Dated: June 30, 2010.

Thomas D. Shope,

Regional Director, Appalachian Region.

[FR Doc. 2010–21645 Filed 8–30–10; 8:45 am]

BILLING CODE 4310–05–P

DEPARTMENT OF JUSTICE

Notice of Lodging of Proposed Consent Decree Under the Clean Water Act

Notice is hereby given that on August 25, 2010, a proposed Consent Decree ("Consent Decree") in *United States* v. *City of Revere, Massachusetts,* Civil Action No. 1:10–cv–11460 was lodged with the United States District Court for the District of Massachusetts.

In a complaint, filed simultaneously with the Decree, the United States alleges that the City of Revere, Massachusetts ("City") violated Sections 301 and 308 of the Clean Water Act, 33 U.S.C. 1311 and 1318, as a result of unauthorized discharges of pollutants including raw sewage from the City's sanitary sewer system and its separate storm sewer system, as well as a failure to report sanitary sewer overflows to the United States Environmental Protection Agency. The proposed Consent Decree resolves the United States' claims for civil penalties and injunctive relief, as alleged in the complaint. Specifically, the proposed Consent Decree requires the City to implement remedial measures, including necessary upgrades to its sanitary sewer system and separate storm sewer system, over a period of approximately twelve years and at an estimated cost of approximately $50 million. The Consent Decree also requires the City to pay a $130,000 civil penalty.

The Department of Justice will receive, for a period of thirty (30) days from the date of this publication, comments relating to the Consent Decree. Comments should be addressed to the Assistant Attorney General, Environment and Natural Resources Division, and either e-mailed to *pubcomment-ees.enrd@usdoj.gov* or mailed to P.O. Box 7611, United States Department of Justice, Washington, DC 20044–7611, and should refer to *United States* v. *City of Revere, Massachusetts,* D.J. Ref. 90–5–1–1–09299.

The Consent Decree may be examined at the Office of the United States Attorney, One Courthouse Way, John Joseph Moakley Courthouse, Boston, Massachusetts 02210, and at U.S. EPA Region 1, Office of Regional Counsel, 5 Post Office Square, Suite 100, Boston, Massachusetts 02109. During the public comment period, the Consent Decree may also be examined on the following Department of Justice Web site, *http://www.usdoj.gov/enrd/Consent_Decrees.html.* A copy of the Consent Decree may also be obtained by mail from the Consent Decree Library, P.O. Box 7611, U.S. Department of Justice, Washington, DC 20044–7611 or by faxing or e-mailing a request to Tonia Fleetwood (*tonia.fleetwood@usdoj.gov*), fax no. (202) 514–0097, phone confirmation number (202) 514–1547. In requesting a copy from the Consent Decree Library, please enclose a check to cover the 25 cents per page reproduction costs in the amount of $16.25 (for Decree without appendix) or $71.75 (for Decree with appendix) payable to the U.S. Treasury or, if by e-mail or fax, forward a check in that amount to the Consent Decree Library at the stated address.

Maureen Katz,

Assistant Chief, Environmental Enforcement Section, Environment and Natural Resources Division.

[FR Doc. 2010–21569 Filed 8–30–10; 8:45 am]

BILLING CODE 4410–15–P

DEPARTMENT OF JUSTICE

[CPCLO Order No. 003–2010]

Privacy Act of 1974; System of Records

AGENCY: Federal Bureau of Investigation, Department of Justice.

ACTION: Notice of a new system of records.

SUMMARY: Pursuant to the Privacy Act of 1974 (5 U.S.C. 552a), the United States Department of Justice (Department), Federal Bureau of Investigation (FBI), proposes to establish a new system of records, the Data Integration and Visualization System, JUSTICE/FBI–021, to support and enhance data search, integration, presentation, and storage capabilities in support of the FBI's multifaceted mission.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), the public is given a 30-day period in which to comment. Therefore, please submit any comments by September 30, 2010.

ADDRESSES: The public, OMB, and Congress are invited to submit any comments to the Department of Justice, *Attn:* Privacy Analyst, Office of Privacy and Civil Liberties, U.S. Department of Justice, National Place Building, 1331 Pennsylvania Ave, NW., Suite 940, Washington, DC 20530–0001, or by facsimile at 202–307–0693.

FOR FURTHER INFORMATION CONTACT: Erin Page, Assistant General Counsel, Privacy and Civil Liberties Unit, Office of the General Counsel, FBI, Washington, DC 20535–0001, telephone 202–324–3000.

