FEDERAL BUREAU OF PRISONS
PRIVACY IMPACT ASSESSMENT (PIA)

System Name:	**ACCESS CONTROL/WEB VISITING**		
OMB Control # For Information Collections (If Available):			
OMB Unique Identifier For IT Systems (If Available):	N/A		
Program Area SME:	Linda Thomas	**Telephone:**	202-307-3078
Job Title:	Chief – Correctional Services Branch		
IT Project SME:	Chris Barnes	**Telephone:**	202-514-4965
Job Title:	Project Manager – Systems Development Branch		
Date:	4/4/06		

Please submit the completed form to the Chief – IT Planning & Development in the Office of Information Systems (OIS). If any question does not apply, state "Not Applicable (N/A)" and briefly explain why it is not applicable.

Part A: Is A PIA Required?

Instructions for this part: If you answer "no" to all of Questions 1-4 below, please briefly describe the IT system being exempted in Part B.1, and submit this document for review and approval. If you answer "yes" to any of Questions 1-4, continue to Question 5.

1. Are you developing or procuring a new IT system or project that collects, maintains, or disseminates information:
   a. about U.S. citizens or aliens lawfully admitted for permanent residence; and
   b. that does NOT pertain only to government employees or contractors?

   Yes

2. Are you initiating a new electronic collection of information under the Paperwork Reduction Act?

   No

3. Are you making a change to an existing IT system that creates new privacy risks? For example:

a. Are you applying a new technology to an existing system that significantly changes how information is managed in the system?

Yes

b. Are you making a change in business processes:

i. that merges, centralizes, matches or otherwise significantly manipulates existing databases?

ii. that results in significant new uses or disclosures of information or incorporation into the system of additional information?

Yes

c. If this information has been collected previously:

i. Are new or significantly larger groups of people being impacted?[1] No

ii. Is new data being added resulting in new privacy concerns? No

iii. Is data being added from a commercial or public source? No

4. Is this information individually identifiable? (Does it pertain to specific individuals who can be identified either directly or in conjunction with other data?) If no, do not answer any more questions and submit this document for review under the PIA process. If yes, continue to the next question.

Yes

5. Has a PIA or similar evaluation been conducted? If yes, does the existing PIA address the questions in Part B? If yes, submit the existing PIA with this document for review under the PIA process. If no, continue to Question 6.

Yes. A Systems of Records Notice was published in 2002. (See Attachment A).

6. Is this a national security system as defined at 40 U.S.C. 11103? 2 If yes, please attach verification and submit this document for review under the PIA process.

No

[1] This includes new electronic collections of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government). See 44 USC Chapter 35 and implementing regulations, 5 CFR Part 1320.8.

Part B: Provide a brief description of what personal information is collected.

1. Please provide a general description of the system, including its purpose.

The Access Control Entry/Exit System (ACES) and Web Visiting system is designed to log and track all persons entering and exiting BOP facilities, including staff, contractors, approved volunteers and approved visitors. Information in the system is collected and maintained to better ensure the safety, security and good order of Bureau facilities; to improve staff ability to quickly account for all persons (inmates, visitors, and staff within an institution in the event of an emergency, such as an institution disturbance or a natural disaster; to identify and, where appropriate, determine the suitability of visitors with respect to entering prison facilities.

2. If this automated system (or Information Collection Request) involves personally identifiable information on members of the public, then ***place an 'X' in any of the categories that apply below:***

Personal Identifiers:

Name	X
Social Security Number (SSN) .	X
Other identification number (specify type):	X (ID Card No., including driver's license; passport no., alien ID no., or state ID no.)
Birth date	X
Home address	X (inmate visitors)
Home telephone	X (inmate visitors)
Personal e-mail address	
Fingerprint/other "biometric"	X
Other (specify):	
None	
Comment:	

Other Sensitive Information:

Race/ ethnicity	X
Gender/ sex	X
Marital status	
Spouse name	X (relationship of visitor to inmate)
# of children	
Employment history	
Education level	
Medical history/information	
Disability	
Criminal record	

Financial Data (salary, accounts, etc.)	
Other (specify):	
Comment:	

3. Type of electronic system or information collection. Fill out Section A, B, or C as applicable.

A. If a new electronic system (or one in development): Is this a new electronic system (implemented after April 2003, the effective date of the E-Government Act of 2002)?

