WORLD **PRIVACY** FORUM

Comments of the World Privacy Forum

To

The Department of Justice regarding System of Records Notice, FBI Insider Threat Program Records (ITPR)," JUSTICE/FBI-023, CPCLO Order No. 007-2016

Via Facsimile

U.S. Department of Justice
Attn: Privacy Analyst,
Office of Privacy and Civil Liberties,
National Place Building,
1331 Pennsylvania Avenue NW., Suite 1000,
Washington, DC 20530–0001

October 12, 2016

The World Privacy Forum welcomes the opportunity to comment on the Federal Bureau of Investigation's proposal to establish a new system of records (SORN) for the FBI Insider Threat Program Records, JUSTICE/FBI–023, CPCLO Order No. 007-2016. The notice appears at 81 Federal Register 64198 (September 19, 2016), https://www.federalregister.gov/d/2016-22410. Please be aware that we submitted comments on the notice of proposed rulemaking regarding the exemption for this system under separate cover.

The World Privacy Forum is a non-profit public interest research and consumer education group. We publish in-depth research papers, policy comments, and consumer education focusing on privacy and security issues. Much of our work explores emerging technology and privacy issues, including health, biometrics, consent, data analytics, and many other rapidly evolving areas of privacy. You can see our publications and more information at www.worldprivacyforum.org.

The Federal Register notice did not provide a method for the electronic submission of comments. **We object to this omission in the strongest possible terms.** Given the limited time allowed for comment, and the near impossibility of using the Postal Service to communicate with any federal agency in a timely manner due to security screening requirements, there is no excuse for not providing for electronic submission. This circumstance should never happen again with any Privacy Act of 1974 request for public comment. Our comments about the specifics of the SORN are below.

I. Clarity

The system notice contains several unclear or confusing elements. First, the SORN references a "Joint Task Force" twice, but there is no explanation of what the Task Force is, what it does, who its members are, or where it is located. Second, the routine uses for the system include unclear terms for potential recipients. We found the following unclear terms:

- person,
- organization,
- government entity,
- entity,
- individual, and
- agencies.

The notice needs more consistent use of language here and clear definitions of the terms used. Is an individual a person? Is an organization also an agency? What is an entity? We suspect that a more complete review of Department system of records notices would uncover similar issues.

II. Blanket Routine Uses

In general, we think it is unhelpful and inappropriate for any agency to refer to blanket routine uses in any of its system of records notices. It is challenging for most readers to understand blanket routine uses and to find them.

As a matter of convenience to the reader and to agency personnel as well, we think that the full text of each routine use applicable to each system should be included in each system notice. The benefits to the reader should be clear. The benefits to the agency are that the inclusion of blanket routine uses will prompt an actual review of their suitability for each system. Not every blanket routine use is appropriate for every agency system of records. We seriously doubt that the Bureau would allow records from this particularly sensitive system of records to be disclosed for all purposes contemplated by the blanket routine uses.

We suggest that the Justice Department phase out references to blanket routine uses, and this is as good a place to start that new policy as any.

III. Blanket Routine Use 6

We object to blanket routine use 6 covering disclosures mandated by law. The notice states:

> As Mandated by Law. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

We do not think it is appropriate to use a non-specific routine use to authorize disclosures mandated by law and we have doubts that this type of routine use is lawful. We cannot object when an agency is legally obliged to make a disclosure. The purpose of publishing routine uses

is to inform the public of the types of disclosures that may occur from any given system of records. The agency publishing a routine use knows what disclosures it must make, but the public does not.

It could take a trained lawyer weeks to review U.S. Code in order to identify all laws that might apply to any given system of records. In our view, it is incumbent on the agency to share its knowledge of required disclosures with the public. We observe that the Congress could have included disclosures required by law as one of the statutory conditions of disclosure in subsection (b) of the Privacy Act of 1974. It did not do so, but provided authority for each agency to define routine uses. The Department may not agree that this routine use is unlawful, but it should decline to continue the routine use as a matter of discretion.

IV. Categories of Records

The description of the categories of records for this system has a reasonable level of detail. We wonder, however, if investigations of insiders will include personal electronic mail, social media activities, and public records. We do not conduct investigations of insider threats, but these additional categories of records and perhaps more would seem to be relevant at times. We gently suggest that the Department review whether the current list is complete.

V. Blanket Routine Use BRU-3 and Routine Use H

Blanket routine use 3 allows disclosure to the public as follows:

> Appropriate Disclosures to the Public. To the news media or members of the general public in furtherance of a legitimate law enforcement or public safety function as determined by the FBI, e.g., to assist in locating fugitives; to provide notifications of arrests; to provide alerts, assessments, or similar information on potential threats to life, health, or property; or **to keep the public appropriately informed of other law enforcement or FBI matters or other matters of legitimate public interest where disclosure could not reasonably be expected to constitute an unwarranted invasion of personal privacy**. (The availability of information in pending criminal or civil cases will be governed by the provisions of 28 CFR 50.2.)

Routine use H allows disclosure --

> To the news media or members of the general public **in furtherance of a legitimate law enforcement or public safety function** as determined by the FBI and, where applicable, consistent with 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

We have two points here. First, both of these routine uses apply to this system, and they overlap or are inconsistent. This illustrates why the automatic application of blanket routine uses is a poor policy. Only one of these routines uses should be used, and we prefer local routine use H.

We still think that the standards for disclosure in routine use H – in furtherance of a legitimate law enforcement or public safety function – are too broad and too unclear. We are at a loss to understand how these types of disclosures are compatible with the purpose of a system that supports insider threat investigations.

Second, the blanket routine use in question includes some types of disclosure that are unobjectionable. In the language quoted above, we highlighted the types of allowable disclosure that are most troublesome. In effect, the routine use establishes authority for broad public disclosure that is standardless and procedureless. Anyone in the Department or the Bureau seemingly has the authority to disclose any personal information from a system of records by deciding that there is a *public interest*. Looked at another way, the authority claimed in the routine use is a "get out of jail free" card that can be cited as a justification for any disclosure that any employee chooses to make.

We object to this broad language generally as well as to its application to this particular system. If the Department insists on keeping the authority for *public interest* disclosures, we suggest that blanket routine use include a much clearer standard as well as a specific procedure.

A routine use adopted by the Department of Homeland Security may be instructive, and it is as follows:

> DHS: 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 the accountability of DHS' officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

We are not endorsing this DHS routine use as written because we think that the language allowing disclosures *necessary to preserve confidence in the integrity of DHS* and *necessary to demonstrate the accountability of DHS' officers, employees, or individuals* is too broad and too unclear.

However, we like the procedure that requires approval of the Chief Privacy Officer in consultation with counsel. This prevents any individual employee from making a wholly independent decision about disclosure and allows for a more consistent determination of necessity.

We suggest that the Department adopt a similar procedure that requires appropriate consultation before any public interest type of disclosure is allowable. The same type of procedure would reduce (but not eliminate) our objections to the *legitimate law enforcement or public safety function* in local routine use H.

VI. Routine Use T

This routine use allows disclosure as follows:

> To designated officers and employees of state, local, territorial, or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant to the recipient agency's decision.

We think that this routine use is inappropriate. The Privacy Act of 1974 allows routine uses when it is not possible to obtain consent from the data subject for a disclosure. **Consent is the preferred way to authorize disclosures from systems of records**. We recognize that consent does not work in many circumstances, including many law enforcement investigations. However, if someone applies for a job and the prospective employer wants a reference from a previous employer, there is no reason why consent cannot be obtained as a condition of the application process. This routine use should be dropped in its entirety.

We find similar language in blanket routine use 10, which we quote here with the objectionable language highlighted.

> BRU–10. Former Employees. The DOJ may disclose relevant and necessary information to a former employee of the Department for purposes of: **responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations**; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility. (Such disclosures will be effected under procedures established in title 28, Code of Federal Regulations, sections 16.300– 301 and DOJ Order 2710.8C, including any future revisions.)

We do not understand why responses to official inquiries are limited to former employees of the Department, but we object to any disclosure for employment or licensing purposes that does not rely on consent of the data subject.

VII. Routine Use U

This routine use allows disclosure as stated below:

> U. To such agencies, entities, and persons as is necessary to ensure the continuity of government functions in the event of any actual or potential disruption of normal government operations. This use encompasses all manner of such situations in which government operations may be disrupted, including: Military, terrorist,

> cyber, or other attacks, natural or manmade disasters, and other national or local emergencies; inclement weather and other acts of nature; infrastructure/ utility outages; failures, renovations, or maintenance of buildings or building systems; problems arising from planning, testing or other development efforts; and other operational interruptions. This also includes all related pre-event planning, preparation, backup/redundancy, training and exercises, and post-event operations, mitigation, and recovery.

We are at a loss to understand this routine use for an insider threat system. If an insider has been determined to be a threat, then it seems unlikely that that insider would be assigned to any activity covered by this routine use. If an insider is under investigation as a threat, we assume that any doubts about the individual would be addressed by assigning the individual to limited duties.

Assigning an insider who is under investigation as a threat to an activity of the type described in the routine use seems unlikely at best. We are having trouble understanding that there would be any assignment to a sensitive task that includes sharing classified or other information about the individual's insider threat investigation with any other *agencies, entities and persons* without limitation. We do not think that this type of sharing would ever occur. We suggest that the routine use be dropped.

We appreciate the opportunity to submit these comments, and we are pleased to answer any questions you may have.

Respectfully submitted,

Pam Dixon