COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE DEPARTMENT OF HOMELAND SECURITY

"Systems of Records Notice"

DHS-2010-0052

and

"Notice of Proposed Rulemaking"

DHS-2010-0053

December 15, 2010

By notice published on November 15, 2010, the Department of Homeland Security ("DHS") Office of Operations Coordination and Planning ("OOCP") is proposing to establish a new system of records. The "Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records,"[1] which allow the DHS OCCP, including the National Operations Center ("NOC") "to collect, plan, coordinate, report, analyze, and fuse infrastructure information related to all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, natural disasters, and other information collected or received from federal, state, local, tribal, and territorial agencies and organizations; foreign governments and international organizations; domestic security and emergency management officials; and private sector entities or individuals into the Department."[2] Under a second notice, published the same day, the DHS seeks to exempt this new records system from

[1] Privacy Act of 1974; Department of Homeland Security Office of Operations Coordination and Planning--003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records, 75 Fed. Reg. 69,689 (Nov. 15, 2010) [hereinafter *Systems of Records Notice*].
[2] *Id*. at 69,689.

multiple requirements set out in the Privacy Act of 1974, 5 U.S.C. § 552a.[3] The system of records will involve an unprecedented collection of personal information, subject to the Privacy Act.

Pursuant to the DHS notice in the Federal Register, the Electronic Privacy Information Center ("EPIC)" submits these comments and recommendations to address the substantial privacy concerns raised by the OOCP proposals. The 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. The EPIC has particular interest in preserving privacy safeguards, established by Congress, in the development of new information systems operated by the federal government.[4]

---

[3] 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. 75 Fed. Reg. 69,604 (Nov. 15, 2010) [hereinafter *Notice of Proposed Rulemaking*].

[4] *See*, *e.g.*, EPIC: Information Fusion Centers and Privacy, http://epic.org/privacy/fusion/; EPIC: EPIC v. Virginia Department of State Police: Fusion Center Secrecy Bill, http://epic.org/privacy/virginia_fusion/; Statement of Lillie Coney, EPIC Associate Director, to the Department of Homeland Security Data Privacy and Integrity Advisory Committee (Sept. 19, 2007), *available at* http://www. epic.org/privacy/fusion/fusion-dhs.pdf; Letter from Marc Rotenberg, EPIC Executive Director and John Verdi, EPIC Staff Counsel to Senate Committee on Homeland Security and Governmental Affairs and the Senate Subcommittee on State, Local, and Private Sector Preparedness and Integration (Apr. 17, 2008), *available at* http://www.epic.org/privacy/fusion/EPIC_ltr_Sen_Fusion_Ctrs.pdf; Press Release, EPIC, EPIC Obtains Documents Revealing Federal Role in State Fusion Center Secrecy (Apr. 11, 2008), *available at* http://epic.org/press/041108.html; Freedom of Information Act Request from John Verdi, Director, EPIC Open Government Project to Virginia State Police (Feb. 12, 2008), *available at* http://www. epic.org/privacy/fusion/VA_FOIA021208.pdf; Complaint, EPIC v. Martin and the Virginia Department of State Police (D. Va 2007), *available at* http://www. epic.org/privacy/fusion/VA_FOIA_lawsuit_032108.pdf; EPIC: Open Government, http://epic.org/open_gov/; EPIC: Spotlight on Surveillance: "National Network" of Fusion Centers Raises Specter of COINTELPRO, http://epic.org/privacy/surveillance/spotlight/0607/; EPIC: Privacy, http://epic.org/privacy/; Statement of Lillie Coney, EPIC Associate Director to ABA Conference, Computing and the Law: From Steps to Strides into the New Age (June 25-26, 2007), *available at* http://www. epic.org/epic/staff/coney/surveillance.pdf; Letter from EPIC, et. al to Representative Bennie G. Thompson, Chair, U.S. House of Representatives Committee on Homeland Security and Representative Peter T. King, Ranking Member, U.S. House of Representatives Committee on Homeland Security (Oct. 23, 2009), *available at* http://www. epic.org/security/DHS_CPO_Priv_Coal_Letter.pdf; EPIC: EPIC Alert 15.10, "EPIC Prevails in Virginia Fusion Center FOIA Case," (May 16, 2008), http://mailinglists.epic.org/pipermail/epic_news/2008-May/000001.html; EPIC: EPIC Alert 14.19, "DHS Privacy Advisory Panel Holds Hearing on Fusion Center," (Sept. 20, 2007), http://epic.org/alert/EPIC_Alert_14.19.html; EPIC: "DHS Releases Fusion Center Privacy Impact Assessment," EPIC Alert 15.25 (Dec. 23, 2008), http://mailinglists.epic.org/pipermail/epic_news/2008-December/000017.html; EPIC: "Documents Reveal Federal Role In Fusion Center Secrecy," EPIC Alert 15.08 (Apr. 17, 2008), http://epic.org/alert/EPIC_Alert_15.08.html; EPIC: Department of Homeland Security Chief Privacy Office and Privacy, http://epic.org/privacy/dhs-cpo.html.