SUPPLEMENTARY INFORMATION: Threats from terrorism, espionage, cyber attacks and more traditional crimes continue to jeopardize the well-being of our nation and its citizens while criminals continue to find new and inventive ways to carry out their reprehensible activities. To stay ahead of the threats the FBI continually searches for ways to more effectively understand the danger posed by those who threaten harm. The FBI has available a number of lawfully collected databases that allow it to conduct investigations and analyze intelligence for this purpose. Historically, FBI personnel searched individual databases to extract relevant information and then compared the extract to other available information in order to form a more complete and accurate threat picture. This was a time-consuming process and led to possible gaps in the collated information.

Continued threats to the national security of the United States and criminal events have strengthened the FBI's resolve to develop more efficient methods to analyze FBI data. The Data Integration and Visualization System, DIVS, will allow authorized system users to more effectively search, integrate, display, maintain, and record relevant information in support of the FBI's multifaceted mission. DIVS will provide users with the ability to simultaneously conduct searches across several databases, extract information, and present the integrated results in a format that the user may sort and display in various modes. In order to do this, DIVS will contain replications of some databases while providing the ability to perform federated queries across other databases. DIVS will allow users to save their queries as well as create a separate record of relevant identifiers and information. One of the results of DIVS will be a new set of records that offers an enhanced view of information already contained in FBI holdings.

DIVS will provide a single user interface that incorporates the rules of behavior for FBI information systems, tools to ensure access controls based on roles and data attributes, entity resolution and appropriate metadata tagging. These tools will help ensure data accuracy and reliability.

To enhance the flexibility of the system, DIVS includes a variety of routine uses that the FBI has used successfully in sharing information from its other record systems. The FBI will

share information learned through DIVS pursuant to the requirements of the Privacy Act and, in the case of its routine uses, when the disclosure is compatible with the purpose for which the information was compiled.

In accordance with Privacy Act requirements of 5 U.S.C. 552a(r), the Department has provided a report to OMB and to Congress on this new system of records.

Dated: August 20, 2010.

Nancy C. Libin,

Chief Privacy and Civil Liberties Officer.

JUSTICE/FBI–021

SYSTEM NAME:

Data Integration and Visualization System (DIVS).

SYSTEM CLASSIFICATION:

Classified, unclassified—law enforcement sensitive, and unclassified.

SYSTEM LOCATION:

Records may be maintained at any location at which the Federal Bureau of Investigation (FBI) operates or at which FBI operations are supported, including: J. Edgar Hoover Building, 935 Pennsylvania Ave., NW., Washington, DC 20535–0001; FBI Academy and FBI Laboratory, Quantico, VA 22135; FBI Criminal Justice Information Services (CJIS) Division, 1000 Custer Hollow Rd., Clarksburg, WV 26306; and FBI field offices, legal attaches, information technology centers, and other components listed on the FBI's internet Web site, *http://www.fbi.gov.* Some or all system information may also be duplicated at other locations for purposes of system backup, emergency preparedness, and/or continuity of operations. Additionally, appropriate offices/employees within the Department of Justice that have an official need to know the information contained in DIVS in order to perform their duties, may also be granted direct access to DIVS.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The categories of individuals covered by this system encompass all individuals who relate in any manner to authorized FBI investigative mission activities, including individuals identified in any of multiple data sets lawfully collected and/or shared with the FBI. These individuals include, but are not limited to subjects, suspects, victims, witnesses, complainants, informants, sources, bystanders, law enforcement personnel, intelligence personnel, other responders, administrative personnel, consultants, relatives, and associates who are relevant to an investigation.

In addition, the categories of individuals covered by this system also include persons who are authorized to access and use DIVS.

CATEGORIES OF RECORDS IN THE SYSTEM:

DIVS contains replications and extractions of information maintained by the FBI in other databases. This information is replicated or extracted into DIVS in order to provide an enhanced and integrated view of that information. DIVS also provides analytic tools that can be applied across the multiple data sets in order to integrate and visually display, and maintain and record the resultant information. Information concerning individuals may be acquired in connection with and relating to the varied mission responsibilities of the FBI. Depending on the nature and scope of the matter, this information may include, among other things: biographical information (such as name, alias, race, sex, date of birth, place of birth, social security number, driver's license number, other identification numbers, addresses, telephone numbers, physical description, photographs); biometric information (such as fingerprints); associates and affiliations; employment and business information; financial information; visa and immigration information; travel; criminal and investigative history; and any other information lawfully acquired by the FBI.

