States except as authorized by the Clean Water Act and Rivers and Harbors Act.

The Department of Justice will accept written comments relating to the proposed consent decree for thirty (30) days from the date of publication of this notice. Comments should be addressed to the Assistant Attorney General, Environment and Natural Resources Division, U.S. Department of Justice, Attention: Wendy L. Blake, Environmental Defense Section, P.O. Box 23986, Washington, D.C. 20026–3986, and should refer to *United States* v. *St. Charles Riverfront Station, Inc.*, DJ Reference No. 90–5–1–1–05577.

The proposed consent decree may be examined at the Clerk's Office of the United States District Court for the Eastern District of Missouri, 1114 Market Street, Room 260, St. Louis, Missouri.

Letitia J. Grishaw,

Chief, Environmental Defense Section, Environment and Natural Resources Division, United States Department of Justice.

[FR Doc. 99–33835 Filed 12–29–99; 8:45 am]

BILLING CODE 4410–15–M

DEPARTMENT OF JUSTICE

Notice of Lodging of Consent Decree Pursuant to the Clean Air Act

In accordance with Departmental policy, 28 CFR 50.7, notice is hereby given that on December 17, 1999, a proposed consent decree in *United States* v. *Titanium Metals Corporation*, CV–9–98–00682–HDM (RLH) (D. Nev.), was lodged with the United States District Court for the District of Nevada. The proposed consent decree would resolve pending claims of the United States against Titanium Metals Corporation (''TIMET''), in the above-referenced action.

The Complaint in the above-referenced civil action seeks injunctive relief and civil penalties for alleged violations of the Clean Air Act, 42 U.S.C. § 7413(b), at TIMET's titanium manufacturing plant in Henderson, Nevada. The complaint alleges that TIMET installed a carbon monoxide (''CO'') burner at its plant prior to obtaining either a Prevention of Significant Deterioration or minor source permit. The installation of the burner in reduced emissions of CO, but increased the facility's potential to emit sulfur dioxide (''SO_2''). Under the proposed Decree, TIMET has agreed to install the Best Available Control Technology to control SO_2 emissions, enforceable limits on CO and SO_2 emissions, and payment of a civil penalty of $430,000 over a two year period.

The Department of Justice will receive, for a period of thirty (30) days from the date of this publication, comments relating to the proposed Consent Decree. Comments should be addressed to the Assistant Attorney General for the Environment and Natural Resources Division, United States Department of Justice, P.O. Box 7611, Ben Franklin Station, Washington, D.C. 20044–7611, and should refer to *United States* v. *Titanium Metals Corporation*, CV–8–87–00682 (D. Nev.), and the Department of Justice Reference No. 90–5–2–1–2235.

The proposed Consent Decree may be examined at the Office of the United States Attorney for the District of Nevada, 701 East Bridger, 8th Floor, Las Vegas, NV 89101; and at the Region IX Office of the United States Environmental Protection Agency, 75 Hawthorne Street, San Francisco, CA 94105. A copy of the proposed Consent Decree may be obtained by mail from the Department of Justice Consent Decree Library, P.O. Box 7611, Washington, DC 20044. In requesting a copy, please refer to DJ #90–5–2–1–2235, and enclose a check in the amount of $7.75 (31 pages at 25 cents per page for reproduction costs). Make checks payable to the Consent Decree Library.

Joel M. Gross,

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

[FR Doc. 99–33834 Filed 12–29–99; 8:45 am]

BILLING CODE 4410–15–M

DEPARTMENT OF JUSTICE

[AAG/A Order No. 189–99]

Privacy Act of 1974; System of Records

Pursuant to the provisions of the Privacy Act of 1974 (5 U.S.C. 552a), the Department of Justice (DOJ) is establishing a system of records entitled ''DOJ Computer Systems Activity and Access Records, DOJ–002.''

Title 5 U.S.C. 552a(e)(4) and (11) provide that the public be given a 30-day period in which to comment on the new system. The Office of Management and Budget (OMB), which has oversight responsibility under the Act, requires a 40-day period in which to review the proposed system. Therefore, please submit any comments by 40 days from publication of this notice. The public, OMB, and the Congress are invited to submit written comments to Mary Cahill, Management and Planning Staff, Justice Management Division, Washington, DC 20530, (202) 307–1823.

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

Dated: December 17, 1999.

Stephen R. Colgate,

Assistant Attorney General for Administration.

SYSTEM NAME:

Department of Justice (DOJ) Computer Systems Activity and Access Records, DOJ–002

SYSTEM LOCATION:

Department of Justice offices (and other sites utilized by the Department of Justice) throughout the world.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who access DOJ network computers or mainframe/enterprise servers, including individuals who send and receive electronic communications, access Internet sites, or access system databases, files, or applications from DOJ computers or sending electronic communications to DOJ computers; and individuals attempting to access DOJ computers or systems without authorization.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system of records may include: records on the use of the interoffice and Internet e-mail systems, including the e-mail address of the sender and receiver of the e-mail message, subject, date, and time; records on user access to DOJ's office automation networks, including user ID, date and time of log on and log off, and denials of access to unauthorized files or directories; records of Internet access from a DOJ computer, such as the Internet Protocol (IP) address of the computer being used to initiate the Internet connection, the site accessed, date, and time; records relating to mainframe/enterprise server access, such as user ID of the individual accessing the mainframe, date and time, and the process being run on the mainframe; records relating to verification or authorization of an individual's access to systems, files, or applications, such as user IDs, passwords, user names, title, and agency.

