



Security

OPERATIONS SECURITY

---

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available electronically on the USTRANSCOM electronic library.

**RELEASABILITY:** There are no releasability restrictions on this publication

---

OPR: TCJ3-S  
Supersedes: USTRANSCOMI 31-11, Chapter 6

Approved By: TCJ3 (MG Michael J. Lally, USA)  
Pages: 9  
Distribution: e-Publishing

---

This instruction establishes the policy and procedures for the United States Transportation Command (USTRANSCOM) operations security (OPSEC) program. The OPSEC Program provides guidance for planning, training, education, and evaluation. This instruction applies to all personnel assigned, attached, or contracted to USTRANSCOM, the Transportation Component Commands (TCC), and the Joint Enabling Capabilities Command (JECC). Refer recommended changes and questions about this instruction to the office of primary responsibility using Air Force Form 847, *Recommendation for Change of Publication*. Ensure that all records created as a result of processes prescribed in this instruction are maintained in accordance with USTRANSCOM Instruction 33-32, *USTRANSCOM Records Management Program*.

**1. References and Supporting Information.** References, related publications, abbreviations, acronyms, and terms used in this instruction are listed in Attachment 1.

**2. General.**

**2.1.** The USTRANSCOM OPSEC program supports the combatant commander by ensuring the command actively practices OPSEC to deny critical information to adversaries. The OPSEC program provides for planning, training, education, and evaluation. It is intended to promote an understanding and awareness of OPSEC among all members of USTRANSCOM, TCCs, and JECC. As part of USTRANSCOM's overall security posture, OPSEC aspects will be integrated in activities and operations.

**2.2.** OPSEC responsibilities must be reflected in contracts. Contracts are publicly released documents which can reveal critical information or indicators of critical information.

**3. Responsibilities.**

**3.1. Commander, USTRANSCOM will:**

**3.1.1.** Ensure OPSEC measures are incorporated into all command operations, plans, and exercises.

**3.1.2.** Ensure OPSEC guidance relating to USTRANSCOM operations is provided to all supporting combatant commands, Services, other agencies, and appropriate public affairs offices.

**3.2. OPSEC Manager, Information Operations Branch (TCJ3-SI) will:**

**3.2.1.** Develop, manage, and maintain the Critical Information List which provides critical information of significance not only to USTRANSCOM and the TCC but to supported combatant commands, national agencies, and Services.

**3.2.2.** Provide the day-to-day management of the USTRANSCOM OPSEC program and conduct annual OPSEC program assessments.

**3.2.3.** Provide to Joint Staff J3, Deputy Director for Global Operations, copies of all current OPSEC program directives and/or policy implementation documents.

**3.2.4.** Identify areas requiring additional Chairman of the Joint Chiefs of Staff guidance, assistance or clarification to the Deputy Director for Global Operations.

**3.2.5.** Provide OPSEC lessons learned to Joint Staff J3 and J7 for inclusion in the joint OPSEC lessons-learned database.

**3.2.6.** Advise Director Operations and Plans (TCJ3), Directors, TCCs, and JECC point of contacts on all significant OPSEC issues.

**3.2.7.** Participate in early deliberate and contingency planning to assist in the development of commander's guidance as it relates to OPSEC and to assist in the development and integration of OPSEC measures into the planning process.

**3.2.8.** Maintain membership on the USTRANSCOM Web Steering Group and train each division gatekeeper on critical information.

**3.2.9.** Conduct an OPSEC review of documents prior to posting to USTRANSCOM public access web page or Intranet.

**3.2.10.** Analyze Joint Communications Security monitoring Agency reports for communications security violations resulting in OPSEC issues.

**3.2.11.** Consult with external agencies (i.e., Interagency OPSEC Support Staff, Joint Information Operations Warfare Center) to request assistance with command OPSEC assessments.

**3.2.12.** Provide OPSEC training to all newcomers within 90 days of arrival.

**3.2.13.** Conduct annual OPSEC reviews with TCCs.

**3.2.14.** Provide initial and annual OPSEC training for USTRANSCOM personnel.

**3.3. USTRANSCOM Acquisition, (TCAQ) will:**

**3.3.1.** Ensure unclassified contracts properly reflect OPSEC responsibilities for contractors. These responsibilities entail contractors not disclosing information pertaining to classified contracts to the public.

**3.3.2.** Coordinate with the OPSEC manager for parameters for releasing contract information for bids.

**3.4. USTRANSCOM Force Protection (TCJ3-FP) will:**

**3.4.1.** Ensure classified contracts properly reflect OPSEC responsibilities for contractors. These requirements are normally entered on the DD Form 254, *Department of Defense Contract Security Classification Specification*, as they are imposed in addition to the standard requirements of the National Information Security Strategic Plan.

**3.5. USTRANSCOM personnel will:**

**3.5.1.** Be familiar with the below USTRANSCOM critical information list.

**3.5.2.** Employ sound OPSEC practices daily (i.e., do not discuss critical information over unsecure means, do not dispose of or release critical information in an inappropriate manner, do not discuss or release sensitive or classified information to those who do not have a need to know).

