a. Does the system/project support criminal, CT, or FCI investigations or assessments?

_____ NO

_____ YES **[If yes, proceed to question 7.]**

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

_____ NO **[The program will need to work with PCLU to develop/implement the necessary form(s).]**

_____ YES **Identify any forms, paper or electronic, used to request such information from the information subject:**

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

_____ NO _____ YES **If yes, check all that apply:**

_____ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

_____ SSNs are necessary to identify FBI personnel in this internal administrative system.

_____ SSNs are important for other reasons. **Describe:**

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

_____ It is not feasible for the system/project to provide special protection to SSNs. **Explain:**

8. Is the system operated by a contractor?

_____No.

_____Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system

collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

_____ NO **If no, indicate reason; if C&A is pending, provide anticipated completion date:**

__X__ YES **If yes, please indicate the following, if known:**

Provide date of last C&A certification/re-certification:

Confidentiality: __Low __Moderate _X_High __Undefined

Integrity: __Low __Moderate _X_High __Undefined

Availability: __Low _X_Moderate __High __Undefined

_____ Not applicable – this system is only paper-based.

Certification and Accreditation Electronic Communication (EC) for OWT [redacted]

Date: 05/05/2010

b7E

Case ID #: 319U-HQ-A1487677-SECD Serial 1871

Certification and Accreditation Electronic Communication (EC) Authority To Test (ATT) for OWT [redacted]

Date: 06/30/2011
Case ID #: 319U-HQ-A1487687-SECD Serial 190

10. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

_____ NO

_____ YES **If yes, please describe the data mining function:**

11. Is this a national security system (as determined by the SecD)?

_____ NO ____ YES

12. Status of System/ Project:

_____ This is a new system/ project in development. **[If you checked this block, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]**

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? April 2009

2. Has the system/project undergone any significant changes since April 17, 2003?

_____ NO [If no, proceed to next question (II.3).]

_____ YES If yes, indicate which of the following changes were involved **(mark all changes that apply, and provide brief explanation for each marked change)**:

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other **[Provide brief explanation]**:

3. Does a PIA for this system/project already exist?

__ __ NO _____ YES

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

___ NO ___ YES

[The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: National Instant Criminal Background Check System

BIKR FBI Unique Asset ID: SYS-0000060

	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
	Name: [redacted] Program Office: NICS Section Division: CJIS Phone: [redacted] Room Number: A3-213	Name: AGC [redacted] Phone: [redacted] Room Number: JEH, 7350

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:
FBIHQ Division: Criminal Justice Information Services Division	Signature: [signature] Date signed: 7/21/11 Name: Amy C. Blasher Title: Acting NICS Section Chief	Signature: [redacted] Date signed: 7/21/11 Name: [redacted] Title: Supervisory Security Specialist

b6
b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

_X_ PIA is required by the E-Government Act.

_____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? _X_ Yes. ___ No

_____ PIA is not required for the following reason(s):
- ___ System does not collect, maintain, or disseminate PII.
- ___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
- ___ Information in the system relates to internal government operations.
- ___ System has been previously assessed under an evaluation similar to a PIA.
- ___ No significant privacy issues (or privacy issues are unchanged).
- ___ Other

Applicable SORN(s): DOJ/FBI-018, National Instant Criminal Background Check System

Notify FBI RMD/RIDS per MIOG 190.2.3? _X_ No ___ Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? ___ No _X_ Yes: The SORN will be modified in order to combine all previous SORN modifications and include upgrades.

Prepare/revise/add Privacy Act (e)(3) statements for related forms? ___ No ___ Yes (indicate forms affected):

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

[redacted] Unit Chief Privacy and Civil Liberties Unit	Signature: [redacted] Date Signed: 12/2/11
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 12-7-11

b6
b7C

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

The National Instant Criminal Background Check System (NICS) is currently undergoing upgrades and alterations. Therefore, a privacy review has been conducted and new privacy documentation is being drafted to reflect the changes to this legacy system. The following describes the present state of the NICS.

The NICS is a national system that queries available records in the National Crime Information Center (NCIC), the Interstate Identification Index (III), the NICS Index, and, for a non-US citizen, the information systems maintained by the United States Immigration and Customs Enforcement in the Department of Homeland Security to determine whether prospective firearm purchasers or firearm permit applicants are disqualified from receiving firearms or associated permits. The NICS is intended to provide the Federal Firearms Licensees (FFLs) with an immediate determination as to whether the transfer of a firearm may proceed, is denied, or more research is required to determine if the transfer would violate federal or state law. Firearm purchasers who are denied may request the reason for the denial and may challenge the accuracy of the record upon which the denial is based.

Criminal Justice Agencies access NICS for firearm permits and NICS may respond to ATF queries in connection with their investigative activities pursuant to the Gun Control Act of 1968 (GCA) and the National Firearms Act of 1938 (NFA), per 28 CFR 25.6(j). The NICS is also accessed by the ATF for information to determine whether to issue explosives permits and licenses.

The NICS contains records collected by the FBI from federal, state, local, [redacted] tribal agencies/organizations, or other entities on individuals who are prohibited by Federal law[1] from receiving or possessing a firearm. These records may include: an individual's name; sex; race; [redacted] complete date of birth; state of residence; sometimes a unique identifying number, such as a Social Security number (but NICS does not require it to be furnished), a military number, other number assigned by federal, state, local, or other authorities; and other descriptors and information collected as a result of arrest, conviction, incarceration, or involuntary commitment. b7E

The records contain the above identifying information, when available, about any individual who:

[1] Federal law also includes a prohibition for individuals who are prohibited on the basis of state law. See 18 U.S.C. 922 (J)(2), (4) & (5).

A. Is under indictment for, or has been convicted in any court of, a crime punishable by imprisonment for a term exceeding one year;
B. Is a fugitive from justice;
C. Is an unlawful user of, or addicted to, any controlled substance;
D. Has been adjudicated as a "mental defective" or has been committed to a mental institution;
E. Is an alien who is illegally or unlawfully in the United States or who has been admitted to the United States under a non-immigrant visa;
F. Has been discharged from the Armed Forces under dishonorable conditions;
G. Having been a citizen of the United States, has renounced such citizenship;
H. Is subject to a court order that restrains the person from harassing, stalking, or threatening an intimate partner or child of such intimate partner (issued after a hearing of which actual notice was received);
I. Has been convicted in any court of a misdemeanor crime of domestic violence (which has as an element of the offense the use or attempted use of physical force, or the threatened use of a deadly weapon, committed by a current or former spouse, parent, or guardian of the victim or by a person with a similar relationship with the victim);
J. Is otherwise disqualified from possessing a firearm under state law;
K. Is or claims to be an FFL, i.e., a person licensed by the ATF, as a manufacturer, dealer, or importer of firearms, or an authorized representative or contact person of an FFL;
L. Has applied for the transfer of a firearm or a firearms-related permit or license and has had his or her name forwarded to the NICS as part of a request for a NICS background check, an appeal, or other inquiry regarding a NICS transaction. (Identifying information may be maintained for those individuals who have requested the reason for a denial or delay from the FBI or from a law enforcement agency serving as a Point of Contact (POC), and/or who have challenged the accuracy or validity of a disqualifying record or otherwise inquired about a NICS transaction. These files may also include names and other information on other individuals pertinent to such inquiry or appeal.);
M. Has provided the FBI with written consent to maintain information about himself or herself in the Voluntary Appeal File (VAF); or
N. Has been granted relief from a firearms or explosives-related disability and/or granted a pardon. (For example, in order to permit faster evaluation and approval of future transactions, the NICS may maintain information on individuals who have been granted relief by the ATF from firearm disabilities, as well as information on individuals who have been granted Presidential pardons.)

