Billing Code: 4151-17

DEPARTMENT OF HEALTH AND HUMAN SERVICES

45 CFR Part 5b

RIN: 0991-AC10

Privacy Act; Implementation

AGENCY: Department of Health and Human Services

ACTION: Notice of Proposed Rulemaking

SUMMARY: In accordance with the Privacy Act of 1974, as amended (the Act), the Department of Health and Human Services (HHS or Department) is proposing to exempt a new system of records, System No. 09-90-1701, HHS Insider Threat Program Records, from certain requirements of the Act.

DATES: Comments on this notice must be received by [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: The public should address written comments on this notice by email to hhsinth@hhs.gov or by mail to the HHS Office of Security and Strategic Information (OSSI), 200 Independence Avenue, SW, Washington, DC 20201.

FOR FURTHER INFORMATION CONTACT: General questions about the NPRM may be submitted to the Assistant Deputy Secretary for National Security by email to hhsinth@hhs.gov, by telephone to (202) 690-5756, or by mail to the HHS Office of Security and Strategic Information (OSSI), 200 Independence Avenue, SW, Washington, DC 20201.

SUPPLEMENTARY INFORMATION:

I. Background on the Insider Threat Program and New System of Records 09-90-1701

Each federal agency is mandated by Presidential Executive Order 13587, issued October 7, 2011, to establish an insider threat detection and prevention program to ensure the security of classified networks and the responsible sharing and safeguarding of classified information consistent with appropriate protections for privacy and civil liberties. The order states in section 2.1:

> The heads of agencies that operate or access classified computer networks shall have responsibility for appropriately sharing and safeguarding classified information on computer networks. As part of this responsibility, they shall implement an insider threat detection and prevention program consistent with guidance and standards developed by the Insider Threat Task Force established in section 6 of this order.

A threat need not be directed at classified information to threaten classified networks. Consequently, insider threats include any of the following: attempted or actual espionage, subversion, sabotage, terrorism, or extremist activities directed against the Department and its personnel, facilities, information resources, and activities; unauthorized use of or intrusion into automated information systems; unauthorized disclosure of classified, controlled unclassified, sensitive, or proprietary information to technology; indicators of potential insider threats or other incidents that may indicate activities of an insider threat; and other threats to the Department, such as indicators of potential for workplace violence or misconduct.

The office that will administer the Department's Insider Threat Program, the Office of Security and Strategic Information (OSSI), serves as the Department's Federal Intelligence Coordinating Office (FICO), which is responsible for coordinating the sharing and safeguarding of classified national security information between HHS and its operating divisions and with the Office of the Director of National Intelligence (ODNI) and its component agencies within the Intelligence Community. Within OSSI, the Directorate of Operations (Counterintelligence) will oversee the

Insider Threat Program; its responsibilities include identifying, countering, mitigating, and deterring exploitation of HHS personnel, information, assets, and other equities by foreign intelligence and security services and agents, terrorists, and transnational criminal organizations working under the direction of a foreign entity. HHS counterintelligence efforts include 1) counterintelligence inquiries and preliminary investigations, 2) national security incident investigations, 3) counterintelligence analysis, 4) insider threats detection and mitigation efforts, 5) counterintelligence and insider threat awareness, and 6) technical threat detection and mitigation.

The records that OSSI compiles to administer the HHS Insider Threat Program, which will be covered by System No. 09-90-1701, may be from any source, including from any HHS component, office, program, record or source, another government agency, or a member of the public; and may include records pertaining to information security, personnel security, or systems security. This system of records includes investigatory material compiled for law enforcement purposes and information classified in the interest of national security.

Note that System No. 09-90-1701 will not cover investigatory material that OSSI compiles solely for the purpose of determining suitability, eligibility, or qualification for federal civilian employment, military service, federal contracts, or access to classified information, because such records are covered by other HHS systems of records; specifically: 09-90-0002 "Investigatory Material Compiled for Security and Suitability Purposes System" with respect to HHS Office of Inspector General determinations, and 09-90-0020 "Suitability for Employment Records" as to all other HHS determinations.

The new system of records will consist of records compiled and used by the Department's Office of Security and Strategic Information (OSSI), within the Immediate Office of the Secretary

(IOS), to administer the Department's Insider Threat Program, including law enforcement investigatory material and classified intelligence information. Such records are eligible to be exempted from certain requirements of the Privacy Act under subsections (k)(1) and (k)(2) of the Act. The exemptions proposed for those records are necessary and appropriate to protect the integrity of insider threat investigations and records and prevent disclosure of information that would reveal investigation subjects, investigative and security techniques, national security information, security sensitive information, personal privacy information, and identities of confidential sources and law enforcement personnel involved in investigations. Elsewhere in today's *Federal Register* HHS has published a System of Records Notice (SORN) for System No. 09-90-1701 for public notice and comment which describes the new system of records in more detail.

