

13. *Notification of a Social Security Number (SSN) To An Employer for Wage Reporting—20 CFR 422.103(a)—0960–0778.* Individuals applying for employment must provide a Social Security Number, or indicate they have applied for one. However, when an individual applies for an initial SSN, there is a delay between the assignment of the number and the delivery of the SSN card. At an individual's request, SSA uses Form SSA–132 to send the

individual's SSN to an employer. Mailing this information to the employer: (1) Ensures the employer has the correct SSN for the individual; (2) allows SSA to receive correct earnings information for wage reporting purposes; and (3) reduces the delay in the initial SSN assignment and delivery of the SSN information directly to the employer. It also enables SSA to verify the employer as a safeguard for the applicant's personally identifiable

information. The majority of individuals who take advantage of this option are in the United States with exchange visitor and student visas; however, we allow any applicant for an SSN to use the SSA–132. The respondents are individuals applying for an initial SSN who ask SSA to mail confirmation of their application or the SSN to their employers.

Type of Request: Revision of an OMB-approved information collection.

Modality of completion	Number of respondents	Frequency of response	Average burden per response (minutes)	Estimated total annual burden (hours)
SSA–132	326,000	1	2	10,867

14. *Social Security Administration Health IT Partner Program Assessment—Participating Facilities and Available Content Form—20 CFR 404.1614 and 416.1014—0960–0798.* The Health Information Technology for Economic and Clinical Health (HITECH) Act promotes the adoption and meaningful use of health information technology (IT), particularly in the context of working with government agencies. Similarly, section 3004 of the Public Health Service Act requires health care providers or health insurance issuers with government contracts to implement, acquire, or

upgrade their health IT systems and products to meet adopted standards and implementation specifications. To support expansion of SSA's health IT initiative as defined under HITECH, SSA developed Form SSA–680, the Health IT Partner Program Assessment—participating Facilities and Available Content Form. The SSA–680 allows healthcare providers to provide the information SSA needs to determine their ability to exchange health information with us electronically. We evaluate potential partners (*i.e.*, healthcare providers and organizations) on: (1) The accessibility

of health information they possess; and (2) the content value of their electronic health records' systems for our disability adjudication processes. SSA reviews the completeness of organizations' SSA–680 responses as one part of our careful analysis of their readiness to enter into a health IT partnership with us. The respondents are healthcare providers and organizations exchanging information with the agency.

Type of Request: Revision of an OMB-approved information collection.

Modality of completion	Number of respondents	Frequency of response	Average burden per response (minutes)	Estimated total annual burden (hours)
SSA–680	30	1	5	150

Date: August 1, 2018.

Faye Lipsky,

Reports Clearance Director, Social Security Administration.

[FR Doc. 2018–16727 Filed 8–3–18; 8:45 am]

BILLING CODE 4191–02–P

SOCIAL SECURITY ADMINISTRATION

[Docket No. SSA–2018–0046]

Privacy Act of 1974; System of Records

AGENCY: Office of the General Counsel, Social Security Administration (SSA).

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act, we are issuing public notice of our intent to establish a new system of records entitled, General Law Litigation Files (60–0272). This notice

publishes details of the new system as set forth under the caption,

SUPPLEMENTARY INFORMATION.

DATES: The system of records notice (SORN) is applicable upon its publication in today's **Federal Register**, with the exception of the routine uses, which are effective September 5, 2018. We invite public comment on the routine uses or other aspects of this SORN. In accordance with 5 U.S.C. 552a(e)(4) and (e)(11), the public is given a 30-day period in which to submit comments. Therefore, please submit any comments by September 5, 2018.

ADDRESSES: The public, Office of Management and Budget (OMB), and Congress may comment on this publication by writing to the Executive Director, Office of Privacy and Disclosure, Office of the General Counsel, SSA, Room G–401 West High

Rise, 6401 Security Boulevard, Baltimore, Maryland 21235–6401, or through the Federal e-Rulemaking Portal at <http://www.regulations.gov>, please reference docket number SSA–2018–0046. All comments we receive will be available for public inspection at the above address and we will post them to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT:

Navdeep Sarai, Government Information Specialist, Privacy Implementation Division, Office of Privacy and Disclosure, Office of the General Counsel, SSA, Room G–401 West High Rise, 6401 Security Boulevard, Baltimore, Maryland 21235–6401, telephone: (410) 965–2997, email: Navdeep.Sarai@ssa.gov.