Scope of the Rulemaking

The DHS describes an unusually broad description of purpose of this system of records. According to the DHS, the agency seeks to "collect, plan, coordinate, report, analyze, and fuse infrastructure information related to all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, natural disasters, and other information collected or received from federal, state, local, tribal, and territorial agencies and organizations; foreign governments and international organizations; domestic security and emergency management officials; and private sector entities or individuals into the Department."[5]

Information the DHS seeks to incorporate into this system of records is extraordinarily broad and includes:

- Full name;
- Date and place of birth;
- Social Security Number (Many state, local, tribal, territorial, domestic security, emergency management, and private sector individuals, organizations and agencies collect/use SSNs as an identifier and may be shared with the Department);
- Citizenship;
- Contact information including phone numbers and email addresses;
- Address;
- Physical description including height, weight, eye and hair color;
- Distinguishing marks including scars, marks, and tattoos;
- Automobile registration information;

[5] Systems of Records Notice, *supra* note 1 at 69,690.

- Watch list information;
- Medical records;
- Financial information;
- Results of intelligence analysis and reporting;
- Ongoing law enforcement investigative information;
- Historical law enforcement information;
- Information systems security analysis and reporting;
- Public source data including commercial databases, media, newspapers, and broadcast transcripts;
- Intelligence information including links to terrorism, law enforcement and any criminal and/or incident activity, and the date information is submitted;
- Intelligence and law enforcement information obtained from federal, state, local, tribal, and territorial agencies and organizations, foreign governments and international organizations;
- law enforcement, domestic security and emergency management officials; and private sector entities or individuals;
- Information provided by individuals, regardless of the medium, used to submit the information;
- Information obtained from the Federal Bureau of Investigation's (FBI) Terrorist Screening Center (TSC), or on terrorist watchlists, about individuals known or reasonably suspected to be engaged in conduct constituting, preparing for, aiding, or relating to terrorism;
- Data about the providers of information, including the means of transmission of the data; (e.g. where it is determined that maintaining the identity of the source of investigative lead information may be necessary to provide an indicator of the reliability and validity of the data provided and to support follow-on investigative purposes relevant and necessary to a legitimate law enforcement or homeland security matter, such data may likely warrant retention. Absent such a need, no information on the provider of the information would be maintained) Scope of terrorist, law enforcement, or natural threats to the homeland; National disaster threat and activity information;
- The date and time national disaster information is submitted, and the name of the contributing/submitting individual or agency;

- Limited data concerning the providers of information, including the means of transmission of the data may also be retained where necessary. Such information on other than criminal suspects or subjects is accepted and maintained only to the extent that the information provides descriptive matters relevant to a criminal subject or organization and has been deemed factually accurate and relevant to ongoing homeland security situational awareness and monitoring efforts;

- Name of the contributing or submitting agency, organization, or individual."[6]

Moreover, the agency claims an unusually broad authority to share this information with both public and private parties. The DHS states that it will assert a routine use exemption for disclosures to:

