U.S. ARMY CONTRACTING COMMAND –DETROIT ARSENAL (ACC-DTA)

OPERATIONS SECURITY (OPSEC) PLAN

October 2023

Distribution Restriction Statement

This document will not be sent over the internet unencrypted or posted to any public websites.

Destruction Notice

Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

Proponent and Exception Authority

The proponent of this OPSEC Plan is ACC-DTA. Submit recommended changes and/or corrections to ACC-DTA OPSEC Officer.

Controlled by: CCTA
CUI Category: OPSEC
Distribution Dissemination Controls:
FEDCON
POC: ACC-DTA Security, ACC-DTA Security Manager, 586-909-8744

CUI

Army Contracting Command-Detroit Arsenal (ACC-DTA)
Operations Security (OPSEC) Plan

Contents

References ……..1
Introduction ……..1
Mission……...2
Applicability……2
OPSEC Program……..2

Responsibilities:
ACC-DTA Executive Director……4
ACC-DTA OPSEC Officer ……..4
ACC-DTA Public Affairs Officer……..6
All Personnel……..6

OPSEC Program Support……8

Administration and Logistics……9

Appendices:

Appendix A – Critical Information List……10
Appendix B – Threats……12
Appendix C – OPSEC Measures, Compromises, and Violations……..13
Appendix D – OPSEC Review Certification (STA 7114)……16
Appendix E – Implementation of AT/OPSEC in the contract support process….17
Appendix F – Controlled Unclassified Information (CUI)……..18
Appendix G – OPSEC and Social Media……19
Appendix H – Security Points of Contact/ACC-DTA OPSEC Managers……22

Army Contracting Command-Detroit Arsenal (ACC-DTA)
Operations Security (OPSEC) Plan

1. References.

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

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

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

   d. AR 380-5 (Army Information Security Program), 25 March 2022

   e. AR 25-2 (Army Cybersecurity), 4 April 2019

   f. AR 360-1 (The Army Public Affairs Program), 25 May 2011

   g. AR 25-1 (Army Information Technology), 15 July 2019

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

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

   j. Army Contracting Command Operations Security Plan

   k. Headquarters, Department of Army (HODA) 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 ACC-DTA personnel, missions and supporting activities daily, from routine duties to planning, testing, exercise and evaluation phases through 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 ACC-DTA 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.

3. 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 ACC-DTA's mission and operations.

4. Mission. Provide guidance and processes to ACC-DTA personnel, allowing for OPSEC measures to be incorporated into all facets of ACC-DTA 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:

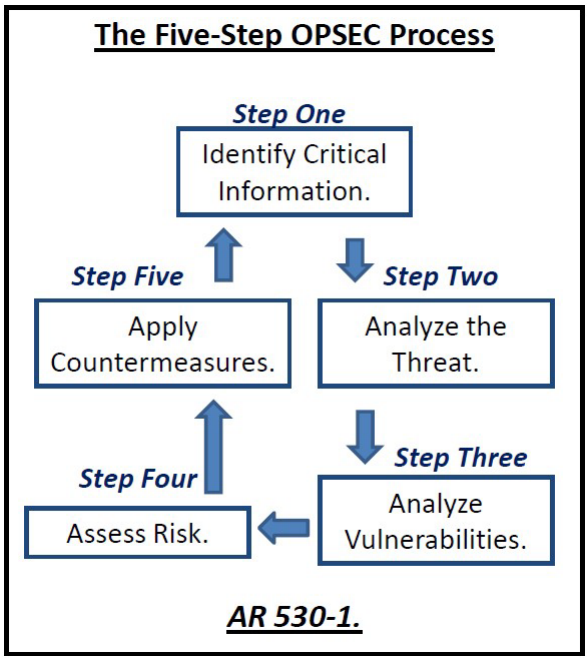
a. Identify those actions that are observable by adversary intelligence systems.

b. 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.

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

5. Applicability. Designed to support the implementation of the Army Contracting Command's (ACC) OPSEC Program, this OPSEC Plan is applicable to all Soldiers, Department of the Army (DA) Civilians, Family members, and Department of Defense (DoD) contractors assigned to ACC-DTA. All future references to ACC-DTA also includes the subordinate units listed in Appendix A.