The NICS system consists of records stored in: 1) the NICS Index; 2) the NICS Audit Log; 3) the Appeals Management Database (AMD); 4) the Voluntary Appeal File (VAF); 5) the FFL File; 6) the Automatic Call Distribution (ACD) System and Fax

Server; and 7) the E-Check System. Additionally, to carry out its work the NICS relies on the 8) Disposition Document File (DDF) (compiled as a result of NICS record research) and the 9) ATF Relief from Disabilities File (RFD) (ATF relief actions). These latter databases (8 and 9) are NICS neutral, which means they contain data that was generated independently of NICS transactions and do not contain any indicators of NICS activity (any indicators are scrubbed from the copy that is kept).

NICS Index

The NICS Index is a compilation of information maintained by the FBI that was created specifically for the NICS. The NICS Index contains records obtained by the Attorney General from federal, state, local, [redacted] tribal agencies/organizations, and other entities on individuals who are prohibited by federal law from receiving or possessing a firearm. These records are limited to: a name and other biographic descriptors; such as an individual's sex; race; [redacted] date of birth; state of residence; and sometimes a unique identifying number, such as a Social Security number (but NICS does not require it to be furnished), a military number, or other number assigned by federal, state, local, or other authorities. The records in the NICS Index include prohibitor information not normally maintained in NCIC or III records. b7E

[redacted] b7E

The NICS Section plans to [redacted]

[redacted] b7E

[redacted] b7E

Audit Log

The NICS Audit Log is a chronological record of system activities that enables the reconstruction and examination of a sequence of events and/or changes in an event related to the NICS operation. When a specific NICS transaction results in a denial response, the audit log will include the name and other identifying information about the

prospective transferee, the type of transaction (inquiry or response), time and date of inquiry, header, message key, Originating Agency Identifier, FFL identifier, inquiry/response data - such as a NICS Transaction Number (NTN, a unique number assigned to each valid background request inquiry), and information found by the NICS search. NICS transactions that result in a proceed response also contain the same information, but exist only for less than 24 hours from the time that the response is communicated to the FFL because proceed transactions must be purged of all identifying information submitted by or on behalf of the transferee. All that remains in the Audit Log is the NTN assigned to the transaction, the date and time of the transaction, status, State of purchase, purpose code, the notification date, source, and the FFL identification number. Within 90 days (usually by day 88) from the issuance of a proceed decision, a second purge occurs and the only information that remains in the Audit Log for a proceed transaction is the NTN and the date of the transaction.

Upon written request from the ATF containing the name and license number of the FFL, the FBI may extract information from the NICS Audit Log and create an individual FFL audit log for transactions originating at the named FFL over a period of time. An individual FFL audit log, the only copy of which is provided to the ATF, may contain all information for denied transactions and the NTN, FFL identifier, and creation date and time for cancelled, open, and delayed transactions. With respect to proceed transactions, only the NTN and date of inquiry are retained in the Audit Log. An individual FFL audit log may only contain up to 60 days worth of proceed transaction transfer records originating at the FFL. Proceed information in the Audit Log may only include information not subject to destruction pursuant to a congressionally mandated restriction.

Appeals Management Database (AMD)

The NICS generates and retains appeal records in the Appeals Management Database (AMD).[2] Information in the AMD reflects inquiries by potential transferees regarding the reason for a delay or denial by the NICS or a Point of Contact (POC) state, challenges to the accuracy or validity of a disqualifying record, and other types of inquiries made by potential transferees about a NICS transaction. A POC state is a state or local law enforcement agency serving as an intermediary between an FFL and the federal databases checked by the NICS. A POC state receives NICS background check requests from FFLs, checks state or local record systems, performs NICS inquiries, determines whether matching records provide information demonstrating that an individual is disqualified from possessing a firearm under Federal or state law, and responds to FFLs with the results of a NICS background check. A POC state is a state agency with express or implied authority to perform POC duties pursuant to state statute, regulation, or executive order. Full POC states perform the firearm background checks for all firearms transferred in that state. Partial-POC states perform firearm checks for handgun permits or transfers within the state and the FBI performs the checks for long guns. The ATF queries the NICS for information that helps ATF determine whether to

[2] The AMD is separate from the Voluntary Appeals File since they have different functions and retention rules.

issue explosives permits and licenses and for its investigations in connection with the GCA and the NFA.

The NICS must destroy identifying information submitted by or on behalf of any person who has been determined not to be prohibited from receiving a firearm no more than 24 hours after the system advises an FFL that the transfer would not violate the Brady Act. If a potential purchaser is delayed or denied a firearm and successfully appeals the decision, the NICS cannot retain the record of the appeal or the supporting documentation for more than 90 days (unless the information is maintained as part of the VAF).

Voluntary Appeal File (VAF)

Because of the purge requirement, individuals who wish to make subsequent purchases may be delayed or denied again until their record has been re-reviewed or until the individual has appealed the denial. In order to prevent future unnecessary delays or erroneous denials, individuals, who are potential transferees, may request that the NICS maintain information about them in a Voluntary Appeal File (VAF).[3] The VAF is a file that will be checked by the NICS for delayed transactions when the potential transferee provides his or her unique personal identification number (UPIN). Only information about lawful potential transferees is kept in the VAF; if an individual is found not to be a lawful transferee, his/her information is not maintained as part of VAF.

The VAF permits individuals to voluntarily submit personal identifying information for the limited purpose of clarifying existing records or proving identity to facilitate future transactions. Potential transferees have the option to request that the NICS maintain personally identifying information about them in the VAF that would otherwise be deleted from NICS. This information may include, but is not limited to, fingerprint cards, photographs, court documentation, correspondence, and information contained in the applicant's appeal file, if one exists. If fingerprint cards are submitted, they must be prepared by a law enforcement agency that must stamp the agency's name, address, and telephone number in the designated area of the fingerprint card. As of May 2010, all VAF records entering the file are kept only in electronic format and archived VAF records are being converted to electronic format.

