epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2018-0029]

Notice of Modified Privacy Act System of Records

October 26, 2018

By notice published September 26, 2018, the Department of Homeland Security ("DHS") has proposed a revised system of records entitled, "DHS/All-016 Correspondence Records System of Records."[1] The agency contends that the modified system of records will become effective on the same day that comments are due—October 26, 2018.

The Electronic Privacy Information Center ("EPIC") objects to the lack of a meaningful opportunity for the DHS to review public comments before the revisions go into effect, as well as the lack of an adequate Privacy Impact Assessment (PIA) to address the privacy risks that the revisions create. Many of the proposed revisions are incompatible with DHS's 2007 Privacy Impact Assessment for the agency's Enterprise Correspondence Tracking System.[2] Specific revisions of system of records notice ("SORN") also contravene the intent of the Privacy Act. The SORN stretches the scope of categories of individuals to include third party subjects of a correspondence

[1] Privacy Act of 1974; Department of Homeland Security/ALL-016 Correspondence Records System of Records, 83 Fed. Reg. 48645 (proposed Sept. 26, 2018), https://www.gpo.gov/fdsys/pkg/FR-2018-09-26/pdf/2018-20876.pdf

[2] Privacy Impact Assessment for the Department of Homeland Security Enterprise Correspondence Tracking System (ECT), DHS/ALL/PIA-007, Dec. 3, 2007, *available at*: https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhsall-015-webportals-january%202017.pdf

who may not be aware that their data is being collected. The proposed "routine uses" undercut Privacy Act limitations on disclosure. EPIC submits these comments to urge DHS to (1) suspend the modified system of records until the agency solicits and considers public comments; (2) conduct a comprehensive Privacy Impact Assessment; (3) withdraw the proposal to allow data collection for individuals who are the subject of a correspondence; and (4) withdraw proposed routine uses E, F, H, J, and K, which vastly expand the agency's authority to disclose personal information contrary to the intent of the Privacy Act.

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.[3] EPIC has a particular interest in preserving privacy safeguards established by Congress, including the Privacy Act of 1974, and routinely comments in public rulemakings on agency proposals that would diminish the privacy rights and agency obligations set out in the federal Privacy Act.[4]

I. DHS' Proposed Information Collection and Routine Uses Would Have a Substantial Effect on Members of the Public and Thus the Administrative Procedure Act Requires Public Notice and Comment Prior to Implementation

[3] *About EPIC*, EPIC (2018), https://epic.org/epic/about.html

[4] *See, e.g.,* Comments of the Electronic Privacy Information Center to the Office of Management and Budget, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act (Oct. 28, 2016), available at: https://epic.org/apa/comments/EPIC-OMB-Cir-A-108-Comments-10-28-2016.pdf; Comments of the Electronic Privacy Information Center to the Department of Homeland Security, Automated Targeting System, Notice of Privacy Act System of Records and Proposed Rule, DHS-2012-0019 and 2012-0020 (June 21, 2012), *available at*: https://epic.org/apa/comments/EPIC-ATS-Comments-2012.pdf; Comments of the Electronic Privacy Information Center to the Department of Homeland Security, Notice of Privacy Act System of Records, DHS-2011-0082 (Nov. 28, 2011), *available* at http://epic.org/privacy/1974act/EPIC-DHS-2011-0082.pdf; Comments of the Electronic Privacy Information Center to the Department of Homeland Security, Notice of Privacy Act System of Records, DHS-2011-0030 (June 8, 2011), *available at* http://epic.org/privacy/EPIC%20E-Verify%20Comments%20Final%2006.08.11.pdf; Comments of the Electronic Privacy Information Center to the Office of the Director of National Intelligence, Notice of Privacy Act System of Records (May 12, 2010), *available at* http://epic.org/privacy/ODNI_Comments_2010-05-12.pdf; Comments of the Electronic Privacy Information Center to the Department of Homeland Security, Notice of Privacy Act System of Records: U.S. Customs and Border Protection, Automated Targeting System, System of Records and Notice of Proposed Rulemaking: Implementation of Exemptions; Automated Targeting System(Sept. 5, 2007), *available at* http://epic.org/privacy/travel/ats/epic_090507.pdf; Comments of the Electronic Privacy Information Center to the Department of Homeland Security United States Customs and Border Protection, Docket No. DHS-2005-0053, Notice of Revision to and Expansion of Privacy Act System of Records (May 22, 2006), *available at* http://epic.org/privacy/airtravel/ges052206.pdf

