

**§ 604.16 Final denial of claim.**

Final denial of an administrative claim shall be made by the General Counsel, or his designee, in writing and sent to the claimant, his attorney, or legal representative by certified or registered mail. The notification of final denial may include a statement of the reasons for the denial and shall include a statement that, if the claimant is dissatisfied with the Agency action, he may file suit in an appropriate U.S. District Court not later than 6 months after the date of mailing of the notification.

**§ 604.17 Action on approved claims.**

(a) Payment of a claim approved under this part is contingent on claimant's execution of (1) a "Claim for Damage or Injury", Standard Form 95, (2) a claims settlement agreement, and (3) a "Voucher for Payment", Standard Form 1145, as appropriate. When a claimant is represented by an attorney, the voucher shall designate both the claimant and his attorney as payees, and the check shall be delivered to the attorney whose address shall appear on the voucher.

(b) Acceptance by the claimant, his agent, or legal representative, of an award, compromise, or settlement made under section 2672 or 2677 of the Act, is final and conclusive on the claimant, his agent or legal representative, and any other person on whose behalf or for whose benefit the claim has been presented, and constitutes a complete release of any claim against the United States and against any employee of the Government whose act or omission gave rise to the claim, by reason of the same subject matter.

**PART 605—NATIONAL SECURITY INFORMATION REGULATIONS**

- Sec.
- 605.1 Basis.
- 605.2 Objective.
- 605.3 Senior agency official.
- 605.4 Original classification.
- 605.5 Classification authority.
- 605.6 Derivative classification.
- 605.7 Declassification and downgrading.
- 605.8 Mandatory declassification review.
- 605.9 Systematic declassification review.
- 605.10 Safeguarding.

AUTHORITY: E.O. 12958 (60 FR 19825, April 20, 1995); Information Security Oversight Office Directive No. 1, 32 CFR 2001.

SOURCE: 61 FR 64286, Dec. 4, 1996, unless otherwise noted.

**§ 605.1 Basis.**

These regulations, taken together with the Information Security Oversight Office Directive No. 1 dated October 13, 1995, provide the basis for the security classification program of the U.S. Arms Control and Disarmament Agency (ACDA) implementing Executive Order 12958, "Classified National Security Information" (the Executive Order).

**§ 605.2 Objective.**

The objective of the ACDA classification program is to ensure that national security information is protected from unauthorized disclosure, but only to the extent and for such a period as is necessary.

**§ 605.3 Senior agency official.**

The Executive Order requires that each agency that originates or handles classified information designate a senior agency official to direct and administer its information security program. The ACDA senior agency official is the Deputy Director. The Deputy Director is assisted in carrying out the provisions of the Executive Order and the ACDA information security program by the Director of Security and by the Classification Adviser.

**§ 605.4 Original classification.**

(a) Definition. Original classification is the initial determination that certain information requires protection against unauthorized disclosure in the interest of national security (i.e., national defense or foreign relations of the United States), together with a designation of the level of classification.

(b) Classification designations—(1) *Top Secret* shall be applied only to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include, but are not limited to, armed hostilities against the United States or its allies;

the compromise of vital national defense plans or cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

(2) *Secret* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security. Examples of "serious damage" include, but are not limited to, disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

(3) *Confidential* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(c) Classification restraints. (1) The classification level of any form of information is premised on an evaluation of its contents as a whole, as well as on its relationship to other information.

(2) In classifying information, the public's interest in access to government information must be balanced against the need to protect national security information.

(3) In case of doubt, the lower level of classification is to be used.

(d) Duration of classification. (1) Information shall be classified for as long as is required by national security considerations, subject to the limitations set forth in section 1.6 of the Executive Order. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified. If a specific date or event for declassification cannot be determined, information shall be marked for declassification 10 years from the date of the original decision, except that the original classification authority may classify for a period greater than 10 years specific information that falls within the criteria set forth in section 1.6(d) of the Executive Order.

(2) An original classification authority may extend the duration of classification or reclassify specific information for successive periods not to exceed 10 years at a time except for records that are more than 25 years old.

(3) Information classified for an indefinite duration under predecessor orders, such as "Originating Agency's Determination Required," shall be subject to the declassification provisions of Part 3 of the Executive Order, including the provisions of section 3.4 regarding automatic declassification of records older than 25 years.