6. 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:



a. Step 1 is identifying 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.

b. Step 2 is analyzing 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.

c. Step 3 is analyzing 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.

d. Step 4 is assessing 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.

e. Step 5 is applying 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.

7. Responsibilities. ACC-DTA OPSEC Officer will execute an OPSEC Program in accordance with HQ-ACC OPSEC Plan, and tenant unit responsibilities per AR 530-1. All Army personnel are ultimately responsible for the security of the information to which he/she has access. Each piece of information that an adversary can access is one more piece of the puzzle as it relates to Army mission.

a. ACC-DTA Executive Director shall:

(1) Appoint in writing, a Primary and an Alternate OPSEC Officer for ACC-DTA. Ensure they are of sufficient rank/grade to execute their responsibilities.

(2) Annually, or as needed, approve the organization’s Critical Information List (CIL), OPSEC Measures, and OPSEC Plan developed and maintained by the ACC-DTA OPSEC Officer. Ensure dissemination to all personnel and subordinate elements as widely as security permits.

b. ACC-DTA OPSEC Officer will:

(1) Be appointed in writing, and complete OPSEC Level II training.

(2) Establish a documented OPSEC Program.

(3) Identify the command's critical and sensitive information and establish a critical information list, to clearly develop and define the specific OPSEC measures that all personnel should practice. Provide critical information list and OPSEC Measures to the Director for review and signature. Update annually or as needed.

(4) Coordinate, as needed, with HQ-ACC for program support.

(5) Maintain liaison with other United States Army Garrison-Detroit Arsenal (USAG-DTA) tenants. Attend OPSEC working groups.

(6) Establish a New Employee Orientation Briefing. Provide briefing within 30 days of individual reporting to organization.

(7) Provide and document OPSEC awareness material for ACC-DTA personnel, to maintain a high-level of OPSEC awareness.

(8) Monitor the completion of OPSEC Level 1 training for all ACC-DTA personnel.

(9) Use the OPSEC Review Form (STA 7114), to conduct OPSEC reviews on, but not limited to, memorandums, letters, e-mail messages, articles, academic papers, videos, web sites, briefings, ACC-DTA specific contract requirement packages, requests for information, news releases, technical documents, proposals, plans, orders, ACC-DTA's comments to audit recommendations, social media message boards, blogs, or other visual or electronic media, prior to release in the public domain.

(10) Coordinate HQ-ACC's Staff Assistance Visits (SAVs) and program assessments.

(11) Ensure ACC-DTA subordinate sites receive OPSEC support at their respective locations and assess accordingly.

(12) Submit, in accordance with AR 530-1 and HQ, ACC OPSEC Plan, the annual OPSEC Program Status Report to HQ-ACC.

(13) Conduct quarterly OPSEC reviews of ACC-DTA publicly accessible web

sites or social media pages.

(14) Pursuant to ALARTACT 015-2012, review contractual documents initiated by ACC-DTA for OPSEC requirements, utilizing the Contract Requirements Package Antiterrorism/Operations Security Cover Sheet, STA Form 255 (see Appendix D).

c. ACC-DTA Public Affairs Officer will:

(1) Ensure that material proposed for public release that mentions the Army Contracting Command-Detroit Arsenal plans, policies, programs, operations, budget, personnel, or activities is cleared through Public Affairs Office and OPSEC channels.

(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 content-approval procedures that include OPSEC and public affairs reviews before updating or posting information on official websites.

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

(5) Ensure all official Army social media sites under ACC-DTA adhere to guidance of DoD Instruction 5400.17, ALARACT 073/2022 and Army social media guidance found at https://www.army.mil/socialmedia/.

(6) Conduct quarterly reviews of ACC-DTA official public websites to ensure compliance with DoD Instruction 5400.17, ALARACT 073/2022, AR 25-1.

(7) Provide unclassified information about the Army and its activities to the public with maximum disclosure and minimum delay, ensuring any information released would not would adversely affect national security, threaten personal safety, or invade the privacy of members of the Armed Forces.