- To the Department of Justice (including United States Attorney Offices) or other federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation: 1. DHS or any component thereof; 2. any employee of DHS in his/her official capacity; 3. any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or 4. the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records;

- To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains;

- To the National Archives and Records Administration or other federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906;

- To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function;

- To appropriate agencies, entities, and persons when: 1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; 2. The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or

[6] *Id*. at 69,691.

programs (whether maintained by DHS or another agency or entity) or harm to the individual that rely upon the compromised information; and 3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

- To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees;

- To an appropriate Federal, State, tribal, 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, where 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;

- To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations or critical infrastructure partners for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk;

- To a Federal, State, tribal, local or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence;

- To Federal and foreign government intelligence or counterterrorism agencies or state, local, tribal or territorial components, and critical infrastructure partners where DHS becomes aware of an indication of a threat or potential threat to national or international security;

- To Federal and foreign government intelligence or counterterrorism agencies or state, local, tribal or territorial components, and critical infrastructure partners where the information is or may be terrorism-related information and such use is to assist in anti-terrorism efforts;

- To an organization or individual in either the public or private sector, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life or property;

- 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 or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS' officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.[7]

The November 15, 2010 Systems of Records Notice clearly states that "information within this system that meets the functional standard of the National Suspicious Activity Reporting Initiative will be placed into the DHS/ALL-031 Information Sharing Environment Suspicious Activity Reporting Initiative."[8] The Information Sharing Environment (ISE) Nationwide Suspicious Reporting Initiative (NSI) seeks to "gather[] information regarding behaviors and incidents associated with criminal activity…and establish[] a standardized process whereby [Suspicious Activity Reporting] information can be shared among agencies."[9]

Information that flows from the ISE into the NSI is accessible over the National Information Exchange Model (NIEM), "a federal, state, local and tribal interagency initiative providing a foundation for seamless information exchange."[10] NIEM was designed to be a "plug and play" environment where participants will use XML-tagging protocol for data elements and characteristics.[11] This system of information sharing has been developed and nurtured by several federal government agencies, which include the Department of Justice, and the Department of

[7] Systems of Records Notice, *supra* note 1 at 69,692.
[8] Systems of Records Notice, *supra* note 1 at 69,690; *See also* Institute for Intergovernmental Research: Nationwide SAR Initiative (NSI), http://nsi.ncirc.gov/.
[9] Information Sharing Environment: Nationwide SAR Initiative, http://www.ise.gov/Pages/NSI.aspx.
[10] Information Sharing Environment: the National Information Exchange Model (NIEM), http://www.ise.gov/Pages/NIEM.aspx.
[11] National Information Exchange Model: Home, http://www.niem.gov/. "XML was created to structure, store, and transport information." W3Schools.com: Introduction to XML, http://www.w3schools.com/XML/xml_whatis.asp.

Homeland Security, though it has been largely untouched by public comment or debate.[12] Further, the Federal government has engaged in an active campaign to promote the adoption of NIEM across the federal government, as well as by private sector data warehouses.[13] In 2010, IBM said that NIEM was "rapidly becoming the most important XML-exchange standard for the U.S. government and its information partners."[14]

The DHS, by its November 15 series of Federal Register Notices, contradicts previous public statements and positions that Fusion Centers were solely state and local entities,[15] and attempts to adopt NIEM into a tool that will be practically indistinguishable from that of the TIA program, shut down by Congress more than seven years ago,[16] and simply re-marketed under a new name.[17] For these reasons EPIC submits the following comments and recommendations.