FFL File

The NICS also retains information about individuals who have registered with ATF to be FFLs. This information is provided by the ATF from the FFL application and includes the FFL's name, codeword,[4] address, phone number(s), the ATF number, names

[3] A PIA for the VAF was completed in January 2006. http://home.fbinet.fbi/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/vaf_pia_rmd_publication.wpd

[4] A codeword is used by the FFL when dealing with the call center or with a NICS Section employee on the phone. The codeword is also used by an FFL when conducting a check on the E-Check system; the FFL has to have both the codeword and a password in order to gain access to E-Check. See next page.

of authorized representatives and contact persons, and similar information used by the NICS to identify, validate, and communicate with FFLs in the course of NICS operations.

ACD System and Fax Server

Two computer systems monitor for audit purposes telephonic and fax transmissions made into and out of the NICS during system operations – the ACD System and the Fax Server. The ACD System operates as a call-routing mechanism that analyzes information on calls referred from the contracted call centers to the NICS Section and directs customer service calls to the most appropriate NICS customer service representative. The ACD System records and retains the incoming phone call and associated data, such as the incoming phone number, the NICS Section employee who answered the call, and the date and time of the incoming call. The Fax Server operates in a similar fashion. When a NICS Section employee faxes a request for information, his or her out-going fax transmission contains a control number that identifies the NICS sender. The reply fax transmission will also contain that control number. The Fax Server automatically directs the return fax transmission to the appropriate sending NICS Section employee. The Fax Server records and retains the date and time of the faxes, the NICS control number, the NICS fax number, and the number of the incoming faxes among other related statistical data.

E-Check

The majority of NICS checks are initiated by FFLs via the telephone. The FFL contacts the NICS and conveys the information to a NICS Customer Service Representative (CSR). The CSR validates the FFL by obtaining the FFL's license number and an assigned codeword. Once validation is complete, the FFL transmits information supplied by the firearm purchaser on the ATF Form 4473. The CSR enters the information transmitted by the FFL into a computer terminal and initiates the background check. Each employee of the FFL uses the same codeword when contacting the NICS via the telephone.

The NICS E-Check was established to meet the legal requirement imposed to provide other electronic means of conducting background checks, in addition to the telephone. The NICS E-Check uses a Public Key Infrastructure (PKI) technology to allow FFLs and their employees to conduct background checks via the Internet. Each individual user is issued a personal digital certificate which acts as a key to gain access to a secure Web page. Once the user gains access, he/she submits the potential firearm purchaser's information securely over the Internet to the NICS and retrieves the results of that background check in the same fashion or in combination with the telephone. FFLs that are willing to abide by certain guidelines outlined in a Memorandum of Understanding (MOU) may obtain a single digital certificate per store, instead of one for each employee. Following the procedures and responsibilities outlined in that MOU allows an FFL to use one digital certificate per physical location, thereby minimizing the administrative overhead of managing multiple digital certificates. The FFL is responsible for proper use of the digital certificate and is responsible (along with the offending

employee) if the certificate is misused. The FFL is subject to random and/or directed audits to detect misuse of system access. Data is collected (the same as already described for an ATF requested report) and made available to the ATF when requested in writing for audit and other authorized purposes concerning system access.

The E-Check database contains the following information entered by the user during online registration (a Privacy Act (e)(3) statement is proved as part of the registration process):

1. User's first, middle, and last name;
2. User's mother's maiden name;
3. User's e-mail address (optional);
4. User's Date of Birth;
5. User Id Name;
6. User's following FFL information:
    a. FFL number,
    b. FFL codeword,
    c. FFL Name of licensee,
    d. FFL Business Name,
    e. FFL address,
    f. FFL phone number,
    g. FFL Fax number,
    h. FFL Contact Name;
7. Date and time user applied to the CA;
8. Date and time CA issued the certificate;

The above information is used to authenticate the identity of specific users before they are permitted to access the NICS through the E-Check System. As part of the Certificate of Authority process, the FFL seeking to authorize individuals to use E-Check on their behalf is required to have its nominated individuals read the FFL Responsibilities information. The FFL is then required to have the authorized individuals fill out and sign the acknowledgement that they have read that information before they send it to the NICS Section. The NICS Section maintains the acknowledgement and matches it with the identities of the users accessing the E-Check system in order to assure their identity and authorization.

Disposition Document File (DDF)

The Disposition Document File (DDF) contains record information that cannot be posted to a subject's criminal history record in the NCIC, updated in the Integrated Automated Fingerprint Identification System (IAFIS), or is missing from those databases. Records found in the DDF may include, but are not limited to, arrest dispositions, warrants, protection orders, police reports, court ordered mental commitments, protection orders, and indictments and informations (if not already posted to an individual's rap sheet). The DDF helps reduce the need for NICS Section personnel and CJIS Division personnel to contact local and state agencies to obtain information. Some of the

information contained in the DDF is data that the Criminal Justice Information Services (CJIS) Division's Biometric Services Section (BSS) cannot post. This information may be rejected by the BSS for various technical reasons: the dates of arrest are not filed; a federal or military disposition is not able to be posted to a date of arrest submitted by a state or local contributor; there are disposition records that the FBI does not control; dispositions and charge records have codes that require translation; a disposition is already on file; fingerprints are illegible; information is not able to be related to a specific date of arrest; or validation is lacking, such as missing a state bureau stamp.

ATF Relief from Disabilities File (RFD)

The ATF Relief from Disabilities (RFD) File is a compilation of applicant information obtained by the ATF when it processed firearm and explosives disability relief applications from 1969 to 1992.[5] Although the ATF stopped processing RFD applications in 1992, these records remain relevant to firearm and explosive permit checks, are retained by the NICS, and are used to evaluate firearm transactions and explosive permit applications.

The NICS Section employees research the DDF, ATF RFD, and VAF for supplemental information that could assist in resolving a delayed firearm or explosive transaction. Research of these three databases is undertaken only after a potential transferee's information results in a hit against a record in the III, NCIC, NICS Index, or U.S. Immigration and Customs Enforcement. The record information in these databases may contain information to assist NICS Section employees in quickly determining the potential transferee's eligibility to possess a firearm or explosives without having to contact outside agencies. As noted above, the VAF is only searched when the potential transferee provides his/her UPIN with the transaction.

The DDF, the ATF RFD, and the VAF are accessible to NICS Section employees via links on the NICS Section employees' tool bar and are accessible to POC and partial-POC states. This enhanced information resource helps foster nationwide consistency in firearms and explosives eligibility determinations.