(8) Ensure that release of information about personnel casualty matters adheres to current policies and procedures guidelines (DoDI 1300.18).

d. All Soldiers, Department of the Army Civilians, and DoD Contractors will:

(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) Become knowledgeable of ACC-DTA's critical information and how to protect it by applying OPSEC measures to prevent inadvertent disclosure.

(5) Implement OPSEC measures as determined by the Executive Director.

(6) Maintain telephone security.

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

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

(9) 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 date 15 July 2019.

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

(11) Handle any attempt by unauthorized personnel to solicit sensitive or critical information as a Threat Awareness and Reporting Program (TARP) incident. Report all facts immediately to the nearest supporting counterintelligence office and ACC-DTA Security.

(12) Know and protect ACC-DTA's Critical Information List (CIL).

(13) 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 and/or emails cannot be created or maintained during working hours.

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

(15) 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.

(16) Promptly report OPSEC and security violations to your supervisor and ACC-DTA Security so mitigation efforts can be quickly initiated, and a damage assessment can be conducted.

(17) Ensure that an OPSEC review (STA Form 7114) is initiated on all information being considered for public release (Annex E OPSEC Review Certification).

(18) Ensure that the most current version of the AT/OPSEC in contracting form (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).

8. OPSEC Program Support.

a. OPSEC Review Certification Form STA 7114 will be used to document OPSEC reviews and information that has been approved for public release. The requester 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 organization's security proponent and the organization that generated the briefing, paper, video, photograph, or product for public release for a minimum of 24 months.

b. The contract requirements package, Antiterrorism/Operations/Information Assurance/Information Security Review/Cover Sheet STA Form 255 will be used within ACC-DTA. Organizations that are not subordinate to ACC-DTA are encouraged (however not required) to use STA Form 255 instead of the DA Contract Requirement Package Antiterrorism Security Review Cover Sheet.

9. 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. Using the Five-Step Process, this would look like:

a. Family Critical Information: PII and military family knowledge. This includes social security number, date of birth, passwords, photographs, 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.

10. Administration and logistics. A copy of the plan will be maintained in an OPSEC binder, and on the ACC-DTA SharePoint. OPSEC program documentation, to include OPSEC measures, will be updated annually or as required.

GALLAGHER.DANIEL.JOSEPH.1034297360
Digitally signed by GALLAGHER.DANIEL.JOSEPH.1034297360
Date: 2023.10.13 07:31:44 -04'00'

DANIEL J. GALLAGHER
Executive Director
Army Contracting Command-Detroit Arsenal

CF:
ACC-DTA
HQ-ACC G-3

Appendix A: Critical Information List (CIL)

1. Mission Statement. ACC-DTA delivers decisive contracting solutions across the full spectrum of conflict in support of the Army and Joint Force Multi-Domain Operations - Anytime, Anywhere.

a. Critical Information is key questions likely to be asked by adversary officials and Intelligence Agencies about specific friendly intentions, capabilities, and activities. The answers to these questions expose our intentions, capabilities, and activities. Therefore, we must not provide answers to the adversaries' questions about our activities, procedures, operations, or planning. Exposure could diminish the effectiveness of operations or actions; compromise classified or sensitive unclassified information; and provide adversaries with information allowing technological, tactical, operational, and/or strategic advantage.

b. Classified Critical Information. Security Classification Guides (SCGs) specifically outline the classified information and hardware directly associated with ongoing and planned weapon systems and technologies. Critical Information can include classified and sensitive unclassified information.

c. Controlled Unclassified Information (CUI). CUI is government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and government wide policies. CUI is not classified information. It is not corporate intellectual property unless created for or included in requirements related to a government contract. Because there are fewer controls over CUI as compared to classified information, CUI is the path of least resistance for adversaries. Loss of aggregated CUI is one of the most significant risks to national security, directly affecting lethality of our warfighters. This category of information was formerly For Official Use Only (FOUO). CUI requires withholding from public disclosure IAW DOD 5200.48.

2. OPSEC POC: Shawn F. O'Neill, ACC-DTA Security Manager/OPSEC Officer, shawn.f.oneill6.civ@army.mil, COMM: 586-909-8744.