Yes. (Note: older system was developed and implemented in 2001; newer version is a web-based version)

B. If an existing electronic system: Mark any of the following conditions for your existing system that OMB defines as a "trigger" for requiring a PIA (if not applicable, mark N/A):

Conversion: When paper-based records that contain personal information are converted to an electronic system	
From Anonymous (Non-Identifiable) to "Non-Anonymous" (Personally Identifiable): When any systems application transforms an existing database or data collection so that previously anonymous data becomes personally identifiable	
Significant System Management Changes: When new uses of an existing electronic system significantly change how personal information is managed in the system. (Example #1: when new "relational" databases could combine multiple identifying data elements to more easily identify an individual. Example #2: when a web portal extracts data elements from separate databases, and thereby creates a more open environment for exposure of personal data)	
Merging Databases: When government databases are merged, centralized, matched, or otherwise significantly manipulated so that personal information becomes more accessible (with special concern for the ability to combine multiple identifying elements)	X (System was converted from client-server framework to web-based)
New Public Access: When new public access is given to members of the public or to business partners (even if the system is protected by password, digital certificate, or other user-authentication technology)	
Commercial Sources: When agencies systematically incorporate into databases any personal data from commercial or public sources (ad hoc queries of such sources using existing technology does not trigger the need for a PIA)	
New Inter-agency Uses: When agencies work together (such as	

the federal E-Gov initiatives), the lead agency should prepare the PIA	
Business Process Re-engineering: When altering a business process results in significant new uses, disclosures, or additions of personal data	
Alteration in Character of Data: When adding new personal data raises the risks to personal privacy (for example, adding financial information to an existing database that contains name and address)	

C. If an Information Collection Request (ICR): Is this a <u>new</u> Request that will collect data that will be in an <u>automated</u> system? Agencies must obtain OMB approval for information collections from 10 or more members of the public. The E-Government Act of 2002 requires a PIA for ICRs only if the collection of information is a <u>new</u> request and the collected data will be in an <u>automated</u> system.

Yes, this is a new ICR and the data will be automated	N/A
No, the ICR does not require a PIA because it is not <u>new</u> or <u>automated</u>)	N/A
Comment:	

Question 3: Why is the personally identifiable information being collected? How will it be used? Mark any that apply:

General:

Inmate Visiting	X
Inmate Correspondence	
Inmate Telephone Calling List	
Employment Application	
FOIA/PA Request	
Litigation/Administrative Claim	
Other (specify):	Access/Accountability

Internal operations:

Employee payroll or personnel records	
Payment for employee travel expenses	
Payment for services or products (to contractors) – if any personal information on the payee is included	
Computer security files – collected in order to grant network/system access	
Other (specify):	

Comment:	

Other lines of business (specify uses):

Correctional Administration	X (ensures security and good order of BOP facilities)

Question 4: Will you share the information with others (e.g., another agency for a programmatic purpose, or outside the government)? Mark any that apply:

Federal agencies? (specify):	X (FBI, DEA, DOJ OIG and other law enforcement agencies for purposes of criminal investigations)
State, local, or tribal governments?	X (as part of approved information sharing initiatives)
Contractors?	X (approved contractors who may support the system)
Others? (specify):	
Comment:	

Question 5: Can individuals "opt-out" by declining to provide personal information or by consenting only to particular use (e.g., allowing their personal information to be used for basic visiting eligibility determination, but for not for sharing with other government agencies)?

Yes, they can "opt-out" by declining to provide private information or by consenting only to particular use	
No, they can't "opt-out" – all personal information is required	X
Comment:	

If Yes, please explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data):

Question 6: How will the privacy of the information be protected/secured? What are the administrative and technological controls? Mark any that apply and give details if requested:

