Air Force Security Review Handbook

Provided by

Secretary of the Air Force
Office of Public Affairs
Security Review

Security Review Guide

A recognized and undisputed fact is that the American public has both the need and the right to know about our Air Force. This knowledge is limited only to the extent that it does not compromise national security and the safety of our people. The Air Force, therefore, has the responsibility to inform the public of its operations and accomplishments.

THE REVIEW PROCESS

Security Review represents an on-going effort to inform and increase the public understanding of the mission, operations and programs of the Air Force. It is a service provided by Public Affairs to ensure that the information is released quickly, and that it is unclassified, accurate, and conforms to established Air Force and Department of Defense policies. Obviously, grave harm to our nation and those serving in the Armed Forces and their families, can occur through unrestricted open access to national security information.

The title "Air Force Security Review" is somewhat misleading. It implies that the review is solely to determine whether classified information is present. The DoD directive that governs the function (DoD 5230.9) is very specific — "material submitted by DoD personnel…shall be cleared for conflict with established DoD and Government policies and programs." What does this mean?

ACCURACY: Information that is released by AF people must accurately reflect the policies, positions and programs of the Department of Defense and the Air Force. Since policy, budget status, programs, etc. are constantly shifting, and Congressional direction in many areas is received throughout the year, Security Review serves as a check to ensure that released material is current and accurate.

ESTABLISHED UNITED STATES POLICY: Quite frequently, the topic of the information to be released is the primary responsibility vested in other Executive Branch departments such as the Department of State, NASA, EPA etc. Coordination with these agencies is accomplished only through DoD levels and often takes much longer than the average case review.

BALANCE: When other services or government agencies may hold differing views about an issue or topic, the best way to gain approval is to have a balanced presentation. Differing views may be included but should be stated as such. A one-sided presentation usually meets great resistance within DoD.

A fine balance between disclosure and non-disclosure can be attained through the use and enforcement of programs already in existence. The directives governing the review of material are not intended to prevent information from being released, suppress people from expressing their opinions and ideas, or conflict with policies concerning openness in government. Security and policy considerations are the only basis for deciding to release the information. **DECIDING WHETHER TO RELEASE, WHEN TO RELEASE, HOW TO RELEASE AND TO WHOM TO RELEASE THE INFORMATION ARE NOT SECURITY REVIEW DECISIONS.**

DELEGATION OF CLEARANCE AUTHORITY

The objective of the security review process at all levels is the maximum clearance of information in minimum time. In support of this objective Air Force policy provides for clearance by the Public Affairs Office at the lowest level where competent authority exists to judge the security and policy aspects of the information submitted for review. In the case of "Electronic Commerce", SAF/AQ is the authority for policy and guidance governing the review and release of *information made available on public web sites in the conduct of electronic commerce*.

SUBMITTING MATERIAL

Who

All Air Force military and civilian personnel, including Air National Guard and Air Force Reserve personnel on active duty or who are writing or speaking on topics related to their active duty assignments must submit information for security review. Former members and retired personnel are encouraged to use this review service to make sure that information they intend to release to the public is consistent with national security.

What

Information in any form proposed for public release concerning plans, policies, programs or operations of the Department of the Air Force, Department of Defense or the Federal Government. Information released electronically, to include Home Pages and responses to electronic mail queries must be cleared in the same manner as hard copy information. Information already in the public domain need not be reviewed again unless it has been updated, revised, added to or is to be presented in a new context.

Where

Information that cannot be cleared locally should be elevated through normal Public Affairs channels. Submissions in the following categories must be forwarded through channels to the Department of Defense:

- Concerning topics of national interest or foreign policy
- Originates or is proposed for release at the seat of U S Government (Washington, DC area) (Technical papers may be exempt, if no other factor requires a DOD review)
- Creating possible inter-service controversy
- Concerning plans, policies, programs, or operations of the Federal Government
- Directed by higher authority
- On other subjects where doubt exits

When

Submit with enough lead time to allow ten workdays for review in SAF/PAS plus transit time. Complex and/or lengthy submissions may require more review time.

How

Include with or attach to each package a memo with enough information to staff your package. See the attachment for a sample memo.

