

**Post-Hearing Questions for the Record  
Submitted to Director Joseph Clancy**

**From Chairman James Lankford and  
Chairman Ron Johnson**

**"Ongoing Challenges at the U.S. Secret Service  
and Their Government-Wide Implications"**

**November 17, 2015**

**United States Senate, Subcommittee on Regulatory Affairs and Federal  
Management  
Committee on Homeland Security and Governmental Affairs**

<b>Question#:</b>	1
<b>Topic:</b>	Inappropriate use of information systems
<b>Hearing:</b>	Examining Ongoing Challenges at the U.S. Secret Service and their Government-Wide Implications
<b>Primary:</b>	The Honorable Ron Johnson
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Inappropriate use of information systems is likely a security violation. What is the status of any ongoing security clearance investigations and adjudications?

**Response:** For the employees who were identified by the Department of Homeland Security (DHS) Office of Inspector General (OIG) as being involved in accessing a record containing personally identifiable information (PII) in the internal database, security clearance warning letters are being issued for inappropriate use of information systems.

<b>Question#:</b>	2
<b>Topic:</b>	Maintaining records
<b>Hearing:</b>	Examining Ongoing Challenges at the U.S. Secret Service and their Government-Wide Implications
<b>Primary:</b>	The Honorable Ron Johnson
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** What is the reasoning for the Secret Service maintaining records of unsuccessful applications for an extended period of time that contain sensitive PII?

Does the Secret Service currently maintain similar records of unsuccessful applications that are not deemed relevant?

**Response:** At the time of the events in question, the Secret Service was still governed by records retention schedules requiring this type of information be retained for twenty years. Due to the fact that these schedules were vetted, approved, and signed by the National Archives and Records Administration (NARA), adherence to these schedules was a matter of legal compliance. New NARA-approved retention schedules have now replaced the legacy schedules, and information relating to applicants who are not hired is held only for two years, unless a formal background investigation is conducted. If a formal background investigation is conducted, the case file is held for five years.

<b>Question#:</b>	3
<b>Topic:</b>	Secret Service Ethics Guide
<b>Hearing:</b>	Examining Ongoing Challenges at the U.S. Secret Service and their Government-Wide Implications
<b>Primary:</b>	The Honorable Ron Johnson
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Please describe the process to verify that Secret Service employees have reviewed the Secret Service Ethics Guide on an annual basis.

**Response:** This guide was distributed electronically and in hardcopy in 2013 in response to one of the Professionalism Reinforcement Working Group (PRWG) recommendations, which reads as follows:

*PRWG Recommendation: Reinforcement of Ethical Behaviors: The USSS notifies its workforce regarding policy changes on discipline, including expectations on ethical behavior and conduct through issuance of policy directives. However, the USSS should use multiple approaches to reinforce the importance of ethical behavior and conduct at all times. For example, the USSS should consider issuing all current employees and all new employees a user friendly, easy to read manual highlighting the organization's core values, compliance principles, standards of conduct, and the expectation that employees adhere to standards of ethical conduct.*

The ethics guide provides a comprehensive summary of relevant statutes, regulations, and policies. Many of the rules in the ethics guide are contained in Secret Service manual sections to which employees certify on an annual basis via SSF 3218.

<b>Question#:</b>	4
<b>Topic:</b>	Personally Identifiable Information 1
<b>Hearing:</b>	Examining Ongoing Challenges at the U.S. Secret Service and their Government-Wide Implications
<b>Primary:</b>	The Honorable James Lankford
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** During your testimony you were asked if the Secret Service maintains paper files with personally identifiable information (PII) in addition to the PII stored on electronic databases.

Does the Secret Service still maintain paper files in any of its offices containing personally identifiable information (PII)?

**Response:** Yes.

**Question:** If so, who has access to such files and how are those files stored?

**Response:** Access to records containing such information is generally controlled by the access procedures set out under the Privacy Act of 1974, title 5 of the United States Code, section 552a (Privacy Act). System of Record Notices (SORNs) required under the Privacy Act which implicate record systems maintained by the Secret Service are published by the Department of Homeland Security (DHS), the Office of Personnel Management, and the Equal Employment Opportunity Commission. The SORN sets forth the routine uses for access to each system as well as the storage requirements for each system. Copies of Secret Service SORNs as most recently published by DHS are attached.

**Question:** If so, what security controls does the Secret Service have in place to prevent, detect, and respond to the unauthorized access of any paper files containing PII in any of its offices?

**Response:** Most types of PII records have specific additional regulatory storage, handling, and reporting protocols (e.g., storing in a locked room with access controls/logs). Information put into inactive storage includes a specific notation on National Archives form SF 135 that the files must be protected under the Privacy Act.

<b>Question#:</b>	5
<b>Topic:</b>	Dismiss employees
<b>Hearing:</b>	Examining Ongoing Challenges at the U.S. Secret Service and their Government-Wide Implications
<b>Primary:</b>	The Honorable James Lankford
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** In the context of Secret Service employee removal authority, you testified that you would like greater ability to dismiss employees that violate agency policy and the law.

What additional removal authority would assist you in changing the current culture and ensure that agency policy and the law is respected?

**Response:** While we believe that current law allows for a reasonable process and means to remove employees from federal employment in misconduct cases, the pace of that removal action is often slow and does not always foster a culture of accountability. For instance, when a case has been referred to, and accepted by, the OIG for investigation, the Secret Service can be delayed in taking action to address instances of employee misconduct, including criminal misconduct. In these instances the Secret Service must wait for the OIG to fully complete their investigation and issue a report which may lack the underlying evidence, sworn statements, and sometimes be in a redacted format. We believe that, if OIG were to provide the Secret Service with real-time information concerning evidence developed during an OIG investigation, we would, in some cases, be able to take expeditious disciplinary action against employees. For instance, if the OIG provided the Secret Service with a sworn statement in which the employee admits to the misconduct, the Secret Service could propose disciplinary action in advance of a receiving a finalized, formal report. In this regard, we will engage with OIG to explore this possible change to existing procedure and any other changes that may lead to a greater culture of accountability in the Service workforce.

<b>Question#:</b>	6
<b>Topic:</b>	Whistleblowers
<b>Hearing:</b>	Examining Ongoing Challenges at the U.S. Secret Service and their Government-Wide Implications
<b>Primary:</b>	The Honorable James Lankford
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Concerning the topic of agency whistleblowers, you stated "everyone in the Service knows that whistleblowers perform a vital function" and "there's no retaliation" against them.

Can you explain the steps the Service is currently taking to ensure that all whistleblowers are properly protected and shielded from retaliation?

**Response:** The Secret Service recognizes its obligation to protect the rights afforded to employees in making protected disclosures, including disclosures made to Congress, and values the benefits derived from the resulting oversight.

The Secret Service is committed to creating open lines of communication within the agency to ensure concerns raised at any level receive the attention they deserve, and to ensure that employees who bring concerns to light are praised for doing so, rather than retaliated against.

Biennial training on certain federal anti-discrimination and "whistleblower" protections is required by the No FEAR Act for all Department of Homeland Security (DHS) employees. This No FEAR Act course was developed by the DHS Office for Civil Rights and Civil Liberties' (CRCL) Equal Employment Opportunity and Diversity Division and its CRCL Institute based on an anti-harassment training course created by the Central Intelligence Agency's Office for Equal Employment Opportunity Office.

Further, an agency-wide message was issued on October 30, 2015, regarding "Whistleblower Protection Awareness" which referenced policy manual sections related to disclosures to Congress and included a link to "information to help employees easily determine what they should report, how to report suspected issues, what training DHS offers, [and] what legal protections are available..."

Additionally, Secret Service Manual guidelines requiring employees to report misconduct or retaliation were reiterated to all employees in an official message to the workforce on March 23, 2015. It is important that employees recognize the agency's position on this issue, and Director Clancy will continue to emphasize it to the workforce. The Secret Service fully respects and supports the rights of whistleblowers, and retaliation of any kind is not and will not be tolerated. These rights and protections are clearly stated in the Secret Service Ethics Guide, the Table of Penalties, and within the Secret Service Manual.

<b>Question#:</b>	7
<b>Topic:</b>	Personally Identifiable Information 2
<b>Hearing:</b>	Examining Ongoing Challenges at the U.S. Secret Service and their Government-Wide Implications
<b>Primary:</b>	The Honorable James Lankford
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Your testimony outlined that recent Secret Service policy now requires the purging of applicant files every two years to improve internal protections of personally identifiable information (PII) housed on its databases.

When did this policy change?

**Response:** This policy changed on October 1, 2015. Please note, at the time of the events in question, the Secret Service was still governed by records retention schedules requiring this type of information be retained for twenty years. Due to the fact that these schedules were vetted, approved, and signed by NARA, adherence to these schedules was a matter of legal compliance. New NARA-approved retention schedules have now replaced the legacy schedules, and information relating to applicants who are not hired is held only for two years, unless a formal background investigation is conducted. If a formal background investigation is conducted, the case file is held for five years.

**Question:** What additional policies and training does the Secret Service have in place to ensure PII housed on its databases is not improperly accessed?

**Response:** A Secret Service Information Resources Management (IRM) directive entitled “IRM Privacy Act Review” includes policy for reviewing new IT systems or changes to existing IT systems to determine Privacy Act impact. Related Secret Service and Department of Homeland Security (DHS) directives help ensure awareness of and compliance with PII regulations, through mechanisms such as the Privacy Threshold Analysis/Privacy Impact Analysis processes.

Existing policies and training include longstanding guidance regarding the proper access to databases and handling of Privacy Act protected information, which is clearly stated in the Secret Service Ethics Guide, in the Table of Penalties, and within the Secret Service Manual sections related to rules of behavior with respect to the use of information technology. Employees are required to certify annually that they have reviewed these manual sections.