Comments and Recommendations

EPIC submits the following comments and recommendations:

[12] Information Sharing Environment: Define ISE Mission Partners, http://ise.gov/Pages/DefMissPartner.aspx.
[13] Erik Pupo, *A Sea Change in Health Info Exchange*, Government Health IT (Sept. 21, 2010), http://govhealthit.com/GuestColumnist.aspx?id=74696.
[14] IBM: Creating a NIEM IEPD, Part 1: Model your NIEM exchange, http://www.ibm.com/developerworks/xml/library/x-NIEM1/index.html?ca=drs-.
[15] The Congressional Research Service points out that there is no single legal authority that governs the operation of Fusion Centers. It states that Fusion Centers were "state-created entities," and that "the federal role in supporting fusion centers consist[ed] largely of providing financial assistance…; sponsoring security clearances; providing human resources; producing some fusion center guidance and training; and providing congressional authorization and appropriation of national foreign intelligence program resources, as well as oversight hearings." The report continues, "Fusion centers are not federal entities and…have no federal statutory basis." This Systems of Records Notice indicates that a key change is being made in government policy, and fusion centers are now to be introduced as entities of the federal government. Congressional Research Service, Fusion Centers: Issues and Options for Congress 10, January 18, 2008, available at http://fpc.state.gov/documents/organization/102652.pdf.
[16] On November 9, 2002, the New York Times disclosed a massive fusion center project by the Department of Defense, created by the Pentagon's Information Awareness Office and managed by the Defense Advanced Research Project Agency (DARPA). The project was known as Total Information Awareness (TIA). TIA was a tracking system intended to detect terrorists by analyzing troves of information. The project called for the development of "revolutionary technology for ultra-large all-source information repositories," containing information from multiple sources in a "virtual, centralized, grand database." The database was designed to include information in financial records, medical records, communication records, and travel records, as well as intelligence data. Congress acted to eliminate the funding for TIA in September 2003, and also closed the Pentagon's Information Awareness Office. EPIC: Terrorism (Total) Information Awareness, http://epic.org/privacy/profiling/tia/.
[17] Institute for Intergovernmental Research: Nationwide SAR Initiative (NSI), http://nsi.ncirc.gov/.

1. *The OOCP's Proposal Contravenes the Purpose and Intent of the Federal Privacy Act*

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal data that federal agencies could collect and requires government agencies to limit the collection, sharing, and use of individuals' personal information.[18] In 2004, the Supreme Court underscored the importance of the Privacy Act's restrictions upon agency use of personal data to protect privacy interests, noting that:

> "[I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies." Privacy Act of 1974, §2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements.[19]

The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]"[20]It is also intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. 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."[21] It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[22]

[18] S. Rep. No. 93-1183 at 1 (1974).
[19] *Doe v. Chao*, 540 U.S. 614, 618 (2004).
[20] S. Rep. No. 93-1183 at 1.
[21] Pub. L. No. 93-579 (1974).
[22] *Id*.

The November 15, 2010 Notice of Proposed Rulemaking (NPRM), published in the Federal Register by the Department of Homeland Security,[23] however, exempts the DHS from nearly all of the Privacy Act provisions, directly contravening the Act's purpose and intent.[24] By invoking these exemptions the DHS seeks to withhold important rights from individuals. According to the SORN,[25] the data to be collected includes some of the most sensitive and invasive information that one can collect about a person: Social Security Number, Medical Records, Financial Information, and all Public Source Data, including "commercial databases, media, newspapers, and broadcast transcripts."[26] Sufficient protections must exist to safeguard and verify the accuracy of this information.

- **Proposed Exemptions from the Federal Privacy Act**

The DHS proposes exemptions from key Privacy Act provisions guaranteeing citizens the right to access records containing information about them and provisions defining the government's obligation to allow citizens to challenge the accuracy of information contained in their records. The exemptions proposed are: "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), and (k)(3)."[27] Among other things, these provisions ensure:

- An agency must give individuals access to the accounting of disclosure of their records;[28]
- An individual may request access to records an agency maintains about him or her;[29]
- An agency must correct identified inaccuracies promptly;[30]
- An agency must make notes of requested amendments within the records;[31]

[23] *Supra* note 3.
[24] *See id*.
[25] *Supra*, note 1.
[26] Systems of Records Notice, *supra* note 1 at 69,691. *See also supra* page 3-5.
[27] Notice of Proposed Rulemaking, *supra* note 3 at 69,606.
[28] 5 U.S.C. § 552a(c)(3) (2010).
[29] 5 U.S.C. § 552a(d)(1) (2010).
[30] 5 U.S.C. § 552a(d)(2)(B), (d)(3) (2010).

- An agency must ensure it only collects data "relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive Order of the President";[32]

- An agency must publish a notice of the existence of records in the Federal Register, along with the procedures to be followed to obtain access;[33] and,

- An agency must establish procedures to handle disputes between the agency and individual as to the accuracy of the records[34]

    - **5 U.S.C. § 552a(c)(3)**

EPIC urges the DHS to limit its exemptions from the Privacy Act's provisions requiring an individual to have access to all disclosures of records kept about them.[35] The DHS insinuates that, if implemented, this requirement would "alert the subject 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."[36]

Although notice may be withheld during the period of a specific investigation, individuals should be able to know, after an investigation is completed or made public, the information stored about them in the system. Since the DHS depends, at least in part, upon informants to initiate investigations, individuals may find themselves investigated due to malicious misinformation spread by bad actors. Access to records of a completed investigation, with appropriate redactions to protect the identities of any confidential informants, would provide individuals with the right to address potential inaccuracies and misinformation resulting from such investigations. Moreover, the idea that information about an individual maintained in

[31] 5 U.S.C. § 552a(d)(4) (2010).
[32] 5 U.S.C. § 552a(e)(1) (2010).
[33] 5 U.S.C. § 552a(e)(4)(G), (e)(4)(H), (f) (2010).
[34] 5 U.S.C. § 552a(f)(4) (2010).
[35] 5 U.S.C. § 552a(d)(1) (2010).
[36] Notice of Proposed Rulemaking, *supra* note 3 at 69,606.

a federal agency system of records would never be made available to the individual because an investigation was ongoing in perpetuity would, of course, be absurd.

In addition, while limiting the right of individuals to know who has access to their information, the DHS retains nearly unfettered power to distribute that information,[37] including "to agencies, organizations, or individuals when there could potentially be a risk of harm to an individual."[38] The standard of "potential risk of harm to an individual" is far too broad to act as a meaningful barrier to the near total dissemination of an individual's most private information,[39] not only across the federal government but also to unnamed third parties. Meanwhile, DHS continues to keep the data secret from the person whose interests should be protected by the Privacy Act. The outcome proposed by the DHS in this rulemaking would stand the purpose of the Privacy Act on its head, making personal information widely available across the government while preventing individuals from learning what information about them has been obtained or how it will be used.

- **5 U.S.C. § 552a(d)**

The Privacy Act requires any agency maintaining a system of records to give an individual access to any records they might have about him or her. That person is allowed to review the record, and make copies of it. If the record is incomplete or in error, he or she is also entitled to ask that his or her record be corrected. The Department of Homeland Security seeks to establish a system that provides neither adequate access nor the ability to amend or correct inaccurate, irrelevant, untimely, or incomplete records. The rights of access and correction were central to what Congress sought to achieve through the Privacy Act:

[37] Systems of Records Notice, *supra* note 1 at 69,691. *See also supra* page 5-7.
[38] Systems of Records Notice, *supra* note 1 at 69,690.
[39] Systems of Records Notice, *supra* note 1 at 69,691. *See also supra* page 3-5.

> The committee believes that this provision is essential to achieve an important objective of the legislation: Ensuring that individuals know what Federal records are maintained about them and have the opportunity to correct those records. The provision should also encourage fulfillment of another important objective: maintaining government records about individuals with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to individuals in making determinations about them.[40]

The DHS indicates that the protections in this section should not be applied because "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 … impos[ing] an unreasonable administrative burden by requiring investigations to be continually reinvestigated."[41] This rationale clearly frustrates any meaningful enforcement of Privacy Act rights. Moreover, it opens the door to even greater abuse in the government's collection of personal data. As stated above, individuals should be able to know, after an investigation is completed or made public, the information stored about them in the system.

This restriction not only contravenes key protections in the Privacy Act, but also may act to hinder some government investigations. In 2007, the Justice Department's Inspector General issued a review of the Transportation Security Administration's (TSA) Terrorist Screening Center, which found that the government's watch lists of known or suspected terrorists were filled with errors.[42] The Inspector General observed that these errors could obstruct the capture of terrorists, and that "inaccurate, incomplete, and obsolete watchlist information increases the chances of innocent persons being stopped or detained during an encounter because of being misidentified on a watchlist."[43]

---

[40] H.R. Rep. No. 93-1416, at 15 (1974).
[41] Notice of Proposed Rulemaking, *supra* note 3 at 69,606.
[42] Office of the Inspector General, Department of Justice, Follow-up Audit of the Terrorist Screening Center, Audit Report 07-41 (Redacted for Public Release) (Sept. 2007), available at http://www.usdoj.gov/oig/reports/FBI/a0741/final.pdf.
[43] *Id*.

Withdrawing a citizen's statutory, judicially enforceable right of access provided by the Privacy Act, without providing an alternative right of access and redress leaves citizens without a way to request records pertaining to them or contest the accuracy of information pertaining to them. It is also likely to lead to decision-making that is less accurate, less reliable, and ultimately less likely to fulfill a legitimate agency purpose. By exempting this Fusion Center data from these Privacy Act provisions, DHS prevents individuals from requesting any information that the DHS may be keeping on them. This access requirement is crucial in any system that is to respect the rights of individuals: without meaningful access to the files kept on them, individuals have no recourse if inaccurate, incomplete, or fraudulent information about them is kept in the system. A person with a faulty file will not only lack the opportunity to correct it, he or she will never learn that it is faulty in the first place.

- **5 U.S.C. § 552a(e)(1)**

EPIC urges the DHS to remove exemptions from the Privacy Act's requirement that records in a system be "relevant and necessary" to the agency's purpose.[44] The Privacy Act's "relevant and necessary" requirement is a fundamental and necessary part of the Privacy Act's protections, as it is

> Designed to assure observance of basic principles of privacy and due process by requiring that where an agency delves into an area of personal privacy in the course of meeting government's needs, its action may not be arbitrary.[45]

Part of the Privacy Act's purpose was to stave off the risk that government databases might become dossiers cataloging the various details of individuals' lives. By limiting the data kept by an agency to what is necessary and relevant to the agency's purpose, the Privacy Act limits the extent to which a system of records may invade privacy. Limiting the data to that

[44] 5 U.S.C. § 552a(e)(1) (2010).
[45] S. Rep. No. 93-3418 at 47 (1974).

which is necessary and relevant also reduces the risk of "mission creep," in which a system is pressed into unintended uses. Such mission creep presents additional opportunity for errors, as was seen, for example, in the demise of the Transportation Security Administration's second-generation Computer Assisted Passenger Prescreening System (CAPPS II) program.[46]

The DHS claims that "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."[47] The DHS also notes, that "it is appropriate to retain all information that may aid in establishing patterns of unlawful activity."[48] The mere fact that accuracy may not be clear on the face of information is no reason for the DHS to absolve itself of its Privacy Act obligations.

A blanket exemption from § 552a(e)(1) requirements would allow the records to contain information unrelated to any purpose of the DHS. Furthermore, in assessing the necessity and relevance of records kept in a system, the nature of the system would be taken into account. Any facts in the system that may be helpful to the DHS in a particular investigation would hopefully be relevant and necessary to the investigation at some stage, and thus in compliance with the Privacy Act. As investigations proceed, information can be added or removed from the system as it becomes more or less relevant and necessary. Therefore, the DHS should not exempt this system of records from the relevance and necessity requirements, diminishing accountability and heightening the risk of misuse of the data on citizens and lawful permanent residents.

- **5 U.S.C. 552a(e)(4)(G)-(I) and (f)**

The DHS proposes to exempt their activities from the requirement that they must promulgate rules to establish procedures whereby an individual can access records pertaining to

[46] Matthew L. Wald and John Schwartz, Screening Plans Went Beyond Terrorism, N.Y. Times, Sept. 19 2004 at A35, *available at* http://query.nytimes.com/gst/fullpage.html?res=9402E6DA1439F93AA2575AC0A9629C8B63.
[47] Notice of Proposed Rulemaking, *supra* note 3 at 69,606.
[48] *Id*.

him or her,[49] thereby shutting off any means by which an individual could seek out records with information concerning him or her. Permitting the operation of the DHS proposed fusion center system without being subject to the publication requirements of the Privacy Act will prevent an individual from ever knowing if records in this system of records are maintained pertaining to him or her.

As justification for these exemptions, the DHS references earlier exemptions, stating "because portions of this system are exempt from individual access provisions … DHS is not required to establish requirements, rules, or procedures with respect to such access."[50] However, for the same reasons given above for why the DHS should not be exempted from the individual access provisions, they should also be required to implement formal procedures by which access could be provided.

While agency records may include sensitive information, the DHS further asserts that "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, potential witnesses, and confidential informants.[51] However, the DHS could promulgate rules that would require notification only after an active investigation had been concluded, or with sensitive information, such as the identity of confidential informants, redacted prior to release.

Fusion centers are a uniquely invasive source of federal surveillance. In order to preserve privacy rights, enumerated in the U.S. Constitution and expanded on by statute, the DHS should narrow its claimed exemptions from the Privacy Act of 1974 and provide for specific procedures and requirements to adequately notify, inform, and protect the American public. The DHS'

[49] *See id*.
[50] *Id*.
[51] *Id*.

proposed program should be suspended until such procedures can be implemented. By placing large amounts of personal data into a federal fusion center, the DHS is creating a flawed system and failing to protect individuals' privacy.

2. *The OOCP's Proposal Requires a Narrow Mission with Clear Oversight Mechanisms and Limiting Guidelines*

According to the agency, the purpose of the proposed system of records is to "collect, plan, coordinate, report, analyze, and fuse infrastructure information related to all-threats and all-hazards, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, natural disasters, and other information collected or received from federal, state, local, tribal, and territorial agencies and organizations; foreign governments and international organizations; domestic security and emergency management officials; and private sector entities or individuals into the Department."[52]

This mission statement is overbroad and justifies the collection of personal information for virtually any reason, or for no reason at all. The DHS must set out a statement for its proposal that offers meaningful guidance on the reasons and purpose for the creation of the system of records. Failing to do so, the DHS grants itself unlimited discretion to collect and retain sensitive information on any individual for an infinite duration of time, in direct violation of due process and the United States Constitution,[53] and the clear intent of the Privacy Act.

In addition, the DHS indicates a range of routine uses for the data collected that are so broad as to make meaningless any intent to restrict use by a person associated with DHS through

[52] Systems of Records Notice, *supra* note 1 at 69,689.
[53] U.S. CONST. amend. V.

a data sharing agreement or contractor relationship.[54] The "routine uses" for the information include dissemination "to an agency, organization, or individual when there could potentially be a risk of harm to an individual."[55] The standard of "potential risk of harm to an individual" is too broad to act as a meaningful barrier to the dissemination of an individual's private information.[56] This standard also increases the risk of "mission creep," causing the information to be used for reasons not related to its original purpose. In order to restrict the uses of this data, limiting factors must be enumerated, with specific reference to the mission and goals of government and non-government agencies to which an individual's information could be transmitted.

3. The OOCP's Proposal Requires a New Privacy Impact Assessment

To fulfill the statutory mission of assuring that new programs do not "erode citizens' privacy,"[57] the Chief Privacy Officer must ensure that DHS' proposed federal fusion center project moves forward with the maximum available oversight and privacy requirements. The Department of Homeland Security Privacy Office is responsible for ensuring that DHS activities are fully compliant with statutory privacy laws. The primary oversight mechanism of the Privacy Office is the Privacy Impact Assessment (PIA).

The Homeland Security Act requires a PIA for all DHS systems, including national security systems, if they contain personal information.[58] The Privacy Office has required 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 privacy

[54] Systems of Records Notice, *supra* note 1 at 69,692. *See also supra* page 5-7.
[55] Systems of Records Notice, *supra* note 1 at 69,690.
[56] Systems of Records Notice, *supra* note 1 at 69,691. *See also supra* page 3-5.
[57] 6 U.S.C. § 142 (2010).
[58] 44 U.S.C. § 3501 (2010).

risks.[59] The PIAs allow standardized evaluation of privacy issues so that problems can be identified.[60] The E-Government Act of 2002 requires the DHS to make PIAs publicly available.[61] In addition, "PIAs should be clear, unambiguous, and understandable to the general public."[62]

In December 2008, the Privacy Office released its PIA for state, local, and regional Fusion Centers.[63] This PIA does not address the current project since it is specifically addressed to "state, local, and regional" fusion centers, not encompassing federal projects.[64] In addition, "even if the collection of information remains the same and is already covered by an existing [System of Records Notice] or PIA, if the technology using the information is changed or updated, a PIA must be completed or updated to analyze the new impact of the technology."[65] However, the 2008 PIA identifies seven "risks to privacy" presented by fusion center programs, then "examines these issues and explains the mitigation strategies for those risks…. Where necessary, the Privacy Office offers recommendations on how DHS…can take additional action to further enhance the privacy interests of the citizens they are charged with protecting."

Mitigation strategies are not solutions, however, and they do not prevent the fusion center program from eroding citizens' privacy. Merely writing the PIA does not provide the proper degree of necessary oversight. Neither does "encouraging" fusion centers to take certain actions without mandating those actions as conditions of funding. The Department of Homeland Security has the ability to require that the federal program utilize privacy protections, such as

[59] 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*].
[60] 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.
[61] Pub. L. 107-347 (2002).
[62] DHS PIA Guidelines at 9, *supra* note 59.
[63] Department of Homeland Security, Privacy Impact Assessment for the Department of Homeland Security State, Local, and Regional Fusion Center Initiative, December 11, 2008, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ia_slrfci.pdf.
[64] *Id*.
[65] DHS PIA Guidelines at 6, *supra* note 59.

those recommended in the Fusion Center Guidelines.[66] In a new PIA for the proposed program, the Privacy Office must require specific actions and safeguards in order to maximize the protection afford to individual's with personal data collected by the DHS' proposed system of records.

Conclusion

For the foregoing reasons, the EPIC recommends that the DHS revise its proposed system of records and to fully assess the privacy and security implications of the program, under the federal Privacy Act. A federal fusion center should, at a minimum: (1) provide individuals judicially enforceable rights of access and correction; (2) create suitable retention and disposal standards; (3) limit the distribution of information; (4) limit the mission and goals of the proposed system of records to enumerate standards to guide the collection of information; (5)

[66] "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 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; Security Safeguards Principle: personal data should be protected by reasonable security safeguards against loss or unauthorized access, destruction, misuse, modification, or disclosure; Openness Principle: there should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller; 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; Accountability Principle: a data controller should be accountable for complying with measures that give effect to the principles stated above." In addition, the Guidelines state that "NCISP recommends that privacy policies should eliminate unnecessary discretion in decision making, guide the necessary discretion, and continually audit the process to ensure conformance with the policy; ensure legitimacy – when an agency is developing a new policy or reviewing existing ones, interested parties and competing viewpoints should be represented; clearly define the parameters of the policy; acknowledge and address important issues that currently are not included in some existing criminal intelligence policies; identify the decision points within the intelligence process and provide appropriate guidance and structure for each." *See* U.S. Department of Justice: Fusion Center Guidelines, Developing and Sharing Information and Intelligence in a New Era (Aug. 2006), *available at* http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

create an independent oversight mechanism to prevent "mission creep" and to uphold reporting standards; and (6) conform to a revised PIA that includes requirements for the agency to respect individuals' rights to control their information in possession of federal agencies, as the Privacy Act requires.

Marc Rotenberg
EPIC President

Lillie Coney
EPIC Associate Director

Amie Stepanovich
EPIC National Security Fellow

December 15, 2010.