The Privacy Act requires "at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency."[5] Paragraph (4)(B) and 4(C) of the subsection refer to "categories of individuals on whom records are maintained in the system" and "categories of records maintained in the system," respectively. Paragraph (4)(D) of the subsection refers to "each routine use of the records contained in the system, including the categories of users and the purposes of such use."[6]

In addition to the Privacy Act's Federal Register public notice requirement, DHS is also obligated under the Administrative Procedure Act ("APA") to provide notice and comment on the proposed updates to the system of records because the system of records' "substantive effect is sufficiently grave so that notice and comment are needed to safeguard the policies underlying the APA."[7] The substantive effect of the proposed routine uses within DHS' system of records is "sufficiently grave" because they "impose directly and significantly upon so many members of the public."[8] DHS' system of records applies to a broad category of individuals, including any "individual[] who submits inquiries, complaints, comments, or other correspondence to DHS," and "individuals who are the subject of the correspondence."[9] The SORN specifies that these categories include "members of the general public."[10] The proposed routine uses and lack of specific data

[5] 5 U.S.C. § 552a(e)(11).
[6] *Id.* at (e)(4)(D).
[7] *EPIC v. U.S. Dep't. of Homeland Sec.,* 653 F.3d 1, 5-6 (D.C. Cir. 2011) (rehearing *en banc* denied)(quoting *Lamoille Valley R.R.Co. v. ICC*, 711 F.2d 295, 328 (D.C. Cir. 1983)); The Administrative Procedure Act, 5 U.S.C.§ 553 (b)-(c)(2011).
[8] *EPIC v. U.S. Dep't. of Homeland Sec.,* 653 F.3d at 6.
[9] 83 Fed. Reg. 48645.
[10] *Id.*

security measures require notice and comment because they create "sufficiently grave" privacy risks to these individuals.

A. DHS Must Consider Public Comments Before It May Implement the Proposed Revisions

The APA notice and comment requirement does not exist in a vacuum. Following the required notice and comment period, § 553(c) of the APA states that "[a]fter consideration of the relevant matter presented, the agency shall incorporate in the rules adopted a concise general statement of their basis and purpose."[11] Indeed, the "essential purpose of those [notice and comment] provisions is the generation of comments that will permit the agency to improve its tentative rule"[12] and to give the agency "the opportunity 'to educate itself on the full range of interests the rule affects'." [13] Additionally, it is well established that agencies must provide rationale for their decision-making processes by "responding to those comments that are relevant and significant."[14]

The SORN invites public comments "on or before October 26, 2018," the same day that the agency proposes to implement the modified system of records.[15] By not considering the public comments it receives in response to the substantial privacy risks the proposed routine uses present, DHS violates § 553(c).

B. Without Public Comment Review, DHS' Proposed Revisions Will Fail on Procedural Grounds

[11] 5 U.S.C. §553(c)
[12] *Am. Fed'n of Labor & Cong. of Indus. Organizations v. Donovan*, 757 F.2d 330, 337 (D.C. Cir. 1985) (quoting *Am. Fed'n of Labor & Cong. of Indus. Organizations v. Donovan*, 582 F. Supp. 1015, 1024 (D.D.C. 1984)).
[13] *Louis v. U.S. Dept. of Labor*, 419 F.3d 970, 976-77 (9th Cir. 2005) (quoting *Alcaraz v. Block*, 746 F.2d 593, 611 (9th Cir. 1984)).
[14] *Grand Canyon* Air *Tour Coal v. FAA*, 154 F.3d 455, 468 (D.C. Cir. 1998); *Cement Kiln Recycling Coalition v. E.P.A.*, 493 F.3d 207, 225 (D.C. Cir. 2007); *Interstate Natural Gas Ass'n of America v. F.E.R.C.*, 494 F.3d 1092, 1096 (D.C. Cir. 2007); *Int'l Fabricare Inst. V. U.S. EPA*, 972 F.2d 384, 389 (D.C. Cir. 1992).
[15] 83 Fed. Reg. 48645.

Courts have consistently held that "[i]f the agency fails to provide this notice and opportunity to comment or the notice and comment period are inadequate, the 'regulation must fall on procedural grounds, and the substantive validity of the change accordingly need not be analyzed.'"[16]

DHS' notice and comment concerning the proposed routine uses is inadequate because the agency does not afford itself opportunity to review the public comments it receives. Therefore, the proposed routine uses must fall on procedural grounds and should not be implemented without the agency reviewing and considering public comment. Because DHS intends to modify the scope of its information collection and routine uses for its Correspondence Records System of Records, it is required to provide a meaningful opportunity for public comment by reviewing public comments.