Telephone Conversation Monitoring and Recording – Quality Control Measure

Currently, there are two occasions during which NICS telephone conversations are monitored - randomly selected NICS Section employee telephone conversations and the telephone conversations between FFLs and Call Center CSRs. The NICS Section employee telephone recordings are conducted for purposes of quality assurance and NICS management's evaluation of employee performance. These recordings are recorded over immediately if there are no adverse findings by NICS management and audit personnel. If there are adverse findings, the recordings are retained until the issue is satisfactorily resolved, at which time they are recorded over. The FFL/CSR telephone recordings involve firearm transactions and customer service calls, are conducted for

[5] The ATF Relief from Disabilities File is not subject to the Brady Act requirement to purge proceed information within 24 hours.

quality assurance, and include a warning that is played before each call is taken. Firearm proceed information is not retained from the FFL/CSR recordings longer than 24 hours unless needed for auditing purposes, and then it will be retained only until the audit issue is resolved.

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

_____ NO

__X__ YES **[If yes, please continue.]**

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

__X__ The information directly identifies specific individuals.

__X__ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

__X__ The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

____ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly.

4. Does the system/project pertain only to government employees, contractors, or consultants?

__X__ NO _____ YES

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

_____ NO. **[If no, skip to question 7.]**

__X__ YES. **[If yes, proceed to the next question.]**

6. Does the system/project collect any information directly from the person who is the subject of the information?

_____ NO **[If no, proceed to question 7.]**

__X__ YES E-Checks, Appeals and the VAF all collect information directly from the person who is the subject of the information.

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

_____ NO

__X__ YES **[If yes, proceed to question 7.]**

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

_____ NO **[The program will need to work with PCLU to develop/implement the necessary form(s).]**

_____ YES **Identify any forms, paper or electronic, used to request such information from the information subject:**

7. Are Social Security Numbers (SSNs) collected, maintained, or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

_____ NO ____X__ YES **If yes, check all that apply**:

_____ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses, or sources in this law enforcement or intelligence activity.

_____ SSNs are necessary to identify FBI personnel in this internal administrative system.

__X__ SSNs are important for other reasons. **Describe:** SSNs are not required, but are valuable information that, when provided, help to establish/confirm the identity of individuals in this activity.

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

__X__ It is not feasible for the system/project to provide special protection to SSNs. **Explain:** The NICS provides special protection to all of the information it maintains, not just SSNs. The information housed in the NICS is limited to only authorized FBI personnel with a need to know for their official duties.

8. Is the system operated by a contractor?

__X__ No.

_____ Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

_____ NO **If no, indicate reason; if C&A is pending, provide anticipated completion date:**

__X__ YES **If yes, please indicate the following, if known:**

Provide date of last C&A certification/re-certification:
Re-certification pending (expires December, 2011), previous C&A levels:

Confidentiality: __Low __X__ Medium __High __Undefined

Integrity: __Low __Moderate __X__ High __Undefined

Availability: __Low __Moderate __X__ High __Undefined

_____ Not applicable – this system is only paper-based.

10. Is this system/project the subject of an OMB-300 budget submission?

_____ NO

__X__ YES **If yes, please provide the date and name or title of the OMB submission:**

August 20, 2010 for 2012; FBI National Instant Criminal Background Check System

11. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

__X__ NO

_____ YES **If yes, please describe the data mining function:**

12. Is this a national security system (as determined by the SecD)?

__X__ NO _____ YES

13. Status of System/ Project:

_____ This is a new system/project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? November 30, 1998

2. Has the system/project undergone any significant changes since April 17, 2003?

_____ NO [If no, proceed to next question (II.3).]

__X__ YES If yes, indicate which of the following changes were involved **(mark all changes that apply, and provide brief explanation for each marked change)**:

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

__X__ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

NICS is able to compile individual audit logs, at ATF's written request, of up to sixty days of an FFL's transactions for ATF inspections. NICS' definition of an "open[6]" transaction status allows a transaction to be retained for up to ninety days. POC states are mandated to transmit their final transaction determinations to NICS, thus providing additional information to NICS. NICS also operates the VAF, which collects and maintains additional PII.

_____ A change that results in a new use or disclosure of information in identifiable form.

__X__ A change that results in new items of information in identifiable form being added into the system/project.

See above explanation regarding individual audit logs and VAF information.

__X__ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other **[Provide brief explanation]:**

3. Does a PIA for this system/project already exist?

__X__ NO _____ YES

There is a PIA for the VAF but not one for the system overall because NICS was considered "grandfathered" at the time of passage of the e-Government Act.

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

___ NO ___YES

[6] "Open" means those non-canceled transactions where the FFL has not been notified of the final determination. In cases of "open" responses, the NICS continues researching potentially prohibiting records regarding the transferee and, if definitive information is obtained, communicates to the FFL the final determination that the check resulted in a proceed or a deny. An "open" response does not prohibit an FFL from transferring a firearm after three business days have elapsed since the FFL provided to the system the identifying information about the prospective transferee. 28 CFR §25.2 (2010).

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: New National Instant Criminal Background Check System (NICS)

BIKR FBI Unique Asset ID: 2010-005-01-P-115-046-2616

	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
	Name: [redacted] 1/23/13 Program Office: New NICS Project Office Division: CJIS Division Phone: [redacted] Room Number: Module A-3	Name: AGC [redacted] Phone: [redacted] Room Number: JEH, 7350

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: [redacted] Date signed: 01/24/2013 Name: Paul Wysopal Title: Section Chief	Signature: [redacted] Date signed: 1/28/13 Name: [redacted] Title: Supervisory IT Specialist
FBIHQ Division: Criminal Justice Information Services (CJIS) Division	Signature: Date signed: Name: Paul Wysopal Title: NICS Section Chief	Signature: Date signed: Name: [redacted] Title: Supervisory Security Specialist

b6
b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

_X_ PIA is required by the E-Government Act.

____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? _X_ Yes. ___ No :

____ PIA is not required for the following reason(s):
- ___ System does not collect, maintain, or disseminate PII.
- ___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
- ___ Information in the system relates to internal government operations.
- ___ System has been previously assessed under an evaluation similar to a PIA.
- ___ No significant privacy issues (or privacy issues are unchanged).
- ___ Other :

Applicable SORN(s): DOJ/FBI-018, National Instant Criminal Background Check System

Notify FBI RMD/RIDS per MIOG 190.2.3? _X_ No ___ Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? ___ No ___ Yes :

Prepare/revise/add Privacy Act (e)(3) statements for related forms? ___ No ___ Yes :

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

[redacted] Acting Unit Chief Privacy and Civil Liberties Unit	Signature: [redacted] Date Signed: 4/15/2008
Jacqueline F. Brown, Acting Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 4/11/08

b6
b7C

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

Purpose: The FBI Criminal Justice Information Services (CJIS) Division's New National Instant Criminal Background Check System (NICS) Project proposes a redesign of the legacy NICS to replace the outdated design and technology of the 13-year-old system. The New NICS will transform the NICS Section's business approach by automating much of the current system functionality.

b7E

NICS and the NICS Electronic Check (E-Check)

b7E

The New NICS will be

b7E

The NICS records are stored in the NICS Index, the NICS Audit Log, the Voluntary Appeal File (VAF), the Appeals Management Database (AMD), the Federal Firearms Licensee (FFL) File, the Automatic Call Distribution (ACD) System, the NICS E-Check System, the National Crime Information Center (NCIC), the Interstate Identification Index (III), and the Fax Server.

