

expressly note that firms had to have first obtained information from abroad for the obligation to evaluate the information to arise. The commentors feared that the omission signaled a possibility that, in evaluating a firm's compliance with the reporting requirements, the Commission might hold a firm responsible for not exercising due diligence to search for and obtain information that was available abroad, but that had not come to the firm's attention. The commentors therefore requested that the final amendment expressly state that a firm only needs to review information that it obtains.

The Commission believes that the amendment as proposed implicitly recognized that, in order to have an obligation to study and evaluate information, a firm must first obtain the information, or be reasonably expected to have obtained it because, for example, of the firm's relationship with or access to a firm or individual who possesses it. To alleviate the apparent confusion, however, the Commission has included in the final amendment an express statement that the information that should be evaluated includes information that a firm "has obtained, or reasonably should have obtained in accordance with section 1115.11" relating to product experience, etc. The Commission has not, however, limited this revision to cover only information that a firm has "actually" obtained, as one commentor requested. As is discussed *infra*, both the CPSA and the interpretative rule recognize that a firm need not have actually obtained information for obligations under section 15(b) to arise, if a reasonable person acting in the circumstances in which the firm finds itself would have obtained the information. Accordingly, the Commission believes that these provisions that address the imputation of knowledge to a firm dictate against further limiting the revision to the amendment. Adopting the restriction suggested by the commentor, on the other hand, could encourage firms to avoid seeking reasonably available information that could ultimately support the need for those firms to take corrective action.

c. Recipients of Information: One commentor stated that the rule should reflect that a firm "obtains" information only when an employee of the firm capable of appreciating the significance of the information actually receives it. Section 1115.11 of the interpretative rule already states that "the Commission will deem a firm to have obtained reportable information when the information has been received by an

official or employee who may reasonably be expected to be capable of appreciating the significance of the information." Because this provision already addresses the commentor's request, no additional revision to the final amendment is necessary.

d. Products Imported into the United States: Section 3(a)(4) of the CPSA, 15 U.S.C. 2051(a)(4) classifies importers as "manufacturers" under the act, while section 15(b) itself imposes reporting obligations on manufacturers, distributors, and retailers of consumer products. The Commission notes that foreign manufacturers export many products into the United States directly to importers, distributors, and retailers. In these circumstances, the Commission reminds importers, distributors, and retailers that they also have obligations under section 15 to conduct reasonable and diligent investigations, and to evaluate and report information about possible safety defects based on information they obtain or should reasonably obtain, including information from outside the United States. Retailers and distributors should refer to section 1115.13(b) of the interpretative rule for procedures for reporting.

Effective Date: This revision becomes effective 30 days after the date of publication of the revised final interpretative rule in the **Federal Register**.

List of Subjects in 16 CFR Part 1115

Administrative practice and procedure, Business and industry, Consumer protection, Reporting and recordkeeping requirements.

In accordance with the procedures of 5 U.S.C. 553 and under the authority of the Consumer Product Safety Act, 15 U.S.C. 2051 *et seq.*, the Commission amends part 1115 of title 16, Chapter II, of the Code of Federal Regulations as follows:

PART 1115—SUBSTANTIAL PRODUCT HAZARD REPORTS

1. The authority citation for part 1115 continues to read as follows:

Authority: 15 U.S.C. 2061, 2064, 2065, 2066(a), 2068, 2070, 2071, 2073, 2076, 2079 and 2084.

2. Section 1115.12(f) introductory text is revised to read as follows:

§ 1115.12 Information which should be reported; evaluating substantial product hazard.

* * * * *
 * * * (f) *Information which should be studied and evaluated.* Paragraphs (f)(1) through (7) of this section are

examples of information which a subject firm should study and evaluate in order to determine whether it is obligated to report under section 15(b) of the CPSA. Such information may include information that a firm has obtained, or reasonably should have obtained in accordance with § 1115.11, about product use, experience, performance, design, or manufacture outside the United States that is relevant to products sold or distributed in the United States. All information should be evaluated to determine whether it suggests the existence of a noncompliance, a defect, or an unreasonable risk of serious injury or death:

* * * * *

Dated: October 24, 2001.

Todd Stevenson,
Acting Secretary, Consumer Product Safety Commission.

[FR Doc. 01-27316 Filed 10-30-01; 8:45 am]

BILLING CODE 6355-01-P

DEPARTMENT OF DEFENSE

32 CFR Part 326

National Reconnaissance Office; NRO Privacy Act Program

AGENCY: National Reconnaissance Office, DOD.

ACTION: Final rule.

SUMMARY: The National Reconnaissance Office (NRO) is exempting two Privacy Act systems of records. The systems of records are QNRO-10, Inspector General Investigative Records and QNRO-15, Facility Security Files. The exemptions are intended to increase the value of the system of records for law enforcement purposes, to comply with prohibitions against the disclosure of certain kinds of information, and to protect the privacy of individuals identified in the systems of records.

EFFECTIVE DATE: October 16, 2001.

FOR FURTHER INFORMATION CONTACT: Ms. Barbara Freimann at (703) 808-5029.

SUPPLEMENTARY INFORMATION: The proposed rules were previously published on August 17, 2001, at 66 FR 43138. No comments were received; therefore, the National Reconnaissance Office is adopting the rules as final.

Executive Order 12866, "Regulatory Planning and Review"

The Director of Administration and Management, Office of the Secretary of Defense, hereby determines that Privacy Act rules for the Department of Defense are not significant rules. The rules do

not (1) Have an annual effect on the economy of \$100 million or more or adversely affect in a material way the economy; a sector of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribal governments or communities; (2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another Agency; (3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or (4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in this Executive order.

Public Law 96-354, "Regulatory Flexibility Act" (5 U.S.C. Chapter 6)

The Director of Administration and Management, Office of the Secretary of Defense, hereby certifies that Privacy Act rules for the Department of Defense do not have significant economic impact on a substantial number of small entities because they are concerned only with the administration of Privacy Act systems of records within the Department of Defense.

Public Law 96-511, "Paperwork Reduction Act" (44 U.S.C. Chapter 35)

The Director of Administration and Management, Office of the Secretary of Defense, hereby certifies that Privacy Act rules for the Department of Defense impose no information requirements beyond the Department of Defense and that the information collected within the Department of Defense is necessary and consistent with 5 U.S.C. 552a, known as the Privacy Act of 1974.

Section 202, Public Law 104-4, "Unfunded Mandates Reform Act"

The Director of Administration and Management, Office of the Secretary of Defense, hereby certifies that the Privacy Act rulemaking for the Department of Defense does not involve a Federal mandate that may result in the expenditure by State, local and tribal governments, in the aggregate, or by the private sector, of \$100 million or more and that such rulemaking will not significantly or uniquely affect small governments.

Executive Order 13132, "Federalism"

The Director of Administration and Management, Office of the Secretary of Defense, hereby certifies that the Privacy Act rules for the Department of Defense do not have federalism implications. The rules do not have substantial direct effects on the States, on the relationship between the

National Government and the States, or on the distribution of power and responsibilities among the various levels of government.

List of Subjects in 32 CFR part 326

Privacy.
32 CFR part 326 is amended as follows:

PART 326—[AMENDED]

1. The authority citation for 32 CFR part 326 continues to read as follows:

Authority: Pub. L. 93-579, 88 Stat 1896 (5 U.S.C. 552a).

2. Section 326.17 is amended by adding paragraphs (f) and (g) to read as follows:

§ 326.17 Exemptions.

* * * * *

(f) *QNRO-10, Inspector General Investigative Files*—(1) Exemption: This system may be exempt pursuant to 5 U.S.C. 552a(j)(2) if the information is compiled and maintained by a component of the agency which performs as its principle function any activity pertaining to the enforcement of criminal laws. Any portion of this system which falls within the provisions of 5 U.S.C. 552a(j)(2) may be exempt from the following subsections of 5 U.S.C. 552a (c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (H), and (I), (e)(5), (e)(8), (f), and (g).

(2) *Authority:* 5 U.S.C. 552a(j)(2)

(3) *Reasons*

(i) From subsection (c)(3) because the release of accounting or disclosure would inform a subject that he or she is under investigation. This information would provide considerable advantage to the subject in providing him or her with knowledge concerning the nature of the investigation and the coordinated investigative efforts and techniques employed by the cooperating agencies. This would greatly impede the NRO IG's criminal law enforcement.

(ii) From subsection (c)(4) and (d), because notification would alert a subject to the fact that an open investigation on that individual is taking place, and might weaken the on-going investigation, reveal investigative techniques, and place confidential informants in jeopardy.

(iii) From subsection (e)(1) because the nature of the criminal and/or civil investigative function creates unique problems in prescribing a specific parameter in a particular case with respect to what information is relevant or necessary. Also, due to NRO IG's close liaison and working relationships with other Federal, state, local and

foreign country law enforcement agencies, information may be received which may relate to a case under the investigative jurisdiction of another agency. The maintenance of this information may be necessary to provide leads for appropriate law enforcement purposes and to establish patterns of activity, which may relate to the jurisdiction of other cooperating agencies.

(iv) From subsection (e)(2) because collecting information to the fullest extent possible directly from the subject individual may or may not be practical in a criminal and/or civil investigation.

(v) From subsection (e)(3) because supplying an individual with a form containing a Privacy Act Statement would tend to inhibit cooperation by many individuals involved in a criminal and/or civil investigation. The effect would be somewhat adverse to established investigative methods and techniques.

(vi) From subsection (e)(4) (G) through (I) because this system of records is exempt from the access provisions of subsection (d).

(vii) From subsection (e)(5) because the requirement that records be maintained with attention to accuracy, relevance, timeliness, and completeness would unfairly hamper the investigative process. It is the nature of law enforcement for investigations to uncover the commission of illegal acts at diverse stages. It is frequently impossible to determine initially what information is accurate, relevant, timely, and least of all complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. (viii) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to law enforcement by revealing investigative techniques, procedures, and existence of confidential investigations.

(ix) From subsection (f) because the agency's rules are inapplicable to those portions of the system that are exempt and would place the burden on the agency of either confirming or denying the existence of a record pertaining to a requesting individual might in itself provide an answer to that individual relating to an on-going investigation. The conduct of a successful investigation leading to the indictment of a criminal offender precludes the applicability of established agency rules relating to verification of record, disclosure of the record to that individual, and record amendment procedures for this record system.

(x) From subsection (g) because this system of records should be exempt to the extent that the civil remedies relate to provisions of 5 U.S.C. 552a from which this rule exempts the system.

(4) Exemptions

(i) Investigative material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

(ii) Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iii) Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(2) and/or (k)(5) from the following subsections of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f).

(5) Authority

5 U.S.C. 552a(k)(2) and (k)(5).

(6) Reasons

(i) From subsection (c)(3) because to grant access to the accounting for each disclosure as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation or prosecutable interest by the NRO or other agencies. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(ii) From subsections (d) and (f) because providing access to investigative records and the right to contest the contents of those records and force changes to be made to the information contained therein would seriously interfere with and thwart the orderly and unbiased conduct of the investigation and impede case preparation. Providing access rights

normally afforded under the Privacy Act would provide the subject with valuable information that would allow interference with or compromise of witnesses or render witnesses reluctant to cooperate; lead to suppression, alteration, or destruction of evidence; enable individuals to conceal their wrongdoing or mislead the course of the investigation; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach in order to satisfy any Government claim growing out of the investigation or proceeding.

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because this system of records is compiled for investigative purposes and is exempt from the access provisions of subsections (d) and (f).

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NRO will, nevertheless, continue to publish such a notice in broad generic terms as is its current practice.

(vi) Consistent with the legislative purpose of the Privacy Act of 1974, the NRO will grant access to nonexempt material in the records being maintained. Disclosure will be governed by NRO's Privacy Regulation, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal or civil violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

(g) QNRO-15, Facility Security Files.

(1) Exemptions

(i) Investigative material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

(ii) Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(iii) Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(k)(2) and/or (k)(5) from the following subsections of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f).

(2) Authority

5 U.S.C. 552a(k)(2) and (k)(5).

(3) Reasons

(i) From subsection (c)(3) because to grant access to the accounting for each disclosure as required by the Privacy Act, including the date, nature, and purpose of each disclosure and the identity of the recipient, could alert the subject to the existence of the investigation or prosecutable interest by the NRO or other agencies. This could seriously compromise case preparation by prematurely revealing its existence and nature; compromise or interfere with witnesses or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(ii) From subsections (d)(1) through (d)(4), and (f) because providing access to investigative records and the right to contest the contents of those records and force changes to be made to the information contained therein would seriously interfere with and thwart the orderly and unbiased conduct of the investigation and impede case preparation. Providing access rights normally afforded under the Privacy Act would provide the subject with valuable information that would allow interference with or compromise of witnesses or render witnesses reluctant to cooperate; lead to suppression, alteration, or destruction of evidence;

enable individuals to conceal their wrongdoing or mislead the course of the investigation; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach in order to satisfy any Government claim growing out of the investigation or proceeding.