Additionally, the Secret Service provides a one-hour briefing to Special Agent and Uniformed Division Training Classes that includes material on the Privacy Act. A senior Government Information Specialist from the Freedom of Information Act and Privacy Act Branch of the Office of Government and Public Affairs teaches the class and focuses, in part, on PII.

<b>Question#:</b>	7
<b>Topic:</b>	Personally Identifiable Information 2
<b>Hearing:</b>	Examining Ongoing Challenges at the U.S. Secret Service and their Government-Wide Implications
<b>Primary:</b>	The Honorable James Lankford
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

A one-hour in-service online training titled “IT Security Awareness” is required as part of the agency’s Federal Information Security Management Act (“FISMA”) obligations. The course outlines the role of federal employees in the protection of information and in ensuring the secure operation of federal information systems.

The Privacy Act is also discussed during in-service ethics classes administered to the field by Secret Service Office of Chief Counsel instructors.

Further, DHS requires Secret Service employees to complete annual in-service online training titled, “Privacy at DHS: Protecting Personal Information.” This training was incorporated into the required curriculum in 2012 and covers proper handling of PII.

Finally, in August, the agency began including a dedicated block of instruction for the new Special Agent Training Classes regarding the Release of Information. The class provides an overview of the Privacy Act and the Freedom of Information Act, reviews employees’ responsibilities under those Acts and the consequences for failing to fulfill them, and more generally, discusses the proper release and use of information employees have access to. A similar block of instruction for the Uniformed Division Training Classes was added in November. Further, additional training is provided to new hires at Secret Service New Employee Orientation.

**Question:** Has the Secret Service implemented any additional policies and training in response to recent improper and illegal accesses?

**Response:** In light of the DHS OIG report of September 25, 2015, and subsequent addendum of October 22, 2015, specific guidelines have been established and are effective for processing disciplinary and adverse actions resulting from the misuse of Secret Service database systems and/or the unauthorized disclosure of sensitive information. Additionally, and as stated above, in August, the agency began including a dedicated block of instruction for the new Special Agent Training Classes regarding the Release of Information. The class provides an overview of the Privacy Act and the Freedom of Information Act, reviews employees’ responsibilities under those Acts and the consequences for failing to fulfill them, and more generally, discusses the proper release and use of information employees have access to. A similar block of instruction for the Uniformed Division Training Classes was added in November. Further, additional training is provided to new hires at Secret Service New Employee Orientation.

[Federal Register Volume 76, Number 154 (Wednesday, August 10, 2011)]  
[Notices]  
[Pages 49497-49500]  
From the Federal Register Online via the Government Printing Office [[www.gpo.gov](http://www.gpo.gov)]  
[FR Doc No: 2011-20226]

-----  
DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2011-0068]

Privacy Act of 1974; Department of Homeland Security/United States Secret Service--001 Criminal Investigation Information System of Records

AGENCY: Privacy Office; DHS.

ACTION: Notice of Privacy Act system of records.

-----  
SUMMARY: In accordance with the Privacy Act of 1974 and as part of the Department of Homeland Security's biennial review of system of record notices, the Department of Homeland Security proposes to update and reissue a current Department of Homeland Security system of records titled, ``Department of Homeland Security/United States Secret Service--001 Criminal Investigation Information System of Records.'' As a result of biennial review of this system, records have been updated within the categories of records, routine uses, and notification procedures of this system of records notice. Additionally, the Department of Homeland Security previously published a Final Rule in the Federal Register to exempt this system of records from certain provisions of the Privacy Act; the current updates to this system of records do not impact the nature of the exemptions claimed. This updated system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Written comments must be submitted on or before September 9, 2011.

ADDRESSES: You may submit comments, identified by docket number DHS-2011-0068 by one of the following methods:

Federal e-Rulemaking Portal: <http://www.regulations.gov>.

Follow the instructions for submitting comments.

Fax: 1-866-466-5370.

Mail: Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

Docket: For access to the docket, to read background documents, or comments received go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Latita Payne (202-406-6370), Privacy Officer, United States Secret Service, 245 Murray Lane, SW., Building T-5, Washington, DC 20223. For privacy issues please contact: Mary Ellen Callahan (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, and as part of the Department of Homeland Security's (DHS) biennial review of system of record notices, DHS/United States Secret Service (USSS) proposes to update and reissue a current DHS system of records titled, DHS/USSS-001 Criminal Investigation Information System. As a result of biennial review of this system, records have been updated within the categories of individuals covered in this system and categories of records in this system in order to further define, narrow, and eliminate duplicative categories.

[[Page 49498]]

Routine Use P was deleted to eliminate duplicative information. The notification procedures were updated to better reflect the reason for exemption and the method for access. This updated system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates individuals' records. The Privacy Act applies to information that is maintained in a ``system of records.'' A ``system of records'' is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR part 5.

The Privacy Act requires that each agency publish in the Federal Register a description denoting the type and character of each system of records in order to make agency recordkeeping practices transparent, to notify individuals about the use of their records, and to assist the individual to more easily find files within the agency. Below is a description of the Criminal Investigation Information System.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this revised system of records to the Office of Management and Budget and to the Congress.

System of Records:

Department of Homeland Security (DHS)/United States Secret Service (USSS)-001.

## System name:

DHS/USSS-001 Criminal Investigation Information System.

## Security classification:

Unclassified and Classified.

## System location:

Records are maintained at the United States Secret Service Headquarters, 950 H St., NW., Washington, DC 20223 and field offices.

## Categories of individuals covered by the system:

Individuals who have been or are currently the subject of a criminal investigation by DHS/USSS in connection with the performance by that agency of its authorized criminal investigative functions;

Individuals who are informants, suspects, defendants, fugitives, released prisoners, organized crime figures, or those associated with these individuals who have been identified by DHS/USSS during the course of official USSS criminal investigations or by information supplied by other law enforcement agencies, government units, and the general public;

Individuals who are witnesses and victims of crime as related to official USSS investigations;

Individuals who are complainants and correspondents; and

Individuals who are payees, registered owners, or endorsers of stolen or lost obligations and other securities of the United States.

## Categories of records in the system:

Records containing information compiled for the purpose of identifying individual criminal offenders and informants, suspects, defendants, fugitives, released prisoners, organized crime figures, or those associated with these individuals in furtherance of an official criminal investigation. The records consist of identifying data, including, but not limited to, name, date of birth, Social Security number, telephone number, home address, business address, spouse and family information, physical description, notations of arrest, the nature and imposition of criminal charges, sentencing, confinement, release, and parole or probations status concerning criminal offenders, defendants and suspects, witnesses, victims, and law enforcement personnel;

Records containing reports identifiable with an individual, compiled at various stages of the process of enforcement of criminal laws from arrest or indictment through release from supervision, including reports of informants and investigators, for the purpose of a criminal investigation;

Records containing investigatory material compiled for law enforcement purposes, including but not limited to, handwriting exemplars; laboratory analyses of inks and papers; handwriting analyses; petitions for the remission of forfeitures; notice of non-receipt of Treasury drafts; affidavits of forged endorsements; opinions of the examiner of questioned documents; reports or opinions from the examination of computer evidence; reports or opinions from the examination of altered cellular telephones; certificates by owners of U.S. registered securities concerning forged requests for payments or assignments; applications for relief on account of loss, theft, or destruction of U.S. Savings Bonds or checks; photographic reproductions of obligations and other securities of the United States; contraband items; claims against the United States for the proceeds of government checks and bonds; reports necessary for the settlement of check and bond claims; polygraph case files; forensic examination information;

search warrants and search warrant returns; indictments; certified inventories of property held as evidence; sworn and unsworn witness statements; state, local, and foreign criminal investigative information and reports; names and telephone numbers of persons intercepted by electronic, mechanical, or other device under the provisions of 18 U.S.C. Sec. 2510 et seq. compiled during the lawful course of a criminal or civil investigation.

Authority for maintenance of the system:

The Homeland Security Act of 2002, Public Law 107-296; Federal Records Act, 44 U.S.C. 3101; 5 U.S.C. 301; 18 U.S.C. 3056 and 3056A; and 6 CFR part 5.

Purpose(s):

The purpose of this system is to collect and maintain criminal records related to individuals being investigated by DHS/USSS in connection with USSS' criminal law enforcement functions, including but not limited to investigating counterfeiting offenses, financial institution fraud, computer and telecommunications fraud, false identification documents, access device fraud, advance fee fraud, and electronic funds transfer fraud.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside the Department of Homeland Security (DHS) as a routine use pursuant to 5 U.S.C. 552a(b) (3) as follows:

A. To the Department of Justice or other federal agency conducting

[[Page 49499]]

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.

B. 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.

C. 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.

D. 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.

E. 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 programs (whether maintained by DHS or another agency or entity) or harm to the individual who relies 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.

F. 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.

G. 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.

H. To employees and officials of financial and commercial business firms and to private individuals, information pertaining to actual or suspected criminal offenders where such disclosure is considered reasonably necessary for the purpose of furthering USSS efforts to investigate the activities of and apprehend criminal offenders and suspected criminal offenders.

I. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosure to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a subpoena from a court of competent jurisdiction.

J. To an appropriate federal, state, local, tribal, territorial, foreign, or international agency, if the information is relevant and necessary to agency's decision concerning the hiring or retention of an individual, the issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit and when disclosure is appropriate to the proper performance of the official duties of the person making the request.

K. To the Integrated Automated Fingerprint Identification System (IAFIS) managed by the Department of Justice, Federal Bureau of Investigations in connection with USSS's utilization.

L. To federal, state, and local government agencies foreign or domestic, having prosecutorial and civil law enforcement functions for use by attorneys, magistrates, and judges, parole or probation authorities and other law enforcement authorities for the purpose of developing a criminal or civil investigation, prosecuting, sentencing, or determining the parole and probation status of criminal offenders or suspected criminal offenders.

M. To personnel of other federal, state, and local law enforcement agencies, foreign or domestic, for the purpose of developing

information on subjects involved in USSS criminal investigations and assisting other law enforcement agencies in the investigation and prosecution of violations of the criminal laws which those agencies are responsible for enforcing.

N. To personnel of federal, state, and local governmental agencies, foreign and domestic, where such disclosure is considered reasonably necessary for the purpose of furthering USSS efforts to investigate the activities of and apprehend criminal offenders and suspected criminal offenders.

O. To personnel of federal, state, and local governmental agencies, foreign and domestic, where there is a showing of reasonable necessity to obtain such information to accomplish a valid law enforcement purpose as agreed to by the USSS.

P. 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's 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.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper and electronic records in this system are stored in secure facilities and/or behind locked doors. Electronic records media, such as magnetic tape, magnetic disk, digital media, and CD ROM are stored in proper environmental controls.

Retrievability:

This system is indexed by name, address, vehicle license number, and/or telephone number, and is retrieved

[[Page 49500]]

through computer search of magnetic media indices both at Headquarters and in the field offices. Additionally, subjects are retrievable from the computerized files by physical description. Access to the physical files containing records is by case number.

Safeguards:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS and USSS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored, processed, and transmitted. Access to the computer system containing the records in this system is limited to those individuals who have a USSS approved need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Retention and disposal:

All judicial cases are retained for a period of 30 years after case closure (unless otherwise required to be held permanently for transfer to the National Archives and Records Administration). Non-judicial

criminal investigative cases (except non-judicial check and bond cases) are retained for 10 years. Non-judicial check claim and bond forgery cases are retained for 5 years. Administrative files of an investigatory nature are retained for 5 years. Investigations for other districts are retained for 2 years. Receipts are retained for a variety of time periods depending on the case file to which they pertain. Arrest history forms are held permanently for transfer to the National Archives and Records Administration. Headquarters criminal investigative case files are retained for 30 years. Consensual and non-consensual interception indices are held for 10 years or when investigative use no longer exists, whichever is longer. Fingerprint and photograph files are retained at varying intervals based on case type and in accordance with record retention schedules approved by the National Archives and Records Administration.

System Manager and address:

Assistant Director, Office of Investigations, U.S. Secret Service,  
245 Murray Lane SW., Building T-5, Washington, DC 20223.

Notification procedure:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, DHS/USSS will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the USSS FOIA Officer, 245 Murray Drive SW., Building T-5, Washington, DC 20223. If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief FOIA Officer, Department of Homeland Security, whose contact information can be found at <http://www.dhs.gov/foia>.

When seeking records about yourself from this system of records or any other USSS system of records, your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, <http://www.dhs.gov> or 1-866-431-0486. In addition you should provide the following:

An explanation of why you believe the Department would have information on you,

Specify when you believe the records would have been created,

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information USSS may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Record access procedures:

See ``Notification procedure'' above.

Contesting record procedures:

See ``Notification procedure'' above.

## Record Source Categories:

The Secretary of Homeland Security has exempted this system from subsections (e) (4) (I) of the Privacy Act pursuant to 5 U.S.C. 552a(j) (2) and (k) (2) and (k) (3); therefore, records sources shall not be disclosed.

## Exemptions claimed for the system:

Pursuant to exemption 5 U.S.C. 552a(j) (2) of the Privacy Act and the limitations therein, this system is exempt from 5 U.S.C. 552a(c) (3) and (4); (d); (e) (1), (e) (2), (e) (3), (e) (4) (G), (e) (4) (H), (e) (4) (I), (e) (5) and (e) (8); (f); and (g). Pursuant to 5 U.S.C. 552a(k) (1), (k) (2), (k) (3) this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a(c) (3), (d), (e) (1), (e) (4) (G), (e) (4) (H), (e) (4) (I), and (f). In addition, to the extent a record contains information from other exempt systems of records; USSS will rely on the exemptions claimed for those systems.

Dated: July 14, 2011.

Mary Ellen Callahan,  
Chief Privacy Officer, Department of Homeland Security.  
[FR Doc. 2011-20226 Filed 8-9-11; 8:45 am]  
BILLING CODE 4810-42-P

[Federal Register Volume 74, Number 167 (Monday, August 31, 2009)]  
[Rules and Regulations]  
[Pages 45086-45087]  
From the Federal Register Online via the Government Printing Office [[www.gpo.gov](http://www.gpo.gov)]  
[FR Doc No: E9-20758]

-----  
DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2009-0076]

Privacy Act of 1974: Implementation of Exemptions; Department of  
Homeland Security; U.S. Coast Guard--029 Notice of Arrival and  
Departure System

AGENCY: Privacy Office, DHS.

ACTION: Final rule.

-----  
SUMMARY: The Department of Homeland Security is issuing a final rule to  
amend its regulations to exempt portions of a Department of Homeland  
Security U.S. Coast Guard system of records entitled the ``Department  
of Homeland Security U.S. Coast Guard--029 Notice of Arrival and  
Departure System of Records'' from certain provisions of the Privacy  
Act. Specifically, the Department exempts portions of the Department of  
Homeland Security U.S. Coast Guard--029 Notice of Arrival and Departure  
system from one or more provisions of the Privacy Act because of  
criminal, civil, and administrative enforcement requirements.

DATES: Effective Date: This final rule is effective September 30, 2009.

FOR FURTHER INFORMATION CONTACT: For general questions please contact:  
David Roberts (202-475-3521), Privacy Officer, United States Coast  
Guard. For privacy issues contact: Mary Ellen Callahan (703-235-0780),  
Chief Privacy Officer, Privacy Office, U.S. Department of Homeland  
Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

Background

The Department of Homeland Security (DHS) published a notice of  
proposed rulemaking in the Federal Register, 73 FR 75373, December 11,  
2008, proposing to exempt portions of the system of records from one or  
more provisions of the Privacy Act because of criminal, civil, and  
administrative enforcement requirements. The system of records is the  
DHS/U.S. Coast Guard (USCG)--029 Notice of Arrival and Departure  
system. The DHS/USCG--029 Notice of Arrival and Departure system of  
records notice was published concurrently in the Federal Register, 73  
FR 75442, December 11, 2008, and comments were invited on both the

notice of proposed rulemaking and system of records notice. No comments were received.

#### Public Comments

DHS received no comments on the notice of proposed rulemaking or system of records notice. DHS will implement the rulemaking as proposed.

#### List of Subjects in 6 CFR Part 5

Privacy, Freedom of information.

0

For the reasons stated in the preamble, DHS amends 6 CFR chapter I as follows:

#### PART 5--DISCLOSURE OF RECORDS AND INFORMATION

0

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

Authority: Public Law 107-296, 116 Stat. 2135, (6 U.S.C. 101 et seq.); 5 U.S.C. 301. Subpart A also issued under 5 U.S.C. 552. Subpart B also issued under 5 U.S.C. 552a.

0

2. At the end of Appendix C to Part 5, add the following new paragraph ``34'':

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

\* \* \* \* \*

34. The DHS/USCG--029 Notice of Arrival and Departure system consists of electronic and paper records and will be used by DHS and its components. The DHS/USCG--029 Notice of Arrival and Departure system is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder. The DHS/USCG--029 Notice of Arrival and Departure system contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies, as well as private corporate or other entities. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c) (3) and (4); (d); (e) (1), (e) (2), (e) (3), (e) (4) (G), (e) (4) (H), (e) (4) (I), (e) (5) and (e) (8); (f), and (g) pursuant to 5 U.S.C. 552a(j) (2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a (c) (3), (d), (e) (1), (e) (4) (G), (e) (4) (H), (e) (4) (I), and (f) pursuant to 5 U.S.C. 552a(k) (2). However, these exemptions apply only to the extent that information in this system of records is recompiled or is created from information contained in other systems of records. After conferring with the appropriate component or

agency, DHS may waive applicable exemptions in appropriate circumstances and where it would not appear to interfere with or adversely affect the law enforcement purposes of the systems from which the information is recompiled or in which it is contained. Exemptions from the above particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, when information in this system of records is recompiled or is created from information contained in other systems of records subject to exemptions for the following reasons:

(a) From subsection (c) (3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part

[[Page 45087]]

of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to national security.

(c) From subsection (e) (1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e) (2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation or subject of interest would alert the subject to the nature or existence of an investigation, thereby interfering with the related investigation and law enforcement activities or national security matter.

(e) From subsection (e) (3) (Notice to Subjects) because providing such detailed information would impede law enforcement in that it could compromise investigations by: Revealing the existence of an otherwise confidential investigation and thereby provide an opportunity for the subject of an investigation to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative efforts; reveal the identity of witnesses in investigations, thereby providing an opportunity for the subjects of

the investigations or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations and discourage members of the public from cooperating as confidential informants in any future investigations.

(f) From subsections (e) (4) (G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e) (5) (Collection of Information) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e) (5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e) (8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

Dated: August 20, 2009.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E9-20758 Filed 8-28-09; 8:45 am]

BILLING CODE 4910-15-P

[Federal Register Volume 76, Number 209 (Friday, October 28, 2011)]

[Notices]

[Pages 66937-66940]

From the Federal Register Online via the Government Printing Office [[www.gpo.gov](http://www.gpo.gov)]

[FR Doc No: 2011-27882]

-----  
DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2011-0082]

Privacy Act of 1974; Department of Homeland Security/United States Secret Service--003 Non-Criminal Investigation Information System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records.