#### § 605.5 Classification authority.

(a) *General*. Classification shall be solely on the basis of national security considerations. In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error, or to prevent embarrassment to a person, organization, or agency.

(b) *Designations*. The following ACDA officials shall have original classification authority in each of the three designations under which they are shown below. This authority vests only in the officials or positions designated and, except as provided in paragraph (c) of this section, may not be redelegated. In the absence of any of the authorized classifiers (for TDY outside Washington, annual leave, temporary position vacancy, etc.), the officer acting in that person's position may exercise the classifier's authority.

- (1) *Top Secret*. (i) Director,
- (ii) Deputy Director.

(2) *Secret*. (i) Officials having Top Secret classification authority,

(ii) such other officials who have a frequent need to exercise Secret authority and are specifically delegated this authority in writing by the Director.

(3) *Confidential*. (i) Officials having Top Secret and Secret classification authority,

(ii) Other officials who have a frequent need to exercise Confidential authority and are specifically delegated this authority in writing by the Director.

(c) Delegation of classification authority. (1) The Executive Order restricts delegation of original classification authority to officials who have a demonstrable and continuing need to exercise such authority. Such delegations shall be held to a minimum.

(2) If in the judgment of bureau or office heads an officer has a demonstrable need for classification authority, a written request over the bureau or office head's signature should be forwarded via the Director of Security to the Deputy Director for action. The request should set forth the officer's name and title, the justification for having the authority, and the level of classification authority sought.

(3) The Director of Security shall maintain a complete current list by classification designation of individuals to whom and positions to which original classification authority has been delegated.

(4) Periodic reviews of delegations of classification authority will be made by the Director of Security to ensure that officials so designated have a continuing need to exercise such authority. Recommendations by the Director of Security for discontinuance of delegations will be forwarded to the Deputy Director for action.

(5) Original classification authority shall not be delegated to persons who only reproduce, extract, or summarize classified information, or who only apply classifications markings derived from source material or as directed by a classification guide.

(d) Classification responsibilities. Each ACDA officer who signs, authenticates, or otherwise produces a document is responsible for determining that it is properly classified and marked. This responsibility includes determining whether the document contains any originally classified material (in which case the classification must be authorized by an appropriate ACDA classifying official) or contains information already classified (in which case the proper derivative markings must be applied). Any significant doubt about the level of classification shall be resolved in favor of the lower level.

(e) Classification challenges. Holders of information who believe that its

classification status is improper are expected and encouraged to challenge the need for classification, the classification level, the duration of classification, the lack of classification or other aspect believed to be improper. Classification challenges shall be directed to and decided by the Deputy Director. If the information was not originated within or classified by ACDA, it will be referred to the Classification Adviser for coordination with the responsible agency or department if declassification, downgrading, classification or other change in its status appears to be warranted. Individuals making challenges to the classification status of information shall not be subject to retribution for such action, and they shall be advised of their right to appeal the Deputy Director's decision on the challenge to the Interagency Security Classification Appeals Panel established by section 5.4 of the Executive Order.

(f) Contractor classification authority. (1) Each ACDA contract calling for classified work shall be processed under the National Industrial Security Program.

(2) Each contract processed under the National Industrial Security Program requires the preparation of a contract security classification specification (DD 254) which serves as the contractor's guidance and authority to apply classification markings.

(3) Each contract processed under the Department of Energy (DOE) Security Requirements (i.e., involving restricted data or formerly restricted data) shall include a provision for naming a classification coordinator in the contractor organization. This individual shall coordinate the derived classification of all documents prepared under the contract in accordance with guidance received from ACDA via the ACDA Contracting Officer's Technical Representative for the contract, or by direct consultation on classification problems with the ACDA Classification Adviser or the Director of Security.

(4) Only designated officials of the U.S. Government may originally classify information. Contractor personnel, as potential developers of classified information, must follow the guidelines

outlined in paragraph (d) of this section entitled "Classification Responsibilities." When there is a question involving the original classification of information, the contractor is obligated to safeguard it in accordance with the classification designation deemed appropriate and submit recommendations to ACDA for classification determination.

(5) In general, the classification of the information provided by ACDA for use or reference in the completion of the contract will be the source of the classification of documents prepared under the contract.