3. ACC-DTA's CIL.

a. The command's Critical Information List (CIL) must be protected by all U.S. Government personnel and contractors supporting Government operations. While the CIL is not classified, it is controlled unclassified information (CUI} and cannot be released to foreign nationals or to personnel and organizations not supporting the command. Notice that the Critical Information are stated in the same manner as an adversary decision maker will state them to his/her intelligence collection personnel. The answers to our Critical Information identify the information we want

to protect. The responsibility to protect the answers to these questions rests with all concerned.

b. ACC-DTA subordinate sites utilizes the critical information written in the TACOM CIL/OPSEC plan and the INSCOM CIL/OPSEC plan. ACC-DTA Security Manager has copies.

c. ACC-DTA's CIL.

(1) Which contractors are bidding on XXX proposal/source selection?

(2) How do you protect classified documents?

(3) What is the capability, limitation, and/or vulnerability of equipment XXX and/or system XXX?

(4) Do you have protection or operation plans? How do you exercise them? When?

(5) The contract you're working on, is it for a planned or future operation? Where is the equipment/service/supply being delivered to?

(6) Where do employees travel and why?

(7) How is employee personally identifiable information (PII) safeguarded?

(8) How many employees are deployed? Where? For how long?

(9) What is the equipment/personnel readiness status for ACC-DTA?

(10) What physical security vulnerabilities exist in your organization?

(11) Capabilities, limitations, and vulnerabilities of equipment, mission-specific software systems (contracting writing systems, etc.).

a. Updates. ACC-DTA's CIL is updated annually or as needed.

Appendix B: Threat

Specific threat information relative to Detroit Arsenal, MI and to ACC-DTA may be requested through ACC-DTA's Antiterrorism Officer (ATO). See Appendix H for ATO contact information.

Appendix C – OPSEC Measures, Compromises and Violations

1. All personnel must know the organization's critical information and the OPSEC measures implemented to protect the information. The following OPSEC measures will be integrated with day-to-day activities and planning for future operations:

a. Communications. When secure telephones are used in areas conducting sensitive and classified operations, the user must be aware of surrounding environment and personnel present. Even though all persons in a secure area may be approved for classified access, they may not have a need-to-know.

b. Information Technology Security. Computer systems must be accredited to the appropriate classification level by the Information System Security Manager (ISSM) or the Corporate Information Office (CIO/G-6). All discs and other magnetic media must be labeled to show the overall highest classification level and stored accordingly. ISSMs and desktop system administrators are assigned to each organization to assist users in security, hardware, and software issues. CUI, legacy FOUO, and privacy act protected information must be CAC encrypted when sent over the NIPRNET/internet. Individuals have been instructed not to leave their CAC unattended (outside of visual contact) and unsecured (no more than an arm's length away). All CACs or Secret Internet Protocol Router Network (SIPRNet) token cards must be removed from any workstation when not in use. The Network Enterprise Center (NEC} conducts scans of the installation network for unauthorized software, hardware and suspect websites are filtered. Do not plug any unapproved devices or wireless devices into any government equipment.

c. Information Security (INFOSEC). Safe combination changes will be recorded on a safe combination sheet (SF 700), and combinations will be changed when the combination has been compromised, or when personnel who had knowledge of the combination are reassigned or no longer require that access, whichever comes first. The classified portion of the SF 700 must be stored in a different GSA approved storage container approved to store classified information at the same level as the SF 700 is marked. This is to ensure that in the event of a lockout, cleared personnel can access the combination to open the safe. Prior to safes being turned in, combinations must be reset to the factory setting of *50-25-50* once the safe has been thoroughly checked and sanitized of any remaining classified materials by a security manager. All materials (papers, audio-visual presentations, etc.) are marked with the appropriate classification level IAW AR 380-5. All classified, CUI or program critical technology and technical information, regardless of its medium, including drafts, must be reviewed, and marked by the author to ensure proper security/classification markings are applied throughout the document and the correct limited dissemination or distribution statement is posted