-----  
SUMMARY: In accordance with the Privacy Act of 1974 and as part of the Department of Homeland Security's biennial review of system of record notices, the Department of Homeland Security proposes to update and reissue a current Department of Homeland Security system of records titled, ``Department of Homeland Security/United States Secret Service--003 Non-Criminal Investigation Information System.'' As a result of biennial review of this system, records have been updated within the categories of individuals covered in this system and categories of records in this system in order to further define and narrow categories. One routine use was revised to further define the purposes of disclosure, and retention and disposal procedures were updated to reflect current retention practices. The notification procedures were updated to clarify the reason for exemption and the method for access. Additionally, the Department of Homeland Security previously published a Final Rule in the

[[Page 66938]]

Federal Register to exempt this system of records from certain provisions of the Privacy Act. The current updates to this system of records do not impact the nature of the exemptions claimed; the exemptions continue to apply to this updated system. This updated system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Written comments must be submitted on or before November 28, 2011.

ADDRESSES: You may submit comments, identified by docket number DHS-2011-0082, by one of the following methods:

Federal e-Rulemaking Portal: <http://www.regulations.gov>.

Follow the instructions for submitting comments.

Fax: 1-(866) 466-5370.

Mail: Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

Docket: For access to the docket, to read background documents, or comments received go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Latita Payne ((202) 406-6370), Privacy Officer, United States Secret Service, 245 Murray Lane SW., Building T-5, Washington, DC 20223. For privacy issues please contact: Mary Ellen Callahan ((703) 235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

#### SUPPLEMENTARY INFORMATION:

##### I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a and as part the Department of Homeland Security's (DHS) biennial review of system of record notices, DHS/United States Secret Service (USSS) proposes to update and reissue a current DHS system of records titled, DHS/USSS-003 Non-Criminal Investigation Information System of Records. As a result of biennial review of this system, records have been updated within the categories of individuals covered in this system and categories of records in this system in order to further define, narrow, and eliminate duplicative categories. Routine Use H was revised to further define the purposes of disclosure, and retention and disposal procedures were updated to reflect current retention practices. The notification procedures were updated to clarify the reason for exemption and the method for access. This updated system will be included in DHS's inventory of record systems.

##### II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR part 5.

The Privacy Act requires that each agency publish in the Federal Register a description denoting the type and character of each system of records in order to make agency recordkeeping practices transparent, to notify individuals about the use of their records, and to assist the individual to more easily find files within the agency. Below is a description on the DHS/USSS-003 Non-Criminal Investigation Information System of Records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this revised system of records to the Office of Management and Budget and to the Congress.

System of Records

Department of Homeland Security (DHS)/United States Secret Service (USSS)-003

System name:

DHS/USSS--003 Non-Criminal Investigation Information System

Security classification:

Unclassified and Classified.

System location:

Records are maintained at the United States Secret Service Headquarters, 950 H St. NW., Washington, DC 20223 and field offices.

Categories of individuals covered by the system:

Individuals who are applicants for employment or are currently employed with the USSS or other federal or state entities and have taken a polygraph; and

Qualified USSS law enforcement officers and qualified USSS retired law enforcement officers who carry concealed firearms.

Categories of records in the system:

Individual's name;  
Social Security number;  
Address;  
Date of birth;  
Case number;

Polygraph examination reports and files;

Records containing investigatory material compiled solely for the purpose of determining suitability, eligibility, and/or qualifications for federal civilian employment or access to classified information; and

Any group of records which have been created by the Law Enforcement Officer Safety Act of 2004, Public Law 108-277, 1, codified at 18 U.S.C. 926 B and C, as amended.

Authority for maintenance of the system:

The Homeland Security Act of 2002, Public Law 107-296; 5 U.S.C. 301; Federal Records Act, 44 U.S.C. 3101; 18 U.S.C. 3056; 18 U.S.C. 3056A; 42 U.S.C. 13031; Executive Order 10450; and 6 CFR part 5.

Purpose(s):

The purpose of this system is to record and maintain files related to applicants for employment or current employees of the USSS or other federal or state entities who have taken a polygraph; and current and retired USSS employees who are qualified to carry a concealed weapon.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside the Department of Homeland Security (DHS) as a routine use pursuant to 5 U.S.C. 552a(b) (3) as follows:

A. To the Department of Justice or other federal agency conducting litigation or in proceedings before any

[[Page 66939]]

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.

B. 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.

C. 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.

D. 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.

E. 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. DHS 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 programs (whether maintained by DHS or another agency or entity) or harm to the individual who relies 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.

F. 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.

G. 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.

H. To Federal, State, or local government agencies for the purpose of developing a relevant ongoing civil, administrative, or background investigation.

I. To private institutions and individuals for the purpose of confirming and/or determining suitability, eligibility, or qualification for federal civilian employment or access to classified

information, and for the purposes of furthering the efforts of the USSS to investigate the activities of individuals related to or involved in non-criminal civil and administrative investigations.

J. To another federal agency or to an instrumentality of any government jurisdiction within or under the control of the United States for the purpose of determining suitability, eligibility, or qualifications for employment with or access to classified information in such other agency instrumentality.

K. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a subpoena from a court of competent jurisdiction.

L. To an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the letting of a contract, or the issuance of a license, grant or other benefit when disclosure is appropriate to the proper performance of the official duties of the person making the request.

M. To state and local school boards, private and public schools, daycare facilities, children's camps, and childcare transportation providers, if information concerns one of their employees, or applicants for employment, when such an individual has admitted to the USSS that they viewed, have taken an interest in, or have engaged in prior activity regarding child pornography, the touching of a child for sexual gratification, or child abuse.

N. 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's 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.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper and electronic records in this system are stored in secure facilities and/or behind locked doors. Electronic records media, such as magnetic tape, magnetic disk, digital media, and CD-ROM are stored in proper environmental controls.

Retrievability:

Records are indexed by name on file at USSS Headquarters, and in field offices and are retrieved through a manual search of index cards and/or through computer search of magnetic media. Access to the physical files is by case number obtained from the name indices.

Safeguards:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS and USSS automated systems security and access policies. Strict controls have

been imposed to minimize the risk of compromising the information that is being stored, processed, and transmitted. Access to the records in this system is limited to those individuals who have a USSS approved need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

[[Page 66940]]

Retention and disposal:

Applicant security and background investigation records of retired or separated USSS employees are retained for 20 years after the date of last action. All judicial case records are retained for 30 years from the date of case closure, unless otherwise required to be held permanently for transfer to the National Archives and Records Administration. Non-judicial and non-criminal case files generally are retained for a period of between 5 years and 30 years from the date of case closure, depending upon the nature or subject of the investigation. All other records, the disposition of which is not otherwise specified, are retained until destruction is authorized.

System Manager and address:

Assistant Director, Human Resources and Training and Assistant Director, Office of Investigation, U.S. Secret Service, 245 Murray Lane SW., Building T-5, Washington, DC 20223.

Notification procedure:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, DHS/USSS will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the USSS FOIA Officer, 245 Murray Drive, SW., Building T-5, Washington, DC 20223. If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief FOIA Officer, Department of Homeland Security, whose contact information can be found at <http://www.dhs.gov/foia>.

When seeking records about yourself from this system of records or any other USSS system of records, your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, <http://www.dhs.gov> or 1-(866) 431-0486. In addition, you should provide the following:

An explanation of why you believe the Department would have information on you;

Specify when you believe the records would have been created; and

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information USSS may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

## Record access procedures:

See ``Notification procedure'' above.

## Contesting record procedures:

See ``Notification procedure'' above.

## Record Source Categories:

Records are obtained from employees, former employees, and applicants for employment with the USSS; federal, state, and local governmental agencies; court systems; executive entities, both foreign and domestic; educational institutions; private businesses; and members of the general public.

## Exemptions claimed for the system:

Pursuant to exemption 5 U.S.C. 552a(j)(2) of the Privacy Act and the limitations therein, this system is exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f); and (g). Pursuant to 5 U.S.C. 552a(k)(1), (k)(2), (k)(3), (k)(5), and (k)(6), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f). In addition, to the extent a record contains information from other exempt systems of records, USSS will rely on the exemptions claimed for those systems.

Dated: September 22, 2011.

Mary Ellen Callahan,  
Chief Privacy Officer, Department of Homeland Security.  
[FR Doc. 2011-27882 Filed 10-27-11; 8:45 am]  
BILLING CODE 4810-42-P

[Federal Register Volume 74, Number 167 (Monday, August 31, 2009)]

[Rules and Regulations]

[Pages 45087-45088]

From the Federal Register Online via the Government Printing Office [[www.gpo.gov](http://www.gpo.gov)]

[FR Doc No: E9-20757]

-----  
DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2009-0046]

Privacy Act of 1974: Implementation of Exemptions; Department of  
Homeland Security U.S. Secret Service--001 Criminal Investigation  
Information System of Records

AGENCY: Privacy Office, DHS.

ACTION: Final rule.

-----  
SUMMARY: The Department of Homeland Security is issuing a final rule to amend its regulations to exempt portions of a Department of Homeland Security U.S. Secret Service system of records entitled the ``Department of Homeland Security U.S. Secret Service--001 Criminal Investigation Information System of Records'' from certain provisions of the Privacy Act. Specifically, the Department exempts portions of the Department of Homeland Security U.S. Secret Service--001 Criminal Investigation Information system from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: Effective Date: This final rule is effective August 31, 2009.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Latita Payne (202-406-6370), Privacy Point of Contact, United States Secret Service, Washington, DC 20223. For privacy issues contact: Mary Ellen Callahan (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

Background

The Department of Homeland Security (DHS) published a notice of proposed rulemaking in the Federal Register, 73 FR 77544, December 19, 2008, proposing to exempt portions of the system of records from one or more provisions of the Privacy Act because of the U.S. Secret Service (Secret Service) protective functions and its criminal, civil, and administrative enforcement responsibilities. The system of records is the DHS/Secret Service--001 Criminal Investigation Information system. The DHS/Secret Service--001 Criminal Investigation Information system

of records notice was published concurrently in the Federal Register, 73 FR 77729, December 19, 2008, and comments were invited on both the notice of proposed rulemaking and system of records notice. No comments were received.