System is only accessible to law enforcement personnel	X (and approved, cleared contractors
System users must log-in with a password	X (passwords changed every 90 days)
When an employee leaves: • How soon is the user ID terminated (1 day, 1 week, 1 month, unknown)? • How do you know that the former employee no longer has access to your system? (explain your procedures or describe mitigating controls):	1 day User accounts are reviewed on a monthly basis and recertified on an annual basis. Employee HR exit procedures include notification to IT staff regarding departures of employees.
Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either: • Full access rights to all data in the system (specify #)? • Limited/restricted access rights to only selected data (specify #)?	Yes ACES: Approx. 3 HR staff per facility and 6 system administrators in Central Office; Web Visiting: Approx. 12 Unit staff per facility ACES: Approx. 16 Department Heads per facility Web Visiting: Approx. 2 Correctional staff in Front Lobby/Visiting Room per facility
Are disks, tapes, and printouts that contain personal information locked in cabinets when not in use? (explain your procedures, or describe mitigating controls):	Yes, sensitive information is secured from inadvertent disclosure. Required handling of sensitive

	information is described in Program Statement 1237.13 "Information Security Programs";
If data from your system is shared with another system or data warehouse, who is responsible for protecting the privacy of data that came from your system but now resides in another? Explain the existing privacy protections, or mitigating controls:	Data is shared and authorized for legitimate law enforcement purposes. Authorized disclosure of BOP sensitive information is described in Program Statement 1351.05 "Release of Information"
Other methods of protecting privacy (specify):	
Comment:	

Question 7: If <u>privacy</u> information is involved, by what data elements can it be retrieved? Mark any that apply:

Name:	X
Social Security Number (SSN)	X
Identification number (specify type)	X (See Q.2)
Birth date	X
Race/ ethnicity	X
Home address	X
Home telephone	X
Personal e-mail address	
Other (specify):	
None	
Comment:	

Other Comments (or details on any Question above):

SECTION 3: DETERMINATION BY BOP PRIVACY OFFICER

_____ _____

Wanda Hunt Date
BOP Privacy Officer/Advocate
Legal Administration – FOIA/Privacy
Office of General Counsel
Federal Bureau of Prisons

SECTION 4: APPROVAL BY BOP CHIEF INFORMATION OFFICER

_____ _____

Sonya D. Thompson Date
Deputy Asst Director/BOP Chief Information Officer
Information, Policy and Public Affairs Division
Federal Bureau of Prisons

Attachment A

U.S. Department of Justice

Federal Bureau of Prisons

Washington, DC 20534

April 19, 2002

MEMORANDUM FOR [SEE DISTRIBUTION BELOW] [redacted]

Libbie Edson

FROM: Elizabeth M. Edson, Assistant General Counsel
Commercial Law Branch

SUBJECT: Published Privacy Act System of Records for the Access Control Entry/Exit System, JUSTICE/BOP-010

I am pleased to announce that the Department of Justice (DOJ) has published notice in the Federal Register that the Bureau of Prisons (BOP) Privacy Act System of Records for the Access Control Entry/Exit System, JUSTICE/BOP-010, is being modified. The notice, (copy attached) was published on April 8, 2002, at 67 FR 16760 and will be effective June 7, 2002.

As described in the preamble, only a few changes were made to the notice originally published in 1995, but we re-published the entire notice for the convenience of our staff and the public. The changes include an expansion of the categories of records to specifically include visitor testing data for drugs, explosives, weapons, and/or other contraband. Previously, it was necessary to rely on general language contained in the 1995 description of records. One Routine Use, (j), has been added to permit the sharing of records to former staff in limited circumstances and two Routine Uses ((h) re: contractors and (g) re: administrative, regulatory and/or court proceedings) have been revised to make the language consistent with DOJ-recommended language for other BOP systems also being modified.

If you have any questions regarding this notice of the modified system, please give me a call at 7-1240, ext. 16

Distribution:

Nancy P. Redding, Chief
Legal Administrative Branch

Wanda Hunt, Chief
FOIA/PA Section

Ron Hill, Administrator
FOIA/PA Section

✓ Earl Franks, Section Chief
Distributed Systems Development
IPPA

Tom Clark, Branch Chief
Systems Development, IPPA

Attachment

BOP-010

States v. *T H Agriculture & Nutrition, L.L.C.*, D.J. Ref. 90–11–3–1426/2.

The Consent Decree may be examined at the Office of the United States Attorney, Middle District of Georgia, 433 Cherry Street, 8th Floor, Macon, Georgia 31202, and at U.S. EPA Region IV, 61 Forsyth Street, Atlanta, Georgia 30303. 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. In requesting a copy, please enclose a check in the amount of $65.50 (25 cents per page reproduction cost) payable to the Consent Decree Library. In requesting a copy exclusive of appendices, please enclose a check in the amount of $11.75 (25 cents per page reproduction cost) payable to the Consent Decree Library.

