclassified information (such as deployment information, military plans, acquisitions, mission capabilities and/or limitations, etc.) can hold great value to an adversary. The answers to these questions are items that must be protected. When traditional security programs cannot maintain adequate protection, the OPSEC Program must provide additional protection measures.

(2) Step Two: Analyze Threats. Analyzing threats provides answers to the question: Who is the adversary? A threat is an adversary that has the capability and intent to take actions detrimental to the success of DoD activities or operations. Common examples of adversaries are sworn enemies, foreign governments or terrorists; however, a threat can be anyone with intent and capability. The adversary agent is often portrayed as a sinister individual secretly photographing classified documents taken from a safe at night. This type of activity constitutes only a very small part of the current approach to intelligence collection. Collection of information concerning a technology and its application to a weapons system and the employment of the system can be compared to putting together the pieces of a puzzle. Various intelligence collection methods are used to identify these pieces and assist in properly placing them in the puzzle. Once a piece is identified and placed, another method may be used to verify the accuracy of the original information.

(3) Step Three: Analyze Vulnerabilities. This step answers the question: What weaknesses can an adversary exploit to uncover critical information? Analysis of vulnerabilities identifies tentative OPSEC measures required to maintain essential secrecy. Essential secrecy is the condition achieved when access to critical information is kept from our adversaries. Adversaries in possession of critical information can hinder or prevent friendly mission accomplishment and essential secrecy is a prerequisite for effective operations. The most desirable OPSEC measures combine the highest protection with the least effect on operational effectiveness. There are three categories of OPSEC measures:

(a) Action control. Alternative ways of conducting actions and activities which avoid indicators that create vulnerabilities. Actions taken by/within organizations to eliminate, prevent or control indicators.

(b) Countermeasures. Disruption of adversary information collection or gathering.

(c) Counter-analysis. Actions to cause misinterpretation of indicators by adversarial analysts.

(4) Step Four: Assess Risks. This involves assessing the adversary's ability to exploit vulnerabilities that could lead to exposure of critical information and the potential impact it would have on the mission. As an individual, whether at work or outside of work, you must be aware of the answers to these questions. As implementation of OPSEC countermeasures usually presents a risk to operational, logistical or procedural effectiveness, an analysis must be made prior to the decision to implement OPSEC measures.

(5) Step Five: Apply OPSEC Measures. This step involves applying measures to protect critical and/or sensitive information. OPSEC measures are implemented based on the commander's guidance, acceptable risk levels and available resources. OPSEC measures can include existing security measures such as use of Common Access Card (CAC), encryption, securing CUI (legacy FOUO information) and OPSEC review of documents.

3. Responsibilities. TACOM will conduct an aggressive OPSEC Program designed to improve mission effectiveness through the identification and elimination of potential OPSEC vulnerabilities. All Army personnel are ultimately responsible for the security of the information to which they have access. Each piece of information that an adversary can access is one more piece of the puzzle as it relates to the overall goal to accomplish the mission. Responsibilities and requirements to implement OPSEC are as follows:

a. TACOM Commander shall:

(1) Ensure implementation of OPSEC measures to protect the sensitive and critical information in all phases of operations, exercises, tests or activities by weighing the risk in the mission against the costs of protection and decide what OPSEC measures to implement.

(2) Establish signed orders, directives or policies that protect critical information and clearly defines OPSEC measures for personnel.

(3) Ensure OPSEC Plan or OPSEC measures are synchronized with supported organizations.

(4) Appoint, in writing, an OPSEC Officer

(5) Review, approve and disseminate the CIL to all subordinates as widely as security permits.

b. TACOM Deputy Chief of Staff G-2 shall:

(1) Serve as the Staff Officer for Security, provide overall management of the OPSEC Program.

(2) Assign a formally trained and certified individual to perform as the OPSEC Officer.

(3) Recommend appropriate OPSEC measures which can be implemented to preserve essential secrecy.

(4) Integrate OPSEC into all activities.

(5) Ensure the OPSEC Plan is reviewed at least annually.

(6) Provide OPSEC Training to the workforce. This may include, but is not limited to, OPSEC news releases in publications, OPSEC information emails and OPSEC awareness briefings.

c. Appointed OPSEC Officer shall:

(1) Prepare and recommend OPSEC countermeasures for implementation into the OPSEC Plan.