on the first page. CUI and legacy FOLIO level information shall be secured in locked desks, cabinets, or rooms when not in use. CUI or personally identifiable information (PII) coversheets are placed on top and at the back of CUI materials and access is limited to those individuals with a lawful government purpose when they are in use. If an Unauthorized Disclosure (UD) of CUI or sensitive program information is suspected, this must be reported to a supervisor or security manager. The security manager will assess the situation and complete required UD of CUI report (reference Annex D, Monthly OPSEC CUI Assessments and Process for Incident Reporting of Unauthorized Disclosure of CUI). An SF 701 (End of Day Checklist) is placed near the organization's primary exit and is reviewed/signed anytime there is activity in an area with restricted access or classified storage containers. This form is unique to each area and must be maintained for 90 days if there was no security violation and for one year if there was. Each day of the month must be accounted for on the SF 701, to include weekends, holidays, and dates when there is no activity in the area. An SF 702 (Security Container Check Sheet) will be utilized for every active classified storage container. A new form will be maintained for each month the container is in use. The form will be annotated to reflect the room number, building number, container number, month, and year at the top of the form. Notations will be made on the SF 702 if the containers are opened during non-duty hours, on weekends, on holidays and whenever there is activity in the work area. All days in the month will be accounted for on the SF 702 regardless of whether checks were made during non-duty hours or holidays IAW AR 380-5.

d. Reproduction. Reproduction equipment showing the highest classification level that may be reproduced on it with administrative and procedural information concerning the use of the copier. Owners of equipment must identify/designate which reproduction/copying equipment in their respective organizations are authorized to reproduce unclassified and classified information and at what level. CUI documents must be destroyed IAW CUI Notice 2019-03: Destroying Controlled Unclassified Information (CUI) in paper form dated 15 July 2019 via use of cross-cut shredders that produce 1 mm x 5 mm (0.04 in. x 0.2 in.) particles (or smaller) by pulverizing/disintegrating the paper using disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen IAW National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88, rev 1, Table A-1: Hard Copy Storage Sanitization. The National Security Agency (NSA) maintains an evaluated products list (EPL) of equipment authorized to destroy hard copy (paper) classified national security information.

e. Publications. Information proposed for public release is subject to utilizing STA Form 7114 (OPSEC Review Certification) located in Annex E. A record of this review will be maintained by ACC-DTA Security for 24 months. Public release includes, but is not restricted to, printed articles, briefings, interviews, and

placement of information on the internet.

f. Personnel Security (PERSEC). Security access for all personnel assigned to ACC-DTA and tenant organizations must be verified through the authorized system of record, the Defense Information System for Security (DISS). All departing personnel (military, civilian or contractor) must contact ACC-DTA Security (see Appendix H) to ensure their access is terminated and that they have received any required debriefings. This should be one of the employees last actions when out processing as their ability to access NIPR will be affected.

g. Physical Security. Each ACC-DTA building is surrounded by a perimeter fence and DoD civilian police patrol control access. Vehicles entering any facility may be subject to random searches. Personnel assigned to ACC-DTA are issued a CAC which they must present to the guard at the gated entrance to gain access to the installation. Video cameras are in place to allow central monitoring of activities. In addition, restricted buildings, sensitive and classified locations have secondary controls and are alarmed.

h. Security Education. Training for INFOSEC, OPSEC and Threat Awareness and Reporting Program (TARP) is an annual requirement and is documented in TED. OPSEC reminder information is posted at various locations across ACC-DTA, available on government websites and periodically distributed by email communications. In addition, individuals who have been issued a SIPRNet token will receive online derivative classification training annually via Center for Development of Security Excellence (CDSE) and provide a copy of the training certificate to ACC-DTA Security.

i. OPSEC Compromise. An OPSEC compromise is the disclosure of sensitive and/or critical information that jeopardizes a unit's ability to execute its mission or to adequately protect its personnel and/or equipment or affects national security. For sensitive and/or critical information that has been compromised and is available in open sources, the public domain should not be highlighted or referenced publicly outside of intra-governmental or authorized official communications as these actions provide further unnecessary exposure of the compromised information. Personnel should not respond to queries to deny or confirm the validity of sensitive information that has been compromised or released to the public. Notify ACC-DTA security manager of all OPSEC compromises.

2. OPSEC Violation. An OPSEC violation occurs when there is a known disclosure of sensitive and/or critical information that has already been identified in our CIL. An OPSEC violation is punishable by the Uniform Code of Military Justice or disciplinary action for civilians.