How Many

- Sufficient copies for expeditious review to reach SAF/PAS as follows:
- Still photos and captions — 10 copies. Photocopies must be of high quality to be accepted
- Videotapes — 2 copies of videotape and 10 copies of script
- Speeches — 10 copies
- Other printed materials or floppy disks — 10 copies

RESPONSIBILITIES OF THE PUBLIC AFFAIRS OFFICE

Security Review is the responsibility of the Public Affairs Office. The scope of this function will vary with the size and mission of the unit or organization. The task may require a few hours a week in one office or the full-time services of one or more individuals in another. It is best to designate one individual as primarily responsible for the security review function.

Responsiveness and good administrative practices are keys to an effective review system. A staffing system should be established through the appropriate staff and other agencies to obtain expert coordination. The Public Affairs Office must get these agencies to agree to a minimum practical suspense for the coordination of review submissions. A log is essential for maintaining continuous control of documents.

Get enough copies from the submitter to allow simultaneous review by the coordinating agencies. These copies should be hand-carried to ensure accountability of the packages and to minimize the time required for the movement of documents. When possible, call ahead to expedite the processing of requests. Make arrangements with staff agencies for expedited handling of the occasional hot item.

Each office should establish a database reference and either an electronic or hard copy file with a minimum of two years of cleared information for research purposes.

After the copies have been returned, reconcile the recommendations of coordinating agencies. The Public Affairs Office has the authority to over-ride the recommendation of a coordinating agency whose position is not or cannot be sufficiently substantiated.

Clear, amend, disapprove, or forward submitted information to higher headquarters, as appropriate (use the marking procedure specified in the next section for coordinators). Disapproval authority must not be delegated to an administrative or command level not functionally competent to assess the content. To keep the process functioning effectively, keep your submitters apprised of the requirements and characteristics of the system. Remember: reviewers should not be identified to submitters without the permission of the coordinator.

Inter-command and Inter-agency coordination

Major Commands should work with each other to obtain inter-command coordination. If the material also requires SAF/PAS review, please indicate what coordination was accomplished in the cover letter. Material requiring review/ coordination by another agency such as NASA, DARPA etc. should also be sent to SAF/PAS. Some units work with and are co-located with organizations from another federal agency. If their coordination is required, obtain it and send it to SAF/PAS if the material warrants.

Electronic Submittal

If Security Review is being processed electronically at your location, care must be taken to ensure protection of the material should classified information be discovered. Some bases use an Intranet system to review and coordinate prior to clearance and publication/posting on the web. At the present time, SAF/PAS is unable to accept electronic submission of cases for review. There are several reasons. First, cases often contain classified material and the email/Internet system we are linked to is not secure (dot mil is not a secure system). Second, many of the cases sent to us for review must be forwarded to DoD and other agencies. They are not accepting electronic submittals at this time.

Speeches/Presentations by high-ranking individuals

A speech or presentation by an individual, who by virtue of rank, position or expertise would be considered an official DoD spokesperson (generally, persons at the Assistant Secretary of the Air Force level or above, or, at the rank of Major General or above) must be submitted for security and policy review a minimum of three working days before the event. Additional time may be needed for complex or potentially controversial speeches or presentations. SAF/PAS forwards these speeches/presentations to DoD/DFOISR for review. Specific criteria, any one of which requires review at DoD, are found in DoDI 5230.29.

Appeals

Appeals are encouraged and vigorously pursued when the submitter can provide compelling rationale or introduce additional factors supporting release not known at the time of turndown. The Public Affairs Office that turned down the request must work the appeal and make the final decision. This may require some close work with the staff agency that made the original objection.

Obligations to the Submitter

Timely coordination, use of BLACK for marking, and the use of source citations are major security review time-savers and are part of our responsibility to the submitter. An explanation of reasons for turndown or amendments to the submitted material with a provision for information that will help to remove objections so that the item can be cleared upon resubmission are another responsibility of the review process and will help ensure the maximum clearance of information in the minimum time.

RESPONSIBILITIES OF REVIEWERS

Identification

We ask the reviewing officer to identify information that is not releasable, i.e., information that is CLASSIFIED, or violates official POLICY.