II. The Proposed Revisions Require a New Privacy Impact Assessment

The Chief Privacy Officer of DHS must ensure that the proposed revisions to the system of records comply with maximum oversight and privacy requirements as applicable, in order to fulfill the Officer's statutory obligation to assure that agency data collection programs do not "erode citizens' privacy."[17] The DHS Privacy Office is responsible for ensuring that DHS activities are fully compliant with privacy laws.

The Homeland Security Act requires a PIA for all DHS record systems.[18] The DHS Privacy Office requires that every PIA must address at least two issues: (1) the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (2) the protections and alternative processes for handling information to mitigate potential

[16] *Public Citizen, Inc. v. Mineta*, 427 F.Supp.2d 7, 12 (D.D.C. 2006) (quoting *AFL-CIO v. Donovan*, 757 F.2d 330, 338 (D.C. Cir. 1985)). *See also Stainback v. Mabus*, 671 F. Supp.2d 126, 135 (D.D.C. 2009); *Steinhorst Associates v. Preston*, 572 F.Supp.2d 112, 124 n. 13 (D.D.C. 2008); *National Ass'n of Home Builders v. U.S. Army Corps of Engineers*, 453 F. Supp. 2d 116, 123 (D.D.C. 2006).
[17] 6 U.S.C. § 142 (2010).
[18] 44 U.S.C. § 3501 (2010),

privacy risks.[19] PIAs standardize agency evaluation of privacy issues so that problems and risks can be identified.[20] The agency is required to conduct a PIA each time a system of records is modified.[21] The agency is required to make all PIAs available to the public under the E-Government Act of 2002.[22] The agency's guidelines require that all PIAs be "clear, unambiguous, and understandable to the general public."[23]

In 2007 DHS released a PIA for the agency's Enterprise Correspondence Tracking System (ECT), which covers the collection of personally identifying information throughout the management of correspondence "from the public, other government agencies, and the private sector."[24] The agency's official privacy guidelines requires DHS to conduct a new PIA before the modified system of records enters into force.[25] Compliance with this requirement is even more important in this particular instance because the 2007 PIA does not cover all revisions of the proposed modified system of records. First, the PIA does not explicitly address the collection and use of third-party data. Rather, the text of the PIA insinuates that the agency may collect personal information from the sender of the correspondence (e.g. name, contact information). There is no mention that third parties' personal data would be collected when that third party had no involvement in sending or handling the correspondence. Second, the proposed categories of records in the SORN contains data that is not covered under the PIA. The SORN indicates that "web form information" will be collected, including but not limited to unique identifiers, such as an "IP

[19] Department of Homeland Security: Privacy Impact Assessments ("The Privacy Office Official Guidance") at 2 (June 2010), *available at* www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf [hereinafter *DHS PIA Guidelines*].
[20] Hearing before the Subcomm. on Commercial and Administrative Law on the Judiciary, 109th Cong. (2006) (statement of Maureen Cooney, Acting Chief Privacy Officer), available at http://www.dhs.gov/dhspublic/interapp/testimony/testimony_0051.xml.
[21] The Privacy Office Official Guidelines, at 6.
[22] Pub. L. 107-347 (2002).
[23] The Privacy Office Official Guidelines, at 6.
[24] Privacy Impact Assessment, *supra* n. 2, at 2.
[25] The Privacy Office Official Guidelines, at 6.

address."[26] The PIA, by contrast, does not speak to the collection of this type of personal identifying information.[27] The agency is obligated to conduct a new PIA, as required in the agency guidelines.[28]

DHS should withdraw the proposed modifications until a comprehensive PIA is conducted that will establish specific actions and safeguards to maximize individual privacy protection for all data collected and used within the system of records indicated.

III. The Proposed Scope of Information Collection Contravenes the Intent of the Privacy Act

A. Categories of Individuals

The agency proposes to expand the categories of individuals subject to agency record-keeping to those who are neither the sender or recipient of an agency correspondence. Under the proposed revisions:

> Individuals who submit inquiries, complaints, comments, or other correspondence to DHS, excluding Privacy Act or FOIA requests, or standard immigration applications; individuals who are the subject of the correspondence; and any responding individual on behalf of DHS are covered by this SORN.[29]

Specifically, the agency proposes to collect personal information on any individual "whose information is submitted by the sender or recipient through an inquiry, comment, or complaint."[30] It

[26] 83 FR 48645
[27] Privacy Impact Assessment, *supra* n. 2, at 3-4
[28] Collection Limitation Principle: there should be limits to the collection of personal data, and any data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject; Data Quality and Integrity Principle: personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and up to date; Purposes Specification Principle: the purposes for which personal data is collected should be specified no later than at the time of data collection. Its subsequent use should be limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose; Use Limitation Principle: personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with Principle 3 except (a) with the consent of the data subject or (b) by the authority of law; Individual Participation Principle: an individual should have the right to (a) obtain confirmation of whether or not the data controller has data relating to him (b) have the data related to him within a reasonable time, cost, and manner an in a form that is readily intelligible to him (c) be given an explanation if a request made under (a) and (b) is denied and be able to challenge such denial and (d) challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended. The Privacy Office Official Guidelines, at 17, 20, 22, 24, and 29.