(2) Provide OPSEC guidance to organization, and tenant activities.

(3) Review CIL at least annually.

(4) Ensure OPSEC training is conducted IAW AR 530-1 and the OPSEC Program. Initial OPSEC training must occur within 30 days of hire.

(5) Conduct the Security portion of the OPSEC review (STA Form 7114) prior to the release of all public information concerning command programs, projects, activities or operations and Freedom of Information Act and contracts.

(6) Conduct quarterly OPSEC reviews (supplementary to PAO and Webmaster required reviews) of publicly accessible websites every 90 days.

(9) Makes recommendations to Leadership on OPSEC measures based on risk to mission, the ability to complete the mission, and the result if an OPSEC measure is not effective.

d. PAO shall:

(1) Ensure PAO personnel successfully complete OPSEC Level II training and coordinate directly with the OPSEC Officer on all questionable releases and for additional guidance on any release.

(2) Consider OPSEC in all public affairs operations IAW AR 525-13 (Antiterrorism), AR 530-1 and AR 360-1.

(3) Comply with Federal, DoD and DA website administration policies and implementing content-approval procedures that include OPSEC and PAO reviews before updating or posting information on all websites, including social networking sites.

(4) Ensure PAO communication products include OPSEC awareness messages when applicable. The author/originator providing the information, materials, or records to the PAO for public release should accomplish OPSEC reviews utilizing STA Form 7114.

(5) Conduct routine reviews of publicly accessible websites and social media sites to ensure compliance with AR 25-1.

e. Cybersecurity Office/Webmaster shall:

(1) Ensure all information or Information System (IS) responses that document or display specific vulnerabilities of a system or network that would aid attempts by an adversary to compromise those critical systems or networks are OPSEC sensitive and will be protected, controlled, marked, or stored at the appropriate classification level for the system concerned. This information will not be made publicly available.

(2) Comply with Federal, DoD and DA website administration policies and implementing content-approval procedures that include OPSEC and PAO reviews before updating or posting on all websites. Identify potential OPSEC violations and coordinate with the PAO for corrective action on all websites IAW AR 25-2, 4-20; AR 530-1 and AR 25-1.

(3) Conduct quarterly reviews of all public websites in conjunction with PAO. Results will be shared with the OPSEC Officer for inclusion in the annual OPSEC reports pursuant to AR 530-1 and AR 25-2.

(4) Coordinate directly with the OPSEC Officer and PAO for additional guidance as needed on any questionable website posting.

f. Detroit Arsenal Tenant Organizations shall:

(1) Provide OPSEC oversight of their organizations and activities.

(2) Participate in and support the OPSEC Plan by either adhering to the current OPSEC plan or developing an OPSEC Plan to meet their specific organizational needs or mission plans.

(3) Develop an organization CIL and disseminate to organizational staff.

(4) Appoint an OPSEC POC for their organization who can perform requirements of OPSEC for the Program Commander per their chosen OPSEC Plan appropriate for that organization.

g. All TACOM Personnel shall:

(1) Receive OPSEC awareness training, both initially and annually.

(2) Understand how OPSEC complements traditional security programs to maintain essential secrecy of U.S. military capabilities, intentions, and plans.

(3) Understand how adversaries aggressively seek information on U.S. military capabilities, intentions, and plans.

(4) Be familiar with this OPSEC Plan and where to obtain additional OPSEC guidance.

(5) Become knowledgeable of their organization's critical information and how to protect it by applying OPSEC measures to prevent inadvertent disclosure. Implement OPSEC measures as determined by the commander and the CIL.

(6) Prevent the disclosure of critical and sensitive information in any public domain to include but not limited to the internet, open source publications and the

media. Be aware that personal social media sites, weblogs also known as blogs and/or emails cannot be created or maintained during working hours.

(7) Maintain telephone security.

(8) Limit distribution of classified information and CUI (legacy FOUO) to those individuals with a valid need to know and the correct eligibility.

(9) Refrain from discussing work issues in public locations where conversations can be overheard.

(10) Ensure all hardcopy CUI (legacy FOUO), technical data and documents are destroyed IAW current shredding standards for CUI identified in the memo, CUI Notice 2019-03: Destroying Controlled Unclassified Information (CUI) in paper form dated 15 July 2019.