SUPPLEMENTARY INFORMATION: We are establishing the General Law Litigation Files to cover information we collect about individuals (including but not

limited to SSA employees, attorneys, witnesses, plaintiffs, defendants, or third parties) who are or who SSA reasonably anticipates may be involved in civil and criminal litigation or administrative proceedings that involve SSA, the United States, or SSA records. This collection will allow us to represent SSA in litigation, prepare for reasonably anticipated litigation, or respond to litigation requests from SSA employee testimony or records.

In accordance with 5 U.S.C. 552a(r), we have provided a report to OMB and Congress on this new system of records.

Dated: May 30, 2018.

Mary Ann Zimmerman,

Acting Executive Director, Office of Privacy and Disclosure, Office of the General Counsel.

SYSTEM NAME AND NUMBER

General Law Litigation Files, 60–0272.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Social Security Administration, Office of the General Counsel, 6401 Security Boulevard, Room 617 Altmeyer Building, Baltimore, Maryland 21235; or Regional Chief Counsel offices in receipt of original requests (See Appendix C—Regional Offices Addresses, 5. Regional Chief Counsel Addresses at https://www.ssa.gov/privacy/sorn/app_c.htm for address information).

SYSTEM MANAGER(S):

Social Security Administration, Office of the General Counsel, 6401 Security Boulevard, Room 617 Altmeyer Building, Baltimore, MD 21235, OGC.OGLCorrespondence@ssa.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Section 702 of the Social Security Act; 5 U.S.C. 552a; 5 U.S.C. 552; 20 CFR part 403; and various other statutes providing for a right of action by or against SSA or the United States.

PURPOSE(S) OF THE SYSTEM:

We will use the information in this system to represent SSA in litigation, prepare for reasonably anticipated litigation, or respond to litigation requests for SSA employee testimony or records.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who are or who SSA reasonably anticipates may be involved in civil and criminal litigation, or administrative proceedings, that involve SSA, its employees, the United States, or SSA records, including but not limited to SSA employees, attorneys,

witnesses, plaintiffs, defendants, or third parties involved in such litigation.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system maintains information collected or generated in response to, or in anticipation of, civil and criminal litigation, or administrative proceedings, which may include: Social Security number (SSN), if applicable; contact information; information pertaining to the subject matter of litigation, complaints, answers, motions, briefs, orders, decisions, correspondence, exhibits, discovery, legal research, hearing and deposition transcripts, communications with the Department of Justice (DOJ), and medical records, such as evaluations by physicians in cases where personal injury or alleged disabling conditions are involved.

RECORD SOURCE CATEGORIES:

We obtain information in this system from existing SSA records; legal pleadings, discovery, and other records exchanged between parties and their attorneys in litigation and pre-litigation; courts; State and local governments; other Federal agencies; and other individuals and entities with information relevant to cases involving SSA, its employees, the United States, or SSA records.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

We will disclose records pursuant to the following routine uses, however, we will not disclose any information defined as “return or return information” under 26 U.S.C. 6103 of the Internal Revenue Service Code, unless authorized by statute, the Internal Revenue Service (IRS), or IRS regulations.

1. To a congressional office in response to an inquiry from that office made on behalf of, and at the request of, the subject of the record or third party acting on the subject’s behalf.

2. To the Office of the President in response to an inquiry from that office made on behalf of, and at the request of, the subject of the record or a third party acting on the subject’s behalf.