DIVS contains records regarding authorized system users, including audit log information and records relating to verification or authorization of an individual's access to one or more databases. This information includes user name, date and time of use, date and time of each searched query, search terms and filters, results that the user accessed, and a user's permissions and authorizations for particular data at that time.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

General authority for FBI mission activities includes: 28 U.S.C., Chapter 33, particularly sections 533 and 534; the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law 107–56, 115 Stat. 272; the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law 108–458, 118 Stat. 3742; the Foreign Intelligence Surveillance Act of 1978 (FISA), Public Law 95–511, 92 Stat. 1783 (50 U.S.C., Chapter 36); E.O. 13356; E.O. 13388; 28 CFR 0.85; and Attorney General's Guidelines for Domestic FBI Operations. Supplemental authorities relating to particular mission activities are found in numerous other Federal statutes, executive orders, Federal regulations, and other Executive Branch directives.

PURPOSE(S):

The purpose of DIVS is to strengthen and improve the methods by which the FBI searches for and analyzes information in support of its multifaceted mission responsibilities to protect the nation against terrorism and espionage and investigate criminal matters. DIVS will provide users with the ability simultaneously to conduct searches across multiple databases (some of which are ingested directly into and exist in DIVS and others of which are searched via DIVS's federated query capability), extract and integrate information, and present the results in a format that the user may sort and display in various modes. DIVS also provides analytic tools that can be applied across the multiple data sets in order to integrate and visually display, maintain, and record the resultant information.

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 FBI as a routine use pursuant to 5 U.S.C. 552a(b)(3) under the circumstances or for the purposes described below, to the extent such disclosures are compatible with the purposes for which the information was collected:

A. Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

B. To any criminal, civil, or regulatory law enforcement authority (whether federal, state, local, territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

C. To a governmental entity lawfully engaged in collecting law enforcement,

law enforcement intelligence, or national security intelligence information for such purposes.

D. To any person, organization, or governmental entity in order to notify them of a serious terrorist threat for the purpose of guarding against or responding to such a threat.

E. To any person or entity if deemed by the FBI to be necessary in order to elicit information or cooperation from the recipient for use by the FBI in performance of an authorized law enforcement activity.

F. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish an agency function related to this system of records.

G. To appropriate officials and employees of a federal agency or entity when the information is relevant to a decision concerning the hiring, appointment, or retention of an employee; the assignment, detail, or deployment of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.

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

I. In an appropriate proceeding before a court, a grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

J. To an organization or individual in both the public or private sector where there is reason to believe the recipient is or could become the target of a particular criminal activity or conspiracy or other threat, to the extent the information is relevant to the protection of life, health, or property. Information may be similarly disclosed to other recipients who share the same interests as the target or who may be able to assist in protecting against or responding to the activity or conspiracy.

K. In any health care-related civil or criminal case, investigation, or matter, information indicating patient harm, neglect, or abuse, or poor or inadequate quality of care, at a health care facility or by a health care provider, may be disclosed as a routine use to any federal, state, local, tribal, foreign, joint, international, or private entity that is responsible for regulating, licensing, registering, or accrediting any health care provider or health care facility, or enforcing any health care-related laws or regulations. Further, information indicating an ongoing quality of care problem by a health care provider or at a health care facility may be disclosed to the appropriate health plan. Additionally, unless otherwise prohibited by applicable law, information indicating patient harm, neglect, abuse, or poor or inadequate quality of care may be disclosed to the affected patient or his or her representative or guardian at the discretion of and in the manner determined by the agency in possession of the information.

L. Information relating to health care fraud may be disclosed to private health plans, or associations of private health plans, and health insurers, or associations of health insurers, for the following purposes: To promote the coordination of efforts to prevent, detect, investigate, and prosecute healthcare fraud; to assist efforts by victims of health care fraud to obtain restitution; to enable private health plans to participate in local, regional, and national health care fraud task force activities; and to assist tribunals having jurisdiction over claims against private health plans.

M. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

N. To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings.

O. To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

P. To federal, state, local, territorial, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

Q. To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

R. To a former employee of the Department for purposes of: Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

S. To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.

T. To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

U. To appropriate agencies, entities, and persons when (1) it is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (2) DOJ 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 the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize or remedy such harm.

V. To the White House (the President, Vice President, their staffs, and other entities of the Executive Office of the President (EOP)), and, during Presidential transitions, the President-Elect and Vice-President Elect and their designees for appointment, employment, security, and access purposes compatible with the purposes for which the records were collected by the FBI, e.g., disclosure of information to assist the White House in making a determination whether an individual should be: (1) Granted, denied, or

permitted to continue in employment on the White House Staff; (2) given a Presidential appointment or Presidential recognition; (3) provided access, or continued access, to classified or sensitive information; or (4) permitted access, or continued access, to personnel or facilities of the White House/EOP complex. System records may be disclosed also to the White House and, during Presidential transitions, to the President-Elect and Vice-President Elect and their designees, for Executive Branch coordination of activities which relate to or have an effect upon the carrying out of the constitutional, statutory, or other official or ceremonial duties of the President, President-Elect, Vice-President or Vice-President Elect.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records in this system are stored on paper and/or in electronic form. Records are stored securely in accordance with applicable executive orders, statutes, and agency implementing recommendations.