[29] 83 Fed. Reg. 48645 (emphasis added).
[30] 83 Fed. Reg. 48645.

is easily foreseeable that a reasonable individual would have no knowledge that he or she was the subject of a correspondence, let alone that his or her data would be collected and transferred to other federal agencies as a result of someone else's interaction with the agency. This is a secret data collection scheme, in direct contradiction to the Fair Information Practices and the Privacy Act. One of the core pillars of the Privacy Act of 1974 was to promote transparency between data subjects and data collectors. Accordingly, the Privacy Act requires agencies to:

> …inform each individual whom it asks to supply information… [of] (A) the authority which authorizes the solicitation of the information…; (B) the principal purpose or purposes for which the information is intended to be used; [and] (C) the routine uses which may be made of the information…[31]

The Privacy Act presumes that the agency will ask the data subject directly to provide his or her personal information. The Privacy Act does not permit agencies to collect and store personal information on third parties when it can be extracted in communications with the agency. The Privacy Act requires agencies to act fairly and transparently when collecting personal information, as illustrated by Section (e)(2) below:

> [Agencies shall] collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs.[32]

The proposed revisions contravene both of the above provisions of the Privacy Act because there is no opportunity for third party data subjects to be informed that his/her personal data is being collected. Third party individuals might never be aware that their personal data was collected or disclosed, contrary to the intent of (e)(3) and (e)(8).

EPIC recommends that the agency withdraw the revision allowing data collection for individuals whose names may appear in correspondence with the agency.

IV. The Proposed Scope of "Routine Uses" Is Inconsistent with the Privacy Act

[31] 5 U.S.C. § 552a(e)(3)(A)-(C)
[32] 5 U.S.C. § 552a(e)(2)

The definition of "routine use" is precisely tailored and has been narrowly prescribed in the Privacy Act's statutory language, legislative history, and relevant case law. However, DHS proposes to significantly increase its authority to disclose records for purposes that are inconsistent with the reasons for which the information was originally gathered and without the consent of the data subject.

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and required agencies to be transparent in their information practices.[33] Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[34]

Accordingly, the Privacy Act prohibits federal agencies from disclosing records they maintain "to any person, or to another agency" without the written request or consent of the "individual to whom the record pertains."[35] The Privacy Act also provides specific exemptions that permit agencies to disclose records without obtaining consent.[36] One of these exemptions is "routine use."[37] The SORN states that "all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3)."[38] The Privacy Act defines "routine use" to mean "with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected."[39]

[33] S. Rep. No. 93-1183 at 1 (1974).
[34] Pub. L. No. 93-579 (1974).
[35] 5 U.S.C. § 552a(b).
[36] *Id*. § 552a(b)(1) – (12).
[37] *Id*. § 552a(b)(3).
[38] 83 Fed. Reg. 48645
[39] 5 U.S.C. § 552a(b)(3) referencing § 552a(a)(7).

The Privacy Act's legislative history and a subsequent report on the Act indicate that the routine use for disclosing records must be specifically tailored for a defined purpose for which the records are collected. The legislative history states that:

> [t]he [routine use] definition should serve as a caution to agencies to think out in advance what uses it will make of information. This Act is not intended to impose undue burdens on the transfer of information . . . or other such housekeeping measures and necessarily frequent interagency or intra-agency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.[40]

The Privacy Act Guidelines of 1975—a commentary report on implementing the Privacy Act— interpreted routine use to mean that a "not only compatible with, but related to, the purpose for which the record is maintained."[41]

Courts interpret the Act to require a precisely defined system of records purpose for a "routine use." In *United States Postal Service v. National Association of Letter Carriers, AFL-CIO*, the Court of Appeals for the D.C. Circuit cited the Privacy Act's legislative history to determine that "the term 'compatible' in the routine use definitions contained in [the Privacy Act] was added in order to limit interagency transfers of information."[42] The Court of Appeals said "[t]here must be a more concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and in its disclosure."[43]

The litany of routine uses contained in the DHS proposed SORN provide the agency with broad authority to disclose individuals' personal information to other federal agencies. In particular,