Marking

Brackets, in BLACK, are the shorthand for identifying non-releasable information. With brackets the coordinating officer is telling the Public Affairs Officer what material should be removed prior to the public release of the document. Brackets signal a mandatory AMENDMENT. Substitute language may be written above the brackets, in BLACK.

Security Review Guide

Amending

AMENDMENTS require the support of specific source citations and rationale. Because the security review process is geared to maximum disclosure, Public Affairs Officers may be asked to defend AMENDMENTS. The reviewing officer must provide sufficient information to enable the Public Affairs Officer to substantiate an AMENDMENT. Proper documentation will eliminate time consuming discussion between the Public Affairs Officer and the reviewing officer.

Source Citation

Frequently cited classified sources include security classification guides, provisions of contracts (DD-254), AF Policy Directives, manuals, Selected Acquisition Reports, development concept papers, source documents or information originators. When the reviewer identifies classified material, the Public Affairs Officer must be notified (he or she will in turn notify other agencies having the document). Immediately, everyone possessing the document must protect it as classified. POLICY sources may be: Presidential announcements, official pronouncements of DOD and AF leaders, AF Policy Directives and manuals, or policy letters. Occasionally, policy is not documented, yet has an identifiable source.

Objection

The reviewer may also make an OBJECTION to approving a document for public release. An OBJECTION requires no marking on the document; however, it must have justification on the same basis as an AMENDMENT or a rewrite for security or policy. An OBJECTION may be made on documents that require such extensive AMENDMENTS or rewrite for accuracy that the changes to permit publication would be impractical.

Editorial Review

EDITORIAL REVIEW is not a responsibility of security review; however, clarity and accuracy are important to the credibility of the information. Reviews should be encouraged to make constructive editorial comments. Editorial amendments (deletions) are lined through once in BLACK. (Do not use brackets.) Correct information should be entered in BLACK. An OBJECTION may be made on documents that require extensive AMENDMENTS or rewrite for accuracy.

Other Reviews

If the reviewer thinks the document needs additional coordination, he or she should immediately notify the responsible Public Affairs Officer. This call could save several days in the review process; the submitter will appreciate the savings.

Maintaining/ Reproducing Copies

It is critical that no copies be kept or reproduced during the coordination process without the express permission of the Public Affairs reviewing authority.

REVIEW CONSIDERATIONS

There are many criteria that must be considered when deciding to release information to the public. Some are governed by public law, others by Executive Orders, Department of Defense and Air Force policies and regulations.

Copyrighted Material

United States laws on copyright, primarily 17 USC 101, et seq., preserve for the owner of copyrighted material the benefits and earnings to be derived from the reproduction and distribution of such works. Material that is subject to copyright protection includes "original works of authorship fixed in any tangible medium…" 17 USC 102(a). It is now accepted that computer software, sequences of code, and instructions, are in fact, subject to copyright.

Legal

Release of copyrighted information via the Internet or other media without authorization of the copyright owner is prohibited. This includes and is not limited to:

- Software distribution of shareware, copyrighted software, etc.
- Graphic images such as symbols, pictures, buttons, and cartoons, e.g. Disney or Hanna Barbera characters, etc.
- Copyrighted text such as published articles, excerpts from published manuals etc. (Reference—AFI 51-503; AFI 33-360)

Security

Operational Security or OPSEC is a process of identifying and analyzing friendly actions attendant to military operations and other activities to:

- Identify those actions that can be observed by potential adversaries
- Determine indicators that could be interpreted or pieced together to derive critical information in time to be useful to an adversary
- Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to exploitation by an adversary

In short, OPSEC provides a step-by-step analysis of operations and behavior, from an adversary's point of view, to determine how to exploit our vulnerabilities. Information that adversaries need to achieve their goals to our detriment constitute the critical information of our operation or program. By identifying and denying this information, we deny any potential adversary an advantage.

The OPSEC analysis examines the planning, preparation, execution, and post execution phases of any activity, across the entire spectrum of military activity, and in any operation environment. Air Force commanders and decision makers should consider OPSEC during both mission and acquisition planning. In fact, the Air Force implements the OPSEC process in all functional areas (AFI 10-11).