Ellen M. Mahan,

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

[FR Doc. 02–8362 Filed 4–5–02; 8:45 am]

BILLING CODE 4410–15–M

DEPARTMENT OF JUSTICE

[AAG/A Order No. 260–2002]

Privacy Act of 1974; System of Records

Pursuant to the Privacy Act of 1974 (5 U.S.C. 552a), notice is given that the Federal Bureau of Prisons (Bureau) proposes to modify a system of records. Specifically:

The "Access Control Entry/Exit System, JUSTICE/BOP–010" (last published on October 4, 1995 (60 FR 52013)).

The system has been only slightly revised to expand the categories of records to specifically include testing data for drugs, explosives, weapons, and other contraband. One Routine Use has been revised and a new Routine Use added. The storage description has been expanded to include compact discs (CDs). This modified system will be effective sixty (60) days from [the publication date].

Title 5 U.S.C. 552a (e)(4) and (11) provide that the public be provided a 30-day period in which to comment. The Office of Management and Budget (OMB), which has oversight responsibilities under the Privacy Act, requires that it be given a 40-day period in which to review the system. Therefore, please submit any comments by May 8, 2002. The public, OMB, and the Congress are invited to send written comments to Mary Cahill, Management and Planning Staff, Justice Management Division, Department of Justice, Washington, DC 20530 (1400 National Place Building).

A description of the modified system is provided below. Although there were only a few changes to the system as previously published, the entire notice is provided below for the convenience of the public.

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

Dated: March 28, 2002.

Robert F. Diegelman,

Acting Assistant Attorney General for Administration.

JUSTICE/BOP–010

SYSTEM NAME:

Access Control Entry/Exit System.

SYSTEM LOCATION:

Records may be retained at the Central Office, Regional offices, and at any of the Bureau of Prisons (Bureau) facilities. A list of these system locations may be found at 28 CFR part 503 and on the Internet at *http://www.bop.gov.*

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Current and former staff, inmates now or formerly under the custody of the Attorney General or the Bureau, and all visitors to Bureau facilities, including law enforcement personnel, contractors, volunteers, and inmate visitors.

CATEGORIES OF RECORDS IN THE SYSTEM:

Information retrieved and stored by the system may include any information relative to providing safe and secure prison facilities, to protecting the prison population and/or the general public, and/or, where appropriate, to otherwise promoting the interests of effective law enforcement.

Examples include:

(a) Identification data (much of which is collected from the individual), such as the person's name, current residence, social security number, employer, place and date of birth, age, height, weight, digital image, biometric identifier information, alien registration number, driver's license number, telephone number, passport number, system-generated number, hair color, eye color, sex, race, escort of visitor into institution, and system classification of individual;

(b) other data collected from the visitor and/or from law enforcement to enable prison officials to determine the suitability/acceptability of a visitor such as: the purpose of the visit, testing data regarding drugs, explosives, weapons and/or other contraband, relationship to the inmate and information indicating whether the visitor is under investigation by law enforcement and/or has ever been convicted of a crime, probation and/or parole status, name of supervising probation/parole officer, etc.;

(c) records generated by the system to report entry/exit activity, e.g. date and time of entry/exit, entry/exit locations used; and location data, including location in the institution visited and/or movement within the institution;

(d) any related law enforcement or investigatory data, provided by third parties such as inmates, courts, and other federal, state, local, and foreign law enforcement agencies, e.g. criminal history and/or investigatory data relating to potential visitors; investigatory data otherwise developed by Bureau officials regarding any activity, or suspicious activity, which may threaten the safe and secure operation of federal correctional facilities, e.g. remarks describing a possible introduction of contraband; drug testing data; and any other information that may enable the Bureau to pursue an internal investigation on a record subject.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

This system is established and maintained under the authority of 18 U.S.C. 3621, 4042, 5003.

PURPOSE(S):

The records in this system are maintained to better ensure the safety, security and good order of Bureau facilities; to improve staff ability to quickly account for all persons (inmates, visitors, and staff) within an institution in the event of an emergency, such as an institution disturbance or a natural disaster; to identify and, where appropriate, determine the suitability of visitors with respect to entering prison facilities; and, to more effectively prevent violations of institution policy and/or criminal activity, such as inmate escapes and the introduction of contraband. Where these efforts fail to prevent such violations, and/or where appropriate, records may be collected and used by the Bureau for internal investigations.