Appendix D: OPSEC REVIEW CERTIFICATION (STA 7114)

1. An OPSEC Review is intended to evaluate a document or other type of information and/or media designated for unclassified and unlimited (public domain) distribution. The purpose of an OPSEC Review is to help ensure the protection of information, which may be sensitive or critical information (AR 530-1.)

2. When information or material is received by ACC-DTA Security containing information which may prove beneficial to an adversary, notification by the ACC-DTA Security reviewer along with his/her recommendations will be provided back to the author for modification. NOTE: ACC-DTA Security will only OPSEC review items that ACC-DTA “owns” or is the “originator”. All other items, i.e., a contract action usually originates from a requiring activity, and therefore, their security POCs would conduct the OPSEC review.

3. The STA 7114 must be used when you plan on making your product (e.g., documents, video tapes, voice tape, briefings, articles, or equipment) available to the general public (Distribution Statement A - Approved for Public Release; distribution unlimited). All documents and/or materials are to be submitted (digital with encryption) through OPSEC Review channels (SME/technical review, supervisory, contracting officer, legal, security/OPSEC officer, and public affairs) and must be accompanied by a properly completed, STA Form 7114 "OPSEC Review Certification" to include:

a. Specific name(s) of individuals responsible for authoring the document.

b. Name, signature, grade, and office symbol of a SME/technical reviewer (management individual who possesses technical expertise regarding the subject matter,) and a supervisor, both of whom must be someone other than the author.

c. A "Purpose of Release and Date of Proposed Release" to provide justification for making the information open source and the benefit in doing so.

4. Items submitted for OPSEC Review (if applicable to ACC-DTA), should be forwarded (encrypted) electronically to the POCs in Appendix H.

5. Originators of items requiring an OPSEC Review should allow for a week planning cycle from submission to finish. This includes receiving legal concurrence, public affairs (if applicable), etc. Note: public affairs are only in the process if the item is to be viewed in the media, in an article, symposium, etc. This ensures conformity and proper aesthetics.

6. Blank 7114: https://acc.aep.army.mil/sites/acc-dta/ERC/Pages/OPSECtpp.aspx

Appendix E: Implementation of Antiterrorism/OPSEC in the contract support process

1. Purpose. In lieu of the DA coversheet (per ALARACT 015/2012), local agencies to include TACOM and those that support TACOM will utilize the STA Form 255. The purpose of the form is 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. Other agencies and organizations (i.e., local Garrisons, PEOs, etc.) are allowed to utilize the standard DA coversheet.

2. The contracting officer will ensure that contractor personnel are appropriately certified and provide verification to the Defense Manpower Data Center (DMDC) database: https://dwp.dmdc.osd.mil/dwp/app/main . Additional training on local or system procedures may be provided by the DoD organization receiving services.

3. See blank STA 255 form: https://armyeitaas.sharepoint-mil.us/sites/HQACC-DTA-BMD/Security/Forms/AllItems.aspx?id=%2Fsites%2FHQACC%2DDTA%2DBMD%2FSecurity%2FAntiterrorism%20%2DForce%20Protection%2FAT%20OPSEC%20guide%5FFourth%20Edition%2Epdf&parent=%2Fsites%2FHQACC%2DDTA%2DBMD%2FSecurity%2FAntiterrorism%20%2DForce%20Protection