Aggregation

Increasingly, the combination of individual and seemingly disparate items of unclassified and non-sensitive information can reveal a “composite” or “mosaic” picture that is sensitive or even classified. The development of Internet search engines and data-mining technology has increased this threat exponentially. For example, individual stock orders may be unclassified and non-sensitive; however, all stock orders for the USAF may be sensitive. Combine that information with operations and/or deployments and it’s classified.

Reviewers must look at information not only on its own merits but also against this larger context. Ask yourself if the information can be combined with other data to provide an advantage to a potential adversary or reduce our edge on the battlefield. Similarly, ask if the data can be added to other data to violate privacy or other statutory protection requirements. There is nothing precise here. It’s often a subjective call. If you have any doubts, protect the information and contact persons who might have knowledge of the potential aggregation problem.

Scientific And Technical Information (STINFO)

The purpose of the STINFO program is to ensure that scientific and technical information makes the maximum impact on the development of Air Force technology, and to ensure that the scientific and technical information generated under Air Force contracts and programs makes maximum contribution to the national economy.

American technology is a valuable commodity and is greatly sought after. Technology in its basic research form is openly distributed and exchanged. However, technology that is nearing application to a military weapon system(s) is considered sensitive as it discloses too much about that potential system. STINFO Officers are responsible for reviewing reports etc. and determining which distribution statements should appear on the data. Only reports determined to be “Statement A” can be forwarded for security and policy review and then considered for release to the public. This is the only technical information that should be considered for a public release. (AFI 61-204)

Security Review Guide

Technology Transfer is a term used to denote the uncontrolled export or disclosure of advanced technology by the US to foreigners. This problem is significant and a public release, either through print, video or the use of web sites may provide easy access to our critical data. If the information is critical to the military and released to the public, the United States could lose its critical edge in that particular area. The Department of Defense and other agencies of the Federal Government have created a series of controls that are in use throughout the review process. Note: Civilian agencies use this term to describe the sharing of Government technology with industry, the program the Defense Department refers to as Domestic Technology Transfer

The **Militarily Critical Technologies List** (MCTL) is published by DoD and used as a reference document, not as a strict regulation or decision tool. It is a guideline listing of those technologies that are critical to the security of our nation. Information cannot be withheld from release solely on the basis that the information is cited on the Militarily Critical Technologies List. It is not recognized or used as an export control list.

International Traffic-in-Arms Regulations (ITAR) is a series of State Department regulations that lists technical data about arms and munitions prohibited from export. It includes any unclassified information that can be used, or be adapted for use, in the design, production, manufacture, repair, overhaul, processing, engineering, development, operations, maintenance, or reconstruction of arms, ammunition, and implements of war contained in the US munitions list.

Export Control Laws are the responsibility of the Department of Commerce, and were established to provide export control policies and practices. A validated license is required from the Department of Commerce for the export of all technical data listed on the Commerce Control List. Care must be taken as clearance of information for public release will allow unlimited distribution of information and may bypass the export control laws that validate information for a designated location and a specific end user.

Basic Research. For purposes of Security Review, basic research is research performed by a university or industry (6.1 funded) or performed on campus at a university (6.2 funded). These efforts generally do not require review under this security review program unless the program manager determines that release of this information may circumvent Export Control laws and regulations, or the research is so tied to military applications that a review is warranted.

FREEDOM OF INFORMATION and PRIVACY ACTS

The Air Force Freedom of Information Act program, as described in DoD 5400.7-R and AFI 37-131, states the public may inspect, review, and receive copies of Air Force records. This applies to all records except for those exempt under the Act. The exemptions fall into 9 categories of information:

1) Classified Records
2) Internal Personnel Rules and Practices
3) Other Laws / statutes
4) Confidential Commercial Information
5) Inter or Intra Agency Records
6) Invasion of Personal Privacy (Privacy Act)
7) Investigative Records
8) Financial Institutions
9) Wells - geological/geophysical information