**3.5.3.** Complete annual OPSEC training.

**3.6. The TCCs and JECC will:**

**3.6.1.** Appoint a designated OPSEC POC and provide contact information to the USTRANSCOM OPSEC manager.

**3.6.2.** Manage their programs in accordance with their Service directives, DODD 3600.1, *Information Operations*, CJCSI 3213.01C, *Joint Operations Security*, and Joint Pub 3-13.3., *Operations Security*.

**3.6.3.** Provide an informational copy of their current OPSEC program directive and/or policy implementation documents, as well as annual command OPSEC reports to TCJ3-SI.

**4. Policies and Procedures.**

**4.1.** It is USTRANSCOM's policy to ensure OPSEC practices prevent the inadvertent disclosure or the compromise of critical information, classified, or sensitive programs, missions, activities, capabilities or intentions. OPSEC is a command responsibility. TCJ3 is the Command OPSEC

office of primary responsibility. The Command OPSEC officer/program manager or designated alternate executes day-to-day program management for USTRANSCOM. Compliance with this policy is mandatory.

## **5. Definitions.**

**5.1.** OPSEC is a process of identifying critical information and analyzing friendly actions attendant to defense acquisition, defense activities, military operations, and other activities to:

**5.1.1.** Identify those actions which can be observed by adversary intelligence operatives and adversary intelligence gathering systems.

**5.1.2.** Identify what friendly information is necessary for the adversary to have complete and accurate knowledge of friendly forces and intentions.

**5.1.3.** Determine indicators which could be used, interpreted, or pieced together by an adversary to derive critical information on friendly operations.

**5.1.4.** Deny adversary decision maker's critical information about friendly forces and intentions.

**5.1.5.** Select and execute measures which eliminate or reduce to an acceptable level the vulnerabilities of friendly actions and information to adversary exploitation.

**5.2.** Critical information is information which provides specific facts about friendly intentions, capabilities, vulnerabilities, activities, or missions. Exploitation of critical information by an adversary enables the adversary to plan and act effectively and produce failure or unacceptable consequences for friendly forces.

## **6. OPSEC Characteristics.**

**6.1.** OPSEC is an integral part of Information Operations (IO) and is concerned with identifying, controlling, and protecting the generally unclassified evidence which is associated with sensitive operations and activities. The process of identifying critical friendly information and taking measures to mask those measures from disclosure to adversaries is only one part of a defense in depth approach to securing friendly information. Because critical friendly measures may be disclosed directly or indirectly to adversary sensors or agents, OPSEC must be complimented by supplemental security actions. Supplemental actions to OPSEC include physical security, measures and programs as part of Information Assurance (IA), Computer Network Defense and personnel programs which screen and limit authorized access. OPSEC and other measures secure critical information for military activities in both the physical and information dimensions. OPSEC with other security measures and programs protect friendly critical information necessary for operations throughout all dimensions of military operations.

**6.2.** OPSEC's most important characteristic is that it is a process. OPSEC is an analytical methodology which can be applied to any operation or activity for the purpose of denying critical information to an adversary.

**6.3.** OPSEC is concerned with identifying, controlling, and protecting generally unclassified information or evidence which is associated with sensitive operations and activities.

**6.4.** OPSEC and security programs must be closely coordinated to ensure all aspects of sensitive operations are protected.

**6.5.** OPSEC acknowledges commanders must be prepared to assume some degree of risk when choosing whether or not to execute OPSEC measures. OPSEC measures may entail the expenditure of resources. In choosing to execute particular OPSEC measures, commanders must decide the assumed gain in secrecy outweighs the costs in resources. If commanders decide not to execute certain measures because the costs outweigh the gain, they are assuming risks. The OPSEC process requires decision makers directly address how much risk they are willing to assume.

**7. USTRANSCOM critical information list** provides the consolidated critical information from USTRANSCOM and the TCC, and lists categories of information considered unclassified but of critical operational nature. Critical information is unclassified data revealing friendly intentions, capabilities, activities and vulnerabilities or other information needed by an adversary to cause interference, delay or mission failure of friendly operations and plans. Accordingly, all personnel assigned to or working in support of USTRANSCOM, USTRANSCOM components, subordinate organizations, and mission partners will take caution when discussing details relating to critical information over non-secure telephones or facsimile in public places where conversations can be overheard or electronically monitored, or through unencrypted non-secure internet protocol router network e-mail. The responsibility to protect critical information resides with every individual assigned to USTRANSCOM. The consistent use of the above communication procedures and abiding by USTRANSCOM's shredding policy will improve USTRANSCOM's OPSEC posture.

**7.1.** USTRANSCOM's critical information list comprises the following items:

**7.1.1.** Current and future exercises/operations:

**7.1.1.1.** Details of all current and future operations, missions, exercises, plans, orders, and programs.

**7.1.1.2.** Indications of the above activities occurring or about to occur (i.e., abnormal shift work, increased or unusual communications/activities, or recalls).