#### § 605.6 Derivative classification.

(a) *Definition.* Derivative classification is the incorporating, paraphrasing, restating or generating in new form information that is already classified and the marking of the new material consistent with the classification of the source material. Duplication or reproduction of existing classified information is not derivative classification.

(b) *Responsibility.* Derivative application of classification markings is the responsibility of those who prepare material using information that is already classified and of those who apply markings in accordance with instructions from an authorized classifier or in accordance with an authorized classification guide.

(c) *Classification guides.* (1) Classification guides used to direct derivative classification and issued by ACDA shall specifically identify the information to be protected, using categorization to the extent necessary to ensure that the information involved can be identified readily and uniformly.

(2) Each classification guide issued by ACDA shall be approved by the Senior Agency Official.

(3) Each classification guide issued by ACDA shall be kept current and shall be reviewed as required by directives issued under the Executive Order. The Director of Security shall maintain a list of all classification guides.

#### § 605.7 Declassification and downgrading.

(a) *Declassification processes.* Declassification of classified information may occur:

(1) after review of material in response to a Freedom of Information Act (FOIA), mandatory declassification review, discovery, subpoena, or other information access or declassification request;

(2) after review as part of ACDA's systematic declassification review program;

(3) as a result of the elapse of the time or the occurrence of the event specified at the time of classification;

(4) by operation of the automatic declassification provisions of section 3.4 of the Executive Order with respect to material more than 25 years old.

(b) *Downgrading.* When material classified at the Top Secret level is reviewed for declassification and it is determined that classification continues to be warranted, a determination shall be made whether downgrading to a lower level of classification is appropriate. If downgrading is determined to be warranted, the classification level of the material shall be changed to the appropriate lower level.

(c) *Authority to downgrade and declassify.* (1) Classified information may be downgraded or declassified by the official who originally classified the information if that official is still serving in the same position, by a successor in that capacity, by a supervisory official of either, by the Classification Adviser, or by any other official specifically designated by the Deputy Director. Contractor personnel do not have authority to downgrade or declassify.

(2) The Director of Security shall maintain a record of ACDA officials specifically designated by the Deputy Director as declassification authorities.

(d) *Declassification after balancing public interest.* It is presumed that information that continues to meet classification requirements requires continued protection. In exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the ACDA official with Top Secret authority having primary jurisdiction over the information in question. That official, after consultation with the

Public Affairs Adviser and the Classification Adviser, will determine whether the public interest in disclosure outweighs the damage to national security that reasonably could be expected from disclosure. If the determination is made that the information should be declassified and disclosed, that official will make such a recommendation to the Director or the Deputy Director who shall make the decision on declassification and disclosure.

(e) *Public dissemination of declassified information.* Declassification of information is not authorization for its public disclosure. Previously classified information that is declassified may be subject to withholding from public disclosure under the FOIA, the Privacy Act, and various statutory confidentiality provisions.

**§605.8 Mandatory declassification review.**

(a) *Action on requests.* (1) All requests to ACDA by a member of the public, a government employee, or an agency to declassify and release information shall result in a prompt declassification review of the information, provided the request describes the document or material containing the information with sufficient specificity to enable ACDA to locate it with a reasonable amount of effort.

(2) If a request does not reasonably describe the information sought, the Classification Adviser will notify the requester that unless additional information is provided or the scope of the request is narrowed, no further action will be taken.

(3) Mandatory declassification review requests should be directed to the Classification Adviser, U.S. Arms Control and Disarmament Agency, 320 21st St., NW., Washington, DC 20451.

(4) If the request requires the rendering of services for which reasonable fees should be charged pursuant to the FOIA and ACDA regulations thereunder (22 CFR part 602), such fees shall be imposed at the FOIA schedule rates and the requester shall be so notified.

(5) The Classification Adviser, in consultation with appropriate ACDA bureaus and offices, will determine whether, under the Executive Order, the requested information may be de-

classified, in whole or in part, and will promptly make any declassified information available to the requester, unless the information is exempt from disclosure under some other provision of law.

(b) *Appeals from denials.* (1) If it is determined that declassification of the information requested is not warranted, in whole or in part, the requester shall be given a brief statement as to the reasons for the decision, a notice of the right to appeal to the Deputy Director, and a notice that any such appeal must be filed with ACDA within 60 days. Appeals shall be addressed to: Deputy Director, U.S. Arms Control and Disarmament Agency, 320 21st St., NW., Washington, DC 20451.