The New NICS NICS and the NICS E-Check.

b7E

---

b7E

[redacted] b7E

[redacted] b7E

The New NICS will provide [redacted] appeal or VAF activities. The New NICS will also [redacted] b7E [redacted] Other changes to legacy parts of NICS are described in more detail below.

a. **The NICS Index**

The NICS Index is a compilation of prohibitive information maintained by the FBI, not otherwise maintained in NCIC or III records, created specifically for the NICS. The identities in the NICS Index are individuals who have been predetermined to be prohibited from possessing or receiving firearms by Federal or state law. The NICS Index is further described in the legacy NICS PTA. When the New NICS becomes operational, [redacted] NICS Index [redacted] b7E [redacted] NICS Index records.

[redacted]

In an April 2012 enhancement to the legacy NICS, the NICS Index [redacted] NICS Index [redacted] b7E [redacted] is further described in the legacy NICS PTA.

With the enhancements planned for the New NICS, [redacted] b7E [redacted] NICS Index records.

c. **The NICS Audit Log**

The NICS Audit Log is a chronological record of system activities which enables the reconstruction and examination of a sequence of events and/or changes in an event related to the NICS operation. The legacy NICS PTA further describes the characteristics of the NICS Audit Log.

The New NICS [redacted] implementation of the New NICS. [redacted] b7E

d. **The Federal Firearms Licensee Audit Log**

Currently, upon written request from the ATF, with the name and license number of the FFL, the FBI may extract information from the NICS Audit Log and create an individual FFL Audit Log for transactions originating at the named FFL over a 60-day period of time. The legacy NICS PTA further describes the characteristics of the FFL Audit Log.

The New NICS [redacted] The New NICS will also [redacted] NICS and the New NICS. b7E

Key elements of the New NICS Database are included below:

[redacted] the New NICS database; [redacted] NICS E-Check database [redacted] the New NICS database; [redacted] the ATF Relief From Disabilities Database (ATFRDD), VAF, Disposition Document File (DDF), NICS Assessment Unit (NAU), AUDIT, Waiting for Disposition (WFD), and AMD [redacted] b7E

e. **The Federal Firearms Licensee File**

The NICS also retains information about individuals registered as FFLs with the ATF. This information is provided by the ATF from the FFL application and includes the FFL name, codeword, address, phone number(s), ATF number, names of authorized representatives and contact persons, and similar information used by the NICS to identify, validate, and communicate with FFLs in the course of NICS operations. The New NICS will [redacted] b7E

f. **The Automatic Call Distribution (ACD) System and the Fax Server**

Similar in function to the Audit Log, two computer systems monitor telephonic transmissions made into and out of the NICS during system operations – the ACD System and the Fax Server. Further descriptions may be found in the legacy NICS PTA.

The New NICS will [redacted] b7E

[redacted] the NICS Section Customer Service. [redacted]

The New NICS will [redacted] b7E

g. **The Appeals Management Database (AMD)**

The NICS also generates and retains "appeal records," which reflect inquiries by individuals regarding the reason for a delay or denial by the NICS or a Point of Contact (POC) state, challenges to the accuracy or validity of a disqualifying record, or other types of inquiries made by individuals about a NICS transaction. Appeals are received from the individual via U.S. Postal Service, facsimile, or e-mail. Appeal records are retained in the AMD.

The New NICS will [redacted] b7E

[redacted] b7E

h. Voluntary Appeal File (VAF)

Under Title 28, Code of Federal Regulations (CFR), subsection 25.10(g), published July 23, 2004, the VAF was established to prevent future unnecessary delays or erroneous denials. The initial rule permits lawful transferees to request the NICS maintain information about themselves in a VAF, a separate computer file checked by the NICS when the transferee provides his or her unique personal identification number (UPIN). Further description of the VAF is available in the legacy NICS PTA.

[redacted] VAF information on the NICS. [redacted] the NICS [redacted] b7E

The New NICS [redacted] b7E

i. The ATF Relief From Disabilities Database (ATFRDD)

The ATFRDD is a separate database consisting of applicant information obtained by the ATF during the time it processed applications for relief from firearm disability from 1969 to 1992. Further description is contained in the legacy NICS PTA.

Research of the ATFRDD is undertaken only after the initial subject search results in a hit against a record in the III, the NCIC, the NICS Index, or the Immigration and Customs Enforcement (ICE) databases. The records in the ATFRDD may contain information that will assist NICS in determining the subject's eligibility to possess a firearm and/or explosives without having to contact outside agencies. The ATFRDD may also contain information which could immediately result in a "proceed" or "deny" determination.

The fields contained in the ATFRDD include: the subject's name, social security number (if provided), date of birth, gender, race, height, weight, address, disability type (as identified by the ATF), ATF field division name,

the ATF Examiner, date assigned, date application was received, and the date the application was issued.

The POC and partial-POC states have access to the ATFRDD. The ATFRDD is also available to the ATF to research when conducting explosives checks. The New NICS [redacted] ATFRDD records. b7E

j. The Disposition Document File (DDF)

The DDF is a separate, NICS-neutral database containing record information that cannot be posted to a subject's criminal history record in the NCIC or updated in the Integrated Automated Fingerprint Identification System (IAFIS). Some of the information contained in the DDF is data the CJIS Division's Biometric Services Section (BSS) cannot post. Further information about the DDF is available in the legacy NICS PTA.

Research of the DDF is undertaken only after the subject search results in a hit against a record in the III, the NCIC, the NICS Index, or the ICE databases. The DDF may contain information which could immediately result in a "proceed" or "deny" determination.