3. To the DOJ, a court or other tribunal, or another party before such court or tribunal, when:

- (a) SSA, or any component thereof; or
- (b) any SSA employee in his/her official capacity; or
- (c) any SSA employee in his/her individual capacity where DOJ (or SSA where it is authorized to do so) has agreed to represent the employee; or
- (d) the United States or any agency thereof where SSA determines the

litigation is likely to affect SSA or any of its components, is a party to the litigation or has an interest in such litigation, and SSA determines that the use of such records by DOJ, a court or other tribunal, or another party before the tribunal is relevant and necessary to the litigation, provided, however, that in each case, the agency determines that disclosure of the records to DOJ, court or other tribunal, or another party is a use of the information contained in the records that is compatible with the purpose for which the records were collected.

4. To contractors and other Federal agencies, as necessary, for the purpose of assisting SSA in the efficient administration of its programs. We will disclose information under this routine use only in situations in which SSA may enter into a contractual or similar agreement with a third party to assist in accomplishing an agency function relating to this system of records.

5. To Federal, State and local government agencies, private individuals, private attorneys, individual law enforcement officers, and other persons or entities with relevant information for the purpose of investigating, settling, or adjudicating claims of violation of law by SSA or its employees and assisting with subsequent litigation.

6. To private attorneys or union representatives, prior to formal litigation proceedings, when SSA determines that due process requires disclosure.

7. To disclose information to officials of labor organizations recognized under 5 U.S.C. chapter 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

8. To student volunteers, individuals working under a personal services contract, and other workers who technically do not have the status of Federal employees, when they are performing work for SSA, as authorized by law, and they need access to personally identifiable information (PII) in SSA records in order to perform their assigned agency functions.

9. To Federal, State and local law enforcement agencies and private security contractors, as appropriate, information necessary:

- (a) To enable them to protect the safety of SSA employees and customers, the security of the SSA workplace, and the operation of SSA facilities, or
- (b) to assist in investigations or prosecutions with respect to activities that affect such safety and security or activities that disrupt the operation of SSA facilities.

10. To the National Archives and Records Administration (NARA) under 44 U.S.C. 2904 and 2906.

11. To appropriate agencies, entities, and persons when:

(a) SSA suspects or has confirmed that there has been a breach of the system of records;

(b) SSA has determined that as a result of the suspected or confirmed breach, there is a risk of harm to individuals, SSA (including its information systems, programs, and operations), the Federal Government, or national security; and

(c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connections with SSA's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

12. To another Federal agency or Federal entity, when SSA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in:

(a) Responding to a suspected or confirmed breach; or

(b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

13. To an appropriate licensing organization or Bar association responsible for investigating, prosecuting, enforcing or implementing standards for maintaining a professional licensing or Bar membership, if SSA becomes aware of a violation or potential violation of professional licensing or Bar association standards or to respond to inquiries or actions from such association about SSA employee conduct.

14. To the Office of Personnel Management, Merit Systems Protection Board, or the Office of Special Counsel in connection with appeals, special studies of the civil service and other merit systems, review of rules and regulations, investigations of alleged or possible prohibited personnel practices, and other such functions promulgated in 5 U.S.C. Chapter 12, or as may be required by law.

15. To the Equal Employment Opportunity Commission when requested in connection with investigations into alleged or possible discriminatory practices in the Federal sector, examination of Federal affirmative employment programs, compliance by Federal agencies with Uniformed Guidelines on Employee

Selection Procedures, or other functions vested in the Commission.

16. To disclose information to the Federal Labor Relations Authority (including its General Counsel) when requested in connection with investigation and resolution of allegations of unfair labor practices, in connection with the resolution of exceptions to arbitrator's awards when a question of material fact is raised, to investigate representation petitions and to conduct or supervise representation elections, and in connection with matters before the Federal Services Impasses Panel.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

We will maintain records in this system in paper and electronic form.