(11) Handle any attempt by unauthorized personnel to solicit sensitive or critical information as a TARP incident. Report all facts immediately to the nearest supporting Army Counterintelligence office, your Security Manager and Security Officer.

(12) Refrain from publicly disseminating or publishing photographs that display critical or sensitive information.

(13) Refrain from referencing, disseminating, or publishing critical or sensitive information that has already been compromised as this provides further unnecessary exposure of the compromised information and may serve to draw undue attention to it.

(14) Promptly report OPSEC and security violations to your supervisor and TACOM G-2 so mitigation efforts can be quickly initiated, and a damage assessment can be conducted.

(15) Ensure that an OPSEC review (STA Form 7114) is initiated on all information being considered for public release.

(16) Ensure that the most current version of the STA Form 255 is used when preparing contract documents or when modifying contracts (Annex F – Implementation of Antiterrorism/Operation Security/Cybersecurity/Information Security Review Requirements into the Contract Support Process).

4. Indicators and Risks. Indicators are friendly, detectable actions that reveal critical information which then leads to vulnerabilities that may be obtained and accurately evaluated by an adversary to provide a basis for effective adversary decision making. These actions are the target of adversary intelligence collection efforts and should be considered when developing OPSEC countermeasures:

a. Lack of OPSEC Awareness. Personnel who do not fully realize their OPSEC responsibilities. They are not aware of the intelligence value of unclassified information and the adversary's capability to decipher important intelligence data from this seemingly non-critical information.

b. Open-Source Literature. Publication and distribution of information without distribution statements or an OPSEC review. Even though papers and presentations undergo a formal process of technical, management and security review, there must be a comprehensive system to analyze the compilation of information found in any combination of these documents. This compilation may reveal sensitive data.

c. Communications. All unsecured telephone conversations, including cellular phones, are vulnerable to monitoring and all long-distance microwave transmissions are subject to intercept. Such vulnerabilities provide a source of information for intelligence agents. Do not use unsecured radios and/or cellular telephone to discuss sensitive or classified information. Communications supporting computer systems and faxes are equally vulnerable. Do not transmit sensitive e-mail or facsimile over non-secure means.

d. Visitor Control. Failure to properly clear personnel/visitors or allowing unescorted visitors in areas where they have not been approved to enter. Foreign visitors who have unauthorized access to areas, equipment, or information outside the scope of their duties. Allowing uncleared personnel to perform maintenance on IS. Visitors within the facility may observe or hear sensitive information, operations, or activities.

e. Operating IS without the proper accreditation, procedures and policies in place and improper storage or handling of classified documents. Magnetic storage media or laptop computers containing sensitive information may not be properly marked, handled, and secured.

f. Assignment of uncleared personnel to duties that provide opportunity for access to classified information.

g. Identifying key personnel and location for classified work.

h. Inadvertent release of information to the media by bypassing the PAO.

i. Improper disposal of unclassified sensitive or classified information.

j. Disgruntled employees and employees with personal problems (adverse information) possessing security clearances, who through circumstances such as criminal behavior, excessive indebtedness and/or indiscriminate use of alcohol present attractive targets to Intelligence Services. Supervisors and/or fellow employees may become aware of these difficulties but may fail to notify management or security to investigate, electing to ignore the problem or rationalizing that some other party will act.

k. Failure to follow security classification guidelines.

l. Failure to publish OPSEC implementing procedures.

m. Failure to maintain, review or enforce physical and automated access controls. Lack of comprehensive physical security measures (fences, guards, alarms, badges, etc.) at building entrances conducting classified or sensitive work.

n. Failure to brief newly assigned personnel on internal OPSEC procedures and measures. (Non-TACOM personnel, such as contractors, performing work on TACOM programs should not be given information relating to security guidance for classified elements of the programs prior to being to being vetted in DISS and commencing work on a current government contract that reflects the approval to classified information.)

o. Failure to ensure all personnel are briefed and updated to the current collection threat and foreign intelligence service(s) operations and activities.

5. OPSEC and the Family. Educate your family about OPSEC and how practicing it can protect our critical information and their personal information. Using current, real-world examples in education and awareness will enable family members to see the bigger picture. The Five-Step Process includes:

a. Family Critical Information: PII and military family knowledge.

(1) PII: Social security number, date of birth, passwords, photographs, etc.