[redacted] b7E
the New NICS, [redacted]
[redacted] New NICS [redacted]
[redacted]

II. The NICS E-Check

The NICS E-Check was established to meet the statutory requirement imposed on the NICS Section to provide an electronic means of conducting background checks in addition to the telephone. The NICS E-Check uses a Public Key Infrastructure (PKI) technology to allow FFLs and their employees to conduct background checks via the Internet. This is done by issuing each individual user a personal digital certificate which acts as a key to gain access to a secure Web page. Once the user gains access, he/she submits the potential firearm purchaser's information securely over the Internet to NICS and retrieves the results of the background check in the same manner or in combination with the telephone. FFLs willing to abide by certain guidelines outlined in a Memorandum of Understanding (MOU) may get a single digital certificate per store, instead of one for each employee. The FFL will be responsible for its proper use and will be responsible (along with the offending employee) if the certificate is misused. The FFL will be subject to random and/or directed audits to detect misuse of system access. Data must be collected and will be made available when requested for audit and other authorized purposes concerning system access. Further information regarding the NICS E-Check is available in the legacy NICS PTA.

and a Privacy Act (e)(3) statement is provided as part of the registration process for the FFL.

With the implementation of the New NICS, NICS and the NICS E-Check [redacted] New NICS. [redacted] b7E

The New NICS will [redacted] b7E

III. CTI

Computer Telephony Integration[7] (CTI) [redacted] b7E

The New NICS [redacted] b7E

The New NICS system will [redacted] b7E

[redacted] b7E

[redacted] b7E

[redacted] b7E

Additionally, [redacted]

[redacted] b7E

The New NICS will [redacted]

The New NICS will [redacted]

[redacted] b7E

Currently, there are two occasions during which the NICS Section telephone conversations are monitored - the telephone conversations between the FFLs and NICS Contracted Call Center Customer Service Representatives (CSR) and between any customer on customer service and the NICS Section employee. The FFL/CSR telephone recordings involve only firearm transactions, are conducted for quality assurance, and a warning is played before each call is taken.

When the New NICS [redacted]

[redacted] b7E

[redacted] b7E

The New NICS will [redacted]

[redacted] b7E

[redacted] b7E

[redacted] b7E

[redacted] b7E

The New NICS [redacted] b7E

[redacted]

[redacted] The New NICS will [redacted] b7E

[redacted]

In addition, the New NICS will [redacted]

[redacted]

The New NICS will also [redacted] b7E

[redacted]

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

_____ NO

__X__ YES **[If yes, please continue.]**

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

__X__ The information directly identifies specific individuals.

__X__ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

__X__ The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

____ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly.

4. Does the system/project pertain only to government employees, contractors, or consultants?

__X__ NO _____ YES

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

_____ NO. **[If no, skip to question 7.]**

__X__ YES. **[If yes, proceed to the next question.]**

6. Does the system/project collect any information directly from the person who is the subject of the information?

_____ NO **[If no, proceed to question 7.]**

__X__ YES The NICS I-Checks, Appeals, and the VAF all collect information directly from the person who is the subject of the information.

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

_____ NO

__X__ YES **[If yes, proceed to question 7.]**

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

_____ NO **[The program will need to work with PCLU to develop/implement the necessary form(s).]**

_____ YES **Identify any forms, paper or electronic, used to request such information from the information subject:**

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

_____ NO __X__ YES **If yes, check all that apply:**

_____ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

_____ SSNs are necessary to identify FBI personnel in this internal administrative system.

__X__ SSNs are important for other reasons. **Describe:** SSNs are not required, but are valuable information that, when provided, help to establish/confirm the identity of individuals in this activity.

_____ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

__X__ It is not feasible for the system/project to provide special protection to SSNs. **Explain:** NICS provides special protection to all of the information it maintains, not just SSNs. Access to the information housed in NICS is limited to only authorized FBI personnel with a need to know for their official duties.

8. Is the system operated by a contractor?

__X__ No.

When an FFL calls in to request a firearm transfer background check, the call is initially received in one of three NICS contractor-operated call centers. However, the call centers are operated within a very narrowly defined and approved boundary and the NICS Section approves the scripts the call center operators use when responding to FFL calls. The CSRs in those centers obtain certain required information from the FFL and enter it into the system which conducts an automated search of the three databases to learn whether there is a match. If there is no hit on any record in the system, the transaction is permitted to "proceed." If there is a hit, the transaction is delayed and the FFL's call is transferred to a NICS Examiner who will complete the transaction. The CSRs have no access to the system other than the ability to enter queries on behalf of the FFLs.

The New NICS will [redacted] the New NICS functionality, [redacted] the New NICS [redacted] b7E

_____ Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be

imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

__X__ NO **If no, indicate reason; if C&A is pending, provide anticipated completion date.**

The New NICS is currently in development. C&A Activities are scheduled for each of the following Life Cycle Management Reviews: Preliminary Design Review (PDR), Critical Design Review (CDR), Final Design Review (FDR), Test Readiness Review (TRR), and System Acceptance Review (SAR). During the SAR, an accreditation package will be submitted for Authority to Operate (ATO) decision, ATO will generate and FC, and an accreditation letter to DOJ will be created.

_____ YES **If yes, please indicate the following, if known:**
Expires

Provide date of last C&A certification/re-certification:

Confidentiality: __Low __Moderate __High __Undefined

Integrity: __Low __Moderate __High __Undefined

Availability: __Low __Moderate __High __Undefined

_____ Not applicable – this system is only paper-based.

10. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

__X__ NO

_____ YES **If yes, please describe the data mining function:**

11. Is this a national security system (as determined by the SecD)?

__X__ NO _____ YES

12. Status of System/ Project:

_____ This is a new system/ project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

The legacy NICS was developed November 30, 1998. The New NICS is currently in development and is estimated to deploy in 2016.

2. Has the system/project undergone any significant changes since April 17, 2003?

_____ NO [If no, proceed to next question (II.3).]

__X__ YES If yes, indicate which of the following changes were involved **(mark all changes that apply, and provide brief explanation for each marked change)**:

_____ A conversion from paper-based records to an electronic system.

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

__X__ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

b7E

b7E

__X__ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

[redacted] NICS and the NICS E-Check [redacted] b7E

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

__X__ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

New NICS processes to [redacted] The New NICS will also [redacted] the NICS and the New NICS. b7E

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

__X__ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other **[Provide brief explanation]**:

3. Does a PIA for this system/project already exist?

__X__ NO _____ YES

However, PIAs exist for various parts of the legacy NICS system and an overall NICS PIA is in draft.

