

will be used by DHS and its components. The DHS/ALL-029 Civil Rights and Civil Liberties Records 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 thereunder; national security and intelligence activities; and protection of the President of the United States or other individuals pursuant to Section 3056 and 3056A of Title 18. The DHS/ALL-029 Civil Rights and Civil Liberties Records System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components 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 limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f) pursuant to 5 U.S.C. § 552a(k)(1), (k)(2), (k)(3), and (k)(5). 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) (Accounting for Disclosures) because release of the accounting of disclosures could alert the individual who is 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 individual who is 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 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.

* * * * *

Dated: June 9, 2011.

Mary Ellen Callahan,
*Chief Privacy Officer, Department of
Homeland Security.*

[FR Doc. 2011-18832 Filed 7-25-11; 8:45 am]

BILLING CODE 9110-9B-P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2011-0054]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security National Protection and Programs Directorate—001 National Infrastructure Coordinating Center Records 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/National Protection and Programs Directorate—001 National Infrastructure Coordinating Center Records System of Records” from certain provisions of the Privacy Act. Specifically, the Department exempts portions of the “Department of Homeland Security/National Protection and Programs Directorate—001 National Infrastructure Coordinating Center Records System of Records” from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement

requirements. The Department will not claim Privacy Act exemption (k)(3) as originally published in the Notice of Proposed Rulemaking.

DATES: *Effective Date:* This final rule is effective July 26, 2011.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Emily Andrew (703-235-2182), Senior Privacy Officer, National Protection and Programs Directorate, Department of Homeland Security, Washington, DC 20525. 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), National Protection and Programs Directorate (NPPD), published a notice of proposed rulemaking (NPRM) in the **Federal Register**, 75 FR 69603, on November 15, 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/NPPD—001 National Infrastructure Coordinating Center (NICC) Records System of Records. The DHS/NPPD—001 NICC Records system of records notice (SORN) was published concurrently in the **Federal Register**, 75 FR 69693, November 15, 2010, and comments were invited on both the NPRM and SORN. The Department will not claim Privacy Act exemption (k)(3) as originally published in the NPRM.

Public Comments

DHS received one set of public comments from the Electronic Privacy Information Center (EPIC). Comments submitted for the NPRM and SORN were identical. Each comment is outlined below followed by the Department’s response.

1. By exempting this system of records from certain provisions of the Privacy Act, DHS is contravening the purpose of the Act.

Comment: EPIC urged DHS to limit its exemptions from the Privacy Act’s provisions, including 5 U.S.C. 552a(c)(3), which entitles individuals to an accounting of disclosures of their records, stating that individuals should be able to know, after an investigation is completed or made public, the information stored about them in the system. Further, EPIC wrote that because information from informants may be used to initiate investigations,

individuals may find themselves investigated due to malicious information. This could be alleviated by providing access to records of completed investigations with appropriate redactions. EPIC also stated that DHS is retaining the right to disseminate using the overly broad standard of “potential risk of harm to an individual,” while limiting access to that same information that may be further disseminated.

Response: DHS recognizes the need to allow individuals the rights to and an account of disclosures of their records. The determination to exempt records from 5 U.S.C. 552a(d) is justified on a case-by-case basis, to be determined at the time a request is made. In those instances where an individual’s records are determined to be exempt from this provision, the individual may seek access to such records under 5 U.S.C. 552.

Comment: EPIC stated that DHS is exempting this system from 5 U.S.C. 552a(d) in order to prevent individuals from avoiding detection or tampering with evidence, which DHS argues would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. EPIC wrote that this restriction would not only contravene the Privacy Act, but may also hinder some government investigations, as was illustrated in a 2007 Department of Justice Inspector General review of the Transportation Security Administration’s (TSA) Terrorist Screening Center, which indicates that errors in the watch list obstruct the capture of actual terrorists and affect innocent individuals. EPIC specifically referenced fusion center data, writing that by exempting this data, DHS would prevent individuals from requesting information that DHS may be keeping on them, limiting their opportunity to seek redress.

Response: DHS recognizes the need to allow individuals the right to seek redress. The determination to exempt records from 5 U.S.C. 552a(d) is justified on a case-by-case basis, to be determined at the time a request is made. In those instances where an individual’s records are determined to be exempt from this provision, the individual may seek access to such records under 5 U.S.C. 552. With respect to EPIC’s specific comment regarding fusion center data that information falls outside the scope of this NPRM and SORN.

Comment: EPIC urged DHS to remove this system’s exemption from 5 U.S.C. 552a(e)(1), requiring that records maintained in this system be relevant

and necessary to accomplish the agency’s purpose, as this standard is a fundamental and necessary part of the Privacy Act protections and staves off mission creep. EPIC cited TSA’s second-generation Computer Assisted Passenger Prescreening System (CAPPS II) program as an example in which mission creep led to additional opportunity for errors. Further, EPIC wrote that this blanket exemption would allow records to contain information unrelated to any purpose of DHS.

Response: In the interest of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity. The information collected in this system that may be helpful in a particular investigation would likely be relevant and necessary to the investigation at some stage, and thus be in compliance with the standards of the Privacy Act.

Comment: EPIC expressed concerns with the operation of a proposed fusion center without being subject to the provisions of 5 U.S.C. 552a(e)(4)(G)–(I) and (f), noting that this would prevent individuals from knowing whether records in this system pertain to them. EPIC wrote that DHS could promulgate rules requiring notification only after an active investigation has been concluded or with sensitive information redacted prior to release.

Response: This comment relates to fusion center activities, which are outside the scope of this NPRM and SORN.