RETRIEVABILITY:

Information is retrieved by an individual's name or other identifying information.

SAFEGUARDS:

Information in this system is safeguarded in accordance with appropriate laws, rules, and policies, including the FBI's automated systems security and access policies, and access to such information is limited to Department personnel, contractors, and other personnel who have an official need for access in order to perform their duties. Records are maintained in a restricted area and directly accessed only by authorized personnel. Electronic records are accessed only by authorized personnel with accounts on the FBI's computer network. Additionally, direct access to certain information may be restricted depending on a user's role and responsibility within the system. Paper records are safeguarded in accordance with appropriate laws, rules, and policies based on the classification and handling restrictions of the particular document.

RETENTION AND DISPOSAL:

Records are retained during their useful life in accordance with the records retention schedules approved by the National Archives and Records Administration.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Federal Bureau of Investigation, 935 Pennsylvania Ave NW., Washington, DC 20535.

NOTIFICATION PROCEDURE:

Same as Record Access Procedures.

RECORDS ACCESS PROCEDURE:

The Attorney General has exempted this system of records from the notification, access, and contest procedures of the Privacy Act. These exemptions apply only to the extent that the information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j) and/or (k). Where compliance would not appear to interfere with or adversely affect the purposes of the system, or the overall law enforcement/intelligence process, the applicable exemption (in whole or in part) may be waived by the FBI in its sole discretion.

All requests for access should follow the guidance provided on the FBI's Web site at *http://foia.fbi.gov/requesting_records.html.* Individuals may mail, fax, or email a request, clearly marked "Privacy Act Request," to the Federal Bureau of Investigation, *Attn:* FOI/PA Request, Record/Information Dissemination Section, 170 Marcel Drive, Winchester, VA 22602–4843; *Fax:* 540–868–4995/6/7; *E-mail:* (scanned copy) *foiparequest@ic.fbi.gov.* The request should include a general description of the records sought and must include either a completed Department of Justice Certification of Identity Form, DOJ–361, which can be located at the above link, or a letter that has been notarized which includes: the requester's full name, current and complete address, and place and date of birth. In the initial request the requester may also include any other identifying data that the requester may wish to furnish to assist the FBI in making a reasonable search. The request should include a return address for use by the FBI in responding; requesters are also encouraged to include a telephone number to facilitate FBI contacts related to processing the request. A determination of whether a record may be accessed will be made after a request is received.

CONTESTING RECORDS PROCEDURE:

Same as Record Access Procedures. Individuals desiring to contest or amend information maintained in the system should also state clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

RECORD SOURCE CATEGORIES:

Sources of information contained in this system are derived from FBI case files and other law enforcement and intelligence records as well as data sets lawfully obtained from other agencies and entities.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted this system of records from subsection (c)(3) and (4); (d)(1), (2), (3) and (4); (e)(1), (2), and (3); (e)(4)(G), (H) and (I); (e)(5) and (8); (f) and (g) of the Privacy Act. These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j) and/or (k). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c), and (e) and have been published in today's **Federal Register**.

[FR Doc. 2010–21248 Filed 8–30–10; 8:45 am]

BILLING CODE 4410–02–P

DEPARTMENT OF LABOR

Office of the Secretary

Submission for OMB Review; Comment Request

ACTION: Notice.

The Department of Labor (DOL) hereby announces the submission of the following public information collection request (ICR) to the Office of Management and Budget (OMB) for review and approval in accordance with the Paperwork Reduction Act of 1995 (Pub. L. 104–13, 44 U.S.C. chapter 35). A copy of this ICR, with applicable supporting documentation; including, among other things, a description of the likely respondents, proposed frequency of response, and estimated total burden may be obtained from the RegInfo.gov Web site at *http://www.reginfo.gov/public/do/PRAMain* or by contacting Linda Watts Thomas on 202–693–4223 (this is not a toll-free number); e-mail mail to: *DOL_PRA_PUBLIC@dol.gov.*

Interested parties are encouraged to send comments to the Office of Information and Regulatory Affairs, *Attn:* OMB Desk Officer for the Department of Labor—Mine Safety and Health Administration (MSHA), Office of Management and Budget, 725 17th Street, NW., Room 10235, Washington, DC 20503, *Telephone:* 202–395–4816/*Fax:* 202–395–5806 (these are not toll-free numbers), *e-mail: OIRA_submission@omb.eop.gov* within