

A “refusal to neither confirm nor deny” response must be used consistently, not only when a record exists, but also when a record does not exist. Otherwise, the pattern of using a “no record” response when a record does not exist, and a “refusal to neither confirm nor deny” when a record does exist will itself disclose national security information. That kind of response is referred to as a “Glomar” denial.

(b) Information that concerns one or more of the classification categories established by Executive order and OPNAVINST 5510.1 series, “Department of the Navy Information and Personnel Security Program Regulation,” shall be classified if its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.

§ 701.23 Procedures for processing classified documents.

(a) The threshold for claiming exemption (b)(1) is that the document is properly and currently classified. Because of that, naval activities should normally refer requests for classified documents to the activity that originally classified the information. If the referring activity has an interest in the matter, they should also provide the receiving activity with a release determination. The receiving activity will then conduct a declassification review and apprise the requester of their determination, i.e., documents are properly and currently classified and therefore must be denied; portions of the documents are releasable; etc. Only an official authorized under § 701.5 to deny requests and who has cognizance over the classified matters in the records, may deny records. Such denial must be based on an approved security classification guide issued under OPNAVINST 5510.1 series or OPNAVINST 5513 series; resource document originated by another naval activity or government agency; an original classification determination with written justification for classification, and the justification remains valid; or, not readily identifiable, but classification is believed warranted because of classification criteria in OPNAVINST 5510.1 series, “Department of the Navy

Information and Personnel Security Program.”

(b) Material that is not classified at the time of the FOIA request may undergo a classification review to determine whether the information should be classified (ensure strict compliance with the provisions of OPNAVINST 5510.1 series regarding classification of information after receipt of a FOIA request).

(c) Executive Order 12356 provides that “information shall be classified as long as required by national security considerations, and time frame no longer triggers automatic declassification.”

(d) If the original classifier of a record receives a request for the record and upon review determines that there is no basis for continued classification, either in whole or part, the record or portions of it should be declassified. The document also undergoes another review to determine whether any other FOIA exemptions apply to the declassified information.

(e) In some instances, the compilation of unclassified information may result in the classification of the record as a whole. This is called the “mosaic” approach—the concept that apparently harmless pieces of information, when assembled together could reveal a damaging picture.

§ 701.24 Exemption (b)(2).

Those related solely to the internal personnel rules and practices of an agency. This exemption has two profiles, high (b)(2) and low (b)(2).

(a) Records qualifying under high (b)(2) are those containing or constituting statutes, rules, orders, manuals, directives, and instructions the release of which would allow circumvention of the records thereby substantially hindering the effective performance of a significant function of the Department of the Navy. Examples include:

(1) Those operating rules, guidelines, and manuals for Department of the Navy investigators, inspectors, auditors, or examiners that must remain privileged in order for the naval activity to fulfill a legal requirement.

(2) Personnel and other administrative matters, such as examination questions and answers used in training

Department of the Navy, DoD

§ 701.25

courses or in the determination of the qualifications of candidates for employment, entrance on duty, advancement, or promotion.

(3) Computer software, the release of which would allow circumvention of a statute or Department of the Navy rules, regulations, orders, manuals, directives, or instructions. In this situation, the use of the software must be closely examined to ensure the possibility of circumvention exists.

(4) Security classification guides.

(b) Records qualifying under the low (b)(2) profile are those that are trivial and housekeeping in nature for which there is no legitimate public interest or benefit to be gained by release, and it would constitute an administrative burden to process the request in order to disclose the records. Examples include, rules of personnel's use of parking facilities or regulation of lunch hours, statements of policy as to sick leave, and trivial administrative data such as file numbers, mail routing stamps, initials, data processing notations, brief references to previous communication, and other like administrative markings.

§ 701.25 Exemption (b)(3).

Those concerning matters that a statute specifically exempts from disclosure by terms that permit no discretion on the issue, or under criteria established by that statute for withholding or referring to particular types of matters to be withheld. Authorization or requirement may be found in the statute itself or in Executive orders or regulations authorized by, or in implementation of a statute. Examples include:

(a) National Security Agency Information Exemption, Pub. L. 86-36, Section 6.

(b) Confidentiality of identity of employee who complains to the IG (5 U.S.C. App., Inspector General Act of 1978, section 7).

(c) Ethics in Government Act of 1978—Protecting Financial Disclosure Reports of Special Government Employees (5 U.S.C. App., Ethics in Government Act of 1978, section 207(a) (1) and (2)).

(d) Civil Service Reform Act—Representation Rights and Duties, Labor Unions, 5 U.S.C. 7114(b)(4).

(e) Authority to Withhold Unclassified Special Nuclear Weapons Information, 10 U.S.C. 128. This statute prohibits the unauthorized dissemination of unclassified information pertaining to security measures, including security plans, procedures, and equipment for the physical protection of special nuclear material.

(f) Authority to Withhold Unclassified Technical Data with Military or Space Application, 10 U.S.C. 130.

(g) Action on Reports of Selection Boards, 10 U.S.C. 618.

(h) Confidentiality of Medical Quality Records: Qualified Immunity Participants, 10 U.S.C. 1102.

(i) Confidentiality of Financial Records, 12 U.S.C. 3403.

(j) Communication Intelligence, 18 U.S.C. 798.

(k) Confidential Status of Patent Applications, 35 U.S.C. 122.

(l) Secrecy of Certain Inventions and Withholding of Patents (specific applicable section(s) must be involved, 35 U.S.C. 181 through 188.

(m) Confidentiality of Invention Information, 35 U.S.C. 205.

(n) Procurement Integrity, 41 U.S.C. 423.

(o) Confidentiality of Patient Records, 42 U.S.C. 290dd-2.

(p) Information regarding Atomic Energy: Restricted and Formerly Restricted Data (Atomic Energy Act of 1954), specific applicable exemptions must be invoked (*e.g.*, 42 U.S.C. 2161 through 2168).

(q) Protection of Intelligence Sources and Methods, 50 U.S.C. 403(d)(3).

(r) Protection of identities of US undercover intelligence officers, agents, informants and sources, 50 U.S.C. 421.

(s) Examples of statutes which DO NOT qualify under exemption (b)(3) include: 5 U.S.C. 552a, Privacy Act; 17 U.S.C. 101 *et seq.*, Copyright Act; 18 U.S.C. 793, Gathering, Transmitting or Losing Defense Information to Aid Foreign Governments; 18 U.S.C. 1905, Trade Secrets Act; and 28 U.S.C. 1498, Patent and Copyright Cases.

[56 FR 66574, Dec. 24, 1991, as amended at 59 FR 29722, June 9, 1994]