4. TPP: https://acc.aep.army.mil/sites/acc-dta/ERC/Pages/atopsectpp.aspx

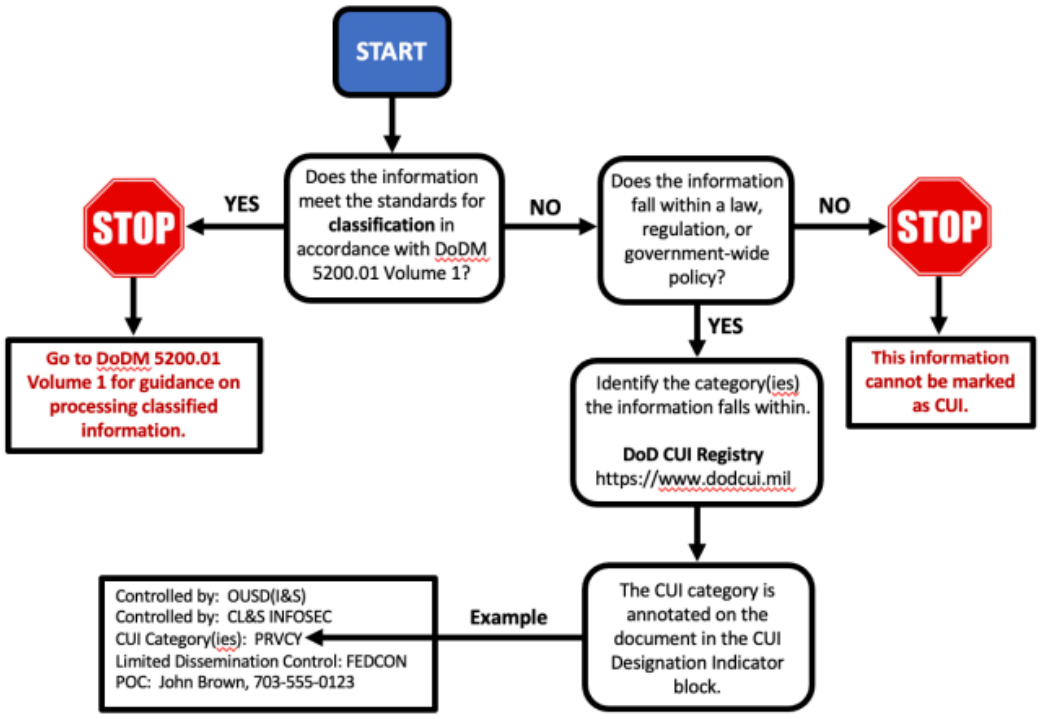
Appendix F: Controlled Unclassified Information (CUI)

What is the difference between FOUO and CUI?

- DoD's legacy "FOUO" marking was authorized to protect UNCLASSIFIED information that "may be exempt from mandatory disclosure under the Freedom of Information Act (FOIA)."
- The CUI Program developed a common marking system across Federal agencies and created categories to capture the many types of UNCLASSIFIED information requiring safeguarding based on existing laws, regulations, and government-wide policies.

What's new with CUI?
- Uniform system
- Indexed guidance (Registry)
- Greater specificity
- Safeguarding standards

How do I determine if information is CUI?



CUI Categories: https://www.archives.gov/cui/registry/category-list

Controlled Unclassified Information (CUI) Program (archives.gov) information on marking, protecting, and reproduction of CUI.

https://www.dodcui.mil for more information.

Appendix G: OPSEC and Social Media

Social media has become a big part of our lives. Social media can help people and Army organizations share information. It also helps Soldiers, family members and Army civilians to stay connected to loved ones. As a culture, we depend on social media, but social media use can be extremely dangerous if you're not careful.

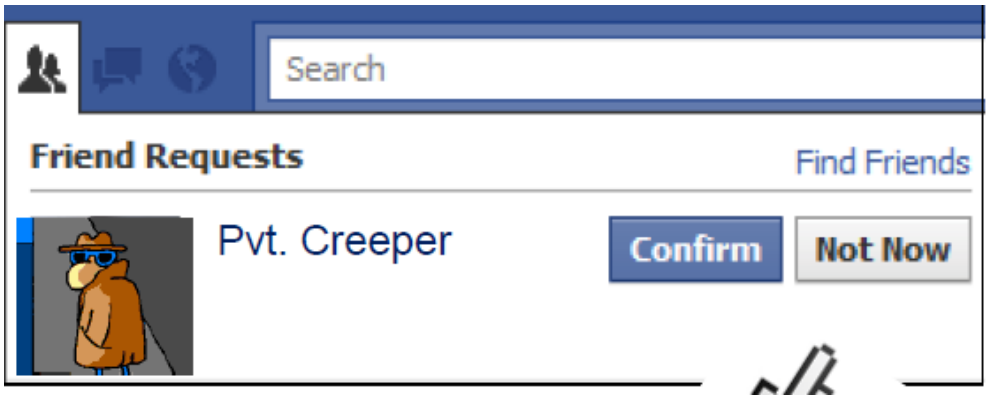
Did you know?