Logs of Internet access from a DOJ computer do not contain names or similar personal identifiers. However, for official government business purposes, a name may be associated with an IP address.

AUTORITY FOR MAINTENANCE OF THE SYSTEM:

The Computer Security Act of 1987, 40 U.S.C. 1441 note, requires Federal

Agencies to plan for the security and privacy of their computer systems.

PURPOSE(S):

the underlying raw data in this system of records is used by DOJ systems and security personnel, or persons authorized to assist these personnel, to plan and manage system services and to otherwise perform their official duties. Authorized DOJ managers may use the records in this system to investigate improper access or other improper activity related to computer system access; to initiate disciplinary or other such action; and/or where the record(s) may appear to indicate a violation or potential violation of the law, to refer such record(s) to the appropriate investigative arm of DOJ, or other law enforcement agency for investigation.

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

Information maybe made available in accordance with the disclosure provisions cited below.

1. To members of Congress or staff to respond to inquiries made on behalf of individual constituents who are record subjects.

2. To representatives of the General Services Administration and/or the National Archives and Records Administration who are conducting records management inspections under the authority of 44 U.S.C. 2904 and 2906.

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

4. To a Federal, state, local, tribal or foreign agency, or a private contractor, in connection with: the hiring or retention of any employee; the issuance of a security clearance; the conduct of a security or suitability investigation or pursuit of other appropriate personnel matter; the reporting of an investigation on an employee; the letting of a contract; or the issuance of a grant, license, or other benefit to an employee by the agency, but only to the extent that the information disclosed is relevant and necessary to the agency's decision on the matter.

5. To provide information to any person(s) authorized to assist in an approved investigation of improper usage of DOJ computer systems.

6. To an actual or potential party or his or her authorized representative for the purpose of negotiation or discussion on such matters as settlement of the case or matter, or informal discovery proceedings.

7. In the event that material in this system of records appears to indicate, either on its face or in conjunction with other information, a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute, or by regulation, rule, or order issued pursuant thereto, to a Federal, State local tribal, or foreign unit of government charged with the responsibility therefor.

8. In a proceeding before a court or adjudicative body, when any of the following is a party to litigation or has an interest in litigation and such records are determined by the DOJ to be arguably relevant to the litigation: the DOJ; any employee of the DOJ in his or her official capacity; or any employee of the DOJ in his or her individual capacity where the DOJ has agreed to represent or has authorized private attorneys to represent the employees; or, the United States, where the DOJ determines that the litigation is likely to affect it or any of its subdivisions.

9. To contractors, grantees, experts, consultants, detailees, and other non-DOJ employees 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.

10. To other government agencies where required by law.

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

Records are stored in electronic and/or paper form.

RETRIEVABILITY:

Records may be retrieved by user name, user ID, e-mail address, or other identifying search term employed, depending on the record category. The Department does not usually connect IP addresses with a person. However, in some instances, for official government business purposes, the Department may connect the IP address with an individual, and records may be retrieved by IP address.

SAFEGUARDS:

Access is limited to those who have an official need to know. Specifically, only systems and security personnel or persons authorized to assist these personnel have access to automated records and magnetic storage media. These records are kept in a locked room with controlled entry. The use of password protection identification features and other automated data processing system protection methods also restrict access. All records are located in buildings with restricted access.

RETENTION AND DISPOSAL:

Records of verification, authorization, computer system access, and other activities generated by the system shall be retained no longer than one year, unless required for management review, then destroyed/deleted. (Records retention schedule pending approval by the Archivist of the United States.)

SYSTEM MANAGER:

Deputy Assistant Attorney General, Information Resources Management, Justice Management Division, Department of Justice, Washington, DC 20530.

NOTIFICATION PROCEDURE:

To determine whether the system may contain records relating to you, write to the System Manager identified above.

RECORD ACCESS PROCEDURES:

Same as ''Notification Procedure'' above. Provide name, assigned computer location, and a description of information being sought, including the time frame during which the record(s) may have been generated. Provide verification of identity as instructed in 28 CFR, § 16.41(d).

CONTESTING RECORD PROCEDURES:

See ''Notification Procedure'' and ''Record Access Procedure'' above. Identify the information being contested, the reason for contesting it, and the correction requested. In general, this information is computer-generated and is not subject to contest.

RECORD SOURCE CATEGORIES:

Most records are generated internally, i.e., computer activity logs; individuals covered by the system; and management officials.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 99–33838 Filed 12–29–99; 8:45 am]

BILLING CODE 4410–OJ–M

DEPARTMENT OF JUSTICE

Drug Enforcement Administration

James Garvey Cavanagh, M.D. Revocation of Registration

On August 5, 1999, the Deputy Assistant Administrator, Office of Diversion Control, Drug Enforcement Administration (DEA), issued an Order