(2) The Deputy Director shall act within 30 days of receipt on all appeals of denials of requests for declassification. The Deputy Director shall determine whether continued classification is required in whole or in part. If the Deputy Director determines that continued classification is required under the Executive Order, the requester shall be so notified and informed of the reasons therefor. The requester shall also be advised of the right to appeal any denial to the Interagency Security Classification Appeals Panel in accordance with section 5.4 of the Executive Order.

(c) Information classified by another agency. When ACDA receives a request for information in its custody that was classified by another agency, the Classification Adviser shall forward the request together with a copy of the document containing the information requested to the classifying agency for review and direct response to the requester. Unless the agency that classified the information objects on the ground that its association with the information requires protection, the Classification Adviser shall also notify the requester of the referral.

(d) Confirmation of existence or nonexistence of document. In responding to a request for mandatory declassification review, the Classification Adviser may refuse to confirm or deny the existence or nonexistence of a document if the fact of its existence or nonexistence would itself be classifiable under the Executive Order.

U.S. Arms Control and Disarmament Agency

§ 606.735-1

§ 605.9 Systematic declassification review.

The Classification Adviser shall be responsible for conducting a program for systematic declassification review of historically valuable records that were exempted from the automatic declassification provisions of section 3.4 of the Executive Order. The FOIA officer shall prioritize such review on the basis of the recommendations of the Information Security Policy Advisory Council established under section 5.5 of the Executive Order and on the degree of researcher interest and likelihood of declassification upon review.

§ 605.10 Safeguarding.

Specific controls on the use, processing, storage, reproduction and transmittal of classified information within ACDA that provide adequate protection and prevent access by unauthorized persons are contained in Part 1 of the ACDA Security Classification Handbook, an internal guidance manual, and shall be followed by ACDA personnel and, when appropriate, by contractors.

PART 606—CONDUCT OF EMPLOYEES

Sec.

606.735-1 Definitions.

Subpart A—Standards of Conduct

- 606.735-10 General.
606.735-11 Ethical and regulatory standards of conduct of employees.
606.735-12 Statutes, rules, and regulations governing conduct of employees.
606.735-13 Outside employment and other activities.
606.735-14 Gifts, entertainment, and favors.
606.735-15 Financial interests.
606.735-16 Private compensation for services to the Government.
606.735-17 Use of Government property.
606.735-18 Gambling, betting, and lotteries.
606.735-19 General conduct prejudicial to the Government.

Subpart B—Activities Relating to Unofficial or Outside Organizations

- 606.735-21 Participation in activities of employee organizations.
606.735-22 Participating in activities of private organizations.

- 606.735-23 Organizations concerned with foreign policy.
606.735-24 Membership in subversive organizations.

Subpart C—Teaching, Speaking, Writing for Publication, and Related Activities

- 606.735-31 General policy
606.735-32 Protecting classified information.
606.735-33 Acceptance of invitations to speak or to accept teaching engagements.
606.735-34 Additional clearance measures.
606.735-35 Writing for publication.

Subpart D—Counseling or Acting as Agent or Attorney

- 606.735-41 Counseling foreign governments.
606.735-42 Involvement in proceedings affecting the United States.

Subpart E—Indebtedness

- 606.735-51 Policy.
606.735-52 Action by Personnel Officer.
606.735-53 Action by Executive Director.

Subpart F—Political Activity

- 606.735-61 Elections.
606.735-62 Activities punishable under the criminal code.

Subpart G—Statements of Employment and Financial Interests

- 606.735-71 Employees required to submit statements.
606.735-72 Submission of statements and supplementary statements.
606.735-73 Contents of statements.
606.735-74 Confidentiality of statements.
606.735-75 Review of statements and report of conflict of interest.
606.735-76 Action by the Director.

AUTHORITY: E.O. 11222, 30 FR 6469, 3 CFR 1964-1965 Comp., page 306; 5 CFR 735.104.

SOURCE: 31 FR 4391, Mar. 15, 1966, unless otherwise noted. Redesignated at 41 FR 8168, Feb. 25, 1976.

§ 606.735-1 Definitions.

As used in this part:

(a) ACDA and Agency mean the U.S. Arms Control and Disarmament Agency.

(b) Employee includes anyone serving in the Agency as:

(1) A person appointed by the President and confirmed by the Senate to a position in the Agency.