POLICIES AND PRACTICES FOR RETRIEVABILITY OF RECORDS:

We will retrieve records by the case name, party names, case number, or names of individuals reasonably anticipated to be involved in litigation.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

In accordance with NARA rules codified at 36 CFR 1225.16, we maintain the general law litigation records in accordance with the approved NARA Agency-Specific Records Schedule N1-047-10-004. Periods of retention vary depending on the type of litigation record. See http://www.archives.gov/records-mgmt/rcs/schedules/independent-agencies/rg-0047/n1-047-10-004_sf115.pdf. The Office of the General Counsel reserves the right to retain for an indefinite period certain records that, in the judgment of that office are of precedential value.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

We retain electronic and paper files with personal identifiers in secure storage areas accessible only by our authorized employees and contractors who have a need for the information when performing their official duties. Security measures include, but are not limited to, the use of codes and profiles, personal identification number and password, and personal identification verification cards. We keep paper records in locked cabinets within secure areas, with access limited to only those employees who have an official need for access in order to perform their duties.

We annually provide our employees and contractors with appropriate security awareness training that includes reminders about the need to protect PII and the criminal penalties that apply to unauthorized access to, or

disclosure of, PII (5 U.S.C. 552a(i)(1)). Furthermore, employees and contractors with access to databases maintaining PII must sign a sanctions document annually, acknowledging their accountability for inappropriately accessing or disclosing such information.

RECORD ACCESS PROCEDURES:

Individuals may submit requests for information about whether this system contains a record about them by submitting a written request to the system manager at the above address, which includes their name, SSN, or other information that may be in this system of records that will identify them. Individuals requesting notification of, or access to, a record by mail must include (1) a notarized statement to us to verify their identity or (2) must certify in the request that they are the individual they claim to be and that they understand that the knowing and willful request for, or acquisition of, a record pertaining to another individual under false pretenses is a criminal offense.

Individuals requesting notification of, or access to, records in person must provide their name, SSN, or other information that may be in this system of records that will identify them, as well as provide an identity document, preferably with a photograph, such as a driver's license. Individuals lacking identification documents sufficient to establish their identity must certify in writing that they are the individual they claim to be and that they understand that the knowing and willful request for, or acquisition of, a record pertaining to another individual under false pretenses is a criminal offense.

These procedures are in accordance with our regulations at 20 CFR 401.40 and 401.45.

CONTESTING RECORD PROCEDURES:

Same as record access procedures. Individuals should also reasonably identify the record, specify the information they are contesting, and state the corrective action sought and the reasons for the correction with supporting justification showing how the record is incomplete, untimely, inaccurate, or irrelevant. These procedures are in accordance with our regulations at 20 CFR 401.65(a).

NOTIFICATION PROCEDURES:

Same as record access procedures. These procedures are in accordance with our regulations at 20 CFR 401.40 and 401.45.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

[FR Doc. 2018–16692 Filed 8–3–18; 8:45 am]

BILLING CODE P

DEPARTMENT OF STATE

[Public Notice: 10488]

E.O. 13224 Designation of Abdul Rehman al-Dakhil, aka Dilshad Ahmad, aka Danish Dilshad, aka Amantullah Ali, aka Amanatullah Ali, aka Amanat Ali, aka Imanat Ullah Iqbal, aka ‘Abd al-Rahman al-Dakhil as a Specially Designated Global Terrorist

Acting under the authority of and in accordance with section 1(b) of Executive Order 13224 of September 23, 2001, as amended by Executive Order 13268 of July 2, 2002, and Executive Order 13284 of January 23, 2003, I hereby determine that the person known as Abdul Rehman al-Dakhil, also known as Dilshad Ahmad, also known as Danish Dilshad, also known as Amantullah Ali, also known as Amanatullah Ali, also known as Amanat Ali, also known as Imanat Ullah Iqbal, also known as ‘Abd al-Rahman al-Dakhil, committed, or poses a significant risk of committing, acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy, or economy of the United States.

Consistent with the determination in section 10 of Executive Order 13224 that prior notice to persons determined to be subject to the Order who might have a constitutional presence in the United States would render ineffectual the blocking and other measures authorized in the Order because of the ability to transfer funds instantaneously, I determine that no prior notice needs to be provided to any person subject to this determination who might have a constitutional presence in the United States, because to do so would render ineffectual the measures authorized in the Order.

This notice shall be published in the **Federal Register**.

Dated: June 20, 2018.