#### Public Comments

DHS received no comments on the notice of proposed rulemaking or system of records notice. DHS will implement the rulemaking as proposed.

#### List of Subjects in 6 CFR Part 5

Freedom of information; Privacy.

0

For the reasons stated in the preamble, DHS amends Chapter I of Title 6, Code of Federal Regulations, as follows:

[[Page 45088]]

#### PART 5--DISCLOSURE OF RECORDS AND INFORMATION

0

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

Authority: Public Law 107-296, 116 Stat. 2135, 6 U.S.C. 101 et seq.; 5 U.S.C. 301. Subpart A also issued under 5 U.S.C. 552. Subpart B also issued under 5 U.S.C. 552a.

0

2. Add at the end of Appendix C to Part 5, Exemption of Record Systems under the Privacy Act, the following new paragraph ``35'':

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

\* \* \* \* \*

35. The DHS/Secret Service--001 Criminal Investigation Information system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/Secret Service--001 Criminal Investigation Information system is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; the protection of the President of the United States or other individuals and locations pursuant to Section 3056 and 3056A of Title 18. The DHS/Secret Service--001 Criminal Investigation Information system contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, international government agencies, as well as private corporate, education and other entities. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f), and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of

Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c) (3), (d), (e) (1), (e) (4) (G), (e) (4) (H), (I), and (f) pursuant to 5 U.S.C. 552a(k) (1), (k) (2), and (k) (3). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c) (3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, or protective inquiry, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or the Secret Service's protective mission. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, or inquiry, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative or inquiry process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, or protective inquiry to the existence of the investigation or inquiry, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation or inquiry, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement or protective activities and/or could disclose security-sensitive information that could be detrimental to homeland security or the protective mission of the Secret Service.

(c) From subsection (e) (1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law or protective inquiries, 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 or protective inquiry. In the interests of effective law enforcement, and/or the protective mission of the Secret Service, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity, or a threat to an individual, location or event protected or secured by the Secret Service.

(d) From subsection (e) (2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation or protective inquiry would alert the subject to the nature or existence of an investigation or inquiry, thereby interfering with the related investigation or inquiry and law enforcement or protective activities.

(e) From subsection (e) (3) (Notice to Individuals Providing Information) because providing such detailed information would impede law enforcement or protective activities in that it could compromise investigations or inquiries by: Revealing the existence of an otherwise confidential investigation or inquiry and thereby provide an opportunity for the subject of an investigation or inquiry to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative or protective efforts; reveal the identity of witnesses in investigations or inquiries, thereby providing an opportunity for the subjects of the

investigations or inquiries or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the informant's usefulness in any ongoing or future investigations or protective activities and discourage members of the public from cooperating as confidential informants in any future investigations or protective activities.

(f) From subsections (e) (4) (G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to the existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative or protective efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e) (5) (Maintenance of Information Used in Making any Determination) because in the collection of information for law enforcement and protective purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e) (5) would preclude Secret Service DHS agents from using their investigative and protective training and exercising good judgment to both conduct and report on investigations or other protective activities.

(h) From subsection (e) (8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, or/and could result in disclosure of investigative or protective techniques, procedures, and evidence.

(i) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

Dated: August 20, 2009.

Mary Ellen Callahan,  
Chief Privacy Officer, Department of Homeland Security.  
[FR Doc. E9-20757 Filed 8-28-09; 8:45 am]  
BILLING CODE 4810-42-P

[Federal Register Volume 76, Number 209 (Friday, October 28, 2011)]  
[Notices]  
[Pages 66940-66944]  
From the Federal Register Online via the Government Printing Office [[www.gpo.gov](http://www.gpo.gov)]  
[FR Doc No: 2011-27883]

-----  
DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2011-0083]

Privacy Act of 1974; Department of Homeland Security/United States Secret Service--004 Protection Information System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records.

-----  
SUMMARY: In accordance with the Privacy Act of 1974, and as part of the Department of Homeland Security's biennial review of system of record notices, DHS/United States Secret Service proposes to update and reissue a current Department of Homeland Security system of records titled, ``Department of Homeland Security/United States Secret Service--004 Protection Information System of Records.'' As a result of biennial review of this system, information has been updated within the categories of individuals covered in this system and categories of records in this system in order to further define and narrow categories. Routine Use I and J were merged for the purpose of narrowing scope and clarifying why information would be shared. The notification procedures were updated to clarify the reason for exemption and the method for access. Additionally, the Department of Homeland Security previously published a Final Rule in the Federal Register to exempt this system of records from certain provisions of the Privacy Act. The current updates to this system of records do not impact the nature of the exemptions claimed; the exemptions continue to apply to this update. This updated system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Written comments must be submitted on or before November 28, 2011.

ADDRESSES: You may submit comments, identified by docket number DHS-2011-0083, by one of the following methods:

Federal e-Rulemaking Portal: <http://www.regulations.gov>.

Follow the instructions for submitting comments.

Fax: 1-(866) 466-5370.

Mail: Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

Instructions: All submissions received must include the agency name

[[Page 66941]]

and docket number for this rulemaking. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

Docket: For access to the docket, to read background documents, or comments received go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Latita Payne (202) 406-6370), Privacy Officer, United States Secret Service, 245 Murray Lane, SW., Building T-5, Washington, DC 20223. For privacy issues please contact: Mary Ellen Callahan (703) 235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

#### SUPPLEMENTARY INFORMATION:

##### I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, and as part of the Department of Homeland Security's (DHS) biennial review of system of record notices, DHS/United States Secret Service (USSS) proposes to update and reissue a current DHS system of records titled, DHS/USSS-004 Protection Information System of Records. As a result of biennial review of this system, records have been updated within the categories of individuals covered in this system and categories of records in this system in order to further define, narrow, and eliminate duplicative categories. Routine Use I and J were merged for the purpose of narrowing scope and clarification. The notification procedures were updated to clarify the reason for exemption and the method for access. This updated system will be included in DHS's inventory of record systems.

Additionally, DHS previously published a Final Rule in the Federal Register to exempt this system of records from certain provisions of the Privacy Act. The current updates to this system of records do not impact the nature of the exemptions claimed; the exemptions continue to apply to this update. This updated system will be included in the Department of Homeland Security's inventory of record systems.

##### II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR part 5.

The Privacy Act requires that each agency publish in the Federal Register a description denoting the type and character of each system of records in order to make agency recordkeeping practices transparent, to notify individuals about the use of their records, and to assist the

individual to more easily find files within the agency. Below is a description of the Protection Information System.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this revised system of records to the Office of Management and Budget and to the Congress.

System of Records

Department of Homeland Security (DHS)/United States Secret Service (USSS)-004

System name:

DHS/USSS-004 Protection Information System

Security classification:

Unclassified and Classified.

System location:

Records are maintained at the United States Secret Service Headquarters, 950 H St., NW., Washington, DC 20223, other locations in Washington, DC, and field offices.

Categories of individuals covered by the system:

Individuals who have been or are currently the subject of a criminal investigation by USSS or another law enforcement agency for the violation of certain criminal statutes relating to the safety of persons or security of properties, facilities, and areas protected by USSS;

Individuals who are the subjects of investigative records and reports supplied to USSS by Federal, State, and local law enforcement agencies, foreign or domestic, other non-law enforcement governmental agencies, or private institutions and individuals, in conjunction with the protective function of USSS;

Individuals who are the subjects of non-criminal protective and background investigations by USSS and other law enforcement agencies;

Individuals who are granted or denied ingress and egress to areas secured by USSS, or to areas in proximity to persons protected by USSS, including but not limited to: invitees; passholders; tradesmen; and law enforcement, maintenance, or service personnel;

Individuals who are witnesses, protectees, suspects, complainants, informants, defendants, fugitives, released prisoners, and correspondents who have been identified by USSS or from information supplied by other law enforcement agencies, governmental units, private institutions, and members of the general public in connection with USSS performance of its authorized protective functions;

Individuals who have sought an audience or contact with persons protected by USSS;

Individuals who have been involved in incidents or events which relate to the protective functions of the USSS; and

Individuals protected by the USSS.

Categories of records in the system:

Individual's name;

Address;

Date of Birth;

Case number;

Arrest record;

Nature and disposition of criminal charges, sentencing, confinement, release, and parole or probation status;

Records concerning agency activities associated with protectee movements and other protective measures taken on a

protectee's behalf;

Records containing information compiled for the purpose of identifying and evaluating individuals who may constitute a threat to the safety of persons or security of areas protected by the USSS;

Records containing information compiled for the purpose of a criminal investigation, including reports of informants and investigators, which are associated with an identifiable individual;

Informant's name and contact information (e.g., address; phone number);

Records containing reports relative to an individual compiled at various

[[Page 66942]]

stages of the process of enforcement of certain criminal laws from arrest or indictment through release from supervision;

Records containing information supplied by other Federal, State, and local law enforcement agencies, foreign or domestic, other non-law enforcement governmental agencies, private institutions and persons concerning individuals who, because of their activities, personality traits, criminal or mental history, or history of social deviancy, may be of interest to the USSS in connection with the performance by that agency of its protective functions; and

Records containing information compiled for the purpose of background investigations of individuals, including but not limited to, passholders, tradesmen, maintenance or service personnel who have access and/or have been denied access to areas secured by or who may be in proximity to persons protected by USSS.

Authority for maintenance of the system:

The Homeland Security Act of 2002, Public Law 107-296; 5 U.S.C. 301; Federal Records Act, 44 U.S.C. 3101; 18 U.S.C. 3056; 18 U.S.C. 3056A and 6 CFR part 5.

Purpose(s):

The purpose of this system is to assist USSS in protecting its protectees by recording information necessary to implement protective measures and to investigate individuals who may come into proximity with a protectee, including individuals who have been involved in incidents or events which relate to the protective functions of the USSS, and individuals who have sought to make contact with a protectee.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside the Department of Homeland Security (DHS) as a routine use pursuant to 5 U.S.C. 552a(b) (3) as follows:

A. To the Department of Justice 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.

B. 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.

C. 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.

D. 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.

E. 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 programs (whether maintained by DHS or another agency or entity) or harm to the individual who relies 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.

F. 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.

G. 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.

H. To the Department of Justice and other Federal, State, and local governmental agencies having a prosecution function for the use of attorneys, magistrates, and judges; and the parole and probation authorities for the purpose of prosecuting, sentencing, and determining the parole and probation status of criminal offenders or suspected criminal offenders; and for civil and other proceedings involving USSS protective functions.

I. To Federal, State, and local governmental agencies, foreign and domestic, for the purposes of developing information on subjects involved in USSS protective investigations and the evaluation of persons considered to be of protective interest and for the purpose of protective functions.

J. To Federal, State, and local governmental agencies, private institutions and private individuals, for the purpose of implementing protective measures.

K. To personnel of Federal, State, and local governmental agencies, foreign and domestic, when reasonably necessary to the exercise of the

USSS protective function.

L. To private institutions and private individuals, identifying information pertaining to actual or suspected criminal offenders or other individuals considered to be of protective interest, for the purpose of furthering USSS efforts to evaluate the danger such individuals pose to persons protected by the agency.

M. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a subpoena from a court of competent jurisdiction.

N. To an appropriate Federal, State, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or the issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to

[[Page 66943]]

a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, the issuance of a license, grant or other benefit and when disclosure is appropriate to the proper performance of the official duties of the person making the request.

O. 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's 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.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper and electronic records in this system are stored in secure facilities behind locked doors. Electronic records media, such as magnetic tape, magnetic disk, digital media, and CD ROM are stored in proper environmental controls.

Retrievability:

This system is indexed by case number, name, and other identifying data and other case related data, in master and magnetic media indices. Records may be retrieved by any of these indices. Access to the physical files is located at field offices, Headquarters, and other Washington, DC locations.

Safeguards:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS and USSS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored, processed, and transmitted. Access to the records in this system is limited to those individuals who have a USSS approved

need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Retention and disposal:

Protective intelligence case records, including non-judicial protective intelligence cases, are routinely retained for a period of up to 5 years from the date of last action; or for 10 years from the date of last action if they contain electronic records. All judicial records are retained for a period of 20 years from the date of last action, unless otherwise required to be held permanently for transfer to the National Archives and Records Administration. Files relating to issuance of White House Complex passes for employees of the White House, Secret Service Employees, press representatives accredited at the White House, and other authorized individuals are retained for a period of 8 years from the date the file is closed. Records pertaining to the administration and operations of Secret Service protective program, shift reports, survey files, and special event files are retained for a period of 3 to 5 years from the end of the event. Records pertaining to trip files for domestic travel are retained for 5 years, and trip files for foreign travel are retained for 10 years from the end of the event. Campaign related files are retained for a period of 30 years after the end of the campaign and subsequently transferred to the National Archives and Records Administration.

System Manager and address:

Assistant Director, Office of Strategic Intelligence and Information; Assistant Director, Office of Technical Development and Mission Support; and Assistant Director, Office of Protective Operations, U.S. Secret Service, 245 Murray Drive SW., Building T-5, Washington, DC 20223.

Notification procedure:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, DHS/USSS will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the USSS FOIA Officer, Freedom of Information and Privacy Acts Program, 245 Murray Drive, SW., Building T-5, Washington, DC 20223. If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the DHS FOIA Officer, whose contact information can be found at <http://www.dhs.gov/foia>.

When seeking records about yourself from this system of records or any other USSS system of records your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, <http://www.dhs.gov> or 1-(866) 431-0486. In addition you should provide the following:

An explanation of why you believe the Department would have information on you;

Specify when you believe the records would have been created; and

If your request is seeking records pertaining to another

living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information USSS may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Record access procedures:

See ``Notification procedure'' above.

Contesting record procedures:

See ``Notification procedure'' above.

Record Source Categories:

The Secretary of Homeland Security has exempted this system from subsections (e) (4) (I) of the Privacy Act pursuant to 5 U.S.C. 552a(j) (2) and (k) (2) and (k) (3); therefore, records sources shall not be disclosed.

Exemptions claimed for the system:

Pursuant to exemption 5 U.S.C. 552a(j) (2) of the Privacy Act and the limitations therein, this system is exempt from 5 U.S.C. 552a(c) (3) and (4); (d); (e) (1), (e) (2), (e) (3), (e) (4) (G), (e) (4) (H), (e) (4) (I), (e) (5) and (e) (8); (f); and (g). Pursuant to 5 U.S.C. 552a (k) (1), (k) (2), and (k) (3) this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a(c) (3), (d), (e) (1), (e) (4) (G), (e) (4) (H), (e) (4) (I), and (f). In addition, to the extent a record contains information from other exempt Systems of Records,

[[Page 66944]]

USSS will rely on the exemptions claimed for those systems.

Dated: September 22, 2011.

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

[FR Doc. 2011-27883 Filed 10-27-11; 8:45 am]

BILLING CODE 4810-42-P

[Federal Register Volume 74, Number 167 (Monday, August 31, 2009)]  
[Rules and Regulations]  
[Pages 45088-45090]  
From the Federal Register Online via the Government Printing Office [[www.gpo.gov](http://www.gpo.gov)]  
[FR Doc No: E9-20756]

-----  
DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2009-0047]

Privacy Act of 1974: Implementation of Exemptions; Department of  
Homeland Security U.S. Secret Service--003 Non-Criminal Investigation  
Information System of Records

AGENCY: Privacy Office, DHS.

[[Page 45089]]

ACTION: Final rule.

-----  
SUMMARY: The Department of Homeland Security is issuing a final rule to  
amend its regulations to exempt portions of a Department of Homeland  
Security U.S. Secret Service system of records entitled the  
``Department of Homeland Security U.S. Secret Service--003 Non-Criminal  
Investigation Information System of Records'' from certain provisions  
of the Privacy Act. Specifically, the Department exempts portions of  
the Department of Homeland Security U.S. Secret Service--003 Non-  
Criminal Investigation Information system from one or more provisions  
of the Privacy Act because of criminal, civil, and administrative  
enforcement requirements.

DATES: Effective Date: This final rule is effective August 31, 2009.

FOR FURTHER INFORMATION CONTACT: For general questions please contact:  
Latita Payne (202-406-6370), Privacy Point of Contact, United States  
Secret Service, Washington, DC 20223. For privacy issues contact: Mary  
Ellen Callahan (703-235-0780), Chief Privacy Officer, Privacy Office,  
U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

Background

The Department of Homeland Security (DHS) published a notice of  
proposed rulemaking in the Federal Register, 73 FR 77546, December 19,  
2008, proposing to exempt portions of the system of records from one or  
more provisions of the Privacy Act because of the U.S. Secret Service's  
(Secret Service) protective functions and its criminal, civil, and

administrative enforcement responsibilities. The system of records is the DHS/Secret Service--003 Non-Criminal Investigation Information system. The DHS/Secret Service--003 Non-Criminal Investigation Information system of records notice was published concurrently in the Federal Register, 73 FR 77813, December 19, 2008, and comments were invited on both the notice of proposed rulemaking and the system of records notice. No comments were received.

#### Public Comments

DHS received no comments on the notice of proposed rulemaking or the system of records notice. DHS will implement the rulemaking as proposed.

#### List of Subjects in 6 CFR Part 5

Freedom of information; Privacy.

0

For the reasons stated in the preamble, DHS amends Chapter I of Title 6, Code of Federal Regulations, as follows:

#### PART 5--DISCLOSURE OF RECORDS AND INFORMATION

0

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

Authority: 6 U.S.C. 101 et seq.; Public Law 107-296, 116 Stat. 2135; 5 U.S.C. 301. Subpart A also issued under 5 U.S.C. 552. Subpart B also issued under 5 U.S.C. 552a.

0

2. Add at the end of Appendix C to Part 5, the following new paragraph ``36'':

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

\* \* \* \* \*

36. The DHS/Secret Service--003 Non-Criminal Investigation Information system of records consists of electronic and paper records and will be used by DHS and its components. The DHS/Secret Service--003 Non-Criminal Investigation Information system is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws; criminal, civil, protective and background investigations and inquiries, and proceedings thereunder; the protection of the President of the United States or other individuals and locations pursuant to Section 3056 and 3056A of Title 18; and the hiring of employees through an application process which includes the use of polygraph examinations. The DHS/Secret Service--003 Non-Criminal Investigation Information system contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies, as well as private corporate, educational and other entities. The Secretary of Homeland Security has exempted this system from the following provisions of the

Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c) (3) and (4); (d); (e) (1), (e) (2), (e) (3), (e) (4) (G), (e) (4) (H), (e) (4) (I), (e) (5) and (e) (8); (f), and (g) pursuant to 5 U.S.C. 552a(j) (2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c) (3), (d), (e) (1), (e) (4) (G), (e) (4) (H), (e) (4) (I), and (f) pursuant to 5 U.S.C. 552a(k) (1), (k) (2), (k) (3), (k) (5), and (k) (6). Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c) (3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, or protective inquiry, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or the Secret Service's protective mission. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation or inquiry, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative or inquiry process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, or protective inquiry to the existence of the investigation or inquiry, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation or inquiry, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement or protective activities and/or could disclose security-sensitive information that could be detrimental to homeland security or the protective mission of the Secret Service.

(c) From subsection (e) (1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law or protective inquiries, 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 or protective inquiry. In the interests of effective law enforcement and/or the protective mission of the Secret Service, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity, or a threat to an individual, location or event protected or secured by the Secret Service.

(d) From subsection (e) (2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation or protective inquiry would alert the subject to the nature or existence of an investigation or inquiry, thereby interfering with the related investigation or inquiry and law enforcement or protective activities.

(e) From subsection (e) (3) (Notice to Individuals Providing Information) because providing such detailed information would impede law enforcement or protective activities in that it could compromise investigations or inquiries by: Revealing the existence of an otherwise confidential investigation or inquiry and thereby provide an opportunity for the subject of an investigation or

inquiry to conceal evidence, alter patterns of behavior, or take other actions that could thwart investigative or protective efforts; reveal the identity of witnesses in investigations or inquiries, thereby providing an opportunity for the subjects of the investigations or inquiries or others to harass, intimidate, or otherwise interfere with the collection of evidence or other information from such witnesses; or reveal the identity of confidential informants, which would negatively affect the

[[Page 45090]]

informant's usefulness in any ongoing or future investigations or protective activities and discourage members of the public from cooperating as confidential informants in any future investigations or protective activities.

(f) From subsections (e) (4) (G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to the existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative or protective efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e) (5) (Maintenance of Information Used in Making any Determination) because in the collection of information for law enforcement and protective purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with (e) (5) would preclude Secret Service agents from using their investigative and protective training, and exercising good judgment to both conduct and report on investigations or other protective activities.

(h) From subsection (e) (8) (Notice on Individuals) because compliance would interfere with DHS' ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal, or could result in disclosure of investigative or protective techniques, procedures, and evidence.

(i) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system. Therefore DHS is not required to establish rules or procedures pursuant to which individuals may seek a civil remedy for the agency's: Refusal to amend a record; refusal to comply with a request for access to records; failure to maintain accurate, relevant, timely and complete records; or failure to otherwise comply with an individual's right to access or amend records.

Dated: August 20, 2009.

Mary Ellen Callahan,  
Chief Privacy Officer, Department of Homeland Security.  
[FR Doc. E9-20756 Filed 8-28-09; 8:45 am]  
BILLING CODE 4810-42-P

**Post-Hearing Questions for the Record  
Submitted to Hon. John Roth  
From Senator Ron Johnson**

**“Examining Ongoing Challenges at the U.S. Secret Service and their Government-wide Implications”  
November 17, 2015**

**United States Senate, Subcommittee on Regulatory Affairs and Federal  
Management  
Committee on Homeland Security and Governmental Affairs**

1. The DHS-OIG concluded that four of the 45 Secret Service employees that accessed the PII information of Congressman Chaffetz were authorized to do so. What was the criterion for determining if the Secret Service employee that accessed the information of Congressman Chaffetz in the MCI database was authorized or unauthorized?

To determine whether Secret Service employees were authorized or unauthorized to access Chairman Chaffetz’ information in the MCI database, we analyzed whether they had an official purpose to access the record. Officials who examined the record in connection with the performance of assigned duties and who had to access the record in order to perform those assigned duties properly were considered authorized.

For example, employees at a specific field office received a press inquiry as to whether Chairman Chaffetz had applied to that office. While the office appropriately declined to comment to the press, as part of their due diligence, they accessed the system to determine whether it was true. Likewise, one employee in headquarters was directed by his superior to do so, as part of deciding what management steps to take.

However, a number of supervisors accessed the information, purportedly to determine whether the talk about Chairman Chaffetz was true. Accessing the record in that circumstance was inappropriate and not in connection with an official purpose because the truth or falsity of the information was irrelevant to directing their subordinates to use Secret Service data systems only for official government purposes, and not to satisfy personal curiosity. This was especially the case since, with a few narrow exceptions, these supervisors did nothing with this information, such as reporting it up the chain to their superiors.

**Post-Hearing Questions for the Record  
Submitted to Hon. John Roth  
From Chairman James Lankford**

**"Ongoing Challenges at the U.S. Secret Service  
and Their Government-Wide Implications"**

**November 17, 2015**

**United States Senate, Subcommittee on Regulatory Affairs and Federal Management  
Committee on Homeland Security and Governmental Affairs**

1. During your testimony you indicated that the MCI database was unable to audit accesses without a specific program written for each search term.
  - a. Since the migration to an updated database system, what audit capability and checks (automatic or manual) are now in place?

We are currently conducting a technical security assessment of the Secret Service's updated database systems that when complete, will answer this question. Specifically, our Office of Information Technology Audits is reviewing the information systems the Secret Service currently uses to store and retrieve data and information previously stored in the MCI database. Our assessment is designed (1) to verify that the MCI is in fact no longer in use, (2) identify which systems currently house MCI data, (3) determine the level of physical and system controls implemented to secure the data from further instances of unauthorized access, and (4) identify gaps in the security posture. We plan to issue our final report in February 2016, and I look forward to discussing our conclusions with you and your staff at that time.

- b. Based on your investigation, would a regularly occurring, agency-wide OIG audit of PII searches help change Secret Service culture regarding the protection of PII?

We believe that the best way to prevent future activity of the type we saw here would be for Secret Service to focus to a greater degree on its information security program. Modern data systems with appropriate audit and access controls, when coupled with appropriate agency processes, policies, and procedures, would prevent unauthorized access to information. Every year, we audit, pursuant to the Federal Information Security Act (FISMA), DHS' information systems. FISMA requires IGs to perform evaluations of Departmental implementation of the 11 program-level security authorization activities. DHS OIG performs tests to determine how the Department's components are implementing these activities.

From FY 2013 to the present, Secret Service has done poorly on these FISMA reviews compared with other DHS components. For example, as of September 2015,

USSS failed to meet the Department’s “security authorizations” target of 100% for “high value assets” and 95% for “all other FISMA systems” as USSS only scored 75% and 58% respectively. In addition, USSS only scored 38% in “weakness remediation,” where the Department’s target was 90%.

We believe that focusing on modernizing and securing Secret Service data systems, in combination with training and other efforts to create an ethical culture (such as a uniformly administered system for dealing with deviations from a defined standard of conduct) are the best way to change the culture with regard to the use of PII.

- c. Based on your investigation, what recommendations would you make to change Secret Service culture regarding PII?

As noted in the above question, the systems that the Secret Service uses to store PII must have audit and access controls that help ensure the security and confidentiality of Privacy Act-protected records. Training about PII and its appropriate handling and safeguarding should be reinforced and reemphasized. Ultimately, change will come when management does not tolerate the deliberate or grossly negligent mishandling of PII and employees who violate Department and Secret Service policies and/or the Privacy Act face disciplinary consequences for their actions.

2. Your testimony reflects that agents seemed to consider personal data on secret service databases as theirs to access as they pleased.

- a. What training policy updates have been or should be made to correct this mindset reflected in your investigation?

Our investigation did not determine what changes, if any, Secret Service has made to their training policies as a result of this incident. Our next FISMA audit will determine the overall level of training Secret Service personnel receive.

3. The September 2015 Department of Homeland Security (DHS) Office of the Inspector General (OIG) report titled “Investigation into the Improper Access and Distribution of Information Contained Within a Secret Service Data System” did not audit the 45 Secret Service employees for unauthorized access of personally identifiable information on the agency’s databases prior to the Congressman Chaffetz matter starting on March 25, 2015.

- a. Should DHS OIG conduct additional audits of these 45 Secret Service employees for unauthorized accesses prior to this date?

We share the concern that it is possible that these specific employees mishandled or accessed files without authorization prior to this specific investigation—whether related to Chairman Chaffetz or others. Due to the technical limitations of the MCI database, it would be nearly impossible for us to conduct additional audits of these 45 employees. Moreover, according to the Secret Service, the MCI mainframe has been

disassembled as of September 2015 so it is unclear whether additional audits can be performed on the system.



U.S. GOVERNMENT ACCOUNTABILITY OFFICE

---

441 G St. N.W.  
Washington, DC 20548

December 16, 2015

The Honorable James Lankford  
Chairman  
Subcommittee on Regulatory Affairs and Federal Management  
Committee on Homeland Security and Governmental Affairs  
U.S. Senate

**Subject: Responses to Questions for the Record – November 17th, 2015, Hearing Titled  
“Examining Ongoing Challenges at the U.S. Secret Service and their Government-Wide  
Implications”**

Dear Mr. Chairman:

This letter responds to your December 1, 2015, request that I reply to additional questions arising from the joint hearing on the challenges at the U.S. Secret Service.

The enclosure provides my responses, which are primarily based on previously issued products. The work supporting these products was performed in accordance with generally accepted government auditing standards.

Should you or your staff have any questions on the matters discussed in this letter, please contact me at (202) 512-6253 or [willemsenj@gao.gov](mailto:willemsenj@gao.gov).

Sincerely yours,

A handwritten signature in cursive script that reads 'Joel Willemsen'.

