All Boxes outlined in RED are required to be filled in/signed.

OPSEC REVIEW CERTIFICATION
(AR 530-1, Operations Security)

STATEMENT BY REVIEWING ORGANIZATIONS

"I am aware that there is foreign intelligence interest in publicly available information. I have sufficient technical expertise in the subject matter to certify that it is appropriate to release this information to the public, because there are no operational, legal or security reasons for withholding its release. Information given a previous OPSEC review may require a second review in case operational circumstances or the original information has changed."

DESCRIPTION OF INFORMATION TO RECEIVE OPSEC REVIEW:

Title of article to be released: _____

(Step 1) Author/Originator (Full Name): _____

Organization: _____

Phone: _____
(Commercial) (DSN)

Forum where this information is to appear: Engineer

Purpose of release: Professional development information
Anticipated date of release: Unknown

(Step 2) Tech Reviewer: (Print full name) _____

Grade:_____ Position: _____Phone: _____

Signature:_____ Date_____

(Step 3) Cdr/Supvr: (Print full name) _____

Grade:_____ Position:_____ Phone:_____

Signature:_____Date:_____

(Step 4) Gov't Contracting Ofc (if applicable)_____

Grade:_____ Position:_____ Phone:_____

Signature:_____Date:_____

(Step 5) Legal Office Reviewer (if applicable):_____

Grade:_____ Position:_____ Phone:_____

Signature:_____ Date:_____

(Step 6) OPSEC Officer (G2/G3) _____ Position:_____

Grade:_____ Position:_____ Phone:_____

Signature:_____ Date:_____

(Step 7) Public Affairs Reviewer:_____ Position:_____

Grade:_____ Position:_____ Phone:_____

Signature:_____ Date:_____

Continued on Page 2 **Required**

OPSEC REVIEW CERTIFICATION
(AR 530-1, Operations Security)
Continuation

	Author	Tech Reviewer	Cdr Supvr	Gov't Contract Officer	Legal	(OPSEC Off)	Public Affairs
a. Concur for Public Release							
b. Concur for Public Release w/comment							
c. Nonconcur							

Initial and date in the appropriate box

a. Recommend approval for public release, distribution is unlimited (Distribution A).
b. Recommend approval for public release subject to changes as noted or attached.
c. Do not recommend public release.

OPSEC Review Process

An operational security (OPSEC) review is intended to evaluate government information (document, videotape, voice tape, briefings, articles or equipment) to determine if it can be designated for unclassified and unlimited (public domain) distribution. The purpose of an OPSEC review is to ensure the continued protection of government information, which for operational, legal or security reasons is considered sensitive or critical information that should not be released to the public.

Before a government employee or contractor can release U.S. government information to the public, it must have an OPSEC and Public Affairs review.

OPSEC review Steps:
Step 1 - Author prepares information for public release.
Step 2 - A technical expert reviews the prepared product for accuracy IAW the federal Quality of Information Act (can be the author).
Step 3 - Government commander/supervisor reviews and approves product for release (cannot be the author).
Step 4 - Government contracting officer reviews **only if contractor or proprietary information** is involved.
Step 5 - Legal office reviews **only if contractor or proprietary information is involved.**
Step 6 - OPSEC (G-2/G-3) reviews for operational security, security classification and foreign disclosure. (OPSEC will provide release approval on STA Form 7114 and return product to originator for release.)
Step 7 - Public Affairs Office reviews for context and if product is consistent with Army mission.
Step 8 - A copy of the STA Form 7114 and a hard copy of the product will be retained by the originator, and a copy will be forwarded for publication. (Article without the STA Form 7114 and this form will not be accepted.)

Examples of potentially inappropriate information for public release.

D Equipment capabilities, limitations, vulnerabilities.
E Detailed mission statement.
F Operation schedules.
G Readiness and vulnerability assessments.
H Test locations and dates.
I Inventory charts and reports.
J Detailed budget data.
K Internal installation maps and photographs.
L Standard operating procedures (SOPs) and tactics, techniques and procedures (TTPs).
M Detailed personal biographies.
N Detailed organization charts (with phone and email listings).
O Sensitive unclassified reports for internal Army use.
P Technical and scientific proprietary data developed by a contractor.
Q Unclassified technical data with military applications.
R Critical maintenance information.
S Information extracted from an intranet Website.
T Personal information pertaining to individuals.
U Lessons-learned that could reveal sensitive military operations, exercises or vulnerabilities.
V Movement of assets where uncertainty of location is a program or operational element.
W Logistics support (munitions, weapons movement).
X Specific, real-time support to current/ongoing military operations.