(2) Military Information: Deployments, special missions/exercises, VIP itineraries, etc.

b. Threats: Hackers, predators, criminal elements, or unscrupulous businesses.

c. Vulnerabilities: Scams, theft, fraud, identity theft and social engineering.

d. Risk: How skilled are the “threats” in your area?” How vulnerable is your family?”

e. How to Protect Need-to-Know: Limit information to members in your immediate family only, limit sensitive discussions in public settings, ensure posted information has no significant value to an adversary and always assume that an “adversary” is reading what you write.

6. Organizational/Program Support:

a. Refer to your organizational/program OPSEC Plan for additional guidance. Organizations may implement their own OPSEC Plan with any local modification as may be necessary.

b. Public and Media Guidance. No portion of the TACOM OPSEC Plan is releasable to the public. CUI level portions of the TACOM OPSEC Plan and Annexes can be released to national, state, county, local intelligence, law enforcement, emergency management agencies and DoD contractors assigned to an active TACOM contract for which they are providing support in the execution of the TACOM mission. The unclassified version marked Distribution A can be release to companies requiring access to an OPSEC Plan as part of a TACOM contract.

c. OPSEC Review Form. The TACOM OPSEC Review Certification Form STA 7114 will be used to document OPSEC reviews and information that has been approved for public release. The requestor will route the document through their organization to include a supervisor and technology reviewer and through security, legal and PAO. A copy of the form will be maintained by the TACOM G-2 and the organization that generated the briefing, paper, video, photograph, or product for public release for a minimum of 24 months. A contracting company will work with the contracting officer to submit a STA 7114 for any release request prior to publishing.

d. The contract requirements package, Antiterrorism/Operations/Information Assurance/Information Security Review/Cover Sheet STA Form 255 will be used within TACOM. Organizations that are not subordinate to TACOM are encouraged to use STA Form 255 instead of the DA Contract Requirement Package Antiterrorism Security Review Cover Sheet.

7. Command and Signal.

a. Command Responsibility. The Security Office is responsible for reviewing the OPSEC Plan annually. If no changes are required, the review will be documented by a memorandum for record signed by the commander. Any new OPSEC Plan will be rewritten whenever large policy changes occur, or once every 5 years, whichever comes first. Recommendations or suggestions for improvements to this OPSEC Plan should be provided to the TACOM OPSEC Officer in G2, ATTN: AMTA-INS.

b. OPSEC Monitoring:

(1) The OPSEC Officer will monitor OPSEC issues.

(2) Monitoring of OPSEC issues may also be conducted by each organization if they have designated an OPSEC POC for their respective area of responsibility who has successfully completed OPSEC Level II training.

c. OPSEC Surveys.

(1) OPSEC surveys and assessments will be conducted as a part of the normal OPSEC process by the installation OPSEC Officer, or upon request of a specific organization.

(2) Internal OPSEC surveys and assessments are authorized and encouraged by the designated OPSEC Officers or POC. OPSEC will be an area checked during Security Assistance Visits (SAV) and TACOM Command Inspection Program (CIP).

d. Signal.

(1) All classified (CONFIDENTIAL and SECRET level) related information will only be transmitted over the SIPRNet, Joint Worldwide Intelligence Communication System (JWICS), classified fax, classified phone or discussed in areas approved by TACOM G-2 for classified discussions.

(2) Only personnel with a favorable background investigation or security clearance and requiring access for a lawful government purpose will be provided information on the OPSEC Plan.

(3) All sensitive and CUI level OPSEC information will be properly marked to show the proper security marking (CUI or UNCLASSIFIED) and can be transmitted over

a classified system or on a CUI level DoD installation level network. Encryption and digital signatures are required for all sensitive and CUI level information that is transmitted over the NIPRNET or internet to any recipient, whether located at TACOM or at a different off-post location.

(4) Classified TACOM OPSEC related information must use equipment approved by TACOM G-2 for classified reproduction. A courier card (DD Form 2501) must be issued by the G-2 Special Security Officer (SSO) to a courier prior to any transport classified materials off the installation. TACOM personnel must use an approved mailing procedure when there is a requirement to send classified materials through the mail. Hand-carrying of classified material/equipment is an exception rather than a rule and should be a final option and DA Form 3964 (Classified Document Accountability Record) must be included in the package and returned to the TACOM sender within 30 days.