**7.1.1.3.** Details of mission-associated information, especially sensitive missions and persons associated with sensitive missions, such as mission capability, personnel/equipment deployment dates, logistics plans, command and control relationships, force structure/composition, and/or locations.

**7.1.1.4.** Exercise planning information including duty rosters, level of effort, and liaisons with external organizations.

**7.1.1.5.** Association of abbreviations, acronyms, nicknames, code words, or mission call signs with projects, plans, operations, or locations.

**7.1.1.6.** Details of agreements and/or arrangements between the USTRANSCOM and external organizations, allies, or coalition partners.

**7.1.1.7.** Research and development activities, science and technology information, and results of experimentation.

**7.1.2.** Personnel, acquisition, and logistics:

**7.1.2.1.** Acquisition support to operations or special activities (including budget information, excluding information readily available in the public domain, planned expenditures, building plans/blueprints, infrastructure improvement, and new capabilities).

**7.1.2.2.** Comprehensive listing of USTRANSCOM personnel and/or organizational code, and/or telephone number, and/or mailing address, and/or email or similar information.

**7.1.2.3.** Diagrams/blueprints/security measures of mission critical facilities.

**7.1.2.4.** Details and locations of assets used in assigned missions including capabilities, the operational use of the assets or their state of readiness.

**7.1.2.5.** Social security numbers of assigned personnel including recall rosters and duty/personnel schedules.

**7.1.2.6.** Manning issues, movements, shortfalls, and projected gains including unfilled billets and their mission impact.

**7.1.3.** Unit/asset/Information Technology critical infrastructure capabilities, vulnerabilities, or degradation:

**7.1.3.1.** Unit or asset capabilities, strengths, weaknesses, gaps, degradations, interdependencies, limitations, or intentions including readiness assessments.

**7.1.3.2.** Operational capabilities or disposition.

**7.1.3.3.** Inspection, evaluation, and testing results which may reveal sensitive capabilities or weaknesses in operational procedures (including security or counterintelligence investigations).

**7.1.3.4.** Details of security procedures, capabilities, and limitations to include the physical security of USTRANSCOM buildings and assets.

**7.1.3.5.** Assessments and perceptions of adversary capabilities and intentions, including success/failure of adversary attacks and attempted attacks (battle damage assessment), intelligence and threat assessments.

**7.1.3.6.** Network system configuration or security measures.

**7.1.3.7.** Details and vulnerabilities of USTRANSCOM command, control, communications, computers, and intelligence systems to include communications systems or network capabilities, architecture/configuration, lists of serial and model numbers, outages, operational status, limitations, passwords, and listings of logins/IP addresses which indicate a pattern.

**7.1.3.8.** Location, operational status and specific capabilities, vulnerabilities or limitations of command and control node.

**7.1.3.9.** A vulnerability or related patch associated with a specific information system or network.

**7.1.3.10.** Listing of information systems or networks with details such as hardware model numbers, locations, and/or serial numbers.

**7.1.4.** Key personnel schedules and travel itineraries:

**7.1.4.1.** US/allied/coalition government movement, transportation, and quartering plans for key civilian and senior military leaders moved by USTRANSCOM (i.e., key leadership and GO/FO/SES/DV schedules).

**7.1.4.2.** Movement of USTRANSCOM GO/FO/SES/DVs including names, daily and routine schedules, detailed itineraries and billeting arrangements.

**7.1.4.3.** Specific temporary duty data, including purpose of travel, number of personnel, duration of stay, location, systems, and itineraries.

**7.1.5.** Emergency or contingency plans:

**7.1.5.1.** Reactions to specific adversary actions or other degradation/outage whether planned or unscheduled (power/network outages/degradation, system-wide network problems, evacuation).

**7.1.5.2.** Details of continuity of operations procedures including critical infrastructure, locations, and capabilities.

**7.1.6.** Changes to or details of normal operating procedures:

**7.1.6.1.** Details of current or any force protection or antiterrorism measures including capabilities, readiness, and rules of engagement for security forces.

**7.1.6.2.** Details of security measures or procedures with other federal, state or local agencies.

**7.1.6.3.** Reasons for or detailed measures taken to respond to defense, readiness, or information condition changes.

**7.1.6.4.** Extraordinary protection measures emplaced to protect critical information.

**7.1.7.** Medical:

**7.1.7.1.** Shortfalls, limitations, and restrictions of medical supplies and medical war reserve material.

**7.1.7.2.** Detailed information regarding medical evacuation.

**7.1.8.** Critical information identified by mission partners.

**7.1.9.** Any information which is identified by other directives as For Official Use Only (FOUO).

**7.2.** All personnel should be familiar with this information in order to appropriately protect USTRANSCOM's Critical Information.

MICHAEL J. LALLY  
Major General, U.S. Army  
Director of Operations and Plans

**Attachment 1**

**GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS**

**Section A – References**

DOD 5205-02, *Operations Security*  
CJCSI 3213.01C, *Joint Operations Security*  
Joint Publication 3-13.3, *Operations Security*

**Section B - Abbreviations and Acronyms**

NOT USED

**Section C - Terms**

NOT USED