Michael R. Pompeo,*Secretary of State.*

[FR Doc. 2018–16781 Filed 8–3–18; 8:45 am]

BILLING CODE 4710-AD-P

DEPARTMENT OF STATE

[Delegation of Authority No. 448]

Delegation of Authority To Concur With Department of Defense Humanitarian and Civic Assistance Activities

By virtue of the authority vested in the Secretary of State by the laws of the United States, including section 1 of the State Department Basic Authorities Act, I hereby delegate to the Under Secretary for Arms Control and International Security, to the extent authorized by law, the authority to concur with the Secretary of Defense on humanitarian and civic assistance activities.

Notwithstanding this delegation of authority, any function or authority delegated herein may be exercised by the Secretary and the Deputy Secretary. The authority delegated herein may be re-delegated, to the extent authorized by law. Any reference in this delegation of authority to any statute or delegation of authority shall be deemed to be a reference to such statute or delegation of authority as amended from time to time.

This delegation of authority shall be published in the **Federal Register**.

Dated: June 29, 2018.

Michael R. Pompeo,*Secretary of State, Department of State.*

[FR Doc. 2018–16782 Filed 8–3–18; 8:45 am]

BILLING CODE 4710-05-P

DEPARTMENT OF TRANSPORTATION

Federal Motor Carrier Safety Administration

[Docket No. FMCSA–2018–0182]

Hours of Service of Drivers: Allied Beverage Group L.L.C. (Allied); Application for Exemption

AGENCY: Federal Motor Carrier Safety Administration (FMCSA), DOT.

ACTION: Notice of application for exemption; request for comments.

SUMMARY: FMCSA announces that it has received an application from Allied Beverage Group L.L.C. (Allied) for an exemption from the requirement that short-haul drivers utilizing the records of duty status (RODS) exception return to their normal work-reporting location within 12 hours of coming on duty. Allied requests that their company drivers be allowed to use the short-haul exception but return to their work-reporting location within 14 hours instead of the usual 12 hours. The requested exemption would apply to all of Allied’s drivers who operate

commercial motor vehicle (CMV) beverage trucks. FMCSA requests public comment on Allied’s application for exemption.

DATES: Comments must be received on or before September 5, 2018.

ADDRESSES: You may submit comments identified by Federal Docket Management System Number FMCSA–2018–0182 by any of the following methods:

- *Federal eRulemaking Portal:* www.regulations.gov. See the *Public Participation and Request for Comments* section below for further information.

- *Mail:* Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Avenue SE, West Building, Ground Floor, Room W12–140, Washington, DC 20590–0001.

- *Hand Delivery or Courier:* West Building, Ground Floor, Room W12–140, 1200 New Jersey Avenue SE, between 9 a.m. and 5 p.m. E.T., Monday through Friday, except Federal holidays.

- *Fax:* 1–202–493–2251.

Each submission must include the Agency name and the docket number for this notice. Note that DOT posts all comments received without change to www.regulations.gov, including any personal information included in a comment. Please see the *Privacy Act* heading below.

Docket: For access to the docket to read background documents or comments, go to www.regulations.gov at any time or visit Room W12–140 on the ground level of the West Building, 1200 New Jersey Avenue SE, Washington, DC, between 9 a.m. and 5 p.m., ET, Monday through Friday, except Federal holidays. The on-line FDMS is available 24 hours each day, 365 days each year.

Privacy Act: In accordance with 5 U.S.C. 553(c), DOT solicits comments from the public to better inform its rulemaking process. DOT posts these comments, without edit, including any personal information the commenter provides, to www.regulations.gov, as described in the system of records notice (DOT/ALL–14 FDMS), which can be reviewed at www.dot.gov/privacy.

FOR FURTHER INFORMATION CONTACT: Mr. Richard Clemente, FMCSA Driver and Carrier Operations Division; Office of Carrier, Driver and Vehicle Safety Standards; Telephone: 202–366–2722. Email: MCPSD@dot.gov. If you have questions on viewing or submitting material to the docket, contact Docket Services, telephone (202) 366–9826.

SUPPLEMENTARY INFORMATION: