

**BY ORDER OF THE SECRETARY
OF THE AIR FORCE**

AIR FORCE INSTRUCTION 35-102

4 MAY 2016

Public Affairs

**SECURITY AND POLICY
REVIEW PROCESS**



COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at www.e-Publishing.af.mil for downloading or ordering

RELEASABILITY: There are no releasability restrictions on this publication

OPR: SAF/PA

Certified by: SAF/PA
(Col Robert Ricker)

Supersedes: AFI 35-102, 20 Oct 2009

Pages: 15

This instruction implements Air Force Policy Directive (AFPD) 35-1, Public Affairs Management. It provides guidance for the release of accurate information that does not contain classified material and does not conflict with established Air Force, Department of Defense (DoD), or U.S. Government policy. It also implements DoD Instruction (DoDI) 5230.29, Security and Policy Review of DoD Information for Public Release. Read this instruction with Joint Publication 3-61, Public Affairs. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, Recommendation for Change of Publication and route AF Form 847s from the field through the appropriate functional's chain of command. This instruction also applies to the Air Force Reserve Command (AFRC) and the Air National Guard unless specifically noted. The authorities to waive wing/unit-level requirements are identified with a tier number ("T-0, T-1, T-2, T-3") following the compliance statement. See AFI 33-360, Publications and Forms Management, Table 1.1, for a description of the authorities associated with tier numbers. Submit requests for waivers through the chain of command to the appropriate tier waiver approval authority or to SAF/PA for non-tiered compliance items. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, Management of Records, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS).

SUMMARY OF CHANGES

This instruction has been substantially revised and must be completely reviewed. Major changes include: identifies (1) tiered waiver authorities for wing/unit level requirements, (2) adds Air Force Installation and Mission Support Center (AFIMSC) security and policy review responsibilities, (3) reorganizes and streamlines content to improve clarity.

1. Purpose and Objectives of Security and Policy Review. Security and policy review represents an ongoing effort to inform and increase public understanding of the mission, operations, and programs of the Air Force. The purpose of the security review is to protect classified information, controlled unclassified sensitive information, or unclassified information that may individually or in aggregate lead to an unauthorized disclosure or controlled unclassified information which can adversely impact national and operational security. The purpose of the policy review is to ensure no conflict exists with established AF, DoD, or other U.S. Government agency policies. The objective of the Security and Policy review process is to ensure the maximum clearance of information in minimum time. The Public Affairs Officer (PAO) at the lowest level where competent authority exists oversees all aspects of the security and policy review of information submitted.

1.1. Public Affairs Officers should coordinate with Operations Security Officers and any other person engaged in security of classified or controlled unclassified information to ensure security and policy reviews are properly processed for release.

1.2. Public Affairs Officers who suspect unauthorized disclosures of classified and controlled unclassified information will report the occurrence to the Wing Information Protection Office in accordance with AFI 16-1404, Air Force Information Security Program. (T-1)

2. General Guidelines.

2.1. Maximum Disclosure. The Air Force is committed and supports the policy of maximum public disclosure about Air Force operations and activities. Air Force PA offices will clear, without delay, the maximum amount of information at the lowest competent and review level. (T-0)

2.2. Clearance Authority. Authority and direction for the conduct of security and policy review is derived from Executive Order 13526, Classified National Security Information, and DoDI 5230.29, Security and Policy Review of DoD Information for Public Release.

2.2.1. Clearance versus Release. The security and policy review process determines the suitability for public release of information. A clearance does not grant an approval to release the information. Release of information is the decision of the originator of the document, often reached through the coordination with his or her chain of command. While the security portion of the security and policy process identifies classified or sensitive information, it does not classify or declassify information.

2.2.2. Air Force material submitted for review may be released to the public domain only after it has been reviewed for security and policy consistency and cleared by an appropriate authority in Public Affairs.

2.2.3. Originators must not release copies of the material outside official channels until the security and policy review authority determines the document is cleared for the public

domain. **(T-0)** To protect against inadvertent public release, distribution of documents under review should be limited until the review is complete.

2.2.4. Disclosure of administrative errors, differences of opinions, or ineptitude are not grounds for a denial of public release.

2.2.5. Air Force offices and functional elements are expected to render expert opinion during the review process and must provide prompt response, guidance, and assistance to the security and policy review authority. **(T-2)**

2.2.6. Air Force personnel should make no commitments, including date of delivery, or to furnish abstracts or manuscripts to non-military publications until cleared through security and policy review channels.

2.2.7. PA offices should be active in educating Airmen about information that must be cleared, regardless of the medium that is used. Often, commanders must approve information for release about the installation's activities. **(T-2)**

3. Major Commands (MAJCOM), Field Operating Agencies, Direct Reporting Units (DRU), and wing-level organizations. Clearance authority should be delegated to the Public Affairs organization at the lowest echelon qualified to evaluate the contents and implications of the subject.

3.1. The Public Affairs organization with security and policy review authority will clear unclassified information of local or regional interest. **(T-1)** This includes speeches, presentations, papers, multimedia and visual information material, and information proposed for release to a publicly accessible web site with the exception of Air Force publications. PA public web site management guidance can be found in AFI 35-107, Public Web Communications.

3.2. The local commander or designated representative clears news or photos of national interest.

4. Air Force Installation and Mission Support Center (AFIMSC). The AFIMSC/PA office, under the direction of AFMC, will serve as the single intermediate headquarters for information originating at the wing-level that requires higher headquarters review by all major commands except Air Force Reserve Command and Air National Guard.

4.1. Active-duty wing-level PA offices that require higher echelon security and policy review of information proposed for release will forward the material to AFIMSC/PA. **(T-2)**

4.2. AFIMSC/PA will develop and distribute guidance to the MAJCOM/PA offices, to share with their subordinate organizations, to detail the process for submitting cases for Security and Policy Review to AFIMSC. For questions, contact AFIMSC/PA at DSN 969-1668/Commercial 210-395-1668.

4.3. AFIMSC/PA will coordinate clearance with the appropriate MAJCOMs, or AFIMSC subject matter experts, as required and forward material to SAF/PA that cannot be cleared at the intermediate level.

5. What Must Be Submitted. Department of Defense Directive 5230.09, Clearance of DoD Information for Public Release, requires information relating to the plans, policies, programs, or operations of DoD or the U.S. Government proposed for public release is sent through PA channels to the next echelon appropriate for review. Whether information is prepared as an official release or a personal enterprise, it must be reviewed and cleared before release. **(T-0)** Originators must ensure disclaimers accompany all documents they authorize in a private capacity. **(T-0)** An appropriate disclaimer is: “The views expressed are those of the author and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, or the U.S. Government.”

5.1. All Air Force military and civilian personnel, including Air National Guard and Air Force Reserve personnel on active duty, who release material related to their active-duty assignment, retired military members, and former Air Force civilian employees will use this review process to ensure DoD-related information released to the public is consistent with their requirement to safeguard classified material. **(T-0)**

5.1.1. Commander/Directors will ensure all active duty military, civilian, and contractor personnel assigned to their organization are briefed on this requirement. (T-1)

5.2. Contractors. Contractors must submit material proposed for public release for review according to valid contract requirements as specified in *Defense Department (DD) Form 254, Department of Defense Contract Security Classification Specification, DoD 5220.22-R, Industrial Security Regulation, and DoD 5220.22-M, National Industrial Security Program Operating Manual*. **(T-0)**

5.3. **DoD School Policy.** DoD gives its personnel in its school environments the widest latitude to express their views. To ensure a climate of academic freedom and to encourage intellectual expression, students and faculty members of an academy, college, university, or DoD school are not required to submit papers or material that are prepared in response to academic requirements and not intended for release outside the academic institution. Information proposed for public release or made available in libraries or databases or on web sites to which the public has access shall be submitted to Air University (AU) for review. AU will perform security and policy review for Air Force schools under its purview including Air Force Institute of Technology (AFIT).

6. Secretary of the Air Force Office of Public Affairs (SAF/PA) and/or Defense Office of Prepublication and Security Review (DOPSR) Clearances. Originators must receive SAF/PA or DOPSR approval for the following types of material requesting public release: **(T-0)**

6.1. Originates, or is proposed for release, in the Washington D.C. metropolitan area. This policy does not apply to technical papers intended for presentation at conferences or meetings that do not fall under other categories of required submission. When in doubt, submit.

6.2. Is, or has the potential to become, an item of national or international interest. All three- and four-star general officers and their civilian equivalents' written and oral public presentations are considered to be “of national and international interest.”

6.3. References President and Secretary of Defense authority.

- 6.4. Affects national security policy or foreign relations.
- 6.5. Concerns subjects of potential controversy among DoD components or with other Federal agencies.
- 6.6. Is information that is presented by a DoD employee who, by virtue of rank, position, or expertise, would be considered an official DoD spokesperson. This information requires DOPSR approval. All three- and four-star generals and their civilian equivalents are considered DoD representatives. Information presented by general officers and civilian equivalents that contains only information that has been previously cleared or released by the Air Force, such as Air Force messages or restatements of the Air Force policies, may be cleared locally.
- 6.7. Contains technical data, including data developed under contract or independently developed and controlled by the International Traffic in Arms Regulations (ITARs) that may be militarily critical and subject to limited , but on which a distribution determination has not been made.
- 6.8. New weapons or weapon systems, significant modifications or improvements to existing weapons or weapon systems, equipment, or techniques.
- 6.9. Military operations, significant exercises, and operations security.
- 6.10. Military activities or applications in space, nuclear weapons, including weapon-effects research; chemical and biological warfare issues; biological and toxin research; high-energy lasers and particle beam technology; and arms control treaty implementation.
- 6.11. Any other contemporary topic that is designated by DOPSR.

7. Information Not Requiring Review.

- 7.1. Information not involving DoD operations or personnel.
- 7.2. Personal letters to the editor, book or theatrical reviews when expressing a personal opinion, and works of fiction (short stories, novels, and plays) that are not derived from DoD experience. However, such information must not imply Air Force or DoD sanction. When there is doubt as to the sensitivity of the information, submit it for review.
- 7.3. Air Force Publications. Air Force publications are not submitted for security and policy review. It is incumbent upon the OPR to ensure the content is unclassified and suitable for public release and posting to a public web site. Detailed instructions for all facets of publications and forms management can be found in AFI 33-360, Publication and Forms Management.

8. What Cannot Be Written About. Air Force military and civilian personnel may write articles for open publication, unless such activity:

- 8.1. Conflicts with the public receiving prompt and complete information on government activities through the media.
- 8.2. Violates laws or policies.
- 8.3. Violates ethical standards or does not comply with *DoDD 5500.7, Standards of Conduct and DoD 5500.07-R, The Joint Ethics Regulation (JER), including Changes 1-7.*

8.4. Uses official DoD information generally not available to the public and that would not be released under *DoD 5400.7-R, Freedom of Information Act (FOIA) Program*.

9. Submitting Material for Review. For planning purposes, allow at least 10 workdays for SAF/PA-level review and clearance and at least 20 workdays for DOPSR and other Federal agency review and clearance. The length, complexity, and content shall determine the number of reviewing Agencies and, consequently, the time required for the complete review process. SAF/PA requires five paper copies of the full and final text of all materials for Air Force-level review and clearance. Drafts, notes, outlines, briefing charts, etc., may not be submitted as a substitute for a complete text. If a submission requires DOPSR clearance, SAF/PA will submit it.

9.1. Electronic Submittal. Do not submit items for clearance via e-mail to SAF/PA (Headquarters Air Force). This system does not permit for official use only (FOUO) information review and often sensitive/classified information is discovered during the security and policy review process. The only exception will be made for news releases, and general officer and civilian equivalent speeches and presentations. Please submit the S&PR request a minimum of 3 workdays before event.

9.1.1. To expedite review and clearance, each package submitted must include a memo containing: **(T-1)**

9.1.1.1. Name, title, and organization of originating unit, author, or speaker.

9.1.1.2. Title of article or presentation.

9.1.1.3. Statement on where, when, and how the information is to be released and the sponsoring organization, if appropriate.

9.1.1.4. Required suspense date for release determination. If suspense date is earlier than date of presentation or publication, give reason.

9.1.1.5. Statement that the information has been reviewed at the appropriate lower level and is recommended for public release.

9.1.1.6. Signed or initialed notation by author or speaker indicating approval of the text.

9.1.1.7. When applicable, include a statement on technical material that outlines restrictions and militarily critical technologies as well as a statement that current Air Force and DOD policies have been considered.” Provide all relevant comments from field unit technical coordinators and attach contractor transmittal letter, if it contains pertinent data.

9.2. Technical Materials. For technical papers, include an abstract in layman’s terms and, if appropriate, tell why releasing the information is important to DoD. An abstract to be published in advance also must be reviewed for clearance. Clearance of an abstract does not fulfill the requirement to submit the full text for clearance before its publication. If an abstract is cleared in advance, always state the previously cleared abstract case number when requesting review of the full text.

9.3. Classified references are not recommended because they provide intelligence “shopping lists” and are not available to the general public.

9.4. Generally, previously cleared information does not need to be submitted for review unless it contains substantial changes or it is used in conjunction with other unclassified material. Previously cleared unclassified information may inadvertently be combined in such a manner that together, the new product becomes classified or raises policy concerns.

9.5. Speeches and Presentations. Speeches and presentations can be submitted in bullet format if the essence of the information is apparent to the reviewer. The clearance of bullet-format material will, however, cover only that information presented for review and does not include extemporaneous remarks made during the presentation. Full text and proposed narrative is strongly recommended.

9.6. Website Publication. Information intended for placement on websites or other publicly accessible computer servers that are available to anyone requires review and clearance for public release. Review and clearance for public release is not required for information to be placed on DoD controlled websites or computer servers that restrict access to authorized users. Ensure websites are registered. Registration process is cover under AFI 35-107.

10. Recommended Program Guidelines. PA offices should appoint one security and policy review authority to operate the program. PA offices should keep potential submitters informed about review requirements and procedures and establish working relationships with staff agencies assisting in the review process. Coordinators must understand thoroughly the purpose of and their responsibility for security and policy review. **(T-1)**

10.1. The following are recommended program guidelines at an installation:

10.1.1. Keep a status log on information being reviewed. The system of choice is the Public Affairs Information Release System (PAIRS). SAF/PA and AFIMSC/PA can provide access, guidance and training on PAIRS.

10.1.2. Maintain an effective suspense system. Allow 10 workdays for normal coordination of cases through the organization. Coordination time increases if material must be elevated to AFIMSC, SAF/PA or DOPSR for processing. Use a standardized form or format to transmit cases to coordinating agencies.

10.1.3. Do not release cases outside official review channels during the security and policy review process.

10.1.4. Make inquiries concerning cases being reviewed at higher levels of command through PA channels.

10.1.5. Use all reasonable measures to expedite staffing at all levels to make sure publication deadlines, speaking dates, and other valid deadlines are met.

10.1.6. Be sure to check release guidance in other regulations, such as *AFI 91-204, Safety Investigations and Reports*, and *AFI 90-301, Inspector General Complaints Resolution*.

10.2. See Paragraph 12 for mandatory step-by-step instructions.

11. Review Considerations. When reviewing material proposed for release, keep the following information in mind:

11.1. Operations Security (OPSEC) considerations. OPSEC is a process of collecting, identifying, and analyzing information on friendly military operations and other activities to identify and minimize actions which inadvertently provide an adversary timely indication of military action or access to critical information. By identifying and denying this information, operational success and force protection are enhanced. 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 operational environment. Air Force commanders and decision makers should consider OPSEC during both mission and acquisition planning.

11.2. Scientific and Technical Information (STINFO). The STINFO program has the maximum impact on the development of Air Force technology and STINFO generated under Air Force contracts and programs make maximum contribution to the national economy.

11.2.1. American technology is a valuable commodity and is greatly sought. Technology for application to a military weapon system may be considered sensitive as it may disclose too much about that potential system.

11.2.2. STINFO officers are responsible for reviewing reports and determining which distribution statements should appear on the data. Only reports marked "Distribution 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 Web page. For more information, refer to AFI 61-204, Disseminating Scientific and Technical Information.

11.3. Technology transfer is the process by which knowledge, facilities, or capabilities developed in one place or for one purpose are transferred and used in another place for another purpose to fulfill actual or potential public or domestic needs. The Air Force Technology Transfer Program was created to ensure all Air Force science and engineering activities promote the transfer or exchange of technology with state and local governments and the private sector. Technology transfers shall comply with AFI 61-301, The Domestic Technology Transfer Process and the Offices of Research and Technology Applications. These activities enhance the economic competitiveness of industry and promote the productivity of state and local governments while leveraging the DoD research and development investment. It is important to ensure that any critical data be reviewed prior to release to the public so that the United States does not lose its critical edge in that particular area. DoD and other agencies of the Federal Government have created a series of controls that are in use throughout the review process.

11.4. The Military 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.

11.5. International Traffic-in-Arms Regulations (ITARs) are a series of Department of State regulations that list 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 U.S. munitions list.

11.6. Export Control Laws are the responsibility of the Department of Commerce and are 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 Commodities Control List.

11.7. Freedom of Information Act (FOIA). The Air Force Supplement to *DoDD 5400.7-R, DoD Freedom of Information Act Program*, states the public will be allowed to inspect, review, and receive copies of Air Force records. This applies to all Air Force records except for those exempt from release under the Act. The exemptions under the FOIA, applicable to Air Force records, are generally:

11.7.1. Classified records.

11.7.2. Internal personnel rules and procedures.

11.7.3. Records exempt from release by other statutes.

11.7.4. Records containing confidential commercial information.

11.7.5. Records otherwise privileged in civil litigation.

11.7.6. Violation of personal privacy requirements IAW AFI 33-332, Air Force Privacy and Civil Liberties Program

11.7.7. Records related to open investigations.

12. Step-by-Step Process.

12.1. The following steps are mandatory at all levels: **(T-1)**

12.1.1. Originators submit required information (see Paragraph 9) and correct number of copies through appropriate channels to the local PA office.

12.1.2. Security and policy review authority logs the case, reviews the material to determine which agencies must see it, establishes a suspense date, and dispatches the case for review. For an audiovisual product, the security and policy review authority reviews the video and script before scheduling a coordination viewing to evaluate the product.

12.1.3. Coordinating agencies identify either classified information or information not consistent with official policy. Information for deletion is enclosed in brackets. Mark classified documents in accordance with DoDM 5200.01, Volume 2, *DOD Information Security Program: Marking of Classified Information*, and AFI 16-1404. If suspected classified information is found, immediately notify SAF/PA, Security and Policy Review office.

12.1.4. The Security Review Authority determines releasability of the material after receiving agency subject matter expert inputs, evaluating subject matter expert comments thoroughly, and contacting subject matter expert to resolve issues or concerns, if applicable.

12.1.5. After the Security Review Authority determines a clearance position, review action is completed, or if required, the case is sent to the next review echelon.

12.1.6. Once cases have been returned from higher-echelon review (AFIMSC, SAF/PA or DOPSR), the security and policy review authority retains one file copy showing final clearance and any changes and markings to the material, plus copies of each reviewing organization's signed remarks.

12.1.7. The originator will receive an email notification from PAIRS and a copy of the cleared material if requested. If public release approval is denied, originator will receive correspondence explaining reason for denial.

13. Subject Matter Expert (SME) Review Marking.

13.1. Marking. Inclusive brackets, in black pen, identify the non-releasable information and signal a mandatory amendment. Bracketed material must be removed before publication of the document. Write substitute language above the brackets. For editorial changes, line through once and provide changes as necessary.

13.2. Amending. Amendments require specific source citations and rationale. The SME must provide sufficient information and justification to enable the security and policy review authority to sustain an amendment. Such documentation eliminates ambiguity and provides the submitter with appropriate sources to substantiate the required change/amendment. If a SME determines a document to be classified, he/she must supply three essential pieces of information: classification authority, level of classification, and downgrading instructions.

13.3. Source Citations:

13.3.1. Classification authority sources most frequently cited are the security classification guides, provisions of classified contracts (*DD Form 254, Department of Defense Contract Security Classification Specification*). When classified material is identified in a security and policy review case, advise everyone possessing the document at once to protect it as classified.