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because this system of records is compiled for investigative purposes and is exempt from the access provisions of subsections (d) and (f).

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. NRO will, nevertheless, continue to publish such a notice in broad generic terms as is its current practice.

(vi) Consistent with the legislative purpose of the Privacy Act of 1974, the NRO will grant access to nonexempt material in the records being maintained. Disclosure will be governed by NRO's Privacy Regulation, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal or civil violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered; the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

Dated: October 19, 2001.

L.M. Bynum,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 01-27185 Filed 10-30-01; 8:45 am]

BILLING CODE 5001-08-P

DEPARTMENT OF DEFENSE

Department of the Navy

32 CFR Part 701

[Secretary of the Navy Instruction 5211.5]

Privacy Act; Implementation

AGENCY: Department of the Navy, DOD.

ACTION: Final rule.

SUMMARY: The Department of the Navy is exempting those records contained in N05211-1, Privacy Act Files and Tracking System, and N05720-1, FOIA Request Files and Tracking System, when an exemption has been previously claimed for the records in 'other' systems of records. The exemptions are intended to preserve the exempt status of records when the purposes underlying the exemption for the original records are still valid and necessary to protect the contents of the records.

EFFECTIVE DATE: October 16, 2001.

FOR FURTHER INFORMATION CONTACT: Mrs. Doris Lama at (202) 685-6545 or DSN 325-6545.

SUPPLEMENTARY INFORMATION: The proposed rule was published on August 17, 2001, at 66 FR 43141. No comments were received therefore the Navy is adopting the rules as final.

Executive Order 12866, "Regulatory Planning and Review"

The Director of Administration and Management, Office of the Secretary of Defense, hereby determines that Privacy Act rules for the Department of Defense are not significant rules. The rules do not: (1) Have an annual effect on the economy of \$100 million or more or adversely affect in a material way the economy; a sector of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribal governments or communities; (2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another Agency; (3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or (4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in this Executive order.

Public Law 96-354, "Regulatory Flexibility Act" (5 U.S.C. Chapter 6)

The Director of Administration and Management, Office of the Secretary of Defense, hereby certifies that Privacy Act rules for the Department of Defense

do not have significant economic impact on a substantial number of small entities because they are concerned only with the administration of Privacy Act systems of records within the Department of Defense.

Public Law 96-511, "Paperwork Reduction Act" (44 U.S.C. Chapter 35)

The Director of Administration and Management, Office of the Secretary of Defense, hereby certifies that Privacy Act rules for the Department of Defense impose no information requirements beyond the Department of Defense and that the information collected within the Department of Defense is necessary and consistent with 5 U.S.C. 552a, known as the Privacy Act of 1974. Section 202, Public Law 104-4, "Unfunded Mandates Reform Act". The Director of Administration and Management, Office of the Secretary of Defense, hereby certifies that the Privacy Act rulemaking for the Department of Defense does not involve a Federal mandate that may result in the expenditure by State, local and tribal governments, in the aggregate, or by the private sector, of \$100 million or more and that such rulemaking will not significantly or uniquely affect small governments.

Executive Order 13132, "Federalism"

The Director of Administration and Management, Office of the Secretary of Defense, hereby certifies that the Privacy Act rules for the Department of Defense do not have federalism implications. The rules do not have substantial direct effects on the States, on the relationship between the National Government and the States, or on the distribution of power and responsibilities among the various levels of government.

List of Subjects in 32 CFR Part 701 Privacy.

32 CFR part 701 is amended as follows:

PART 701—[AMENDED]

1. The authority citation for 32 CFR part 701, Subpart G continues to read as follows:

Authority: Pub. L. 93-579, 88 Stat. 1896 (5 U.S.C. 552a).

2. Section 701.118, is amended by adding paragraphs (v) and (w) as follows:

§ 701.118 Exemptions for specific Navy record systems.

* * * * *

(v) *System identifier and name:*