Rules and Regulations

Federal Register
Vol. 75, No. 244
Tuesday, December 21, 2010

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS–2010–0089]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/ALL–031 Information Sharing Environment Suspicious Activity Reporting Initiative System of Records

AGENCY: Privacy Office, DHS.

ACTION: Final rule.

SUMMARY: The Department of Homeland Security is issuing a final rule to amend its regulations to exempt portions of a newly established system of records titled, "Department of Homeland Security/ALL–031 Information Sharing Environment Suspicious Activity Reporting Initiative System of Records" from certain provisions of the Privacy Act. Specifically, the Department exempts portions of the "Department of Homeland Security/ALL–031 Information Sharing Environment Suspicious Activity Reporting Initiative System of Records" from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: *Effective Date:* This final rule is effective December 21, 2010.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Ronald Athmann (202–447–4332), Office of Intelligence and Analysis, Department of Homeland Security, Washington, DC 20528. For privacy issues please contact: Mary Ellen Callahan (703–235–0780), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

Background

The Department of Homeland Security (DHS) published a notice of proposed rulemaking in the **Federal Register**, 75 FR 55290, September 10, 2010, proposing to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. The system of records is the DHS/ALL–031 Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Initiative System of Records. The DHS/ALL–031 ISE–SAR Initiative system of records notice was published concurrently in the **Federal Register**, 75 FR 55335, September 10, 2010, and comments were invited on both the notice of proposed rulemaking (NPRM) and system of records notice (SORN).

Public Comments

DHS received four comments on the NPRM. One commenter submitted the same set of comments for both the NPRM and the SORN.

All four comment submissions were in support of the DHS ISE–SAR Initiative and the proposed exemptions to the Privacy Act. One of the four commenters, BITS, a membership organization comprised of financial intuitions and financial-services vendors who own, operate, and/or develop critical infrastructure information systems, requested clarification on the scope of the ISE–SAR Initiative and the potential use of SAR filed by financial institutions and the proposed public-private partnership. In addition, the organization commented on the application of Freedom of Information Act (FOIA) exemptions particularly to any potential plans to collect cybersecurity information from private entities regarding cyber attacks. Lastly, the organization requested that the Department consider providing protections to private sector regulated entities that submit ISE–SARs to DHS.

BITS Comment: It is our understanding that the purpose of the DHS–ALL/031 ISE–SAR Initiative System of Records is to create a database of physical security threats and would not include the Bank Secrecy Act (BSA) related SARs filed with FinCEN. The ISE–Functional Standards do not expressly exclude BSA-related SARs, but the ISE Functional Standards restrict the scope of a SAR to "official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity." Likewise, the ISE–Functional Standards guidance criteria for determining whether a SAR constitutes an ISE–SAR, does not embrace financial crimes. Given these parameters, BITS questions whether BSA-related SARs may be included in the ISE–SARs database because of their potential nexus to terrorism information, as defined in the Intelligence Reform and Terrorism Prevention Act (IRTPA).

BITS respectfully asks the Department to clarify whether the proposed ISE–SARs database will include or exclude ISE–SARs filed pursuant to the BSA and Anti-Money Laundering regulations. The government's use of the classified sources and materials and aggregated BSA data could provide Federal agencies with a rich source of investigative leads relating to terrorism financing. These leads may flag previously unidentified anomalous behavior that becomes suspicious only when it is combined with aggregated investigative data sources, such as FinCEN's database of cross-border electronic funds transactions. BTS asks the Department to balance the potential benefits of this broad interpretation with the potential privacy, operational, and legal hazards.

Response: DHS participation in the Nationwide Suspicious Activity Reporting Initiative (NSI), which is overseen by the Department of Justice, adheres to the requirements established by the NSI requiring participants to apply the ISE–SAR Functional Standard Version 1.5 in determining whether a suspicious activity is an ISE–SAR. DHS would like to clarify that suspicious activities that meet the ISE–SAR Functional Standard Version 1.5 are not limited to physical security threats. Further, DHS submission of ISE–SARs to the NSI Shared Space does not explicitly exclude, nor does it include any specific category or source of information; rather DHS submissions of ISE–SARs to the NSI Shared Space adhere to the ISE–SAR Functional Standard Version 1.5. For further clarification on the scope and application of the ISE–SAR Functional Standard Version 1.5, DHS recommends that BITS reach out to the NSI Program

Management Office and review materials available on the NSI Web site available at *http://nsi.ncirc.gov.*

BITS Comment: BITS values the Department's commitment and efforts to improve information-sharing of security threats between the public and private sector. As partners with law enforcement, we have a long history of positive collaboration with law enforcement officials in the areas of cybersecurity, fraud, and money laundering. The financial services industry has a vested interest in protecting the financial system from illicit activities that could harm national security. As such, we are interested in the Department's plan to make the ISE–SARs available to "federal departments and agencies, state, local, and tribal law enforcement agencies, and the private sector." We hope the Department will provide additional information about: (1) the identities of the as-yet unnamed "private sector" partners or industries who would have access to ISE–SARs; and (2) private-sector and public law-enforcement credentialing requirements.

Response: DHS would like to clarify that DHS's contribution of ISE–SARs to the NSI Shared Space will make this information available only to *authorized* NSI participants. DHS does not maintain a list of private sector partners or entities who are authorized NSI participants. As previously noted, the NSI is not just a DHS initiative; it is overseen by the Department of Justice and authorized participants may include federal departments, state, local, and tribal law enforcement agencies, and the private sector. Accordingly, DHS recommends that BITS reach out to the Department of Justice NSI PMO regarding information on private sector industries who would have access to the NSI Shared Space as well as any requirements for becoming an authorized participant. Information about NSI partners is available at the NSI Web site at *https://nsi.ncirc.gov.*

BITS Comment: We applaud the Department's promulgation of an explicit exemption from certain parts of the Freedom of Information Act (FOIA) for the ISE–SARs program, although we encourage the Department to revisit the strength and application of the exemption, particularly if the Department plans to collect cybersecurity information from private entities regarding cyber attacks.

Because of the sensitivity and potential for severe damage associated with reported cyber attacks and vulnerabilities, we hope the Department will provide a blanket exemption from FOIA for ISE–SARs filed by a private-sector entity reporting an information-security related attack. A blanket FOIA exemption would further the Department's goals of information-sharing because it would increase the likelihood that institutions would voluntarily report suspected or confirmed cyber attacks that are not required to be reported. In the past, institutions have been reluctant to share information regarding suspected cyber attacks because of the potential for endangering their customers and their institutions. The creation of a standard, blanket exemption for the identifying information of the reporting entity would eliminate the reticence in the private sector and support more robust participation levels.

Response: DHS would like to clarify that the NPRM is exempting the DHS/ALL–031 ISE–SAR Initiative System of Records from certain portions of the Privacy Act, not the FOIA, as commenter suggests. When DHS processing either a Privacy Act or FOIA request, both applicable Privacy Act and appropriate FOIA exemptions are applied. With respect to applying FOIA exemptions, DHS applies FOIA exemptions available under current law. The FOIA currently does not provide for a standard "blanket exception" for ISE–SARs data filed by a private-sector entity reporting an information-security related attack. Nevertheless, if DHS were to receive a FOIA request for such information, it would apply applicable FOIA exemptions (*e.g.,* Exemption 4 which applies to trade secrets and commercial or financial information obtained from a person that is privileged or confidential may apply in this instance).

BITS Comment: Given the likelihood that BSA-related ISE–SARs may be aggregated into the ISE–SAR central data warehouse, we urge the Department to consider providing a dual "safe-harbor" provision to protect private-sector, regulated entities that submit reports to the ISE–SAR database.

First, a safe harbor should be created to address the liabilities associated with the provision of personally identifiable information to the ISE. We understand that the Department will exercise the utmost caution to protect the integrity of PII, but we also recognize that the provision of PII in such a large scale to federal agencies or private entities inevitably raises the specter of data compromise, identity theft, and fraud. Thus, we respectfully request that entities providing such PII in the requisite format be shielded from civil and criminal liability arising from the provision of PII to the ISE–SAR database.

We also suggest the creation of a "safe harbor" to protect prudentially regulated, private-sector entities (such as financial institutions) who: (1) Are compliant with relevant federal regulations; and (2) submit data to the ISE–SAR database in good faith, from adverse regulatory findings based on conclusions resulting from governmental use of the ISE–SAR database.