- A U.S. Government official on sensitive travel to Iraq created a security risk for himself and others by Tweeting his location and activities every few hours.
- A Family on vacation kept friends up-to-date via online profiles; their home was burglarized while they were away.
- New computer viruses and Trojans that successfully target information on social networking sites are on the rise.
- Information on social networking sites has led to people losing job offers, getting fired and even being arrested.
- Social networking sites have become a haven for identity thieves and con artists trying to use your information against you.
- Several kidnapping, rape and murder cases were linked to social networking sites where the victims first connected with their attackers.
- According to the Al Qaeda Handbook, terrorists search online for data about "Government personnel and all matters related to them (residence, work place, times of leaving and returning, children and places visited.)"

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. For more on this, check out this article about the Robin Sage Experiment: "Fictitious femme fatale fooled cybersecurity"

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.



What not to post

- 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.

MAKING DANGEROUS SOCIAL MEDIA POSTS SAFER	
Dangerous	Safer
My Soldier is in XYZ at ABC Camp in ABC City, Afghanistan.	My Soldier is deployed to Afghanistan.
My Soldier will be leaving Kuwait and heading to Iraq in three days.	My Soldier deployed this week.
My Soldier is coming back at XYZ time on XYZ day.	My Soldier will be home this summer.
My family is back in Edwardsville, IL.	I'm from the Midwest.

Social media OPSEC concerns for families and Family Readiness Groups

- Social media helps Family Readiness Groups and Army family members stay connected, but OPSEC should always be the primary concern.
- Family Readiness Groups, Army spouses and Army Family members need to know that posting sensitive information can be detrimental to Soldier safety.
- Ensure that information posted online has no significant value to the enemy. Always assume that the enemy is reading every post made to a social media platform.
- Even seemingly innocent posts about a family member's deployment or redeployment date can put them at risk.

Security items to consider

- Take a close look at all privacy settings. Set security options to allow visibility to "friends only."
- Do not reveal sensitive information about yourself such as schedules and event locations.
- Ask, "What could the wrong person do with this information?" and "Could it compromise the safety of myself, my family or my unit?"
- Geotagging is a feature that reveals your location to other people within your network. Consider turning off the GPS function of your smartphone.
- Closely review photos before they go online. Make sure they do not give away sensitive information which could be dangerous if released.
- Make sure to talk to family about operations security and what can and cannot be posted.
- Videos can go viral quickly, make sure they don't give away sensitive information.

Social media concerns for Army children

What is the best way to protect your kids online? Talk to them. Research suggests that when children want important information, most rely on their parents.

The important thing is to start the education early. Talk to your children about online risks and make sure you create an honest and open environment.

https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security for additional resources.

Appendix H: Security Points of Contact/ACC-DTA OPSEC Managers:

ACC-DTA Mission Assurance Mailbox: usarmy.detroit.acc.mbx.acc-dta-mission-assurance@army.mil

SHAWN F. O'NEILL
Security Manager
US Army Contracting Command – Detroit Arsenal (ACC-DTA)
CCTA-CB/MS: #314
6501 E Eleven Mile Rd
Detroit Arsenal, MI 48397-5000
Office: 586-282-9516
DSN: 786.9516
Gov't Cell: 586-909-8744
Teams: 571-588-9360
NIPR: shawn.f.oneill6.civ@army.mil
SIPR: shawn.f.oneill6.civ@mail.smil.mil
JWICS: shawn.f.oneill.civ@army.ic.gov
LE: shawn.oneill@leo.gov

Richard T. Murphy, Jr.
Alternate Security Manager
US Army Contracting Command – Detroit Arsenal (ACC-DTA)
CCTA-CB, M/S 314
6501 East 11 Mile Road
Detroit Arsenal, Michigan 48397-5000
COMM: (586) 282-5413
TEAMS: (571) 588-9195
DSN: 786-5413
NIPR: richard.t.murphy65.civ@army.mil
SIPR: richard.t.murphy65.civ@mail.smil.mil