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

Relevant data from this system will be disclosed as follows:

(a) To federal, state, local, foreign and international law enforcement agencies who have a need for the information to perform their duties, e.g. in the course

of apprehensions, investigations, possible criminal prosecutions, civil court actions, regulatory proceedings, inmate disciplinary hearings, parole hearings, responding to emergencies, or other law enforcement activity;

(b) to federal, state, local, foreign and international law enforcement agencies in order to solicit or obtain data needed by prison officials for law enforcement purposes, e.g. to determine whether a visitor may be under investigation, have a criminal record, or otherwise be unsuitable to visit; or to obtain any information that may enable the Bureau to pursue an internal investigation pertaining to any record subject based on information developed by the Bureau;

(c) to the news media and the public 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;

(d) 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;

(e) to the National Archives and Records Administration (NARA) and to the General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(f) to a court or adjudicative body before which the Department of Justice or the Bureau is authorized to appear when any of the following is a party to litigation or has an interest in litigation and such records are determined by the Bureau to be arguably relevant to the litigation: (1) The Bureau, or any subdivision thereof, or (2) any Department or Bureau employee in his or her official capacity, or (3) any Department or Bureau employee in his or her individual capacity where the Department has agreed to provide representation for the employee, or (4) the United States, where the Bureau determines that the litigation is likely to affect it or any of its subdivisions;

(g) in an appropriate proceeding before a court or administrative or regulatory body when records are determined by the Department of Justice to be arguably relevant to the proceeding, including federal, state, and local licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit;

(h) 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;

(i) to any person or entity to the extent necessary to prevent immediate loss of life or serious bodily injury; and

(j) pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information 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.

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

STORAGE:

Information maintained in the system is stored in electronic media in Bureau facilities via a configuration of personal computer, client/server, and mainframe systems architecture. Computerized records are maintained on hard disks, floppy diskettes, compact discs (CDs), magnetic tape and/or optical disks. Documentary records are maintained in manual file folders and/or index card files.

RETRIEVABILITY:

Records are retrievable by identifying data, including last name, inmate register number, system classification category, Social Security number, alien registration number, system-generated identification number, passport number, employee badge number and/or miscellaneous identification number as provided by the visitor and/or other law enforcement agencies.

SAFEGUARDS:

Information is safeguarded in accordance with Bureau rules and policy governing automated information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the system. Similarly, paper records are stored in secured areas to prevent unauthorized access. Only those Bureau personnel who require access to perform their official duties may access the records described in this system of records.

RETENTION AND DISPOSAL:

Records generated by the system to report entry/exit and internal movement activities are retained in accordance with General Records Schedule (GRS) 18. All other records in the system of records are retained until such time as the records no longer serve the purpose described by this system of records. At such time, these records (including investigatory records and/or records relating to disciplinary hearings and/or other appropriate personnel actions) may be incorporated into an appropriate, published BOP system of records with an approved retention schedule, or destroyed. Computerized records are destroyed by shredding, degaussing, etc., and documentary records are destroyed by shredding.

SYSTEM MANAGER(S) AND ADDRESS:

Assistant Director, Information, Policy, and Public Affairs Division, Federal Bureau of Prisons, 320 First Street NW., Washington, DC 20534.

NOTIFICATION PROCEDURE:

Inquiries concerning this system should be directed to the System Manager listed above.

RECORD ACCESS PROCEDURES:

All requests for records may be made by writing to the Director, Federal Bureau of Prisons, 320 First Street NW., Washington, DC 20534, and should be clearly marked "Privacy Act Request." This system is exempt, under 5 U.S.C. 552a (j)(2) or (k)(2), from some access. A determination as to exemption shall be made at the time a request for access is

CONTESTING RECORD PROCEDURES:

Same as above.

RECORD SOURCE CATEGORIES:

Records are generated by: (1) Individuals covered by the system; (2) federal, state, local, tribal, foreign and international law enforcement agencies; and (3) federal and state probation and judicial offices.

SYSTEM EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

Pursuant to 5 U.S.C. 552a(j)(2) or (k)(2), the Attorney General has exempted this system from subsections (c)(3) and (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(5) and (e)(8), and (g) of the Privacy Act. Rules have been promulgated in accordance with the requirements of 5