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

___ NO _X_ YES

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [redacted] b7E

BIKR FBI Unique Asset ID: SYS-000071

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [redacted] Program Office: TMSU/OSSO Division: OTD Phone: [redacted] Room Number: B223	FBI OGC/PCLU POC Name: AGC [redacted] Phone: [redacted] Room Number: 7350 JEH

b6 b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Operational Technology Division (OTD)	Signature: [redacted] Date signed: 7/22/2012 Name: [redacted] Title: Unit Chief, Technical Mgmt Services	Signature: [redacted] Date signed: 6/13/2012 Name: [redacted] Title: Assistant Section Chief
FBIHQ Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6 b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

__X__ PIA is required by the E-Government Act. PIAs will be required for the [redacted] b7E

____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ___ Yes. ___ No:

__X__ PIA are not required for the remainder of the [redacted] (other than the [redacted] b7E for the following reason(s):

___ System does not collect, maintain, or disseminate PII.
___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
__X__ Information in the system relates to internal government operations.
___ System has been previously assessed under an evaluation similar to a PIA.
___ No significant privacy issues (or privacy issues are unchanged).
___ Other:

Applicable SORN(s): FBI-002, The FBI Central Records System, 63 Fed. Reg. 8671 (Feb. 20, 1998), as amended 66 Fed. Reg. 8425 (Jan. 31, 2001), 66 Fed. 17,200 (Mar. 29, 2001), 66 Fed. Reg. 33,558 (June 22, 2001), 70 Fed. Reg. 7513, 17 (Feb. 14, 2005), 72 Fed. Reg. 3410 (Jan. 25, 2007) and DOJ-002, Department of Justice Computer Systems Activity and Access Records, 64 Fed. Reg. 73,585 (Dec. 30, 1999), as amended 66 Fed. Reg. 8425 (Jan. 31, 2001) and 72 Fed. Reg. 3410 (Jan. 25, 2007).

Notify FBI RMD/RIDS per MIOG 190.2.3? ___No __X__Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? __X__No ___Yes:

Prepare/revise/add Privacy Act (e)(3) statements for related forms? ___No __X__Yes : [redacted] request form requires an (e)(3) statement. FBI/OGC will prepare a statement and send to [redacted] b7E

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

[redacted] Acting Unit Chief Privacy and Civil Liberties Unit	Signature: [redacted] Date Signed: 11/8/2013
Jacqueline F. Brown, Acting Deputy General Counsel Acting FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 11/14/13

b6
b7C

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

The Operational Technology Division runs the [redacted] which provides [redacted] to the FBI. [redacted] consists of a [redacted] for the Operational Technology Division (OTD) [redacted] Among the services provided [redacted] Below is a description of these services: b7E

- [redacted] – Allows FBI employees and contractors to enter information regarding [redacted] has the option of using this tool whenever an administrative need exists. The information contained in the system includes [redacted] name and contact information, name of the individual who authorized [redacted] A user of the system can search for information by [redacted] or by [redacted] name. Access to the system is controlled by a user name and password given by a system administrator. Individual users may only see [redacted] for which they have been granted access privileges. The system keeps track of the user names and passwords of all individuals who have access; it also keeps an audit log. No systems external to [redacted] facilitate access to the [redacted] Information from this system can only be shared if the user downloads the information to the user's desktop and then either transmits the information electronically or prints the information and shares a hard copy. Other than information contained in the audit logs and access controls, information from the [redacted] is kept separate from the information in the other parts of [redacted] b7E

- [redacted] FBI personnel send to the Security Compliance Management Unit (SCMU) an email, including personally identifiable information (PII), [redacted] SCMU [redacted] b7E

[redacted] OTD SCMU retains, for future reference, PII in electronic form about the [redacted] b7E [redacted] The SSNs are maintained in [redacted] as encrypted values and are masked from view, except for the last four digits. Access to even these last four digits of the SSNs, as well as access to all of the records in the [redacted] is restricted to individuals within the Compliance Management Unit. Information can be retrieved from the system by [redacted] tracks the user names and passwords of all individuals with system access and maintains an audit log.

- [redacted] - Enables OTD secretaries to [redacted] for review within OTD prior to [redacted] external to OTD. The personally identifiable information (PII) in this application includes names of secretaries and individuals in OTD reviewing [redacted] b7E Information can be retrieved by secretary or reviewer's name. The application tracks the user names and passwords of all individuals with access and maintains an audit log. The application contains no additional PII.

- [redacted] This application provides a means of [redacted] of OTD, [redacted] This application tracks and documents [redacted] The application includes names of people involved in [redacted] and the [redacted] manager [redacted] b7E Only the names are provided – no other personally identifiable information. The only people with access to these reports are the manager of the [redacted] and the OTD [redacted] manager. The application keeps track of the user names and passwords of all individuals who have access and maintains an audit log. In addition, the application keeps track of the dates of [redacted]

- [redacted] Tracks the [redacted] The application includes the names of lab personnel [redacted] b7E The

system can be searched by [redacted]. The application keeps track of the user names and passwords of all individuals who have access and keeps an audit log. b7E

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

_____ NO

__X__ YES **[If yes, please continue.]**

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.
(Check all that apply.)

__X___ The information directly identifies specific individuals.

_____ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

_____ The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 4.

___ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly.

4. Does the system/project pertain only to government employees, contractors, or consultants?

__X__ NO _____ YES

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

_____ NO. **[If no, skip to question 7.]**

___X__ YES. **[If yes, proceed to the next question.]**

6. Does the system/project collect any information directly from the person who is the subject of the information?

_____ NO **[If no, proceed to question 7.]**

__X__ YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

__X__ NO

_____ YES **[If yes, proceed to question 7.]**

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

__X__ NO **[The program will need to work with PCLU to develop/implement the necessary form(s).]**

The FBI has a Privacy Act (e)(3) notice regarding audit logs that is visible on user login screens. In addition, the FBI provides FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form, FD-889, that meet the requirements of an (e)(3) notice during employee orientation. The FBI is presently developing an (e)(3) notice that can be provided to [redacted] b7E

_____ YES **Identify any forms, paper or electronic, used to request such information from the information subject:**

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

_____ NO __X__ YES **If yes, check all that apply:**

__X__ SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

_____ SSNs are necessary to identify FBI personnel in this internal administrative system.

_____ SSNs are important for other reasons. **Describe:**

__X__ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

SSNs are encrypted. The majority of [redacted] users see only the last four digits of a SSN. SSNs may be viewed by a small number of FBI personnel who must [redacted] b7E

_____ It is not feasible for the system/project to provide special protection to SSNs. **Explain:**

8. Is the system operated by a contractor?

__X__ No.

_____ Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

_____ NO **If no, indicate reason; if C&A is pending, provide anticipated completion date:**

__X__ YES **If yes, please indicate the following, if known:**

Provide date of last C&A certification/re-certification: July 29, 2010

Confidentiality: __Low __Moderate __X__ High __Undefined

Integrity: __X__ Low __Moderate __High __Undefined

Availability: __X__ Low __Moderate __High __Undefined

_____ Not applicable – this system is only paper-based.

10. Is this system/project the subject of an OMB-300 budget submission?

__X__ NO

_____ YES **If yes, please provide the date and name or title of the OMB submission:**

11. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

__X__ NO

_____ YES **If yes, please describe the data mining function:**

12. Is this a national security system (as determined by the SecD)?

__X__ NO _____ YES

13. Status of System/ Project:

_____ This is a new system/ project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? 1998

2. Has the system/project undergone any significant changes since April 17, 2003?

_____ NO [If no, proceed to next question (II.3).]

__X__ YES

Changes to the system since 2003 have generally been server upgrades, updates to software licenses, and the addition of [redacted] that did not significantly change the collection, maintenance, or dissemination of personally identifiable information (PII). However, one significant change has occurred. b7E

If yes, indicate which of the following changes were involved **(mark all changes that apply, and provide brief explanation for each marked change)**:

__X__ A conversion from paper-based records to an electronic system. (This change is only regarding the [redacted]). b7E

_____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

_____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

_____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

_____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

_____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

_____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

_____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system/project.

_____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

_____ Other **[Provide brief explanation]:**

3. Does a PIA for this system/project already exist?

__X__ NO _____ YES

If yes: A PTA was completed on 02/20/2007 (at which time, this system was grandfathered from the PIA requirement).