The Privacy Act requirements from which HHS is proposing to exempt eligible records in System No. 09-90-1701 are those contained in subsections (c)(3), (d)(1)-(4), (e)(1), (e)(4)(G), (H), and (I), and (f) of the Privacy Act, which require the agency to provide an accounting of disclosures; provide notification, access, and amendment rights, rules, and procedures; maintain only relevant and necessary information; and identify categories of record sources. If the HHS Insider Threat Program obtains law enforcement investigatory material from another Privacy Act system of records that has been exempted from Privacy Act requirements based on subsection (j)(2) of the Act, that material will be exempt in System No. 09-90-1701 to the same extent it is exempt in the source system, so may be exempt from any of these subsections of the Act: (c)(3)-(4); (d)(1)-(4); (e)(1)-(3), (e)(4)(G)-(I), (e)(5), (e)(8), (e)(12); (f); (g); and (h).

II. Proposed Exemptions and Affected Records

The Insider Threat Program system of records includes investigatory material compiled for law enforcement purposes and information classified in the interest of national security. While OSSI does not perform criminal law enforcement activity as its principal function, OSSI may compile in System No. 09-90-1701 material obtained from other agencies or components which perform as their principal function activities pertaining to the enforcement of criminal laws, and which have exempted their records from certain Privacy Act requirements, based on 5 U.S.C. 552a(j)(2). All other investigatory material compiled for law enforcement purposes is eligible to be exempted from certain Privacy Act requirements based on 5 U.S.C. 552a(k)(2). Information classified in the interest of national security is eligible to be exempted from certain Privacy Act requirements, based on 5 U.S.C. 552a(k)(1). Accordingly, the Department is establishing these exemptions for System No. 09-90-1701:

- Law enforcement investigatory material that is from another system of records in which such material was exempted from access and other requirements of the Privacy Act (the Act), based on 5 U.S.C. 552a(j)(2), will be exempt in System No. 09-901701 on the same basis (5 U.S.C. 552a(j)(2)) and from the same requirements as in the source system, which may include any of these requirements of the Act: (c)(3)-(4); (d)(1)-(4); (e)(1)-(3), (e)(4)(G)-(I), (e)(5), (e)(8), (e)(12); (f); (g); and (h);
- All other law enforcement investigatory material in System No. 09-90-1701 will be exempt, based on 5 U.S.C. 552a(k)(2), from the requirements in subsections (c)(3), (d)(1)-(4), (e)(1), and (e)(4)(G)-(I), and (f) of the Act, However, if any individual is denied a right, privilege, or benefit to which the individual would otherwise be entitled by Federal law or for which the individual would otherwise be eligible, access will be granted, except to the extent that the disclosure would reveal the identity of a source who

furnished information to the Government under an express promise of confidentiality; and

- Information that is classified in the interest of national security will be exempt, based on 5 U.S.C. 552a(k)(1), from the requirements in subsections (c)(3), (d)(1)-(4), (e)(1), and (e)(4)(G)-(I), and (f) of the Act.

III. Exemption Rationales

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k). Where HHS determines compliance would not appear to interfere with or adversely affect the purpose of this system to detect, deter, or mitigate insider threats, the applicable exemption may be waived by HHS in its sole discretion. Exemptions from the particular subsections are necessary and appropriate, and justified for the following reasons:

- 5 U.S.C. 552a(c)(3) (the requirement to provide accountings of disclosures) and 5 U.S.C. 552a(d)(1)-(4) (requirements addressing notification, access, and amendment rights, collectively referred to herein as access requirements). Providing individual record subjects with accountings of disclosures and with notification, access, and amendment rights with respect to Insider Threat Program records could reveal the existence of an investigation, investigative interest, investigative techniques, details about an investigation, security-sensitive information such as information about security measures and security vulnerabilities, information that must remain non-public to protect national security or personal privacy–identities of law enforcement personnel, or other sensitive or classified information. Revealing such information to record subjects would thwart or impede pending and future law enforcement investigations and efforts to protect national security, and would violate personal privacy. Revealing the information would enable

record subjects or other persons to evade detection and apprehension by security and law enforcement personnel; destroy, conceal, or tamper with evidence or fabricate testimony; or harass, intimidate, harm, coerce, or retaliate against witnesses, complainants, investigators, security personnel, law enforcement personnel, or their family members, their employees, or other individuals. With respect to investigatory material compiled for law enforcement purposes, the exemption pursuant to 5 U.S.C. 552a(k)(2) from access requirements in subsection (d) of the Act is statutorily limited. If any individual is denied a right, privilege, or benefit to which the individual would otherwise be entitled by Federal law or for which the individual would otherwise be eligible, access will be granted, except to the extent that the disclosure would reveal the identity of a source who furnished information to the Government under an express promise of confidentiality.

- 5 U.S.C. 552a(e)(1) (the requirement to maintain only relevant and necessary information authorized by statute or Executive Order). It will not always be possible to determine at the time information is received or compiled in this system of records whether the information is or will be relevant and necessary to a law enforcement investigation or to protecting national security. For example, a tip or lead that does not appear relevant or necessary to uncovering an insider threat by itself or at the time the tip or lead is received may prove to be relevant and necessary when combined with other information that reveals a pattern or that comes to light later.
- 5 U.S.C. 552a(e)(4)(G) and (H) (the requirements to describe procedures by which subjects may be notified of whether the system of records contains records about them and seek access or amendment of a record). These requirements concern individual access to records, and the records are exempt under (c) and (d), as described above. To

the extent that (e)(4)(G) and (H) are interpreted to require more detailed procedures regarding record notification, access, or amendment than have been published in the **Federal Register**, exemption from those provisions is necessary for the same rationale as applies to (c) and (d).

- 5 U.S.C. 552a(e)(4)(I) (the requirement to describe the categories of record sources). To the extent that this subsection is interpreted to require a more detailed description regarding the record sources in this system than has been published in the **Federal Register,** exemption from this provision is necessary to protect the sources of law enforcement and intelligence information and to protect the privacy and safety of witnesses and informants and others who provide information to HHS. Further, greater specificity of sources of properly classified records could compromise national security. Moreover, because records used in the Insider Threat Program could come from any source, it is not possible to know every category in advance in order to list them all in the SORN. Some record source categories may not be appropriate to make public in the SORN if, for example, revealing them could enable record subjects or other individuals to discover investigative techniques and devise ways to bypass them to evade detection and apprehension.
- 5 U.S.C. 552a(f) (the requirement to promulgate rules to implement provisions of the Privacy Act). To the extent that this subsection is interpreted to require agency rules addressing the above exempted requirements, exemption from this provision is also necessary to protect the sources of law enforcement and intelligence information and to protect the privacy and safety of witnesses and informants and others who provide

information to HHS. Greater specificity in rulemaking regarding properly classified records could compromise national security.

IV. Analysis of Impacts

The agency has reviewed this rule under Executive Orders 12866 and 13563, which direct agencies to assess costs and benefits of available regulatory alternatives and, if regulation is necessary, to maximize the net benefits. The agency believes that this rule is not a significant regulatory action under Executive Order 12866, and therefore does not constitute an Executive Order 13771 regulatory action, because it will not (1) have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local or tribal governments or communities; (2) create a serious inconsistency or otherwise interfere with an action taken or planned by another agency; (3) materially alter the budgetary impact of entitlements, grants, user fees or loan programs, or the rights and obligations of recipients thereof; or (4) raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in Executive Order 12866.

The Regulatory Flexibility Act requires agencies to analyze regulatory options that would minimize any significant impact of a rule on small entities. Because the rule imposes no duties or obligations on small entities, the Department certifies that the rule will not have a significant economic impact on a substantial number of small entities.

Section 202(a) of the Unfunded Mandates Reform Act of 1995 requires that agencies prepare a written statement, which includes an assessment of anticipated costs and benefits, before proposing "any rule that includes any Federal mandate that may result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100,000,000 or

more (adjusted annually for inflation) in any one year." The current threshold after adjustment for inflation is $144 million, using the most current (2015) Implicit Price Deflator for the Gross Domestic Product. The Department does not expect that this final rule would result in any one-year expenditure that would meet or exceed this amount.

List of Subjects in 45 CFR Part 5b

Privacy.

For the reasons stated in the preamble, the Department's Privacy Act Regulations, part 5b of 45 CFR Subtitle A, are proposed to be amended as follows:

PART 5b—PRIVACY ACT REGULATIONS

1. The authority citation for Part 5b continues to read as follows:

Authority: 5 U.S.C. 301, 5 U.S.C. 552a

2. Section 5b.11 is amended by adding paragraph (b)(2)(viii)(A) to read as follows:

§ 5b.11 Exempt systems

*****

(b) ***

(2) ***

(viii) ***

(A) HHS Insider Threat Program Records, 09-90-1701.

Dated: June 29, 2018

Michael Schmoyer
Assistant Deputy Secretary for National Security

Dated: August 13, 2018

Alex M. Azar II
Secretary

[FR Doc. 2018-17888 Filed: 8/22/2018 8:45 am; Publication Date: 8/23/2018]