13.3.2. Documentation sources can be presidential pronouncements; Defense and Air Force official statements; and Air Force policy directives, manuals, or policy letters.

13.4. Objection. A coordinator may make overall objection to clearing a case. An objection does not require marking on the document, but it does require detailed supporting justification. A SME may make a total objection to the public release if a case requires extensive amendment or rewrite for security or policy concerns.

13.5. Editorial Review. Editorial review is not a responsibility of the security and policy review authority, but SMEs may edit for clarity and accuracy. Editorial recommendations are lined through once and include suggested substitution information.

13.6. Other Coordination. If an agency SME thinks the case should be reviewed by another agency, he or she should advise the security and policy review authority. An early call can save several days in the review process.

13.7. Timeliness. Major security and policy review time-savers include timely coordination, proper marking, and accurate citing of classification sources.

14. Appeal Procedures. All amendments or “not cleared” determinations may be appealed in writing by the requester within 60 days. Appeals must provide strong supporting rationale and authoritative evidence. Review authorities evaluate and decide appeals based only on the additional evidence or reasoning provided. All appeals will be resolved at the next echelon level. When necessary, AFIMSC will elevate active-duty wing-level appeals to SAF/PA. SAF/PA will arrange for the appeal to be considered at the Air Force or DOPSR level, as appropriate.

KATHLEEN A. COOK, Brigadier General, USAF
Director of Public Affairs

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

Executive Order 13526, Classified National Security Information, 29 Dec 2009

DODM 5200.01, V2, DOD Information Security Program: Marking of Classified Information, February 24, 2012, Incorporating Change 2, March 19, 2013

DOD 5400.7-R, DOD Freedom of Information Act Program, 2 Jan 2008

DOD 5220.22-M, National Industrial Security Program Operating Manual, 28 Feb 2006

DOD 5220.22-R, Industrial Security Regulation, 4 Dec 1985

DODD 5230.09, Clearance of DOD Information for Public Release, 16 Mar 2016

DODD 5500.7, Standards of Conduct, 29 Nov 2007

DODI 5230.29, Security and Policy Review of DOD Information for Public Release, 13 Aug 2014

DODD 5205.02E, DOD Operations Security (OPSEC) Program, June 20, 2012

DODI 8550.01, DoD Internet Services and Internet-Based Capabilities, September 11, 2012

Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 12 Apr 2001, as amended through 17 Oct 2008

Joint Publication 3-61, Public Affairs, 25 Aug 2010

AFI 33-332, Air Force Privacy and Civil Liberties Program, 12 Jan 2015

AFI 33-360, Publication and Forms Management, 15 Sep 2013

AFI 35-107, Public Web Communications, 21 Oct 2009

AFI 61-204, Disseminating Scientific and Technical Information, 30 Aug 2002

AFI 90-301, Inspector General Complaints Resolution, 23 Aug 2011

AFMAN 33-363, Management of Records, 1 Mar 2008

AFPD 35-1, Public Affairs Management, 28 Sep 2012

AFI 16-1401 Air Force Information Security Program,, 29 May 2015

Air Force Records Disposition Schedule (RDS) located in AFRIMS, <https://www.my.af.mil/afirms/afirms/afirms/rims.cfm>

Abbreviations and Acronyms

AF—Air Force

AFI— Air Force Instruction

AFIT—Air Force Institute of Technology

AFIMSC—Air Force Installation and Mission Support Center

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

DD— Defense Department

DoD— Department of Defense

DoDD—Department of Defense Directive

DoDI— Department of Defense Instruction

DOPSR— Defense Office of Prepublication and Security Review

DRU— Direct Reporting Unit

EO— Executive Order

FOA— Field Operating Agency

FOIA— Freedom of Information Act

ITAR— International Traffic in Arms Regulation

MAJCOM—Major Command

MCTL— Military Critical Technologies List

OPSEC— Operations Security

PA— Public Affairs

PAIRS—Public Affairs Information Release

SME— Subject Matter Expert

STINFO—Scientific and Technology Information

Terms

Access—the ability or opportunity to gain knowledge of classified information.

Agency—any “Executive agency,” as defined in 5 U.S.C. 105; any “Military department” as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

Appeals— All amendments or “not cleared” determinations may be appealed in writing by the requester within 60 days to DOPSR.