Response: DHS is one of many authorized NSI participants and therefore cannot comment on whether a "large scale of BSA-related ISE–SARs" will be included in the NSI Shared Space. To the extent DHS enters in ISE–SAR data obtained from an external entity into the NSI Shared Space, it will entail the use of the Summary ISE–SAR Information format, which excludes privacy fields or data elements that contain PII as identified in Section IV of the ISE–SAR Functional Standard. It is believed the data contained within a Summary ISE–SAR Information format will support sufficient trending and pattern recognition to trigger further analysis and/or investigation where additional information can be requested from the submitting organization. Accordingly, DHS does not see the need to create a "dual safe harbor provision" as the commenter suggests.

After consideration of public comments, the Department will implement the rulemaking as proposed.

List of Subjects in 6 CFR Part 5

Freedom of information, Privacy.

■ For the reasons stated in the preamble, DHS amends Chapter I of Title 6, Code of Federal Regulations, as follows:

PART 5—DISCLOSURE OF RECORDS AND INFORMATION

■ 1. The authority citation for part 5 continues to read as follows:

Authority: 6 U.S.C. 101 *et seq.;* Pub. L. 107–296, 116 Stat. 2135; 5 U.S.C. 301. Subpart A also issued under 5 U.S.C. 552. Subpart B also issued under 5 U.S.C. 552a.

■ 2. Add at the end of appendix C to part 5, the following new paragraph "52":

Appendix C to Part 5—DHS Systems of Records Exempt From the Privacy Act

* * * * *

52. The DHS/ALL—031 ISE SAR Initiative System of Records consists of electronic records and will be used by DHS and its components. The DHS/ALL—031 ISE SAR Initiative System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under;

national security and intelligence activities; and protection of the President of the U.S. or other individuals pursuant to Section 3056 and 3056A of Title 18. The DHS/ALL—031 ISE SAR Initiative System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS, its components, as well as other federal, state, local, tribal, or foreign agencies or private sector organization and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), and (e)(12); (f); (g)(1); and (h) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitation set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2) and (k)(3). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (c)(4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (e)(12) (Computer Matching) if the agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the **Federal Register** notice of such establishment or revision.

(j) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

(k) From subsection (h) (Legal Guardians) the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

Dated: December 9, 2010.

Mary Ellen Callahan

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2010–32000 Filed 12–20–10; 8:45 am]

BILLING CODE 9110–9B–P

DEPARTMENT OF AGRICULTURE

Office of the Secretary

7 CFR Part 2

RIN 0503–AA43

Revision of Delegation of Authority

AGENCY: Office of the Secretary, USDA.

ACTION: Final rule.

SUMMARY: This document amends the delegation of authority from the U.S. Department of Agriculture's Under Secretary for Marketing and Regulatory Programs (MRP) to the Deputy Under Secretary for MRP to establish the order in which a Deputy Under Secretary may perform the duties and exercise the powers of the Under Secretary during the absence or unavailability of the Under Secretary when there is more than one Deputy Under Secretary.

DATES: *Effective Date:* December 21, 2010.

FOR FURTHER INFORMATION CONTACT: Ms. Karen Grillo, Chief of Staff, Marketing and Regulatory Programs, USDA, 1400 Independence Avenue, SW., Washington, DC 20250; 202–7204–256.

SUPPLEMENTARY INFORMATION: Pursuant to 7 CFR 2.77, the Under Secretary for Marketing and Regulatory Programs (MRP) has delegated to the Deputy Under Secretary for MRP the following authority, to be exercised only during the absence or unavailability of the Under Secretary: Perform all the duties and exercise all the powers which are now or which may hereafter be delegated to the Under Secretary. This final rule amends 7 CFR 2.77 to establish the order in which a Deputy Under Secretary may exercise that delegation when the MRP mission area has more than one Deputy Under Secretary. The authority shall be exercised by the respective Deputy Under Secretary in the order in which he or she has taken office as the Deputy Under Secretary.

This rule relates to internal agency management. Therefore, this rule is exempt from the provisions of Executive Orders 12866 and 12988. Moreover, pursuant to 5 U.S.C. 553, notice of proposed rulemaking and opportunity for comment are not required for this rule, and it may be made effective less