2. The NICC Proposal Requires a Narrow Mission with Clear Oversight Mechanisms and Limiting Guidelines.

Comment: EPIC wrote that the NICC mission statement is overly broad and justifies the collection of personal information for virtually any reason or for no reason at all. Instead, EPIC would advocate for meaningful guidance on the reasons and purpose of the creation of the system of records, arguing that the range of routine uses proposed by DHS are so broad as to make meaningless any intent to restrict data, furthering the possibility of mission creep.

Response: Consistent with DHS’s information sharing mission, information contained in the system of records may be shared with other DHS components, as well as appropriate Federal, state, local, Tribal territorial, foreign or international government agencies. The sharing will only take place after DHS determines that the receiving component or agency has a verifiable need to know the information to carry out national security, law enforcement, immigration, intelligence-

related activities, or to the functions consistent with the routine uses. DHS has provided notice of the purpose of the creation of this system of records in the form of NPRM, the SORN, and the Privacy Impact Assessment (PIA).

3. The NICC Proposal Requires a New PIA.

Comment: EPIC called for a new PIA to be drafted, which would cover fusions centers encompassing Federal projects, as opposed to covering only state, local, and regional fusion center projects.

Response: This comment relates to fusion center activities, which are outside the scope of this NPRM and SORN.

After careful review and consideration of these public comments alongside the published PIA and SORN, 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 “59”:

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

* * * * *

59. The DHS/NPPD–001 NICC Records System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/NPPD–001 NICC Records 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. The DHS/NPPD–001 NICC Records System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components 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 limitations set forth in 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) pursuant to 5 U.S.C.

552a(k)(1) and (k)(2). 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) (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 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.

Dated: June 28, 2011.

Mary Ellen Callahan,
Chief Privacy Officer, Department of
Homeland Security.

[FR Doc. 2011-18828 Filed 7-25-11; 8:45 am]

BILLING CODE 9110-9P-P

DEPARTMENT OF AGRICULTURE

Animal and Plant Health Inspection Service

7 CFR Part 301

[Docket No. APHIS-2009-0079]

Karnal Bunt; Regulated Areas in Arizona, California, and Texas

AGENCY: Animal and Plant Health
Inspection Service, USDA.

ACTION: Final rule.

SUMMARY: We are adopting as a final rule, with one change, an interim rule that amended the Karnal bunt regulations to make changes to the list of areas or fields regulated because of Karnal bunt, a fungal disease of wheat. Specifically, the interim rule added portions of the Buckeye/Pretoria area of Maricopa County, AZ, to the list of regulated areas and removed Throckmorton and Young Counties, TX, portions of Riverside County, CA, and certain areas in La Paz, Maricopa, and Pinal Counties, AZ, from the list of regulated areas based on our determination that those fields or areas meet our criteria for release from regulation. The interim rule was necessary to prevent the spread of Karnal bunt to noninfected areas of the United States and to relieve restrictions on certain areas that are no longer necessary. In the interim rule, we inadvertently removed two areas in Maricopa County, AZ, from the list of regulated areas. We are returning those areas to the list in this final rule.

DATES: *Effective Date:* July 26, 2011.

FOR FURTHER INFORMATION CONTACT: Ms. Lynn Evans-Goldner, Karnal Bunt Program Manager, Plant Pathogen and Weed Programs, EDP, PPQ, APHIS, 4700 River Road, Unit 26, Riverdale, MD 20737-1236; (301) 734-7228.

SUPPLEMENTARY INFORMATION:

Background

Karnal bunt is a fungal disease of wheat (*Triticum aestivum*), durum wheat (*Triticum durum*), and triticale (*Triticum aestivum* X *Secale cereale*), a hybrid of wheat and rye. Karnal bunt is caused by the fungus *Tilletia indica* (Mitra) Mundkur and is spread primarily through the planting of

infected seed followed by very specific environmental conditions matched during specific stages of wheat growth. The U.S. Department of Agriculture's Animal and Plant Health Inspection Service regulates the movement of articles in the United States that could spread Karnal bunt and works toward eventual eradication of Karnal bunt through biosanitary measures.

In an interim rule¹ effective and published in the **Federal Register** on November 10, 2010 (75 FR 68942-68945, Docket No. APHIS-2009-0079), we amended the Karnal bunt regulations in 7 CFR 301.89-1 through 301.89-16 by adding the Buckeye/Pretoria area of Maricopa County, AZ, to the list of regulated areas. The interim rule also removed Throckmorton and Young Counties, TX, portions of Riverside County, CA, and certain areas in La Paz, Maricopa, and Pinal Counties, AZ, from the list of regulated areas in § 301.89-3 based on our determination that those fields or areas meet our criteria for release from regulation.

We solicited comments concerning the interim rule for 60 days ending January 10, 2011. We did not receive any comments. However, after the publication of the interim rule, we noted that in amending the entry for Maricopa County, AZ, in § 301.89-3, we inadvertently removed paragraphs (3) and (4) in the description of the quarantined areas in that county. We are reinstating those paragraphs in this final rule.

Therefore, for the reasons given in the interim rule, we are adopting the interim rule as a final rule with change discussed in this document.

This action also affirms the information contained in the interim rule concerning Executive Order 12866 and the Regulatory Flexibility Act, Executive Orders 12372 and 12988, and the Paperwork Reduction Act.

Further, for this action, the Office of Management and Budget has waived its review under Executive Order 12866.

Effective Date

Pursuant to the administrative procedure provisions in 5 U.S.C. 553, we find good cause for making this rule effective less than 30 days after publication in the **Federal Register**. The interim rule adopted as final by this rule became effective on November 10, 2010. This rule reinstates two paragraphs of the description of the regulated area in Maricopa County, AZ. Immediate action

¹ To view the interim rule and a correction that restored several missing hyphens in the rule text, go to <http://www.regulations.gov/fdmspublic/component/main?main=DocketDetail&d=APHIS-2009-0079>.