---

[40] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[41] *Id*.
[42] *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993).
[43] *Id*. at 145 (quoting *Britt v. Natal Investigative Serv*., 886 F.2d 544, 549-50 (3d. Cir. 1989). *See also Doe v. U.S. Dept. of Justice*, 660 F.Supp.2d 31, 48 (D.D.C. 2009) (DOJ's disclosure of former AUSA's termination letter to Unemployment Commission was compatible with routine use because the routine use for collecting the personnel file was to disclose to income administrative agencies); *Alexander v. F.B.I*, 691 F. Supp.2d 182, 191 (D.D.C. 2010) (FBI's routine use disclosure of background reports was compatible with the law enforcement purpose for which the reports were collected).

proposed routine uses E, F, H, J, and K vastly expand DHS's authority to disclose information in conflict with the Privacy Act's language, legislative history, and interpretative case law.

> Under proposed routine use E, the agency may disclose information:
>
> To appropriate agencies, entities and persons when…DHS has determined that as a result of [a] suspected or confirmed breach there is a risk of harm to individuals…[44]
>
> Under proposed routine use F, the agency may disclose information:
>
> To another Federal agency or Federal entity, when DHS determines that information in this system of records is reasonably necessary to assist the recipient agency or entity in…preventing, minimizing the risk of harm to individuals…resulting from a suspected or confirmed breach.

Each of these proposed routine uses give the agency significant discretion to disclose personal information, following a suspected or confirmed breach. It is unclear how the agency would make a determination that a potential breach occurred, if there is a risk of harm, if and how much data is necessary to mitigate that risk, or how frequently proactive disclosure may occur in absence of a genuine breach. Until these concerns are addressed through a comprehensive Privacy Impact Assessment, the agency should remove routine uses E and F.

> Proposed routine use H would permit the agency to disclose information:
>
> To an appropriate Federal, state, tribal, territorial, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.
>
> Proposed routine use J would permit the agency to disclose information:
>
> To unions recognized as exclusive bargaining representatives of the individual under the Civil Service Reform Act of 1978, 5 U.S.C. 7111 and 7114, the Merit Systems Protection Board, the arbitrators, the Federal Labor Relations Authority, and other parties responsible for the administration of the Federal labor-management program for the purpose of processing any corrective action, or grievances, or conducting

[44] 83 Fed. Reg. 48645.

> administrative hearings or appeals, or if needed in the performance of other authorized duties.

The proposed routine uses above allow the agency to disclose personal information for purposes unrelated to the data's collection. The Correspondence Records System is designed to help DHS track and manage agency correspondence, not to assist law enforcement agencies in potential investigations, to contribute to labor union proceedings, or to provide information for news media and the public. These routine uses directly contradict Congressman William Moorhead's testimony that the Privacy Act was "intended to prohibit gratuitous, ad hoc, disseminations for private or otherwise irregular purposes."[45] Moreover, proposed routine use H would expose individuals' information to uses that are not protected by the Privacy Act. The Privacy Act only applies to records maintained by United States government agencies, not to foreign, international, or private authorities.[46] Releasing information to private and foreign entities does not protect individuals covered by this records system from Privacy Act violations. Because these routine uses significantly threaten the privacy of many individuals who communicate or who are a subject of communications with the agency, DHS should withdraw these routine uses.

Proposed routine use K would permit the agency to disclose information:

> To the news media and the public with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate accountability of DHS's officers, employees, or individuals covered by the system, except to the extent that the Chief Privacy Officer determines that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.[47]

The phrase "when disclosure is necessary to preserve confidence in the integrity of DHS" in Routine Use K is discordant with the Privacy Act because it gratuitously puts the face of the agency above an

[45] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[46] 5 U.S.C. §552a(b).
[47] 83 FR 48645

individual's right to privacy. The term "necessary" is ambiguous; DHS could take advantage of this criterion to unduly influence its image. DHS should withdraw this proposed routine use because creating a category that is too broad can easily lead to the abuse of privacy rights of individuals whose data has been gathered and stored by DHS.

V. Conclusion

For the foregoing reasons, EPIC urges the Department of Homeland Security to withdraw the proposed modifications to the Correspondence Records System of Records to allow opportunity for public comment, and to conduct a Privacy Impact Assessment. EPIC also urges the agency to withdraw proposed routine uses E, F, H, J, and K to safeguard individual privacy. If the revised system of records remains unchanged, the modifications undercut the purpose of the Privacy Act, conflict with the law, and exceed agency authority.

Respectfully submitted,

/s/ *Marc Rotenberg*
EPIC President and Executive Director

/s/ *Jeramie D. Scott*
EPIC National Security Counsel

/s/ *Spencer K. Beall*
EPIC Administrative Law Fellow