Audiovisual—The use of sound and visual imagery displays to communicate information (motion pictures, television, still photographs, slides and film strips, radio, recordings, graphic illustration models, videos, and demonstrations)

Classification—the determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made.

Classification Guidance—any instruction or source that prescribes the classification of specific information.

Classified National Security Information or Classified Information—official information that has been determined to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Cleared for Public Release.—The information may be released without restriction by the originating DoD Component or its authorized official. DOPSR may require a disclaimer to accompany the information, as follows: “The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.”

Cleared “With Recommendations” for Public Release.— Optional corrections, deletions, or additions are included. Although DOPSR has no responsibility for correcting errors of fact or making editorial changes, obvious errors may be identified in the text and noted as “recommended.” These corrections are not binding on the author or originator.

Cleared “As Amended” for Public Release.—Amendments, made in red, are binding on the originator. Red brackets identify information that must be deleted. If the amendments are not adopted, then the DoD clearance is void. When possible, alternative wording is provided to substitute for the deleted material. Occasionally, wording will be included that must be added to the text before public release. A disclaimer, as shown in paragraph a(1) of this section, may also be required.

Declassification Authority—the official who authorized the original classification, if that official is still serving in the same position; the originator's current successor in function; a supervisory official of either; or officials delegated declassification authority in writing by the agency head or the senior agency official.

Document—any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

Downgrading—a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level. Federally Funded Research and Engineering. Originators will comply with the DoD guidance in federally funded research and engineering in DoDI 3200.12 and DoDI 3200.14 (References (r) and (s)), which requires originators to send the final published document or final author’s referenced manuscript to the Defense Technical Information Center (DTIC).

Field Operating Agency (FOA)—A subdivision of the Air Force, directly subordinate to a HQ USAF functional manager. FOAs perform field activities beyond the scope of any of the major commands. Their activities are specialized or associated with an Air Force wide mission.

Information—any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, which is owned by, produced by or for, or is under the control of the United States Government. —Controll means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

ITAR—Information generated from IR&D first should be checked against the State Department’s International Traffic-In-Arms Regulations (ITAR). This is a document detailing the United States munitions and procedures for export of defense articles and defense services. If the information in the material to be released is specified in the ITAR, then it could be subject to Department of State licensing. Technical papers intended for public release may be submitted to the Washington Headquarters Service, Office of Security Review (WHS/ESD/OSR) located in

the Pentagon. If cleared for release and placed in the public domain by the contractor, the technical paper is exempt from export licensing requirements. This review authority has not been delegated to the individual military services.

Not cleared for public release.—The information submitted for review may not be released.

Open Publication—The release or dissemination of information outside official government channels.

Operations Security (OPSEC) Considerations—. OPSEC is a process of collecting, identifying, and analyzing information on friendly military operations and other activities to identify and minimize actions which inadvertently provide an adversary timely indication of military action or access to critical information. By identifying and denying this information, operational success and force protection are enhanced.

Original Classification—an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

Originator—Creator of the document (i.e. article, presentation, manuscript)

Public Domain—That area owned by the public. Information is in the public domain when it has been made available to the public.

Records—the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

Security Review.—The security review protects classified information, controlled unclassified information, or unclassified information that may individually or in aggregate lead to the compromise of classified information or disclosure of operations security.

Scientific and Technical Information (STINFO).—The STINFO program ensures scientific and technical information make the maximum impact on the development of Air Force technology and ensures the scientific and technical information generated under Air Force contracts and programs make maximum contribution to the national economy.

Unauthorized Disclosure—a communication or physical transfer of classified information to an unauthorized recipient.

Violation—(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; (2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or (3) any knowing, willful, or negligent action to create or continue a SAP contrary to the requirements of this order.

Website Publication.—Information intended for placement on websites or other publicly accessible computer servers that are available to anyone requires review and clearance for public release if it meets the requirements of section 1 of this enclosure and DoDI 8550.01 (Reference (p)). Website clearance questions should be directed to the Component's website manager. Review and clearance for public release is not required for information to be placed on DoD controlled websites or computer servers that restrict access to authorized users