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

__ NO ___ YES

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [redacted] b7E

BIKR FBI Unique Asset ID: 2010-011-01-P-404-140-9999

	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
	Name: [redacted] [redacted] 2/20/13 Program Office: ITPMS/APU Division: ITMD Phone: [redacted] Room Number: Crystal City #400	Name: [redacted] Phone: [redacted] Room Number: JEH, 7350

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: ITMD	Signature: [redacted] Date signed: 2/27/13 Name: [redacted] Title: ITMD/APU Unit Chief	Signature: [redacted] Date signed: 3/2/13 Name: [redacted] Title: IT Specialist
Program Division: ITED	Signature: [redacted] Date signed: Name: [redacted] 3-22-13 Title: ISMEU Unit Chief	
Program Division: ITED	Signature: [redacted] Date signed: 3-26-13 Name: [redacted] Title: EES Assistant Section Chief	

b6
b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

____ PIA is required by the E-Government Act.

____ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? ___ Yes. ___ No :

__X_ PIA is not required for the following reason(s):
___ System does not collect, maintain, or disseminate PII.
___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
_X_ Information in the system relates to internal government operations.
___ System has been previously assessed under an evaluation similar to a PIA.
___ No significant privacy issues (or privacy issues are unchanged).
___ Other :

Applicable SORN(s): Justice/FBI-002; *Bureau Personnel and Management System*, Justice/FBI-008; *DOJ Computer Systems and Activity and Access Records*, DOJ-002.

Notify FBI RMD/RIDS per MIOG 190.2.3? _X__ No ___ Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? _X__ No ___ Yes :

Prepare/revise/add Privacy Act (e)(3) statements for related forms? ___ No ___ Yes :

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

[redacted] Acting Unit Chief Privacy and Civil Liberties Unit	Signature: [redacted] Date Signed: 2/5/2015
Brian F. Binney, Acting Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 2/5/2015

b6
b7C

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

[redacted] b7E

The Information Technology Branch's (ITB) implementation of the [redacted] will fulfill an immediate need to modernize and expedite access processes across the organization. Central to these efforts is the utilization of a primary technology tool [redacted] which will deliver access improvement solutions to all employees no matter where they are located, providing "one-stop shopping" for user access needs. b7E

The overall objective of [redacted] is to provide an enterprise level identity management solution for the FBI. To address this complex endeavor, the ITB has developed an incremental strategy that involves the execution of individual task orders. The initial task order will establish a foundational identity management framework to support the capability to provision/de-provision basic access privileges with future task orders focusing on the more advanced features of identity management on the main FBI network (FBINET). The FBI plans to execute additional task orders to implement the advanced capabilities over the next couple of years pending availability of funding. Additional privacy documentation will be prepared as necessary. b7E

In the initial task order, [redacted] with the mainframe to allow for self-service mainframe password reset functionality. Before [redacted] mainframe password reset was a [redacted] manual process performed by the Enterprise Operations Center (EOC) or the field office Supervisory Information Technology Specialist (SITS). b7E

[redacted] will function as an enterprise system and be available on FBINet. [redacted] focuses the provisioning[2] and de-provisioning[3] [redacted] for all employees and contractors when they join and leave the Bureau, first at the headquarters level and then for field offices. [redacted] also includes an automation of the name change process for these same resources. Provisioning, de-provisioning, and name changes will be triggered automatically based on changes in Bureau Personnel Management System (BPMS) (the Bureau's authoritative source of employee and contractor information). b7E

[redacted] b7E

[2] Provisioning is the process of giving individuals new or additional access to FBI systems.
[3] De-provision is the process of removing access from individuals who have either moved within the FBI and no longer need access or they have left the FBI.

In the future, business unit owners or Information Technology Specialists (ITS) personnel may have role-based authority to enter and approve certain requests. For example, upon an employee's transfer or assumption of a new role within the FBI ("Mover"), supervisors or ITS personnel may be able to use a [redacted] to enter this request, which would automate the processes to 'move' the user's access as well as create an auditable workflow. In addition, all users will eventually be able to utilize a self-service interface to request access to desired applications and specific software packages, and subsequently track the status of their requests online. b7E

[redacted] is complete and has delivered a self-service Mainframe Password Reset functionality and provisioning a user to the core IT system components on the main FBINet. b7E

[redacted] builds on the technical capabilities delivered in [redacted] will be designed, developed, and deployed within the FBINet to provide a [redacted] capable of provisioning new user accounts, and de-provisioning user accounts for employees or contractors leaving the Bureau. b7E

This PTA covers [redacted] Functionality, including the deployment of:

- Headquarters Core 'Joiner/Leaver'[4]
- Field Office 'Joiner/Leaver' (to include Name Change) Implementation
- 'Mover' Implementation at Headquarters and Field Office
- Subsumption of the existing [redacted] functionality into the [redacted] framework [redacted] currently enables: b7E
  - Infrastructure support
  - Application Management
  - Business Process Coordination
- Installation and Configuration of [redacted] within the COOP Virtual Environment.

A limited amount of Personally Identifiable Information (PII) will be needed by [redacted] in order to correlate a proposed user with his/her digital identity in the desired IT application or system. PII contained in the BPMS will be imported to [redacted] to facilitate processing access requests. PII contained in [redacted] includes the user's name, FBI unique identifying number, and social security number (SSN), which is the universal identifier in BPMS. Other than the information necessary to complete a specific task, such as the proposed user's name, no other PII will be visible to the individual approving the request. Further, other than that approving authority, no other users of the system will be able to see any PII relating to any other user. [redacted] user screens will not display user SSNs. b7E

[4] Joiner/Leaver is a term used by the [redacted] project for the core provisioning and de-provisioning that occurs when a user enters and exits the Bureau's identity ecosystem. b7E