Joel C. Willemsen  
Managing Director, Information Technology

Enclosure

**Questions submitted by the Honorable James Lankford, Chairman**  
**Subcommittee on Regulatory Affairs and Federal Management**

**1. Your testimony reflects that the Social Security Agency has personal identifying information (PII) on nearly every U.S. citizen, and that agencies such as the VA, Department of Education, and CFPB also house substantial amounts of PII.**

**a. What are the most effective means for auditing employee access of PII at these agencies?**

As we reported in September 2015,<sup>1</sup> agencies should use audit and monitoring controls to establish individual accountability, monitor compliance with security policies, and investigate security violations. These controls help determine what, when, and by whom specific actions have been taken on a system and can be used to monitor users' access of sensitive information, such as personally identifiable information (PII).<sup>2</sup>

To monitor users' access and actions, agencies can install software that provides an audit trail or logs of system activity that can be used to determine the source of an action or activity. Agencies can also monitor users' access by implementing other technologies such as network- and host-based intrusion detection systems, security event correlation tools, and computer forensics. Network-based intrusion detection systems capture or "sniff" and analyze network traffic in various parts of a network.

**b. Which government-wide, unimplemented GAO recommendations concerning PII protection should be put into place first?**

We currently have one government-wide PII-related recommendation whose implementation status we are evaluating. This recommendation was made to the Office of Management and Budget (OMB) in our 2013 report<sup>3</sup> regarding our finding that the eight agencies we reviewed had inconsistently implemented data breach policies and procedures. We recommended that, to improve the consistency and effectiveness of government-wide data breach response programs, OMB should update its guidance on federal agencies' responses to PII-related data breaches. OMB neither agreed nor disagreed with our recommendation.

---

<sup>1</sup>GAO, *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*, GAO-15-714 (Washington, D.C.: Sept. 29, 2015).

<sup>2</sup>PII is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, Social Security number, or other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

<sup>3</sup>GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, GAO-14-34 (Washington, D.C.: Dec. 9, 2013).

According to OMB, it has set a date of March 16, 2016, for updating its PII protection guidance to reflect current best practices and recent lessons learned regarding privacy protections and data breach standards.

**2. You testified that it was perplexing to you why the Secret Service would still have PII information on Congressman Chaffetz from 2003, given the National Archives and Records Administration (NARA) requirement to properly dispose of such information once it is no longer needed.**

**a. How well are agencies complying with the NARA requirements to dispose or archive personal information once it is no longer needed?**

We have not performed work specifically addressing the extent to which agencies are complying with the National Archives and Records Administration's (NARA) requirements for disposing or archiving personnel information that is no longer needed. However, in May 2015, we reported that federal agencies took actions toward implementing requirements set forth in a NARA and OMB joint directive on managing government records.<sup>4</sup> To illustrate:

- Twenty-three of the 24 federal agencies we reviewed implemented the requirement to develop and begin implementing plans to manage all permanent records in an electronic format.
- Twenty-one of these 24 agencies implemented the requirement to identify for transfer and reporting those permanent records in existence for more than 30 years.
- Twenty of the 24 agencies implemented the requirement to identify all unscheduled records that have not been properly scheduled.<sup>5</sup>

Nevertheless, five agencies we reviewed did not fully meet those requirements, and we recommended that they and NARA take certain corrective actions. We did not make any recommendations to the Department of Homeland Security (DHS).

---

<sup>4</sup>GAO, *Information Management: Additional Actions Are Needed to Meet Requirements of the Managing Government Records Directive*, GAO-15-339 (Washington, D.C.: May 14, 2015).

<sup>5</sup>Scheduling is the means by which agencies identify federal records, determine time frames for their disposition, and identify permanent records of historical value that are to be transferred to NARA for preservation and archiving. Unscheduled records are those records that have not had their value assessed or their disposition determined.

**3. Under the Federal Information Security Modernization Act of 2014 (FISMA) the Office of Management and Budget (OMB) is required to maintain oversight responsibilities of federal information security programs and ensure minimum security requirements for government-wide information security programs and practices.**

**a. What is your assessment of OMB's fulfillment of these responsibilities over the last several years?**

During the 12 years from when the Federal Information Security Management Act of 2002 (FISMA 2002) was enacted into law to when it was largely replaced by FISMA 2014,<sup>6</sup> executive branch oversight of agency information security has evolved. As part of its FISMA 2002 oversight responsibilities, OMB issued annual instructions for agencies and inspectors general to meet FISMA 2002 reporting requirements. During that time we made recommendations to OMB for improving its oversight of agencies' security programs. For example, in 2013 we recommended<sup>7</sup> that OMB and DHS provide insight into agencies' security programs by developing additional metrics for key security areas such as those for periodically assessing risk and developing subordinate security plans. We also recommended that metrics for FISMA reporting be developed to allow inspectors general to report on the effectiveness of agencies' information security programs. OMB generally agreed with our recommendations. DHS also agreed with our recommendations and identified the actions it had taken or planned to take to address them.

In February 2013, we reported<sup>8</sup> that when OMB transferred several of its oversight responsibilities to DHS through a joint memorandum,<sup>9</sup> it was not clear how the two organizations would share these responsibilities. In that report, we suggested that Congress consider legislation to better define roles and responsibilities for implementing and overseeing federal information security programs. In December 2014, Congress passed FISMA 2014 to improve cybersecurity and clarify cybersecurity oversight roles and responsibilities, among other things.

---

<sup>6</sup>The Federal Information Security Modernization Act of 2014 was enacted as Pub. L. No. 113-283 (Dec. 18, 2014). FISMA 2014 largely supersedes the very similar Federal Information Security Management Act of 2002 (FISMA 2002), Pub. L. No. 107-347, Title III (Dec. 17, 2002), and expands the role and responsibilities of the Department of Homeland Security, but retains many of the requirements for federal agencies' information security programs previously set by the 2002 law.

<sup>7</sup>GAO, *Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness*, GAO-13-776 (Washington, D.C.: Sept. 26, 2013).

<sup>8</sup>GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187 (Washington, D.C.: Feb. 14, 2013).

<sup>9</sup>OMB, Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security* (Washington, D.C.: July 6, 2010).

FISMA 2014 is intended to address the increasing sophistication of cybersecurity attacks, promote the use of automated security tools with the ability to continuously monitor and diagnose the security posture of federal agencies, and provide for improved oversight of federal agencies' information security programs. The act also clarifies and assigns additional responsibilities to OMB, DHS, and federal executive branch agencies.

In carrying out its FISMA responsibilities, OMB has increased its efforts to oversee agencies' implementation of information security. For example, OMB created the Cyber and National Security Team, called the E-Gov Cyber Unit, to strengthen federal cybersecurity through targeted oversight and policy issuance. In September 2015, we reported that OMB, along with DHS, had increased oversight and assistance to federal agencies in implementing and reporting on information security programs.<sup>10</sup>

In June 2015, in response to the Office of Personnel Management security breaches and to protect federal systems from emerging threats, the Federal Chief Information Officer launched a 30-day Cybersecurity Sprint.<sup>11</sup> As part of this effort, the Federal Chief Information Officer instructed federal agencies to immediately take a number of steps to further protect federal information and assets and to improve the resilience of federal networks.

Most recently, in October 2015, OMB issued a cybersecurity strategy implementation plan that is intended to strengthen federal civilian agencies' cybersecurity.<sup>12</sup> The plan is to address government-wide cybersecurity gaps through five objectives: (1) prioritized identification and protection of high-value information and assets; (2) timely detection of and rapid response to cyber incidents; (3) rapid recovery from incidents when they occur and accelerated adoption of lessons learned from the Cybersecurity Sprint assessment; (4) recruitment and retention of the most highly-qualified cybersecurity workforce; and (5) efficient and effective acquisition and deployment of existing and emerging technology. The plan address our recommendation that the White House develop an overarching strategy for improving cybersecurity.<sup>13</sup>

---

<sup>10</sup>GAO-15-714.

<sup>11</sup>In June 2015, the Federal Chief Information Officer launched the 30-day Cybersecurity Sprint, during which agencies were to take immediate actions to combat cyber threats within 30 days. Actions included patching critical vulnerabilities, tightening policies and practices for privileged users, and accelerating the implementation of multi-factor authentication.

<sup>12</sup>OMB, Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government* (Washington, D.C.: Oct 30, 2015).

<sup>13</sup>GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187 (Washington, D.C.: Feb. 14, 2013).

**b. What GAO findings regarding OMB's oversight of government-wide information security programs demonstrate the greatest risks for exposure of PII?**

As previously mentioned, we reported<sup>14</sup> that the eight federal agencies we reviewed generally developed, but inconsistently implemented, policies and procedures for responding to data breaches involving PII that addressed key practices specified by OMB and the National Institute of Standards and Technology. We attributed agencies' inconsistent implementation of data breach policies and procedures to incomplete guidance from OMB.

Also, in 2012, we reiterated<sup>15</sup> our previous finding reported in 2008<sup>16</sup> that while the Privacy Act, the E-Government Act, and related OMB guidance set minimum requirements for agencies, such laws and guidance may not consistently protect PII in all circumstances of its collection and use throughout the federal government and may not fully adhere to key privacy principles. We stressed that unilateral action by OMB might not be the best way to strike an appropriate balance between the government's need to collect, process, and share personally identifiable information and the rights of individuals to know about such collections and be assured that they are only for limited purposes and uses. We suggested that Congress consider amending applicable laws such as the Privacy Act and E-Government Act by

- revising the scope of the laws to cover all PII collected, used, and maintained by the federal government;
- setting requirements to ensure that the collection and use of personally identifiable information is limited to a stated purpose; and
- establishing additional mechanisms for informing the public about privacy protections by revising requirements for the structure and publication of public notices.

---

<sup>14</sup>GAO-14-34.

<sup>15</sup>GAO, *Privacy: Federal Law Should Be Updated to Address Changing Technology Landscape*, GAO-12-961T (Washington, D.C.: July 31, 2012).

<sup>16</sup>GAO, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, GAO-08-536 (Washington, D.C.: May 19, 2008).