(5) Sensitive and CUI level OPSEC related information may be copied on unclassified copiers, must be locked in a file cabinet, desk, or office when not in use and may be sent using first class mail.

(6) Only approved copiers will be utilized for reproduction of classified documents.

(7) Classified information WILL NOT be discussed, prepared, or transferred over automated IS or communications systems that have not been accredited to process that level of classified information.

(8) Portable Electronic Devices (PED) restriction information will be posted at the entrance of any open storage area or controlled meeting room area to advised “PED 0” during any classified meeting or discussion.

Note: This plan was last reviewed and updated on 6 June 2023.

Annex A - OPSEC AND SOCIAL MEDIA

1. Social media has become a big part of our lives. Social medial can help people and organization share information. As a culture, we depend on social media, but social media can be extremely dangerous if you are not careful. Operations Security (OPSEC) and personal privacy concerns should be paramount when using social media.

Be cautious when accepting friend requests and interacting with people online. You should never accept a friend request from someone you do not know, even if they know a friend of yours. Don't share information that you don't want to become public. Be careful about what you post about yourself on social media platforms. Once you put something out there, you can't control where it goes. Someone might target you based simply because you work in the DoD. Be cautious when listing your job, military organization, education and contact information. Providing too much information in your profile can leave you exposed to people who want to steal your identity or steal sensitive operational information.

When using Facebook and other social media platforms, do not post personally identifiable information and any information that can damage Army operations. Think about what you're posting before hitting share. Many times, you can avoid releasing sensitive information by simply rephrasing your social media post. If you aren't comfortable placing the same information on a sign in your front yard, don't put it online. Understanding what you can and cannot post on social media platforms goes a long way in protecting you, your family, and the Army online.

2. Geotagging safety. Location-based social networking is quickly growing in popularity. A variety of applications are capitalizing on users' desire to broadcast their geographic location. The increased popularity of these applications is changing the way we as a digital culture view security and privacy on an individual level. These changes in perception are also creating OPSEC concerns on an Army level. Deployed Soldiers, or Soldiers conducting operations in classified areas should not use location-based social networking services. These services will bring the enemy right to the Army's doorstep. Want to avoid giving away location? Disable the GPS function on your smartphone.

3. Security items to consider with social media:

a. Take a close look at all privacy settings. Set security options to allow visibility to "friends only."

b. Do not reveal sensitive information about yourself such as schedules and event locations.

c. Ask, “What could the wrong person do with this information?” and “Could it compromise the safety of myself, my family, or my unit?”

d. Geotagging is a feature that reveals your location to other people within your network. Consider turning off the GPS function of your smartphone.

e. Closely review photos before they go online. Make sure they do not give away sensitive information which could be dangerous if released.

f. Make sure to talk to family about operations security and what can and cannot be posted.

g. Videos can go viral quickly, make sure they don’t give away sensitive information.

h. Remember that while we all have the freedom of speech, as a part of the Department of the Army, what we post on social media, not only represents us as individuals, but also reflects on our employer as well.

Annex B - Glossary of Acronyms

AMC – Army Material Command

AR – Army Regulation

AT – Antiterrorism

CAC – Common Access Card

CALI – capabilities, activities, limitations, and intentions

CIL – Critical Information List

CIP – Command Inspection Program

CUI – Controlled Unclassified Information

DISS – Defense Information System for Security

DoD – Department of Defense

DoDD – Department of Defense Directives

DoDI – Department of Defense Instructions

DoDM – Department of Defense Manual

EEFI – Essential Elements of Friendly Information

FOUO – For Official Use Only

HQDA – Headquarters Department of Army

IAW – In Accordance With

INFOSEC – Information Security

IS – Information System

ISOO – Information Security Oversight Office

JWICS – Joint Worldwide Intelligence Communication System

NIPRNet – Non-Classified Internet Protocol Router Network

OPSEC – Operations Security

PAO – Public Affairs Officer

PED – Personnel Electronic Device

PII – Personal Identifiable Information

POC – Point of Contact

SAV – Security Assistance Visit

SIPRNet – Secure Internet Protocol Router Network

SSO – Special Security Officer

TACOM – U.S. Army Tank-Automotive and Armaments Command

TARP – Threat Awareness and Reporting Program

VIP – Very Important Person