REFERENCES

AFI 10-1101 Operations Security
AFPD 16-2 Disclosure of Military Information to Foreign Governments and International Organizations
AFPD 16-11 International Technology Transfer and Security Controls
AFI 33-129 Transmission of Information via the Internet
AFI 35-101 Security and Policy Review
AFPD 36-601 Industrial Security Program Management
AFI 37-131 Freedom of Information Act Program
AFI 37-132 Privacy Act Program
AFI 61-204 Dissemination of Scientific and Technical Information
DoD 5200.1-R Information Security Program Regulation
DoD 5200.22 Industrial Security Program
DoD 5330.9 Clearance of Information for Public Release
DoD 5230.25 Withholding of Unclassified Technical Data from Public Disclosure
DoD 5400.7-R DoD Freedom of Information Act Program

CHECKLIST FOR APPROVING/CLEARING INFORMATION:

Is the Information:

❑ Unclassified, not sensitive (FOUO), accurate and suitable for release?

❑ Timely, accurate and current?

❑ Coordinated with the appropriate OPSEC monitor? (AFI 10-11)

❑ Does the information proposed for release provide details on military operations or activities (including lessons learned, analysis of operations, unit movements or plans etc.) which, if combined with other information already in the public domain, would compromise planned or ongoing operations? (DoD 5200.1-R para 2-400)

❑ Subject to Privacy Act restrictions? (AFI 37-132)

❑ Information, the release of which would be a clearly unwarranted invasion of personal privacy to include the following categories about US citizens, DoD employees and military personnel:

- Social Security numbers, Dates of Birth, home address, telephone numbers other than duty offices that are made available to the general public.
- Duty phone numbers of units described in C.3.2.1.6.2.2 of DoD 5400.7R-(reference (j) may not be posted.
- Names, locations and other identifying information about family members
- Official travel itineraries of individuals and units before or while it is performed?

❑ Subject to the Freedom of Information Act restrictions or exemptions? (DoD 5400.7-R/AFI 37-131)

❑ Suitable to bear Distribution Statement “A” (AFI 61-204)

❑ No Scientific, technical, research and development information covered by AFI 61-204

❑ Contain copyrighted material without written permission from the owner?

❑ Contain a commercial trademark, logo or other information that implies endorsement of a non-federal entity or product.

❑ Does the information contain Export Controlled technical data involving military or space applications meeting the requirements of ITAR, para 120.10

- Information required for design, development, production, manufacture, assembly, operation, repair, test, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions and documentation. It does not include information concerning general scientific, mathematical or engineering principles taught in schools, colleges or universities or information in the public domain.
- Classified information relating to defense articles and defense services
- Information covered by an invention secrecy order.
- Software as defined in the ITAR para 121.8f directly related to defense articles

NOTE: Export controlled technical data is exempt from public release. Reviewers should state that this information should not be released to the public and cite a specific reference such as Exemption 3 of the FOIA, Export Control Laws -Title 22, USC 2751 etc. (see DoD 5230.25 or AFI 64-204)

□ Does this document contain proprietary data? If yes, then coordination and approval must be obtained in writing by the person or agency with proprietary interest.
□ Does the information contain FOIA exempt data?

AFHQ Form 0-201

Reviewer clearing release of information should indicate their coordination in block 12 and complete blocks 13-15. This allows SAF/PAS to direct specific questions to the appropriate reviewer.

SAMPLE COVER LETTER

Date

MEMORANDUM FOR SAF/PAS

FROM:

SUBJECT: Security and Policy Review

1. The attached material, described below, is forwarded for security and policy review in accordance with AFI35-205:

TITLE: (*exact title and medium of the document. Example: speech, article, book, report. Please indicate number of pages*)

AUTHOR/ORGANIZATION: (*who is presenting the speech, who wrote the article, etc*)

PRESENTATION TO: (*if being presented, to whom: general public, conference, symposium, etc*)

DATE: (*when will this document be published or presented*)

LOCATION: (*where will this document be published or presented or N/A*)

PUBLICATION IN: (*or N/A*)

SUBMITTAL DEADLINE: (*or N/A*)

REQUEST REPLY BY: (*the date you would like a response or normal review time. Standard is 10 working days. NO ASAP*).

2. This line is for any comments or recommendations you may have in reference to the document you are submitting for review. Note if any coordination has been performed in your organization. Also, include the POC and telephone number for the document.

SIGNATURE
(*requester or submitter*)

Attachment
10 copies (*required*)